Ökad och rättvis tillgång till data

– kompletterande bestämmelser
till EU:s dataförordning

Betänkande av Utredningen om
kompletterande bestämmelser till EU:s dataförordning

Stockholm 2025

STATENS OFFENTLIGA UTREDNINGAR

SOU 2025:118

SOU och Ds finns på regeringen.se under Rättsliga dokument.

Svara på remiss – hur och varför
Statsrådsberedningen, SB PM 2021:1.
Information för dem som ska svara på remiss finns tillgänglig på regeringen.se/remisser.

Layout: Kommittéservice, Regeringskansliet
Omslag: Åtta45
Tryck och remisshantering: Åtta45, Stockholm 2025

ISBN 978-91-525-1429-0 (tryck)
ISBN 978-91-525-1430-6 (pdf)
ISSN 0375-250X

Till statsrådet Erik Slottner

Regeringen beslutade den 17 oktober 2024 att uppdra åt en särskild utredare att föreslå kompletterande bestämmelser till Europaparlamentets och rådets förordning (EU) 2023/2854 av den 13 december 2023 om harmoniserade regler för skälig åtkomst till och användning av data och om ändring av förordning (EU) 2017/2394 och direktiv (EU) 2020/1828 (dataförordningen) och lämna förslag på övriga åtgärder (Fi 2024:06).

Som särskild utredare förordnades samma dag enhetschefen Eva Maria Broberg Lennartsson.

Den 30 april 2025 beslutades om tilläggsdirektiv till utredningen.

Som sakkunnig i utredningen förordnades från och med den 10 februari 2025 kanslirådet Richard Vesterberg (Finansdepartementet). Som experter att ingå i utredningen förordnades från och med den 10 februari 2025 rättssakkunniga Clara Bergström (Justitiedepartementet), experten på digital policy Carola Ekblad (Svenskt Näringsliv), informationsarkitekten Mattias Ekhem (Myndigheten för digital förvaltning), juristen Mathea Franzén (Myndigheten för digital förvaltning), juristen Emma Gunnesson (Post- och telestyrelsen), managern för regulation management Mikael Johansson (Volvo Group Trucks Technology), digitaliseringsstrategen Torbjörn Karlsson (Sveriges kommuner och regioner), utvecklingsledaren Helena Nilsson (Region Örebro län), näringspolitiske experten Fredrik Sand (TechSverige), handläggaren Martin Snygg (Myndigheten för samhällsskydd och beredskap) och handläggaren Oskar Vilhelmsson (Post- och telestyrelsen).

Mathea Franzén entledigades från sitt uppdrag som expert från och med den 15 april 2025. Samma dag förordnades juristen Martin Wetzler (Integritetsskyddsmyndigheten) till expert i utredningen.

Som sekreterare i utredningen anställdes från och med den 1 november 2024 verksjuristen Johanna Wasteson Lundberg. Som

sekreterare anställdes från och med den 4 november 2024 juristen Emma Nörler Trautmann. Johanna Wasteson Lundberg entledigades från uppdraget från och med den 1 januari 2025. Som huvudsekreterare anställdes i utredningen från och med den 13 januari 2025 verksjuristen Philip Levin.

Utredningen redogör för uppdraget med användande av vi-form även om det inte funnits fullständig samsyn i alla delar. Utredningen överlämnar härmed betänkandet *Ökad och rättvis tillgång till data – kompletterande bestämmelser till EU:s dataförordning* (SOU 2025:118). Uppdraget är med detta slutfört.

Vintrosa i december 2025

Eva Maria Broberg Lennartsson

Philip Levin
Emma Nörler Trautmann

Innehåll

Sammanfattning

EU:s dataförordning

Europaparlamentets och rådets förordning (EU) 2023/2854 av den 13 december 2023 om harmoniserade regler för skälig åtkomst till och användning av data och om ändring av förordning (EU) 2017/2394 och direktiv (EU) 2020/1828, i detta betänkande kallad EU:s dataförordning eller dataförordningen, ska tillämpas från och med den 12 september 2025.

Syftet med dataförordningen är att stärka EU:s dataekonomi och främja en konkurrenskraftig datamarknad genom att öka tillgängligheten och användbarheten av data och uppmuntra datadriven innovation. Den syftar även till att uppnå en rättvis fördelning av värdet av data mellan aktörerna i dataekonomin. Förordningen är tillämplig i alla sektorer. Sammanfattningsvis innehåller den regler inom följande områden.

- Regler om åtkomst till och användning och delning av data som genereras av uppkopplade produkter och tillhörande tjänster. Reglerna syftar bl.a. till att ge användare av sådana produkter, dvs. företag eller enskilda som äger, hyr eller leasar en sådan produkt, större kontroll över de data som genereras.
- Regler om villkor som ska gälla när ett företag är skyldigt enligt EU-rätt eller nationell rätt att dela data med ett annat företag, inklusive regler som skyddar företag mot oskäliga avtalsvillkor och om vilken ersättning som får tas ut av datahållarna.
- Regler för att öka rättvisan och konkurrensen på den europeiska marknaden för databehandlingstjänster, t.ex. molntjänster. De innebär exempelvis att byte av databehandlingstjänster ska kunna ske avgiftsfritt.

- Bestämmelser som ger offentliga organ inom EU möjlighet att begära tillgång till data från företag vid ett exceptionellt behov, t.ex. vid ett allmänt nödläge.
- Bestämmelser om skyddsåtgärder för att förhindra att myndigheter i tredjeländer får tillgång till icke-personuppgifter i strid med EU:s eller nationell lagstiftning.
- Grundläggande krav på interoperabilitet för att säkerställa att data smidigt kan delas mellan sektorer och medlemsstater.

Uppdraget

EU:s dataförordning är direkt tillämplig i medlemsstaterna. Vårt uppdrag är att lämna förslag på de kompletterande författningsbestämmelser som behövs för att Sverige ska uppfylla de krav som ställs på medlemsstaterna för att säkerställa att förordningen efterlevs, samt lämna förslag på övriga åtgärder.

Nationella bestämmelser behövs för att uppfylla kravet i förordningen på effektiva och avskräckande sanktioner vid överträdelser av förordningen och vi ska därför föreslå sådana bestämmelser. En central del av uppdraget är att utreda vilka befogenheter den behöriga myndigheten behöver enligt förordningen. Vidare ska vi föreslå nödvändiga organisatoriska och resursmässiga förstärkningar för den behöriga myndigheten samt ta ställning till om andra berörda myndigheter behöver tilläggsuppdrag. Vi ska även föreslå de nödvändiga åtgärder som behövs för att uppfylla dataförordningens krav i fråga om tillgång till certifierade tvistlösningsorgan.

Vi ska lämna förslag om åtgärder för att möjliggöra att offentliga organ kan ta emot data vid exceptionella behov. Dessutom ska vi identifiera vilka administrativa och rättsliga hinder svenska företag och offentliga organ kan möta vid tillämpningen av dataförordningen och föreslå åtgärder som kan minimera sådana hinder. Enligt uppdraget ska vi också föreslå hur tekniska och semantiska standarder och interoperabiliteten mellan system kan förbättras.

Behovet av kompletterande regelverk

Vi föreslår att de svenska bestämmelser som behöver komplettera EU:s dataförordning ska samlas i en ny lag och en ny förordning. I betänkandet benämns de föreslagna författningarna kompletteringslagen respektive kompletteringsförordningen. Vidare föreslår vi att ord och uttryck i kompletteringslagen och kompletteringsförordningen ska ha samma betydelse som i dataförordningen. Vi föreslår också att hänvisningarna till dataförordningen i kompletteringslagens bestämmelser om sanktionsavgift och anmärkning ska vara statiska, dvs. avse förordningen i den ursprungliga lydelsen. Övriga hänvisningar ska vara dynamiska, dvs. avse förordningen i den vid varje tidpunkt gällande lydelsen.

Vidare föreslår vi att det ska införas en ny upplysningsbestämmelse i 49 § upphovsrättslagen (1960:729) för att säkerställa ett den lagen tillämpas i enlighet med dataförordningens bestämmelse om rätten av sitt eget slag i EU:s databasdirektiv.

Vi föreslår också ändringar i förordningen (2007:951) med instruktion för Post- och telestyrelsen och förordningen (2016:602) om finansiering av Post- och telestyrelsens verksamhet.

Vi föreslår att kompletteringslagen, kompletteringsförordningen och övriga författningsändringar ska träda i kraft den 1 juli 2026. Det behövs inte några övergångsbestämmelser.

En behörig myndighet ska säkerställa efterlevnad av EU:s dataförordningen

Medlemsstaterna ska enligt dataförordningen utse en eller flera behöriga myndigheter som ska säkerställa efterlevnaden av förordningen. Om flera sådana myndigheter utses ska en av dem utses till datasamordnare. Vi föreslår att det ska anges i kompletteringslagen att regeringen ska utse en eller flera behöriga myndigheter och att en av dessa ska utses till datasamordnare, om flera behöriga myndigheter utses.

Regeringen har gett Post-och telestyrelsen (PTS) i uppdrag att vara behörig myndighet enligt dataförordningen. Uppdraget ska gälla under 2025 och 2026. Vi har alltså inte haft i uppdrag att föreslå vilken eller vilka myndigheter som ska vara behörig myndighet.

I betänkandet har vi utgått ifrån att PTS ska vara enda behöriga myndighet i Sverige och vi föreslår att regeringen i kompletteringsförordningen ska utse PTS till behörig myndighet.

Dataförordningen föreskriver vilka befogenheter behöriga myndigheter ska ha och att befogenheterna ska vara väl definierade. Vi föreslår därför att myndighetens befogenheter och uppgifter ska anges i författning. Vissa av dessa innebär myndighetsutövning mot enskild och bör anges i kompletteringslagen medan andra uppgifter kan beslutas med stöd av restkompetensen, dvs. av regeringen i kompletteringsförordningen.

Myndigheten ska enligt kompletteringslagen kunna ingripa mot överträdelser av dataförordningen genom att besluta om sanktionsavgift eller meddela anmärkning. Den ska även kunna besluta om förelägganden t.ex. om att upphöra med en viss åtgärd. Förelägganden ska kunna förenas med vite.

Vi föreslår att sanktionsavgift ska tas ut med ett minsta belopp om 5 000 kronor och ett högsta belopp om 20 miljoner kronor. För fysiska personer som inte bedriver näringsverksamhet föreslår vi att beloppet ska vara lägst 1 000 kronor och högst 10 000 kronor.

Vi föreslår bestämmelser i kompletteringslagen om möjligheten att överklaga av den behöriga myndighetens beslut till allmän förvaltningsdomstol. De innebär exempelvis att den som har gett in ett klagomål ska ha rätt att överklaga myndighetens beslut att inte vidta åtgärder med avseende på klagomålet.

Den behöriga myndigheten ska utöver detta ha de befogenheter och uppgifter som anges i kompletteringsförordningen. Dessa innefattar att myndigheten ska hantera klagomål och undersöka frågor som rör tillämpningen av dataförordningen. Myndigheten ska även, för att säkerställa en konsekvent och effektiv tillämpning av dataförordningen, samarbeta med behöriga myndigheter i andra medlemsstater och med kommissionen eller Europeiska datainnovationsstyrelsen (EDIB). Samarbete ska även ske med relevanta behöriga myndigheter som ansvarar för genomförandet av andra unions- eller nationella rättsakter. Vidare ska den behöriga myndigheten bl.a. främja kunskap om dataförordningen och datakompetensen.

En statlig myndighet ska certifiera tvistlösningsorgan

För att lösa vissa tvister ska bl.a. användare, datahållare och datamottagare enligt dataförordningen ha tillgång till ett tvistlösningsorgan som certifierats enligt förordningen. Förordningen ställer inte krav på att medlemsstaterna ska inrätta eller utse ett tvistlösningsorgan. I stället anges att medlemsstaterna på begäran av ett tvistlösningsorgan ska certifiera detta, om det uppfyller de krav som ställs. Vi föreslår därför att det i kompletteringslagen ska anges att regeringen ska utse en statlig myndighet som ska ha i uppgift att certifiera tvistlösningsorgan enligt dataförordningen (en certifierande myndighet). Vi föreslår att PTS ska utses till certifierande myndighet. PTS ska ha möjlighet att ta ut en ansökningsavgift från tvistlösningsorgan som ansöker om att bli certifierat.

Åtgärder för att säkerställa att offentliga organ kan begära och använda data vid exceptionellt behov

Offentliga organ kan med stöd av kapitel V i dataförordningen begära data från företag om organen har ett exceptionellt behov av data. Ett exceptionellt behov kan föreligga bl.a. om data behövs för att hantera ett allmänt nödläge. Vi bedömer att offentliga organ i Sverige behöver stöd i tillämpningen av kapitlet. Åtgärder för att underlätta tillämpningen av kapitlet bör prioriteras för att hantera exceptionella behov som grundar sig i hantering av allmänna nödlägen.

Regeringsuppdrag till Myndigheten för samhällsskydd och beredskap

Vi föreslår att regeringen ska ge Myndigheten för samhällsskydd och beredskap (MSB) i uppdrag att ge stöd till svenska offentliga organ i deras arbete med att förbereda för att vid behov begära, ta emot och använda data vid exceptionellt behov för att hantera allmänna nödlägen. Uppdraget ska vara tidsbegränsat till ett år. I uppdraget ska ingå att identifiera om det finns behov av fortsatta åtgärder samt om uppdraget ska vara en permanent uppgift för myndigheten.

Regeringsuppdrag till sektorsansvariga beredskapsmyndigheter

Vi föreslår att regeringen ska ge sektorsansvariga beredskapsmyndigheter i uppdrag att kartlägga tekniska och organisatoriska förutsättningar inom respektive beredskapssektor för att begära, ta emot och använda data vid allmänt nödläge. Vid behov ska myndigheterna lämna förslag till åtgärder som kan vidtas för att förbättra förutsättningarna. Uppdraget ska vara tidsbegränsat till ett år.

Åtgärder för att minska administrativa hinder för företag och offentliga organ

Dataförordningen är ett nytt och komplext regelverk och det råder osäkerhet om hur den ska tillämpas. Osäkerheten beror bl.a. på att många bestämmelser lämnar utrymme för tolkning. Sammantaget ställer förordningen upp många nya krav som berörda företag och organisationer måste anpassa sina verksamheter efter. Detta innebär en administrativ börda och kostnader för aktörerna.

Eftersom dataförordningen utgör direkt tillämplig rätt är utrymmet begränsat för att på nationellt plan vidta åtgärder för att minska administrativa hinder som uppstår. I stället kommer EU och medlemsstaternas behöriga myndigheter, genom kommissionen och EDIB, ha viktiga roller för att tydliggöra hur dataförordningen ska tolkas och tillämpas. PTS kommer som behörig myndighet att ha en viktig roll för att främja kunskapen om dataförordningen och datakompetensen.

Vidare bör enligt vår bedömning arbetet med tekniska och semantiska standarder och interoperabilitet med anledning av dataförordningen bedrivas på EU-nivå.

Regeringsuppdrag till PTS att inrätta regulatorisk testverksamhet

För att underlätta för aktörer att tolka och tillämpa dataförordningen föreslår vi att PTS ges i uppdrag att införa regulatorisk testverksamhet för att lämna fördjupad vägledning om tillämpningen av dataförordningen. Med sådan testverksamhet avser vi fördjupad vägledning till en eller flera aktörer inom ett avgränsat område eller i relation till en specifik aktivitet om hur dataförordningen bör tolkas och tillämpas.

Ett sådant arbetssätt understödjer syftet med dataförordningen, dvs. att skapa en rättvis, konkurrenskraftig och innovativ europeisk datamarknad. Detta ger PTS en möjlighet att i rollen som behörig myndighet anlägga ett utforskande och lärande perspektiv som inte är möjlig inom ramen för formell tillsyn. Det ger även PTS en möjlighet att bygga ökad kunskap om förordningen genom ett utforskande arbetssätt tillsammans med aktörer som berörs av dataförordningen. Uppdraget ska vara tidsbegränsat till två år.

Konsekvenser

Våra förslag syftar till att uppfylla kraven på nationella åtgärder enligt dataförordningen och bidra till ett ändamålsenligt och effektivt genomslag av förordningen.

Våra förslag berör framför allt PTS som behörig myndighet och certifierande myndighet. Det nya uppdraget kommer att innebära utökade arbetsuppgifter vilket ställer resursmässiga krav. Vi föreslår att finansieringen bör ske genom ökade anslag.

Därutöver berörs MSB samt de sektorsansvariga beredskapsmyndigheterna i och med att vi föreslår att de ska ges särskilda regeringsuppdrag. För att finansiera de ökade kostnader hos MSB som förslaget bedöms ge upphov till föreslår vi att myndigheten tillförs medel. Kostnader som uppstår till följd av uppdraget till de sektorsansvariga beredskapsmyndigheterna bör enligt vår bedömning kunna hanteras inom befintlig ekonomisk ram.

Vidare bedömer vi att förslagen inte leder till ökade kostnader för kommuner och regioner eller att de inskränker den kommunala självstyrelsen. Förslagen förväntas leda till något ökade kostnader för förvaltningsdomstolarna. Kostnadsökningarna bedöms åtminstone initialt inte vara större än att de kan hanteras inom befintliga ekonomiska ramar.

Summary

The Data Act

Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828, hereinafter referred as the EU Data Act or the Data Act, entered into application on 12 September 2025.

The aim of the Data Act is to enhance the EU's data economy and foster a competitive data market by making data more accessible and usable and to encourage data-driven innovation. It also aims to ensure a fair distribution of the value of data amongst the actors in the data economy. It applies across all economic sectors. In summary, it contains rules in the following areas.

- Rules on access to and use and sharing of data generated by connected products and related services. These rules aim, among other things, to give users of connected products, that is companies or individuals who own, rent, or lease such a product, greater control over the data generated by these products.
- Rules on applicable terms and conditions when businesses, in business-to-business relations, are obliged to make data available under EU or national legislation, including rules that protect companies against unfair contractual terms and rules on compensation for data being shared.
- Rules to enhance fairness and competition in the European market for data processing services, such as cloud services. As an example, switching between data processing services should be free of charge.

- Provisions enabling public sector bodies within the EU to request data from companies on the basis of an exceptional need, such as a public emergency.
- Provisions on safeguards to prevent public authorities in third countries from accessing non-personal data in violation of EU or national legislation.
- Essential interoperability requirements to ensure that data can flow seamlessly between sectors and Member States.

The inquiry's remit

The EU Data Act is directly applicable in the Member States. Our task is to propose the supplementary legislative provisions necessary for Sweden to meet the requirements placed on Member States to ensure compliance with the Act, as well as to propose other necessary measures.

National provisions are required to meet the obligation to establish effective and dissuasive sanctions for infringements of the Data Act, and we are therefore to propose such provisions. A central part of the inquiry is to assess what powers the competent authority needs to enforce the Act. Furthermore, we are to propose the organisational and resource-related reinforcements necessary for the competent authority, as well as to determine whether other authorities need additional tasks. We are also to propose the measures required to fulfil the Data Act's requirements concerning access to certified dispute resolution bodies.

In addition, we are to propose measures enabling public bodies to request data in situations of exceptional need. We are also to identify the administrative and legal obstacles that Swedish companies and public bodies may face in applying the Data Act and to propose measures to minimise such obstacles. Finally, the inquiry includes proposing measures to improve technical and semantic standards and the interoperability between systems.

Supplementary legislation

We propose that the Swedish provisions required to complement the EU Data Act be gathered in a new act and a new ordinance, hereinafter the referred to as the Supplementary Act and the Supplementary Ordinance. Furthermore, we propose that the terms and expressions used in the Supplementary Act and the Supplementary Ordinance shall have the same meaning as in the Data Act.

We also propose that references to the Data Act in provisions concerning administrative fines and reprimands be static, meaning that they refer to the Act in its original version. Other references should be dynamic, meaning that they refer to the Act as in force at any given time.

In addition, we propose the introduction of a new information provision in Section 49 of the Swedish Copyright Act (1960:729) to ensure that the Act is applied in accordance with the Data Act's provision on the *sui generis* right in the EU's Database Directive.

We also propose amendments to the Ordinance (2007:951) containing instructions for the Swedish Post and Telecom Authority and to the Ordinance (2016:602) on the financing of the activities of the Swedish Post and Telecom Authority.

We propose that the Supplementary Act, the Supplementary Ordinance, and the other legislative amendments enter into force on 1 July 2026. No transitional provisions are deemed necessary.

A competent authority shall ensure compliance with the EU Data Act

Under the Data Act, Member States are required to designate one or more competent authorities responsible for ensuring compliance with the Regulation. If several such authorities are designated, one of them must be appointed as data coordinator. We propose that the Supplementary Act specify that the Government shall designate one or more competent authorities.

The Government has assigned the Swedish Post and Telecom Authority (PTS) to act as the competent authority under the Data Act. This assignment applies for 2025 and 2026. We have not been tasked with proposing which authority or authorities should serve

as the competent authority. In this report, we have assumed that PTS will be the sole competent authority in Sweden, and we propose that the Government, through the Supplementary Ordinance, designate PTS as the competent authority.

The Data Act stipulates the tasks and powers that competent authorities must have and requires that these are clearly defined. We therefore propose that the authority's tasks and powers be set out in legislation. Some of these powers involve the exercise of public authority over individuals and should therefore be specified in the Supplementary Act, while other tasks may be determined under the residual competence of the Government, i.e. in the Supplementary Ordinance.

According to the Supplementary Act, the authority shall be able to take action against infringements of the Data Act by imposing administrative fines or issuing a reprimand. It shall also be able to issue injunctions, for example, to cease a certain action. Injunctions may be subject to a penalty payment.

We propose that administrative fines should be imposed with a minimum amount of 5 000 SEK and a maximum amount of 20 million SEK. For natural persons not engaged in business activities, we propose that the amount should be at least 1 000 SEK and at most 10 000 SEK.

We also propose provisions in the Supplementary Act concerning the possibility to appeal decisions made by the competent authority to a general administrative court. Inter alia, a person who has submitted a complaint should have the right to appeal the authority's decision not to take action in response to the complaint.

In addition, the competent authority shall have the powers and duties set out in the Supplementary Ordinance. These include handling complaints and investigating matters related to the application of the Data Act. To ensure a consistent and effective application of the Regulation, the authority shall also cooperate with competent authorities in other Member States, as well as with the European Commission and the European Data Innovation Board (EDIB). The authority shall further cooperate with other national authorities responsible for implementing related legislation.

Moreover, the competent authority shall, among other things, promote awareness of the Data Act and enhance data literacy.

A government agency to certify dispute settlements bodies

According to the Data Act users, data holders and data recipients shall, in order to resolve certain disputes, have access to a dispute settlement body that has been certified in accordance with the Act. The Data Act does not require Member States to establish or designate a dispute settlement body. Instead, it states that Member States shall, upon request from a dispute settlement body, certify it if it meets the specified requirements.

We therefore propose that the Supplementary Act stipulates that the Government shall designate a government agency responsible for certifying dispute settlement bodies in accordance with the Data Act (the certifying authority). We propose that PTS be appointed as the certifying authority. PTS shall have the right to charge an application fee from dispute settlement bodies applying for certification.

Measures to ensure that public sector bodies can access and use data in exceptional circumstances

Public sector bodies may, under Chapter V of the Data Act, request data from companies if the bodies have an exceptional need for the data. An exceptional need may exist, for example, if the data is required to handle a public emergency. We assess that public authorities in Sweden will need support regarding the application of Chapter V. Measures to facilitate application should prioritise exceptional needs based on handling of public emergencies.

Government assignment to the Swedish Civil Contingencies Agency

We propose that the government assign the Swedish Civil Contingencies Agency, MSB, to provide support to Swedish public authorities in their work to prepare for requesting, receiving, and using data in cases of exceptional need to manage public emergencies. The assignment should be time-limited to one year. The assignment should include identifying whether there is a need for further measures and whether the task should become a permanent task for the authority.

Government assignment to emergency service sector-responsible authorities

We propose that the government assign emergency service sector-responsible authorities to map the technical and organisational conditions within each emergency service sector for requesting, receiving, and using data in the event of a public emergency. If necessary, the authorities should provide proposals for measures that can be taken to improve these conditions. The assignment should be time-limited to one year.

Measures to minimise administrative barriers for businesses and public bodies

The EU Data Act is a new and complex set of rules, and there is uncertainty as to how it should be applied. The uncertainty is partly due to the fact that many provisions leave room for interpretation. Overall, the regulation imposes many new requirements that affected businesses and organizations must adapt their operations to. This entails an administrative burden and costs for the actors involved.

Since the Data Act constitutes directly applicable law, the scope for taking national measures to reduce administrative barriers is limited. Instead, the EU and the competent authorities of the Member States, through the European Commission and EDIB, will play important roles in clarifying how the Data Act should be interpreted and applied. We assess that PTS, as the competent authority, will have an important role in promoting knowledge of the Data Act and data literacy.

Furthermore, in our assessment, work on technical and semantic standards and interoperability in connection with the Data Act should be carried out at the EU level.

Government assignment to PTS to establish a regulatory sandbox

To facilitate actors in interpreting and applying the regulation, we propose that PTS be given a government assignment to establish a regulatory sandbox to provide in-depth guidance on the application

of the Data Act. With this, we mean providing detailed guidance to one or more actors within a specific area or in relation to a specific activity on how the Data Act should be interpreted and applied.

This approach supports the purpose of the Data Act, namely to enhance a fair, competitive, and innovative European data market. It gives PTS an opportunity, in its role as the competent authority, to adopt an exploratory and learning-oriented perspective that is not possible within the framework of formal supervision. It also allows PTS to build increased knowledge about the regulation through an exploratory approach together with actors affected by the Data Act.

The assignment should be time-limited to two years.

Impact assessment

Our proposals aim to fulfil the requirements for national measures under the Data Act and contribute to an appropriate and effective implementation and application of the Act.

Our proposals primarily impact PTS as the competent authority and certifying authority. This will entail additional tasks, which imposes resource requirements. We propose that funding should be provided through increased appropriations.

In addition, MSB and emergency service sector-responsible authorities are affected, as we propose that they be given specific government assignments. To finance the increased costs for MSB that the proposal is expected to generate, we propose that the authority be allocated additional funds. Costs arising from assignments to emergency service sector-responsible authorities should, in our assessment, be manageable within the existing budget.

Furthermore, we assess that the proposals are not expected to lead to increased costs for municipalities and regions or affect municipal self-government. The proposals may lead to slightly increased costs for the administrative courts. These cost increases are initially assessed not to exceed what can be managed within the existing budget.

1 Författningsförslag

1.1 Förslag till lag med kompletterande bestämmelser till EU:s dataförordning

Härigenom föreskrivs följande.

Lagens syfte

1 § Denna lag kompletterar Europaparlamentets och rådets förordning (EU) 2023/2854 av den 13 december 2023 om harmoniserade regler för skälig åtkomst till och användning av data och om ändring av förordning (EU) 2017/2394 och direktiv (EU) 2020/1828 (dataförordningen), i denna lag benämnd EU:s dataförordning.

Ord och uttryck i lagen

2 § Ord och uttryck i lagen har samma betydelse som i EU:s dataförordning.

Behöriga myndigheter och datasamordnare

3 § Den eller de myndigheter som regeringen bestämmer ska vara behörig myndighet enligt EU:s dataförordning, denna lag och föreskrifter som har meddelats i anslutning till lagen.

Om regeringen bestämmer att fler än en myndighet ska vara behörig myndighet enligt första stycket ska regeringen bestämma vilken myndighet som ska vara datasamordnare enligt EU:s dataförordning.

Begäran om upplysningar och handlingar

4 § Den som omfattas av EU:s dataförordning ska på begäran av en behörig myndighet lämna de upplysningar och handlingar som behövs för att säkerställa att EU:s dataförordning, denna lag och föreskrifter som har meddelats i anslutning till lagen följs.

Föreläggande och vite

5 § En behörig myndighet får besluta de förelägganden som behövs för att EU:s dataförordning, denna lag eller föreskrifter som har meddelats i anslutning till lagen ska följas.

Om det finns särskilda skäl får den behöriga myndigheten besluta om förelägganden enligt första stycket för tiden till dess saken slutligt har avgjorts.

En behörig myndighet får förena ett föreläggande enligt första och andra stycket med vite.

Sanktionsavgift och anmärkning

6 § En behörig myndighet ska besluta att ta ut en sanktionsavgift från följande aktörer vid överträdelse av följande artiklar i EU:s dataförordning, i den ursprungliga lydelsen:

– tillverkare, försäljare, uthyrare, leasegivare eller leverantörer av tillhörande tjänster vid överträdelse av någon av sina skyldigheter enligt artikel 3.1, 3.2 eller 3.3,

– datahållare vid överträdelse av någon av sina skyldigheter enligt artikel 4.1, 4.2, 4.4, 4.5, 4.7, 4.8, 4.13, 4.14, 5.1, 5.4, 5.6, 5.10 5.11, 8.1, 8.3, 8.4, 9.7 eller 18.1,

– användare vid överträdelse av någon av sina skyldigheter enligt artikel 4.7, 4.10 eller 4.11,

– tredje parter vid överträdelse av någon av sina skyldigheter enligt artikel 5.5, 6.1, 6.2, 11.2 eller 19.2,

– datamottagare vid överträdelse av någon av sina skyldigheter enligt artikel 11.2,

– grindvakter vid överträdelse av någon av sina skyldigheter enligt artikel 5.3,

– offentliga organ vid överträdelse av någon av sina skyldigheter enligt artikel 19,

– leverantörer av databehandlingstjänster vid överträdelse av någon av sina skyldigheter enligt artikel 25.1, 25.2, 25.3, 26, 28, 29.1–6, 32.1, 32.3, 32.4 eller 32.5,

– säljare av en applikation som använder smarta kontrakt eller, i avsaknad av en sådan, den person vars närings- eller yrkesverksamhet inbegriper användning av smarta kontrakt för andra inom ramen för genomförandet av ett avtal eller en del av det om att tillgängliggöra data vid överträdelse av någon av sina skyldigheter enligt artikel 36.1 eller 36.2, eller

– enheter som gör uppkopplade produkter tillgängliga eller erbjuder tillhörande tjänster som inte utser rättslig företrädare enligt artikel 37.12.

7 § Om det kan anses tillräckligt får en behörig myndighet vid överträdelser enligt 6 § meddela en anmärkning i stället för att ta ut en sanktionsavgift.

8 § En sanktionsavgift enligt 6 § ska bestämmas till lägst 5 000 kronor och högst 20 000 000 kronor för juridiska personer och för fysiska personer som bedriver näringsverksamhet.

En sanktionsavgift enligt 6 § ska bestämmas till lägst 1 000 kronor och högst 10 000 kronor för fysiska personer som inte bedriver näringsverksamhet.

En behörig myndighet får avstå från att ta ut en sanktionsavgift helt eller delvis om överträdelsen är ringa eller ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften.

9 § En sanktionsavgift får inte tas ut om:

1. överträdelsen omfattas av ett föreläggande som har förenats med vite och överträdelsen ligger till grund för en ansökan om utdömande av vitet, eller

2. den som avgiften ska tas ut av inte har fått tillfälle att yttra sig inom två år från den dag då överträdelsen ägde rum.

10 § Ett beslut om sanktionsavgift ska delges.

11 § En sanktionsavgift ska betalas till den behöriga myndighet som har beslutat om avgiften, eller till den myndighet som den behöriga myndigheten anger, inom 30 dagar från det att beslutet om att ta ut avgiften fick laga kraft eller inom den längre tid som anges i beslutet.

Om sanktionsavgiften inte betalas inom den tid som anges i första stycket, ska myndigheten lämna den obetalda avgiften för indrivning. Bestämmelser om indrivning finns i lagen (1993:891) om indrivning av statliga fordringar m.m.

En sanktionsavgift tillfaller staten.

Certifiering av tvistlösningsorgan

12 § Ett tvistlösningsorgan som är etablerat i Sverige får ansöka om att bli certifierat enligt EU:s dataförordning.

13 § Den myndighet regeringen bestämmer ska pröva ansökningar som avses i 12 § (certifierande myndighet).

14 § Ett tvistlösningsorgan som uppfyller villkoren i artikel 10.5 i EU:s dataförordning ska certifieras av den certifierande myndigheten.

Certifieringen enligt första stycket ska återkallas av den certifierande myndigheten om tvistlösningsorganet inte längre uppfyller villkoren i artikel 10.5 i EU:s dataförordning.

15 § Den certifierande myndigheten får ta ut avgift för att pröva en ansökan om certifiering.

16 § Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om den avgift som avses i 15 §.

Underrättelse till den som har lämnat in ett klagomål

17 § I förhållande till den som har lämnat in ett klagomål till en behörig myndighet ska 33 § förvaltningslagen (2017:900) gälla.

Överklagande

18 § En behörig myndighets beslut enligt EU:s dataförordning och denna lag får överklagas till allmän förvaltningsdomstol.

En myndighet får överklaga en behörig myndighets beslut.

Den som har lämnat in ett klagomål får överklaga en behörig myndighets beslut att inte vidta åtgärder med avseende på klagomålet.

Prövningstillstånd krävs vid överklagande till kammarrätten.

19 § Beslut av den certifierande myndigheten att inte certifiera ett tvistlösningsorgan enligt 14 § första stycket eller att återkalla en certifiering enligt 14 § andra stycket får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Denna lag träder i kraft den 1 juli 2026.

1.2 Förslag till lag om ändring i lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk

Härigenom föreskrivs att 5 kap. 49 § lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*

5 kap.

49 §[1]

Den som har framställt en katalog, en tabell eller ett annat dylikt arbete i vilket ett stort antal uppgifter har sammanställts eller vilket är resultatet av en väsentlig investering har uteslutande rätt att framställa exemplar av arbetet och göra det tillgängligt för allmänheten.

Rätten enligt första stycket gäller till dess femton år har förflutit efter det år då arbetet framställdes. Om arbetet har gjorts tillgängligt för allmänheten inom femton år från framställningen, gäller dock rätten till dess femton år har förflutit efter det år då arbetet först gjordes tillgängligt för allmänheten.

Bestämmelserna i 2 § andra-fjärde styckena, 6–9 §§, 11 § andra stycket, 12 § första, andra och fjärde styckena, 13–16 §§, 16 a § tredje stycket, 16 e–17 c, 17 e, 19–22, 25–26 b och 26 e §§, 26 g § femte och sjätte styckena samt i 42 a–42 k §§ ska tillämpas på arbeten som avses i denna paragraf. Är ett sådant arbete eller en del av det föremål för upphovsrätt, får upphovsrätten också göras gällande.

Ett avtalsvillkor som utvidgar framställarens rätt enligt första stycket till ett offentliggjort arbete är ogiltigt,

Av artikel 43 i Europaparlamentets och rådets förordning (EU) 2023/2854 av den 13 december 2023 om harmoniserade regler för skälig åtkomst till och användning av data och om ändring av förordning (EU) 2017/2394 och direktiv (EU) 2020/1828 (dataförordningen), framgår att rätten av sitt eget slag enligt artikel 7 i direktiv 96/9/EG

[1] Senaste lydelse 2025:547.

inte ska tillämpas när data erhålls från eller genereras av en uppkopplad produkt eller en tillhörande tjänst som omfattas av förordningen, särskilt med avseende på artiklarna 4 och 5 i förordningen.

Denna lag träder i kraft den 1 juli 2026.

1.3 Förslag till förordning med kompletterande bestämmelser till EU:s dataförordning

Härigenom föreskrivs följande.

Allmänna bestämmelser

1 § Denna förordning innehåller bestämmelser som kompletterar

1. Europaparlamentets och rådets förordning (EU) 2023/2854 av den 13 december 2023 om harmoniserade regler för skälig åtkomst till och användning av data och om ändring av förordning (EU) 2017/2394 och direktiv (EU) 2020/1828 (dataförordningen), i denna förordning benämnd EU:s dataförordning, och

2. lagen (2026:XXX) med kompletterande bestämmelser till EU:s dataförordning.

2 § Denna förordning är meddelad med stöd av

– 3 och 13 §§ lagen (2026:XXX) med kompletterande bestämmelser till EU:s dataförordning i fråga om 3 och 5 §§,

– 8 kap. 7 § regeringsformen i fråga om 4 §.

Behörig myndighet och befogenheter

3 § Post- och telestyrelsen är behörig myndighet enligt lagen (2026:XXX) med kompletterande bestämmelser till EU:s dataförordning.

4 § Den behöriga myndigheten har i uppgift att:

1 att öka datakompetensen och medvetenheten bland de användare och enheter som omfattas av EU:s dataförordning om deras rättigheter och skyldigheter enligt förordningen,

2. att hantera klagomål som härrör från påstådda överträdelser av EU:s dataförordning, inbegripet vad gäller företagshemligheter, och i lämplig utsträckning undersöka föremålet för klagomålen,

3. regelbundet informera den som har lämnat in ett klagomål om hur utredningen fortskrider och om resultatet av den,

4. utföra undersökningar om frågor som rör tillämpningen av EU:s dataförordning,

5. att övervaka den tekniska och relevanta kommersiella utveckling som är relevant för tillgängliggörande och användning av data,

6. samarbeta med behöriga myndigheter i andra medlemsstater och, i förekommande fall, med Europeiska kommissionen eller Europeiska datainnovationsstyrelsen, för att säkerställa en konsekvent och effektiv tillämpning av EU:s dataförordning,

7. samarbeta med relevanta behöriga myndigheter som ansvarar för genomförandet av andra unionsrättsakter än EU:s dataförordning eller nationella rättsakter för att säkerställa att EU:s dataförordning verkställs i överensstämmelse med annan unionsrätt och nationell rätt,

8. samarbeta med relevanta behöriga myndigheter för att säkerställa att artiklarna 23–31, artikel 34 och 35 i EU:s dataförordning verkställs i överensstämmelse med annan unionsrätt och självreglering som är tillämplig på leverantörer av databehandlingstjänster,

9. säkerställa att bytesavgifter avskaffas i enlighet med artikel 29 i EU:s dataförordning, och

10. granska begäranden om data som gjorts enligt kapitel V i EU:s dataförordning.

Certifiering av tvistlösningsorgan

5 § Post- och telestyrelsen är certifierande myndighet enligt 13 § lagen (2026:XXX) med kompletterande bestämmelser till EU:s dataförordning.

Denna förordning träder i kraft den 1 juli 2026.

1.4 Förslag till förordning om ändring i förordningen (2007:951) med instruktion för Post- och telestyrelsen

Härigenom föreskrivs att 4 § förordningen (2007:951) med instruktion för Post- och telestyrelsen ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*

4 §[1]

Post- och telestyrelsen har till uppgift att

1. främja tillgången till säkra och effektiva elektroniska kommunikationer, inbegripet att se till att samhällsomfattande tjänster finns tillgängliga, och att främja tillgången till ett brett urval av elektroniska kommunikationstjänster,

2. främja utbyggnaden av och följa tillgången till bredband och mobiltäckning i alla delar av landet, inbegripet att skapa förutsättningar för samverkan mellan myndigheter som kan bidra till utbyggnaden av bredband,

3. svara för att möjligheterna till radiokommunikation och andra användningar av radiovågor utnyttjas effektivt,

4. svara för att nummer ur nationella nummerplaner utnyttjas på ett effektivt sätt,

5. främja en effektiv konkurrens,

6. övervaka pris- och tjänsteutvecklingen,

7. bedriva informationsverksamhet riktad till konsumenter,

8. följa utvecklingen när det gäller säkerhet vid elektronisk kommunikation och uppkomsten av eventuella miljö- och hälsorisker,

9. pröva frågor om tillstånd och skyldigheter, fastställa och analysera marknader samt utöva tillsyn och pröva tvister enligt lagen (2022:482) om elektronisk kommunikation,

10. meddela föreskrifter enligt förordningen (2022:511) om elektronisk kommunikation,

11. upprätta och offentliggöra planer för frekvensfördelning till ledning för radioanvändningen samt offentliggöra information av allmänt intresse om rättigheter, villkor, förfaranden och avgifter som rör radiospektrumanvändningen,

[1] Senaste lydelse 2025:510.

12. tillhandahålla information om frekvensanvändning till Europeiska radiokommunikationskontorets frekvensinformationssystem (EFIS),

13. vara marknadskontrollmyndighet enligt radioutrustningslagen (2016:392),

14. vara tillsynsmyndighet enligt lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering och ge stöd och information till myndigheter och enskilda när det gäller betrodda tjänster,

15. följa utvecklingen när det gäller toppdomäner med geografiska namn som har anknytning till Sverige,

16. vara tillsynsmyndighet enligt lagen (2006:24) om nationella toppdomäner för Sverige på internet samt meddela föreskrifter enligt förordningen (2006:25) om nationella toppdomäner för Sverige på internet,

17. verka för robusta elektroniska kommunikationer och minska risken för störningar, inbegripet att upphandla förstärkningsåtgärder, och verka för ökad krishanteringsförmåga,

18. verka för ökad nät- och informationssäkerhet i fråga om elektronisk kommunikation, genom samverkan med myndigheter som har särskilda uppgifter inom informationssäkerhets-, säkerhetsskydds- och integritetsskyddsområdet samt med andra berörda aktörer,

19. lämna råd och stöd till myndigheter, kommuner och regioner och till företag, organisationer och andra enskilda i frågor om nätsäkerhet,

20. vara tvistlösnings- och tillsynsmyndighet enligt lagen (2016:534) om åtgärder för utbyggnad av bredbandsnät och ansvara för informationstjänsten för utbyggnad av bredbandsnät enligt samma lag,

21. vara tillsynsmyndighet enligt lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster,

22. vara tillsynsmyndighet enligt lagen (2024:500) med kompletterande bestämmelser till EU:s dataförvaltningsförordning, och

23. vara marknadskontrollmyndighet och tillsynsmyndighet enligt lagen (2023:254) om vissa produkters och tjänsters tillgänglighet,

24. vara behörig myndighet enligt lagen (2026:XXX) med kompletterande bestämmelser till EU:s dataförordning, och

25. vara certifierande myndighet enligt lagen (2026:XXX) med kompletterande bestämmelser till EU:s dataförordning.

Denna förordning träder i kraft den 1 juli 2026.

1.5 Förslag till förordning om ändring i förordningen (2016:602) om finansiering av Post- och telestyrelsens verksamhet

Härigenom föreskrivs att 1 § förordningen (2016:602) om finansiering av Post- och telestyrelsens verksamhet ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*

1 §[1]

Denna förordning gäller i fråga om avgifter enligt

– 4 kap. 21 § postlagen (2010:1045),

– 10 § lagen (2019:181) med kompletterande bestämmelser till EU:s förordning om gränsöverskridande paketleveranstjänster,

– 14 kap. 1 och 2 §§ lagen (2022:482) om elektronisk kommunikation,

– 15 § radioutrustningslagen (2016:392),

– 5 kap. 1 § lagen (2016:534) om åtgärder för utbyggnad av bredbandsnät,

– 7 § lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering, och

– 16 § lagen (2024:500) med kompletterande bestämmelser till EU:s dataförvaltningsförordning,

– 15 § lagen (2026:XXX) lagen med kompletterande bestämmelser till EU:s dataförordning.

Avgifterna ska betalas till Post- och telestyrelsen, som får disponera avgiftsinkomsterna i verksamheten.

Denna förordning träder i kraft den 1 juli 2026.

[1] Senaste lydelse 2024:1336.

2 Utredningens uppdrag och arbete

2.1 Utredningens uppdrag

Regeringen beslutade den 17 oktober 2024 att ge en särskild utredare i uppdrag att föreslå kompletterande bestämmelser till Europaparlamentets och rådets förordning (EU) 2023/2854 av den 13 december 2023 om harmoniserade regler för skälig åtkomst till och användning av data och om ändring av förordning (EU) 2017/2394 och direktiv (EU) 2020/1828, och lämna förslag på övriga åtgärder. Förordningen benämns i detta betänkande EU:s dataförordning eller dataförordningen.

I uppdraget ingår att lämna förslag om de författningsändringar och andra åtgärder som behövs för att berörda myndigheter ska kunna utöva sina befogenheter och vidta de åtgärder som krävs enligt dataförordningen. Detta inkluderar att analysera vilka sanktionsbestämmelser som behövs för att uppfylla kravet på sanktioner vid överträdelser av förordningen och lämna nödvändiga författningsförslag. Vidare ingår i uppdraget att analysera befintliga möjligheter till tvistlösning genom tvistlösningsorgan och lämna förslag på nödvändiga åtgärder för att uppfylla förordningens krav i fråga om tvistlösning. I uppdraget ingår även att lämna förslag om åtgärder för att säkerställa att offentliga organ kan ta emot data under exceptionella omständigheter och lämna de författningsförslag i övrigt som är nödvändiga för att uppfylla kraven i förordningen.

Av direktiven framgår att regeringen avser att ge en myndighet i uppdrag att fullgöra uppgiften som behörig myndighet enligt dataförordningen. Regeringen fattade den 2 oktober 2025 beslut att utse Post- och telestyrelsen (PTS) till behörig myndighet. Uppdraget ska pågå under 2025 och 2026. En central del av vårt uppdrag är att utreda vilka befogenheter den behöriga myndigheten behöver enligt förord-

ningen och att vid behov föreslå kompletterande reglering till stöd för att myndigheten ska kunna utöva befogenheterna. I uppdraget ingår vidare att analysera behovet av nödvändiga organisatoriska och resursmässiga förstärkningar för den behöriga myndigheten, överväga och ta ställning till om andra myndigheter behöver tilläggsuppdrag eller instruktionsändringar samt föreslå de författningsändringar och andra åtgärder som behövs för att de berörda myndigheterna ska kunna utöva sina befogenheter och vidta de åtgärder som krävs enligt förordningen.

Vi ska enligt utredningsdirektiven vidare bl.a. identifiera vilka administrativa och rättsliga hinder svenska företag och offentliga organ kan möta vid tillämpningen av dataförordningen samt föreslå åtgärder som bör vidtas för att minimera dessa hinder. I uppdraget ingår även att föreslå hur tekniska och semantiska standarder och interoperabiliteten mellan system kan förbättras för att underlätta för svenska aktörer att uppfylla kraven i förordningen.

Utredningens direktiv finns bifogade i betänkandet i bilaga 1 och bilaga 2.

2.2 Utredningens arbete

Utredningen inledde sitt arbete den 1 november 2024. Regeringen förordnade experter att från och med den 10 februari 2025 bistå utredningen. Under utredningstiden har vi haft fem sammanträden med expertgruppen.

Under utredningsarbetet har vi haft möten med företag, branschorganisationer och statliga myndigheter. Vi har fört dialog med de myndigheter som främst berörs av våra förslag, bl.a. PTS och Myndigheten för samhällsskydd och beredskap. Vidare har vi inhämtat information från sektorsansvariga beredskapsmyndigheter.

Vi har fört samtal med Implementeringsrådet (KN 2024:04), Underrättelseutredningen (Fö 2023:04), Utredningen om AI-förordningen (Fi 2024:05) och Utredningen om integritetsbevarande metoder för en mer datadriven och samverkande förvaltning (Fi 2025:07).

Underlag avseende utmaningar och hinder för företag att leva upp till kraven på datadelning mellan andra företag i enlighet med dataförordningen har på vårt uppdrag tagits fram av Governo AB.

2.3 Utgångspunkter för arbetet

En EU-förordning är direkt tillämplig i medlemsstaterna. Det betyder att en förordning inte får införlivas i eller omvandlas i nationell rätt och att medlemsstaterna är förhindrade att närmare tolka bestämmelserna vid införandet av nationell rätt. Medlemsstaterna får inte heller uttala sig om tillämpningen av en EU-förordning eller förtydliga innebörden av begrepp som förekommer i en förordning. Utgångspunkten för vårt arbete har, i enlighet med våra utredningsdirektiv och allmänna EU-rättsliga principer, varit att utreda behovet av kompletterande bestämmelser till dataförordningen. Vi har inom ramen för arbetet visserligen behövt tolka bestämmelser i förordningen som innebär att medlemsstaterna ska vidta åtgärder men detta enbart i syfte att fastställa vilka åtgärder vi ska föreslå och hur de bör utformas. I betänkandet redovisar vi bedömningar avseende tolkning och tillämpning av bestämmelser som har relevans för nationella kompletterande åtgärder, inte övriga bestämmelser i dataförordningen.

Enligt våra utredningsdirektiv bör en central utgångspunkt i utredningens arbete vara att skapa en balans mellan effektiv tillsyn och administration och minimering av den administrativa bördan för företag och myndigheter. Vidare ska vi beakta vikten av att underlätta för svenska företag, särskilt små och medelstora företag, att följa de nya reglerna utan att skapa onödiga hinder för innovation och tillväxt. Vi har under utredningsarbetet försökt få en så heltäckande bild som möjligt av om hur företag bedömer att de påverkas av förordningen. Vissa av dataförordningens bestämmelser leder till ökad administrativ börda för företag. Vi har dock arbetat utifrån utgångspunkten att de förslag vi lämnar i möjligaste mån ska underlätta för svenska företag och inte leda till ökad administrativ börda.

2.4 Betänkandets disposition

I kapitel 3 presenteras dataförordningen och bakgrunden till förordningen.

I kapitel 4 behandlar vi uppgifter och befogenheter för behöriga myndigheter enligt förordningen samt lämnar ett antal förslag avseende behöriga myndigheter i Sverige. Vi behandlar även dataförordningens krav på rätt till effektivt rättsmedel och lämnar förslag om möjligheten att överklaga m.m.

Kapitel 5 innehåller förslag om sanktioner som behöriga myndigheter ska kunna fatta beslut om i syfte att säkerställa efterlevnad av förordningen.

I kapitel 6 redogör vi för förordningens bestämmelser om certifiering av tvistlösningsorgan och lämnar förslag till en ordning för certifiering i Sverige.

I kapitel 7 behandlar vi möjligheten för offentliga organ att vid exceptionella behov begära data från företag med stöd av dataförordningen.

Kapitel 8 innehåller vår analys av rättsliga och administrativa hinder i relation till dataförordningen och vi lämnar förslag om bl.a. regeringsuppdrag.

I kapitel 9 behandlar vi sekretess- och dataskyddsfrågor.

Kapitel 10 innehåller en beskrivning av dataförordningens bestämmelse som påverkar på rätten av sitt eget slag i EU:s databasdirektiv och vårt förslag med anledning av den bestämmelsen.

I kapitel 11 redogör vi för konsekvenserna av våra förslag.

I kapitel 12 behandlas ikraftträdande och i kapitel 13 finns författningskommentarerna.

3 EU:s dataförordning

3.1 Inledning

Inom EU har det under lång tid bedrivits arbete för att stärka den digitala inre marknaden och stimulera dataekonomin. Arbetet har resulterat bl.a. i ett flertal rättsakter som på olika sätt reglerar digitala tjänster, tillgängliggörande av data och hur data ska hanteras. Dataförordningen är en av rättsakterna inom detta område. I detta kapitel presenterar vi förordningen och dess bestämmelser.

3.2 Bakgrund till dataförordningen

Europeiska kommissionen har behörighet att agera som EU:s verkställande organ och en av dess huvuduppgifter är att föreslå rättsakter. Strategidokument och andra meddelanden från kommissionen är till stor hjälp för att förstå bakgrunden till de rättsakter kommissionen föreslår. Kommissionen har under lång tid arbetat med frågor som rör digitaliseringen och dess påverkan på samhället. Arbetet har över tid skiftat från att främst fokusera på att främja den fria rörligheten på EU:s inre marknad till att även beakta värdet av data och de fördelar ökad tillgång till data och användning av data kan leda till.

Kommissionen presenterade år 2015 strategin för en digital inre marknad.[1] I strategin beskriver kommissionen den digitala inre marknaden som en marknad där varor, personer, tjänster och kapital kan röra sig fritt och där privatpersoner och företag, oberoende av nationalitet och bostadsort, obehindrat kan använda sig av nättjänster under rättvisa konkurrensförhållanden och med ett gott konsument-

[1] Meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén, En strategi för en inre digital marknad i Europa, COM(2015) 192 final.

och personuppgiftsskydd. Syftet med strategin är att komma till rätta med fragmentering mellan medlemsstaterna och hinder mot den fria rörligheten på den digitala inre marknaden. Därigenom skapas de bästa förutsättningarna för att göra Europa världsledande inom den digitala ekonomin. I strategin framhåller kommissionen att dataekonomin skulle kräva ramar som möjliggör att digital information kan användas genom hela värdekedjan i vetenskaps-, samhälls- och näringssyfte.

Som ett led i att genomföra strategin för en digital inre marknad publicerade kommissionen år 2017 ett meddelande om satsningen på att skapa en europeisk dataekonomi.[2] Dataekonomin mäter de totala effekterna av datamarknaden, det vill säga marknaden för datatjänster där digitala data utbyts som produkter eller tjänster som härrör från rådata, på ekonomin i sin helhet. Den omfattar generering, insamling, lagring, bearbetning, distribution, analys, utveckling, leverans och det nyttjande av data som möjliggjorts genom digital teknik. I meddelandet konstaterar kommissionen att information är en viktig resurs för att skapa ekonomisk tillväxt, arbete och samhällsutveckling. Information bär på enorm potential för ny innovation och optimering av processer och beslutsfattande inom en rad olika områden, t.ex. hälsosektorn, energisektorn, smarta städer och transportsystem. Kommissionen konstaterar också att allt större datamängder produceras av den nya teknikens maskiner och processer såsom sakernas internet, framtidens fabriker och autonoma, uppkopplade system.

I meddelandet beskriver kommissionen olika problem. Ett problem som beskrivs är att producenter eller tjänsteleverantörer i praktiken kan bli de som ”äger” de uppgifter som deras maskiner eller processer genererar även om själva maskinerna ägs av användarna. Detta kan vara problematiskt, eftersom användarna ofta förhindras av tillverkarna att ge någon annan part rätt att använda uppgifterna. Kommissionen anser att en strategi som inte är samordnad på EU-nivå skulle riskera att skapa fragmentering och skulle vara till nackdel för utvecklingen av EU:s dataekonomi och för gränsöverskridande tjänster och teknik på den inre marknaden. Kommissionens angreppssätt i detta skede får sammantaget anses

[2] Meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén, Att skapa en europeisk dataekonomi, COM(2017) 9 final.

vara av utforskande karaktär för att bättre förstå marknaderna och behovet av eventuella åtgärder. Kommissionen aviserar bl.a. att den har för avsikt att inleda en dialog med medlemsstaterna och andra intressenter för att undersöka en eventuell framtida EU-ram för tillgång till data.

År 2020 presenterade kommissionen meddelandet En EU-strategi för data.[3] I strategin är kommissionen mer konkret vad gäller behov av åtgärder än i meddelandet från 2017 om satsningen på en europeisk dataekonomi. En utgångspunkt i strategin är att den digitala tekniken under de senaste åren totalt har förändrat ekonomin och samhället genom sin inverkan på alla verksamhetssektorer och européernas vardag. Data står i centrum för förändringen och kommer att bli allt viktigare. Enligt kommissionen är data livsnerven i ekonomisk utveckling. I strategin fastslås att slutmålet för EU är att dra nytta av fördelarna med bättre dataanvändning. Dessa fördelar kan vara ökad produktivitet och konkurrenskraftiga marknader men även förbättringar inom hälsa och välbefinnande, miljö, transparent styrning och bekväma offentliga tjänster. Data är grunden för många nya produkter och tjänster och skapar både produktivitetsvinster och resurseffektivitet inom alla sektorer av ekonomin. Data möjliggör mer individualiserade produkter och tjänster, bättre beslutsfattande samt uppgradering av offentliga tjänster och är en viktig resurs för att uppstartsföretag och små och medelstora företag ska kunna utveckla produkter och tjänster. Kommissionen konstaterar också att tillgång till data krävs för att träna AI-system, med produkter och tjänster som snabbt går från igenkänning av mönster och generering av insikter till mer sofistikerade prognostekniker och därmed bättre beslut.

Av strategin framgår att ett mål för kommissionen är att skapa ett gemensamt europeiskt dataområde – en genuin inre marknad för data, öppen för data från hela världen – där både personuppgifter och icke-personuppgifter, inklusive känsliga företagsuppgifter, är säkra och företagen ändå lätt kan få åtkomst till en närapå oändlig mängd industriella data av hög kvalitet. Det främjar tillväxt och skapar värde samtidigt som människans koldioxidavtryck och miljöavtryck minimeras. Enligt kommissionen bör det gemensamma europeiska dataområdet vara ett område där EU-rätten kan verkställas på ett

[3] Meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén, En EU-strategi för data, COM(2020) 66 final.

effektivt sätt och där alla datadrivna produkter och tjänster uppfyller normerna för EU:s inre marknad. Kommissionen menar också att EU i detta syfte bör kombinera ändamålsenlig lagstiftning för att säkerställa tillgången till data med investeringar i standarder, verktyg, infrastrukturer och kompetens att hantera data. I strategin varnar kommissionen för att splittring mellan medlemsstaterna är en stor risk för visionen om ett gemensamt europeiskt dataområde och för vidareutvecklingen av en genuin inre marknad för data.

I strategin konstaterar kommissionen att tillgång till data är viktigt och att värdet av data ligger i deras användning och vidareutnyttjande. Kommissionen menar dock att det finns ett flertal problem, bl.a. att det inte finns tillräckligt med data tillgängliga för innovativt vidareutnyttjande och att det finns problem avseende tillgången till data för det allmännas bästa. Data som skapas av samhället kan enligt kommissionen användas exempelvis för att förbättra de offentliga finanserna, säkerställa effektivare brottsbekämpning och hantera nödsituationer såsom översvämningar och skogsbränder.

I strategin konstaterar kommissionen vidare att tillhandahållandet av molntjänster och datainfrastrukturer är mycket koncentrerat och att det finns obalanser på marknaden när det gäller tillgång till och användning av data, t.ex. tillgången till data för små och medelstora företag. Obalanser kan exempelvis uppstå i situationer gällande åtkomst till gemensamt genererade data från sakernas internet i industri- och konsumentprodukter. Eftersom allt större mängder data genereras av konsumenter när de använder utrustning med sakernas internet och digitala tjänster riskerar konsumenterna att utsättas för diskriminering, orättvis praxis och inlåsningseffekter.

I strategin anges ett flertal s.k. nyckelåtgärder som syftar till att lösa problem som beskrivs i strategin. En av dessa åtgärder är att, om det är lämpligt, föreslå en dataakt år 2021. I en dataakt kan flera frågor drivas, bl.a. främja datadelning från företag till myndigheter i allmänhetens intresse och stödja datadelning mellan olika företag, i synnerhet genom att komma till rätta med problem kring användningsrättigheter till data som genererats gemensamt (t.ex. data från sakernas internet i industriella miljöer), vilka vanligen fastställts i privata avtal. Kommissionens förslag till dataakt presenterades ett år

senare, år 2022.[4] Den förordning som slutligen beslutades av Europaparlamentet och rådet fick på svenska namnet dataförordningen.

3.3 Dataförordningens syfte

Syftet med dataförordningen är att skapa ett enhetligt och rättvist regelverk inom EU för att underlätta och reglera tillgången till och användningen av data. Genom att underlätta delning och användning av data mellan företag, offentliga organ, såsom myndigheter, kommuner och regioner, och individer ska dataförordningen stimulera innovation, öka företagens konkurrenskraft och driva ekonomisk tillväxt inom EU. Förordningen ska säkerställa rättvisa och transparenta villkor för dataåtkomst och dataanvändning, förhindra oskäliga avtalsvillkor och ge tydliga riktlinjer för datadelning. Genom förordningen får offentliga organ dessutom möjlighet att vid exceptionella behov begära data från företag. Förordningen syftar vidare till att underlätta byte av databehandlingstjänster och främjar interoperabilitet mellan it-system. Vidare stärker förordningen skyddet av individens grundläggande rättigheter, inklusive skyddet av personuppgifter och integritet. Den syftar också till att förhindra att myndigheter i länder utanför EU får olaglig åtkomst till data.

3.4 Dataförordningens bestämmelser

I detta avsnitt presenterar vi förordningens kapitelindelning och ger kortfattade beskrivningar av innehållet i respektive artikel. Ett flertal av förordningens artiklar behandlas i detalj i andra kapitel i betänkandet.

3.4.1 Kapitel I Allmänna bestämmelser

I artikel 1 finns bestämmelser om förordningens tillämpningsområde. Bl.a. framgår vilka aktörer som omfattas av förordningen och vad som inte omfattas av tillämpningsområdet.

[4] Europeiska kommissionen, Förslag till Europaparlamentets och rådet förordning om harmoniserade regler för skälig åtkomst till och användning av data (dataakten), COM(2022) 68 final.

I artikel 2 finns definitioner. Ett centralt begrepp för dataförordningen är av naturliga skäl data. Data definieras i artikel 2.1 som digital återgivning av handlingar, fakta eller information och varje sammanställning av sådana handlingar, fakta eller information, även i form av ljudupptagningar, bildupptagningar eller audiovisuella upptagningar. Definitioner i förordningen kommer att presenteras allteftersom i betänkandet, när definitionen av begreppet behövs för att förstå dess innebörd.

3.4.2 Kapitel II Datadelning mellan företag och konsumenter och mellan företag

Kapitel II är omfattar delning av produktdata och data från tillhörande tjänster, till skillnad från andra kapitel i förordningen som omfattar även andra data. I artikel 3 föreskrivs bl.a. en skyldighet att utforma och tillverka uppkopplade produkter samt utforma och tillhandahålla tillhörande tjänster så att produktdata och data från tjänsterna som standard är direkt tillgängliga för användarna.

I artikel 4 regleras rättigheter och skyldigheter avseende åtkomst till, användning av och tillgängliggörande av produktdata och data från tillhörande tjänster. Om en användare inte har direkt tillgång till data från en uppkopplad produkt eller en tillhörande tjänst ska datahållaren göra dessa data tillgängliga för användaren om denne begär det. Datahållare definieras i artikel 2.13 som ”en fysisk eller juridisk person som har en rätt eller skyldighet, i enlighet med denna förordning, tillämplig unionsrätt eller nationell lagstiftning som antagits i enlighet med unionsrätten, att använda och tillgängliggöra data, inbegripet produktdata eller data från tillhörande tjänster som denne har hämtat eller genererat under tillhandahållandet av en tillhörande tjänst, om detta avtalats”. Artikel 4 innehåller ett flertal villkor för tillgängliggörandet. Det är också möjligt för parterna att under vissa förutsättningar genom avtal begränsa åtkomst, användning eller ytterligare datadelning. Företagshemligheter ska bevaras och får endast röjas om parterna före utlämnandet vidtar alla nödvändiga åtgärder för att bevara dess konfidentialitet, särskilt avseende tredje parter. Användaren får inte använda de data som den erhåller för att utveckla en uppkopplad produkt som konkurrerar med den uppkopplade produkt som data härrör från. Användaren får inte heller dela data med tredje part i detta syfte. Artikeln innehåller även

bestämmelser som begränsar tillgängliggörandet av personuppgifter och i vissa fall också icke-personuppgifter.

Artikel 5 behandlar användarens möjlighet att låta en datahållare tillgängliggöra data för tredje part. Artikeln i sig nämner inte produktdata eller data från tillhörande tjänster men eftersom en användare enligt artikel 2.12 definieras som en ”fysisk eller juridisk person som äger en uppkopplad produkt eller till vilken tillfälliga rättigheter att använda den uppkopplade produkten har överlåtits genom avtal, eller som erhåller tillhörande tjänster” är det endast dessa användare som kan åberopa artikeln. En användare av t.ex. en tjänst som inte är tillhörande en uppkopplad produkt kan inte åberopa artikeln. Företagshemligheter ska bevaras och får endast röjas för tredje parter i den mån röjandet är absolut nödvändigt för att uppfylla det syfte som överenskommits mellan användaren och den tredje parten. Det finns ytterligare bestämmelser om företagshemligheter i artikeln.

Artikel 6 innehåller bestämmelser om tredje parts behandling av data som görs tillgängliga enligt artikel 5. Tredje part får behandla data endast för de ändamål och på de villkor som överenskommits med användaren, med förbehåll för unionsrätt och nationell rätt om skyddet av personuppgifter.

I artikel 7 föreskrivs vissa begränsningar i tillämpningsområdet för skyldigheterna i artikel 4–6. Skyldigheterna ska inte gälla data som genereras genom användning av uppkopplade produkter som tillverkas eller utformas, eller tillhörande tjänster som tillhandahålls av, ett mikroföretag eller ett litet företag. Begränsningar för medelstora företag förskrivs också. Vidare framgår av artikeln att avtalsvillkor som till nackdel för användaren utesluter tillämpning av, avviker från eller ändrar verkan av användarens rättigheter enligt artikel 4–6 inte ska vara bindande för användaren.

3.4.3 Kapitel III Skyldigheter för datahållare som är skyldiga att göra data tillgängliga enligt unionsrätten

I artikel 8 finns bestämmelser som är tillämpliga när en datahållare tillgängliggör data mot bakgrund av artikel 5 i förordningen eller annan tillämplig unionsrätt eller nationell lagstiftning som antagits i enlighet med unionsrätten. Datahållaren ska då komma överens med en datamottagare om villkoren för att göra data tillgängliga och ska göra detta på rättvisa, rimliga och icke-diskriminerande villkor

och på ett öppet sätt. I artikeln finns ytterligare bestämmelser om bl.a. oskäliga avtalsvillkor och icke-diskriminering.

Enligt artikel 9 ska ersättning som en datahållare och en datamottagare kommer överens om för att göra data tillgängliga i förbindelser mellan företag vara icke-diskriminerande och rimlig och får inbegripa en marginal. Artikeln innehåller mer detaljerade bestämmelser om ersättningsberäkningen samt att kommissionen ska anta riktlinjer för beräkningen av rimlig ersättning.

Artikel 10 innehåller bestämmelser om tvistlösning. Användare, datahållare och datamottagare ska ha tillgång till ett certifierat tvistlösningsorgan för att lösa tvister som härrör från vissa utpekade bestämmelser i förordningen samt tvister avseende rättvisa, rimliga och icke-diskriminerande villkor för tillgängliggörande av data på ett öppet sätt. Vidare ska kunder och leverantörer av databehandlingstjänster ha tillgång till ett tvistlösningsorgan för att lösa tvister som rör överträdelser av kundernas rättigheter och de skyldigheter som i dataförordningen åläggs leverantörer av databehandlingstjänster. I artikeln ställs krav på tvistlösningsorganen samt att medlemsstaterna på begäran av ett tvistlösningsorgan ska certifiera organet om det lever upp till vissa villkor.

En datahållare får med stöd av artikel 11 vidta lämpliga tekniska skyddsåtgärder för att förhindra obehörig åtkomst till data och för att säkerställa överensstämmelse med artiklarna 4, 5, 6, 8 och 9 i förordningen samt med de överenskomna avtalsvillkoren för tillgängliggörande av data. Användare, tredje parter och datamottagare får inte ändra eller avlägsna tekniska skyddsåtgärder såvida inte datahållaren samtycker till det.

Av artikel 12 framgår att artikel 8–11 ska tillämpas om en datahållare i förbindelser mellan företag är skyldig att göra data tillgängliga för en datamottagare enligt artikel 5 i förordningen eller enligt tillämplig unionsrätt eller nationell lagstiftning som antagits i enlighet med unionsrätten. Ett avtalsvillkor i ett datadelningsavtal som, till nackdel för en part eller, där detta är tillämpligt, till nackdel för användaren, utesluter tillämpningen av artikel 8–11, avviker från det eller ändrar dess verkan, ska inte vara bindande för den parten.

3.4.4 Kapitel IV Oskäliga avtalsvillkor i samband med åtkomst till och användning av data mellan företag

Kapitlet består av en artikel, artikel 13. I artikeln finns bestämmelser om när avtalsvillkor som ett företag ensidigt ålägger ett annat företag ska anses vara oskäliga. I artikeln beskrivs vissa avtalsvillkor som i synnerhet ska anses vara oskäliga. Ett avtalsvillkor som ensidigt ålagts ett företag ska inte vara bindande för det senare företaget om det är oskäligt.

3.4.5 Kapitel V Göra data tillgängliga för offentliga organ, kommissionen, Europeiska centralbanken och unionsorgan på grundval av ett exceptionellt behov

Kapitlet innehåller bestämmelser om att ett offentligt organ, kommissionen, Europeiska centralbanken eller ett unionsorgan får begära data från företag om den begärande parten visar att det finns ett exceptionellt behov att använda vissa data för att fullgöra sina lagstadgade skyldigheter av allmänt intresse. Om det föreligger ett exceptionellt behov ska datahållare som är andra juridiska personer än offentliga organ och som innehar dessa data enligt artikel 14 göra dem tillgängliga på vederbörligen motiverad begäran.

Artikel 15 anger vilka förutsättningar som ska vara uppfyllda för att ett exceptionellt behov av att använda data ska anses föreligga. Det rör sig antingen om data som behövs för att hantera ett så kallat allmänt nödläge eller en situation där ett organ som agerar på grundval av unionsrätten eller nationell rätt har identifierat att det saknar vissa specifika data och att detta hindrar organet från att utföra en specifik uppgift av allmänt intresse som är föreskriven i lag.

Enligt artikel 16 ska bestämmelserna i kapitel V inte påverka skyldigheter som fastställs i unionsrätten eller nationell rätt vad gäller bl.a. rapportering att tillmötesgå begäranden om åtkomst till information. Kapitlet ska inte heller tillämpas på offentliga organ, kommissionen, Europeiska centralbanken eller unionsorgan som bedriver verksamhet som syftar till att förebygga, förhindra, utreda, upptäcka eller lagföra brott eller administrativa överträdelser eller verkställa straffrättsliga påföljder, eller på tull- eller skatteförvaltning.

Artikel 17 föreskriver hur en begäran om att tillgängliggöra data ska göras och vad en begäran ska innehålla. Ett offentligt organ, kom-

missionen, Europeiska centralbanken eller ett unionsorgan får inte göra data tillgängliga för vidareutnyttjande. Sådana organ får dock under vissa förutsättningar utbyta data.

Av artikel 18 framgår att en datahållare som mottar en begäran om att göra data tillgängliga ska göra dessa data tillgängliga utan oskäligt dröjsmål, med beaktande av nödvändiga tekniska, organisatoriska och rättsliga åtgärder.

I artikel 19 finns bestämmelser som riktar sig till ett offentligt organ, kommissionen, Europeiska centralbanken eller ett unionsorgan som tar emot data till följd av en begäran enligt artikel 14. Organet får t.ex. inte använda dessa data på ett sätt som är oförenligt med det ändamål för vilket de begärdes. I artikeln finns också bestämmelser om företagshemligheter.

Artikel 20 innehåller bestämmelser om ersättning för data som begärs enligt kapitel V. Datahållare som inte är mikroföretag eller små företag ska kostnadsfritt tillgängliggöra de data som är nödvändiga för att hantera ett allmänt nödläge. Om det exceptionella behov som ligger till grund för en begäran inte grundar sig i hantering av ett allmänt nödläge ska datahållare ha rätt till skälig ersättning för att göra data tillgängliga.

I artikel 21 finns bestämmelser om under vilka förutsättningar ett offentligt organ, kommissionen, Europeiska centralbanken eller ett unionsorgan ska ha rätt att dela data som mottagits enligt kapitel V. Sådana data får delas med enskilda personer eller organisationer i syfte att bedriva vetenskaplig forskning eller analys som är förenlig med det ändamål för vilket data begärdes. De får även delas med nationella statistikbyråer och Eurostat för framställning av officiell statistik. Artikeln innehåller också bestämmelser för dem som tar emot data med stöd av artikeln.

I artikel 22 anges att offentliga organ, kommissionen, Europeiska centralbanken och unionsorgan ska samarbeta och bistå varandra för att genomföra kapitel V på ett konsekvent sätt. Om ett offentligt organ avser att begära data från en datahållare som är etablerad i en annan medlemsstat, ska organet först underrätta den behöriga myndighet i den medlemsstaten om avsikten att begära data. Begäran ska granskas av den behöriga myndigheten i den medlemsstat där datahållaren är etablerad. Den behöriga myndigheten ska pröva om begäran ska lämnas vidare till datahållaren eller om den ska avslås.

3.4.6 Kapitel VI Byte av databehandlingstjänster

Kapitel VI innehåller bestämmelser som är tillämpliga för leverantörer av databehandlingstjänster och som syftar till att underlätta byte av sådana tjänster. Databehandlingstjänst definieras i artikel 2.8 som ”en digital tjänst som tillhandahålls en kund och som möjliggör allmän nätverkstillgång på begäran till en gemensam pool av konfigurerbara, skalbara och elastiska databehandlingsresurser av centraliserad, distribuerad eller mycket distribuerad art och som snabbt kan tillhandahållas och levereras med minsta möjliga administration eller interaktion med tjänsteleverantören.” Definitionen innefattar enligt skäl 78 i förordningen molntjänster och edgetjänster.

Enligt artikel 23 ska leverantörer av databehandlingstjänster vidta de åtgärder som föreskrivs i förordningen i syfte att göra det möjligt för kunder att byta till en databehandlingstjänst som omfattar samma tjänstetyp och som tillhandahålls av en annan leverantör av databehandlingstjänster, byta till lokal IKT-infrastruktur eller använda flera leverantörer av databehandlingstjänster samtidigt. Leverantörer av databehandlingstjänster ska inte införa utan i stället undanröja förkommersiella, kommersiella, tekniska, avtalsmässiga och organisatoriska hinder som hindrar kunderna från att vidta vissa åtgärder, t.ex. överföra (portera) kundens exporterbara data och digitala tillgångar till en annan leverantör av databehandlingstjänster eller till lokal IKT-infrastruktur, även efter att ha utnyttjat ett gratiserbjudande.

I artikel 24 föreskrivs att ansvaret för leverantörer av databehandlingstjänster enligt artiklarna 23, 25, 29, 30 och 34 endast ska gälla de tjänster, avtal eller affärsmetoder som tillhandahålls av den ursprungliga leverantören av databehandlingstjänster.

Enligt artikel 25 ska kundens rättigheter och leverantörens skyldigheter vad gäller ett byte av leverantör av databehandlingstjänster eller, i tillämpliga fall, till lokal IKT-infrastruktur tydligt anges i ett skriftligt avtal. I artikeln framgår också vad ett avtal ska innehålla samt diverse bestämmelser om tidsgränser.

Av artikel 26 framgår att leverantören av databehandlingstjänster ska förse kunden med information om dels tillgängliga förfaranden för byte och portering till databehandlingstjänsten, dels en hänvisning till ett uppdaterat onlineregister som sköts av leverantören av

databehandlingstjänster, med uppgifter om alla datastrukturer och dataformat samt relevanta standarder och öppna interoperabilitetsspecifikationer i vilka de exporterbara data som avses i artikel 25.2 e är tillgängliga.

Enligt artikel 27 ska alla berörda parter, inbegripet destinationsleverantörer av databehandlingstjänster, samarbeta i god tro för att göra bytesprocessen effektiv, möjliggöra snabb överföring av data och bibehålla databehandlingstjänstens kontinuitet.

I artikel 28 finns avtalsenliga insynsskyldigheter i fråga om internationell åtkomst och överföring. Leverantörer av databehandlingstjänster ska på sina webbplatser informera om vilken jurisdiktion som den IKT-infrastruktur som används för databehandling av deras enskilda tjänster tillhör samt en allmän beskrivning av de tekniska, organisatoriska och avtalsmässiga åtgärder som leverantören av databehandlingstjänster vidtagit för att förhindra internationell statlig åtkomst till eller överföring av icke-personuppgifter som innehas i unionen. Detta under förutsättning att sådan åtkomst eller överföring skulle strida mot unionsrätten eller den berörda medlemsstatens nationella rätt.

I artikel 29 föreskrivs att leverantörer av databehandlingstjänster inte får ta ut några bytesavgifter av kunden för bytesprocessen från och med den 12 januari 2027. Borttagandet av bytesavgifter får ske gradvist och från och med den 11 januari 2024 till och med 12 januari 2027 får leverantörer av databehandlingstjänster ta ut nedsatta bytesavgifter av kunden för bytesprocessen.

I artikel 30 regleras tekniska aspekter av byte av databehandlingstjänster. Kraven skiljer sig åt beroende på om databehandlingstjänsten är begränsat till infrastrukturella element eller inte. Det regleras även vad som gäller om gemensamma standarder eller specifikationer saknas. I artikeln föreskrivs också begränsningar i leverantörernas skyldigheter.

Av artikel 31 framgår att vissa artiklar om databehandlingstjänster i förordningen inte omfattar vissa tjänster, bl.a. databehandlingstjänster där de flesta huvudfunktioner har skräddarsytts för att tillgodose en enskild kunds särskilda behov eller där alla komponenter har utvecklats för en enskild kunds räkning.

3.4.7 Kapitel VII Olaglig internationell statlig åtkomst till och överföring av icke-personuppgifter

Kapitlet innehåller bestämmelser som syftar till att förhindra olaglig internationell statlig åtkomst till och överföring av data som inte är personuppgifter. I artikel 32 föreskrivs att leverantörer av databehandlingstjänster ska vidta alla adekvata tekniska, organisatoriska och rättsliga åtgärder, inbegripet avtal, för att förhindra internationell statlig åtkomst och tredjeländers statliga åtkomst till och överföring av icke-personuppgifter som innehas i unionen, om en sådan överföring eller åtkomst skulle strida mot unionsrätten eller den berörda medlemsstatens nationella rätt. I artikeln finns särskilda bestämmelser avseende situationer då det finns beslut eller domar från en domstol i ett tredjeland, eller beslut från en administrativ myndighet i ett tredjeland, om att data ska tillgängliggöras.

3.4.8 Kapitel VIII Interoperabilitet

Kapitel VIII innehåller bestämmelser om interoperabilitet för deltagare i dataområden, databehandlingstjänster samt krav som avser smarta kontrakt. I artikel 33 fastställs ett antal väsentliga krav som deltagare i dataområden, som erbjuder data eller datatjänster till andra deltagare, ska uppfylla. Kraven syftar bl.a. till att för att underlätta interoperabiliteten mellan data, datadelningsmekanismer och datadelningstjänster samt mellan gemensamma europeiska dataområden.

I artikel 34 anges att vissa krav i kapitel VI om byte av databehandlingstjänster ska gälla även för att underlätta interoperabilitet för parallell användning av databehandlingstjänster. Det anges även att leverantörerna av databehandlingstjänster vid sådan parallell användning får påföra uttagsavgifter för data.

Artikel 35 innehåller bestämmelser om öppna interoperabilitetsspecifikationer och harmoniserade standarder för databehandlingstjänster. I artikeln föreskrivs vad specifikationer och standarder ska uppnå och hantera. Det finns också bestämmelser om förfaranden för framtagande av dem.

I artikel 36 fastställs väsentliga krav avseende smarta kontrakt för genomförande av datadelningsavtal. Kraven ställs primärt på säljare av applikationer som använder smarta kontrakt eller säljare av smarta kontrakt.

3.4.9 Kapitel IX Genomförande och efterlevnad

Kapitel IX innehåller bl.a. bestämmelser om åtgärder som medlemsstaterna ska vidta för att genomföra och säkerställa efterlevnad av dataförordningen. I artikel 37 finns bestämmelser om behöriga myndigheter. Varje medlemsstat ska utse en eller flera behöriga myndigheter som ska ansvara för tillämpningen och efterlevnaden av förordningen. Om en medlemsstat utser fler än en behörig myndighet ska en så kallad datasamordnare utses för att underlätta samarbetet mellan de behöriga myndigheterna. Artikeln innehåller en detaljerad och omfattande uppräkning av uppgifter och befogenheter som de behöriga myndigheterna ska ha samt annat som är kopplat till organisationen och utövandet av uppgifterna och befogenheterna.

Fysiska och juridiska personer har enligt artikel 38 rätt att enskilt eller, i förekommande fall, kollektivt lämna in ett klagomål till den relevanta behöriga myndigheten i den medlemsstat där de har sin hemvist, sin arbetsplats eller sin etableringsort, om de anser att deras rättigheter enligt förordningen har kränkts. Den behöriga myndighet till vilken klagomålet har lämnats in ska i enlighet med nationell rätt underrätta klaganden om hur förfarandet fortskrider och om det beslut som fattats.

Enligt artikel 39 ska berörda fysiska och juridiska personer ha rätt till ett effektivt rättsmedel avseende rättsligt bindande beslut som fattats av behöriga myndigheter. Om en behörig myndighet underlåter att vidta åtgärder med avseende på ett klagomål ska berörda fysiska och juridiska personer, i enlighet med nationell rätt, antingen ha rätt till ett effektivt rättsmedel eller tillgång till omprövning av en opartisk myndighet som besitter lämplig sakkunskap.

Enligt artikel 40 ska medlemsstaterna fastställa regler om sanktioner för överträdelse av bestämmelserna i förordningen och vidta alla nödvändiga åtgärder för att säkerställa att de tillämpas. Sanktionerna ska vara effektiva, proportionella och avskräckande.

Artikel 41 föreskriver att kommissionen före den 12 september 2025 ska utarbeta och rekommendera icke-bindande standardavtalsvillkor för åtkomst till och användning av data samt icke-bindande standardavtalsklausuler för molnavtal för att hjälpa parterna att utarbeta och förhandla fram avtal med rättvisa, rimliga och icke-diskriminerande avtalsenliga rättigheter och skyldigheter.

I artikel 42 finns bestämmelser om Europeiska datainnovationsstyrelsen, som inrättats av kommissionen som en expertgrupp enligt EU:s dataförvaltningsförordning[5] (se avsnitt 3.5.2 nedan). I styrelsen ska bl.a. behöriga myndigheter vara företrädda. Styrelsen ska stödja en konsekvent tillämpning av dataförordningen.

3.4.10 Kapitel X Rätten av sitt eget slag enligt direktiv 96/9/EG

Kapitel X innehåller en artikel om undantag från rätten av sitt eget slag, artikel 43. Artikeln föreskriver att rätten av sitt eget slag enligt artikel 7 i EU:s databasdirektiv[6] inte ska tillämpas när data erhålls från eller genereras av en uppkopplad produkt eller en tillhörande tjänst som omfattas av denna förordning, särskilt med avseende på artiklarna 4 och 5 i förordningen. Enligt artikel 7 i databasdirektivet ska medlemsstaterna tillerkänna en databasproducent som vid anskaffning, granskning eller presentation visar sig innehålla en kvantitets- eller kvalitetsmässigt sett väsentlig investering, rätten att förbjuda utdrag och/eller återanvändning av hela eller en kvalitativt eller kvantitativt sett väsentlig del av databasens innehåll.

3.4.11 Kapitel XI Slutbestämmelser

Kapitel XI innehåller bestämmelser om förordningens förhållande till andra rättsakter, utövande av delegering samt kommittéförfarande.

Artikel 44 beskriver hur dataförordningen ska samspela med andra unionsrättsakter som reglerar rättigheter och skyldigheter avseende åtkomst till och användning av data, särskilt att dataförordningen inte påverkar sådana skyldigheter som gäller enligt rättsakter som trätt i kraft före dataförordningens ikraftträdande eller unionsrätt som fastställer sektorsspecifika krav. Artikel 45 innehåller bestämmelser om kommissionens befogenhet att anta delegerade akter och artikel 46 anger att kommissionen ska biträdas av den kommitté som inrättats genom dataförvaltningsförordningen.

[5] Europaparlamentets och rådets förordning (EU) 2022/868 av den 30 maj 2022 om europeisk dataförvaltning och om ändring av förordning (EU) 2018/1724 (dataförvaltningsakten).
[6] Europaparlamentets och rådets direktiv 96/9/EG av den 11 mars 1996 om rättsligt skydd för databaser.

Artikel 47 och 48 innehåller ändringar i EU:s förordning om konsumentskyddssamarbete[7] och i direktivet om grupptalan[8].

Enligt artikel 49 ska kommissionen senast den 12 september 2028 genomföra en utvärdering av dataförordningen och lämna en rapport om de viktigaste resultaten till Europaparlamentet, rådet och Europeiska ekonomiska och sociala kommittén.

I artikel 50 föreskrivs att förordningen ska tillämpas från och med den 12 september 2025. De skyldigheter som följer av artikel 3.1 i förordningen ska dock tillämpas på de uppkopplade produkter och de tillhörande tjänster som släpps ut på marknaden efter den 12 september 2026. Särskilda bestämmelser finns också för vissa typer av avtal. Tidpunkten för avtalens ingående påverkar när förordningen ska tillämpas.

3.5 Andra EU-rättsakter inom digitaliseringsområdet

EU har över tid antagit ett flertal rättsakter som på olika sätt reglerar digitaliseringsområdet. Dessa rättsakter bildar tillsammans med dataförordningen en helhet av EU:s nuvarande reglering av området. Nedan presenterar vi kortfattat ett urval av dessa rättsakter samt i förekommenade fall kompletterande svenska bestämmelser. Det finns fler relevanta rättsakter än de som presenteras nedan, både horisontella rättsakter och sektorspecifika rättsakter.

3.5.1 Öppna data-direktivet

Öppna data-direktivet[9] är en omarbetning av EU-direktivet om vidareutnyttjande av information från den offentliga sektorn[10]. Öppna data-direktivets övergripande syfte är att främja användningen av öppna data och stimulera innovation inom produkter och tjänster

[7] Europaparlamentets och rådets förordning (EU) 2017/2394 av den 12 december 2017 om samarbete mellan de nationella myndigheter som har tillsynsansvar för konsumentskyddslagstiftningen och om upphävande av förordning (EG) nr 2006/2004.
[8] Europaparlamentets och rådets direktiv (EU) 2020/1828 av den 25 november 2020 om grupptalan för att skydda konsumenters kollektiva intressen och om upphävande av direktiv 2009/22/EG.
[9] Europaparlamentets och rådets direktiv (EU) 2019/1024 av den 20 juni 2019 om öppna data och vidareutnyttjande av information från den offentliga sektorn.
[10] Europaparlamentets och rådets direktiv 2003/98/EG av den 17 november 2003 om vidareutnyttjande av information från den offentliga sektorn.

genom vidareutnyttjande av information som tillgängliggörs av den offentliga sektorn. Direktivet har anpassats till de senaste framstegen inom digital teknik och ska ytterligare främja digital innovation, särskilt beträffande artificiell intelligens. Direktivets reglering strävar mot att hantera kvarstående och nya hinder som motverkar ett brett vidareutnyttjande av information.

Öppna data-direktivet genomfördes i Sverige primärt genom införandet av en ny lag, lagen (2022:818) om den offentliga sektorns tillgängliggörande av data. Lagen syftar till att främja den offentliga sektorns tillgängliggörande av data för vidareutnyttjande, särskilt i form av öppna data, under förutsättning att krav på informationssäkerhet och skydd av personuppgifter kan upprätthållas och att det inte innebär risker för Sveriges säkerhet.

3.5.2 Dataförvaltningsförordningen

Dataförvaltningsförordningen har sitt ursprung i EU-strategin för data som nämns ovan. Förordningen syftar till att öka förtroendet för datadelning, stärka mekanismerna för att öka tillgången till data och övervinna tekniska hinder för vidareutnyttjande av data. Dataförvaltningsförordningen reglerar villkoren för vidareutnyttjande inom unionen av vissa kategorier av data som innehas av offentliga myndigheter. Vidare reglerar förordningen en ram för anmälan av och tillsyn över tillhandahållandet av dataförmedlingstjänster och en ram för frivillig registrering av enheter som samlar in och behandlar data som tillhandahålls för altruistiska ändamål.

Genom förordningen inrättas också Europeiska datainnovationsstyrelsen (EDIB). Avsikten med inrättandet av styrelsen är att den ska komma att spela en central roll i utvecklingen av interoperabilitet vid datadelning på EU-nivå. EDIB består av företrädare för de behöriga myndigheterna för dataförmedlingstjänster och de behöriga myndigheterna för registrering av dataaltruismorganisationer i alla medlemsstater, Europeiska dataskyddsstyrelsen, Europeiska datatillsynsmannen, Enisa, kommissionen, EU-företrädare för små och medelstora företag eller en företrädare utsedd av nätverket av företrädare för små och medelstora företag och andra företrädare för relevanta organ inom enskilda sektorer samt organ med specifik sakkunskap. Som

nämns ovan ska även behöriga myndigheter enligt dataförordningen vara företrädda i EDIB.

EDIB ska enligt dataförvaltningsförordningen bestå av minst tre undergrupper, varav en för tekniska diskussioner om standardisering, portabilitet och interoperabilitet. Kommissionen ska vara ordförande vid styrelsens sammanträden och tillhandahålla ett sekretariat. EDIB ska bl.a.:

- Bistå kommissionen om prioriteringsordningen för sektorsövergripande standarder som ska användas och utvecklas för bl.a. dataanvändning och sektorsöverskridande datadelning mellan framväxande gemensamma europeiska dataområden.
- Bistå kommissionen med att förbättra den gränsöverskridande, sektorsövergripande interoperabiliteten för data och datadelningstjänster mellan olika sektorer och områden, baserat på befintliga europeiska, internationella eller nationella standarder.
- Föreslå riktlinjer för gemensamma europeiska dataområden (i form av ändamåls- eller sektorspecifika eller sektorsöverskridande interoperabla ramar med allmänna standarder för att underlätta datadelning i unionen).

Det kan noteras att EDIB har särskilda uppgifter även enligt dataförordningen, vilka beskrivs i kapitel 8 i betänkandet.

Kompletterande bestämmelser till dataförvaltningsförordningen finns i lagen (2024:500) med kompletterande bestämmelser till EU:s dataförvaltningsförordning, förordningen (2024:502) med kompletterande bestämmelser till EU:s dataförvaltningsförordning och lagen om den offentliga sektorns tillgängliggörande av data.

3.5.3 Förordningen om digitala tjänster

I förordningen om digitala tjänster[11] fastställs harmoniserade regler för tillhandahållandet av förmedlingstjänster på den inre marknaden. Förmedlingstjänster är i synnerhet tjänster för enbart vidarebefordran, cachningstjänster och värdtjänster. Värdtjänster kan inkludera t.ex.

[11] Europaparlamentets och rådets förordning (EU) 2022/2065 av den 19 oktober 2022 om en inre marknad för digitala tjänster och om ändring av direktiv 2000/31/EG (förordningen om digitala tjänster).

onlineplattformar, såsom sociala nätverk eller onlineplattformar som gör det möjligt för konsumenter att ingå distansavtal med näringsidkare. Förordningen innehåller bestämmelser om villkorat undantag från ansvar för leverantörer av sådana tjänster och om särskilda krav på tillbörlig aktsamhet som är anpassade för specifika kategorier av leverantörer. Förordningen innehåller även regler för genomförandet och kontrollen av efterlevnaden av förordningen, även vad gäller samarbete och samordning mellan behöriga myndigheter. Slutligen fastställer den ett ramverk för samarbete och efterlevnadskontroll mellan kommissionen och nationella myndigheter.

I Sverige finns kompletterande bestämmelser till förordningen i lagen (2024:954) med kompletterande bestämmelser till EU:s förordning om digitala tjänster samt förordningen (2024:958) med kompletterande bestämmelser till EU:s förordning om digitala tjänster.

3.5.4 Förordningen om artificiell intelligens

Förordningen om artificiell intelligens[12] (AI-förordningen) innehåller bl.a. harmoniserade regler för utsläppande på marknaden, ibruktagande och användning av AI-system i unionen, förbud mot vissa AI-användningsområden samt särskilda krav för AI-system med hög risk och skyldigheter för operatörer av sådana system. Syftet med förordningen är att förbättra den inre marknadens funktion, främja användningen av människocentrerad och tillförlitlig artificiell intelligens (AI) och främja innovation samtidigt som en hög skyddsnivå säkerställs för hälsa, säkerhet och grundläggande rättigheter mot skadliga effekter av AI-system. AI-förordningen brukar sägas vara den första heltäckande lagstiftningen om AI. Den sträcker sig över i princip samtliga av samhällets sektorer och är tillämplig för både privata och offentliga aktörer (SOU 2025:101 s. 27).

Utredningen om AI-förordningen lämnade den 6 oktober 2025 sina förslag till anpassningar till AI-förordningen i Sverige (SOU 2025:101). Utredningen föreslår bl.a. att det ska införas en ny lag och en ny förordning med kompletterande bestämmelser till AI-förordningen.

[12] Rådets och Europaparlamentets förordning (EU) 2024/1689 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens).

3.5.5 Förordningen om ett interoperabelt Europa

Förordningen om ett interoperabelt Europa[13] syftar till utveckling av det sedan tidigare existerande Europeiska interoperabilitetsramverket och är tänkt att stärka den gränsöverskridande interoperabiliteten och samarbeten inom den offentliga sektorn på den inre marknaden. Förordningen ska tillämpas av offentliga myndigheter i medlemsstaterna och av unionens institutioner, organ och byråer som tillhandahåller eller förvaltar nätverks- eller informationssystem som gör det möjligt att leverera eller förvalta offentliga tjänster elektroniskt.

Förordningen innehåller en styrningsmodell som ska ge berörda aktörer möjlighet att uttrycka sina synpunkter och är tänkt att stödja delning och återanvändning av bl.a. data. Detta ska bidra till gemensamma lösningar för interoperabilitet i EU. Vidare innehåller förordningen en mekanism för inrättandet av interoperabilitetsbedömning. Förordningen omfattar även rättsliga förutsättningar för att stödja testmiljöer för innovativa interoperabilitetslösningar i regulatoriska sandlådor.

Det har i Sverige inte införts några kompletterande bestämmelser till interoperabilitetsförordningen i lag.[14] Vi noterar dock att regeringen i budgetpropositionen för 2026 föreslår att medel tilldelas Myndigheten för digital förvaltning och Post- och telestyrelsen för den offentliga förvaltningens datadelning enligt kommande lagstiftning om interoperabilitet (prop. 2025/26:1 Utgiftsområde 22 s. 127 och 135).

[13] Europaparlamentets och rådets förordning (EU) 2024/903 om åtgärder för en hög nivå av interoperabilitet inom den offentliga sektorn i hela unionen (förordningen om ett interoperabelt Europa).
[14] Enligt 1 d § förordningen (2018:1486) med instruktion för Myndigheten för digital förvaltning är dock den myndigheten behörig myndighet och enda kontaktpunkt enligt artikel 17 i interoperabilitetsförordningen.

3.6 Kommissionens förenklingsarbete och förslag till ändringar i dataförordningen

I kommissionens arbetsprogram för 2025[15] och i meddelandet Ett enklare och snabbare Europa[16] har kommission aviserat att den ska arbeta med bl.a. förenkling av reglering och effektivare genomförande. Av meddelandet framgår att det innefattar nya mål för att reducera administrativa bördor samt prioritering av nya förenklingsåtgärder. Av arbetsprogrammet framgår att kommissionen kommer att presentera ett antal så kallade omnibus-paket som innehåller förslag om förenkling av olika delar av EU-lagstiftningen. Ett flertal sådana paket har presenterats, exempelvis inom områdena hållbarhet[17] och kemikalieprodukter[18].

Den 19 november 2025 presenterade kommissionen det digitala omnibus-paketet (Digital omnibus på engelska). Paketet innehåller bl.a. förslag till ändringar i AI-förordningen[19] och förslag till en förordning om digitala plånböcker för företag[20]. Paketet innehåller också förslag till ändringar i dataförordningen.[21] Kommissionen föreslår att dataförvaltningsförordningen upphävs och att väsentliga bestämmelser flyttas till dataförordningen. Vidare föreslår kommissionen att bestämmelser som i dagsläget är delade mellan dataförvaltningsförordningen och öppna data-direktivet ska sammanföras till ett kapitel i dataförordningen. Dessutom föreslår kommissionen att förordningen om det fria flödet av andra data än personuppgifter[22]

[15] Meddelande från kommissionen till Europaparlamentet, rådet, europeiska ekonomiska och sociala kommittén samt regionkommittén, Kommissionens arbetsprogram 2025, COM(2025)45 final.
[16] Meddelande från kommissionen till Europaparlamentet, rådet, europeiska ekonomiska och sociala kommittén samt regionkommittén, Ett enklare och snabbare Europa: Meddelande om genomförande och förenkling, COM(2025) 47 final.
[17] Se kommissionens dokument COM(2025)80, COM(2025)81 och COM(2025)87.
[18] Se kommissionens dokument COM(2025)531, SWD(2025)531 och COM(2025)526.
[19] European Commission, Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI), COM(2025) 836 final.
[20] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the establishment of European Business Wallets, COM(2025) 838 final.
[21] European Commission, Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/1679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854, (EU) 2024/1689 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus), COM(2025) 837 final.
[22] Europaparlamentets och rådets förordning (EU) 2018/1807 av den 14 november 2018 om en ram för det fria flödet av andra data än personuppgifter i Europeiska unionen.

upphävs. Detta eftersom den förordningens funktion enligt kommissionen redan täcks av dataförordningen.

Kommissionens förslag till förordning om ändringar i bl.a. dataförordningen ska förhandlas innan den kan beslutas och träda i kraft. Det har inte varit möjligt för oss att i vårt arbete beakta de eventuella ändringar som kommissionens förslag kan leda till.

4 En behörig myndighet ska säkerställa efterlevnad

4.1 Inledning

Enligt artikel 37.1 i dataförordningen ska varje medlemsstat utse en eller flera behöriga myndigheter som ska ansvara för tillämpningen och genomförandet av förordningen. Av skäl 107 i förordningen framgår att de behöriga myndigheternas ansvar innebär att de ska säkerställa tillämpningen och efterlevnaden av förordningen. Ansvaret som föreskrivs i artikel 37.1 bör enligt vår uppfattning i ljuset av skäl 107 förstås som att behöriga myndigheter ska säkerställa tillämpning och efterlevnad av förordningen. Vi kommer därför i det fortsatta att primärt hänvisa till att den övergripande uppgiften för behöriga myndigheter är att säkerställa tillämpning och efterlevnad av förordningen.

I detta kapitel behandlar vi frågor kopplade till den behöriga myndigheten i Sverige, vilka uppgifter myndigheten har samt vilken författningsreglering utöver bestämmelserna i dataförordningen som vi bedömer behövs för att myndigheten ska kunna utföra uppgiften som behörig myndighet. Vi behandlar även vilka författningsändringar som behövs för att säkerställa rätten till effektivt rättsmedel enligt dataförordningen, inklusive för den som gett in ett klagomål till den behöriga myndigheten.

4.1.1 Post- och telestyrelsen är behörig myndighet i Sverige

Medlemsstaterna får enligt artikel 37.1 i dataförordningen inrätta en eller flera nya myndigheter för ändamålet att vara behöriga myndigheter, eller förlita sig på befintliga myndigheter.

Det framgår av våra utredningsdirektiv att regeringens avsikt är att den ska utse en myndighet till behörig myndighet i Sverige. Regeringen fattade den 2 oktober 2025 beslut om att utse Post- och telestyrelsen (PTS) till behörig myndighet enligt dataförordningen.[1] Regeringsuppdraget för PTS gäller till och med 2026. Regeringen har inte aviserat att den har för avsikt att utse fler myndigheter till behöriga myndigheter enligt förordningen.

PTS är en förvaltningsmyndighet med ett samlat ansvar inom postområdet och området för elektronisk kommunikation.[2] Myndigheten har ett flertal uppgifter inom dessa områden och är även bl.a. tillsynsmyndighet samt samordnare för digitala tjänster enligt lagen (2024:954) med kompletterande bestämmelser till EU:s förordning om digitala tjänster[3] och tillsynsmyndighet enligt lagen (2024:500) med kompletterande bestämmelser till EU:s dataförvaltningsförordning[4]. Myndigheten har därför redan i dag i uppdrag att samordna samt utöva tillsyn inom områdena tillgängliggörande av data och digitala tjänster.

Det ingår alltså inte vårt uppdrag att föreslå vilken eller vilka myndigheter som ska vara behöriga myndigheter. Däremot ska vi analysera behovet av nödvändiga organisatoriska och resursmässiga förstärkningar för den behöriga myndigheten.

Sverige behöver utse en behörig myndighet enligt dataförordningen även för tiden efter 2026. Mot bakgrund av våra utredningsdirektiv och regeringsuppdraget till PTS bygger våra förslag och bedömningar avseende den behöriga myndigheten och dess verksamhet på att PTS är behörig myndighet i Sverige även efter 2026. Eftersom det inte ingår i vårt uppdrag har vi inte övervägt andra myndigheter som behörig myndighet. Vi har heller inte övervägt om det bör utses fler än en behörig myndighet.

Vidare har vi att överväga och ta ställning till om andra myndigheter behöver tilläggsuppdrag eller instruktionsändringar. Sådana förslag finns i kapitel 7 i betänkandet. Vi ska även föreslå de författningsändringar och andra åtgärder som behövs för att de berörda myndigheterna, utöver den behöriga myndigheten, ska kunna utöva

[1] Regeringsbeslut, 2025-10-02, Fi2025/01829.
[2] 1 § förordningen (2007:951) med instruktion för Post- och telestyrelsen.
[3] 4 § förordningen (2024:958) med kompletterande bestämmelser till EU:s förordning om digitala tjänster.
[4] 3 § förordningen (2024:502) med kompletterande bestämmelser till EU:s dataförvaltningsförordning.

sina befogenheter och vidta de åtgärder som krävs enligt förordningen. Vi har inte identifierat ett sådant behov.

4.2 En ny lag och en ny förordning ska komplettera EU:s dataförordning

Förslag: En ny lag och en ny förordning med bestämmelser som kompletterar EU:s dataförordning ska införas.

Ord och uttryck i den nya lagen och den nya förordningen ska ha samma betydelse som i dataförordningen.

4.2.1 Det behövs en ny lag och en ny förordning

Enligt artikel 288 andra stycket i EUF-fördraget är EU-förordningar till alla delar bindande och direkt tillämpliga i medlemsstaterna. Det innebär att en förordning inte får införlivas i eller omvandlas i nationell rätt och att medlemsstaterna är förhindrade att närmare tolka bestämmelserna vid införandet av bestämmelser i nationell rätt. Medlemsstaterna får inte heller uttala sig om tillämpningen av en EU-förordning eller förtydliga innebörden av begrepp som förekommer i en förordning. Tolkning av en EU-förordning är förbehållen de myndigheter och domstolar som tillämpar förordningen i respektive medlemsstat. I sista hand är det EU-domstolen som genom sin praxisbildning har tolkningsrätt över en EU-förordning.

Medlemsstaterna ska endast införa kompletterande bestämmelser i den mån EU-förordningen överlämnar något till medlemsstaterna att reglera. Detta gäller vanligtvis processuella regler i enlighet med principen om nationell processuell autonomi. Medlemsstaterna har även en skyldighet att se till att en EU-förordning kan tillämpas i praktiken och får ett effektivt genomslag i respektive medlemsstat. I många fall förutsätter en EU-förordning därför att medlemsstaterna inför nationella regler av verkställande karaktär.

Dataförordningen överlämnar uttryckligen vissa frågor till medlemsstaterna att reglera, t.ex. vilka myndigheter som ska utses till nationella behöriga myndigheter, att myndigheterna ska ges vissa befogenheter och hur sanktionssystemet ska utformas. Eftersom sådana frågor bl.a. rör myndighetsutövning mot enskilda ska den

regleringen ske i lag. I vissa avseenden kan normgivningsmakten dock tillfalla regeringen. Regleringen ska då i dessa avseenden ske i förordning. Normgivningsmakten behandlas i avsnitt 4.5.2 nedan.

I Sverige finns inget regelverk som motsvarar dataförordningen. Hade ett sådant funnits hade det varit naturligt att ändra bestämmelser, eller införa nya bestämmelser, i det regelverket med anledning av dataförordningen. Vi har övervägt om de författningsbestämmelser som vi föreslår kan inordnas i befintliga lagar och förordningar, men inte funnit någon naturlig hemvist. Vi ser också en fördel i att bestämmelserna hålls samlade för tydlighetens och översiktlighetens skull. Vi föreslår därför att det införs en ny lag och en ny förordning som kompletterar dataförordningen. Vi föreslår att de ska heta lagen med kompletterande bestämmelser till EU:s dataförordning respektive förordningen med kompletterande bestämmelser till EU:s dataförordning. I det fortsatta refererar vi till dem som kompletteringslagen och kompletteringsförordningen.

Ord och uttryck i lagen

Artikel 2 i dataförordningen innehåller definitioner. Eftersom medlemsstaterna inte får uttala sig om tillämpningen av en EU-förordning eller förtydliga innebörden av begrepp som förekommer i en förordning ska ord och uttryck ha samma betydelse som i dataförordningen. Att så är fallet ska av tydlighetsskäl framgå av en bestämmelse i kompletteringslagen och i kompletteringsförordningen.

Dataförordningen överlåter åt medlemsstater att utforma systemet för sanktioner. Vi har valt att använda svenska vedertagna begrepp i den delen (se kapitel 5). Förordningen överlåter också åt medlemsstaterna att utforma en ordning för certifiering av tvistlösningsorgan. Vi har valt att använda begreppet certifierande myndighet (se kapitel 6).

4.2.2 Hänvisningar till dataförordningen i kompletteringslagen

Förslag: Hänvisningar till dataförordningen i kompletteringslagen som innehåller bestämmelser om sanktionsavgift och anmärkning ska vara statiska. Övriga hänvisningar till förordningen i kompletteringslagen ska vara dynamiska, dvs. avse förordningen i den vid varje tidpunkt gällande lydelsen.

Kompletteringslagen ska läsas tillsammans med dataförordningen och för att undvika dubbelreglering är det lämpligt att hänvisa till förordningen i kompletteringslagen. Hänvisningar till EU-rättsakter i författningar kan göras antingen statiska eller dynamiska. En statisk hänvisning innebär att hänvisningen avser EU-rättsakten i en viss angiven lydelse. Detta anges i författning genom att det i hänvisningen till rättsakten läggs till ”i dess ursprungliga lydelse”. En följd av denna hänvisningsteknik är att den nationella författningen normalt behöver ändras varje gång EU-bestämmelsen ändras. En dynamisk hänvisning innebär att hänvisningen avser EU-rättsakten i den vid varje tidpunkt gällande lydelsen. Om EU-rättsakten ändras behöver alltså inte hänvisningen i den svenska författningen ändras. Fördelen med dynamisk hänvisning är att ändringen i EU-rättsakten omedelbart får genomslag i den nationella regleringen.

Gröna boken, Riktlinjer för författningsskrivning (Ds 2014:1), rekommenderar att hänvisningar till EU-förordningar, t.ex. vid införande av sanktionsbestämmelser, som utgångspunkt bör ske genom statisk hänvisningsteknik. I vissa fall kan det finnas skäl att använda en annan hänvisningsteknik. En upplysningsbestämmelse som inte tillför lagtexten något materiellt innehåll behöver inte innehålla en hänvisning som anger vilken lydelse av rättsakten som avses. I lagen med kompletterande bestämmelser till EU:s dataförvaltningsförordning är hänvisningen till dataförvaltningsförordningen dynamisk. Hänvisningen är även dynamisk i lagen med kompletterande bestämmelser till EU:s förordning om digitala tjänster, förutom hänvisningarna till sanktionsavgift enligt olika artiklar i förordningen om digitala tjänster (23 §). Detta motiverades av Utredningen om kompletterande bestämmelser till EU:s förordning om digitala tjänster med att bestämmelser om sanktioner bör innehålla statiska hänvisningar till förordningen med hänsyn till behovet av förutsebarhet

i fråga om vilka sanktioner som kan bli följden av överträdelser (SOU 2023:39 s. 74).

Även vi anser att hänvisningarna till bestämmelserna i kompletteringslagen som avser sanktionsavgift och anmärkning ska vara statiska, med hänsyn till behovet av förutsebarhet. Övriga bestämmelser i kompletteringslagen där det hänvisas till dataförordningen är sådana att eventuella ändringar i förordningen bör få omedelbart genomslag i regleringen. För dessa bestämmelser bör hänvisningarna till dataförordningen därför vara dynamiska.

4.3 Regeringen ska utse en eller flera behöriga myndigheter

Som vi redan har konstaterat ska medlemsstaterna enligt artikel 37.1 i dataförordningen utse en eller flera behöriga myndigheter. Om flera behöriga myndigheter utses ska en av dem vara s.k. datasamordnare. I detta avsnitt redovisar vi vår bedömning av hur detta bör regleras i kompletteringslagen och kompletteringsförordningen.

4.3.1 Val av begrepp och reglering av uppgifter och befogenheter

Förslag: Begreppet behöriga myndigheter ska användas i kompletteringslagen och i kompletteringsförordningen.

Uppgifter och befogenheter för behöriga myndigheter ska anges i författning.

Enligt artikel 37.5 i dataförordningen ska uppgifterna och befogenheterna för behöriga myndigheter vara tydligt definierade. Det bör förstås som ett krav på medlemsstaterna att tydligt definiera uppgifterna och befogenheterna i nationell rätt. Vi har övervägt tre alternativ för att uppnå det.

Det första alternativet är att i lag hänvisa till att en behörig myndighet har befogenhet att utföra de uppgifter och vidta de åtgärder som framgår av artikel 37.5 i förordningen, utan ytterligare lagstiftningsåtgärder. Vi bedömer emellertid inte att det uppfyller kravet i

förordningen att uppgifterna och befogenheterna ska vara tydligt definierade. Detta alternativ har vi därför avfärdat.

Det andra alternativet är att i lag införa begreppet tillsynsmyndighet och att en sådan myndighet ska utöva tillsyn över dataförordningen. Det finns i Sverige ingen legaldefinition av tillsyn men en allmän förklaring av vad tillsyn innebär är granskning av hur verksamheter följer de lagar och regler som gäller för dem. Ett skäl som talar för att införa begreppet tillsyn i lag är att många av de uppgifter och befogenheter som föreskrivs i artikel 37.5 i förordningen är av sådan karaktär att de ingår i vad som vanligen avses med tillsyn. Genom att ge tillsynsmyndigheter i uppdrag att utöva tillsyn skulle ett flertal av uppgifterna och befogenheterna ingå i tillsynsuppdraget. Om begreppet tillsynsmyndighet skulle användas i en lag bör det också framgå att en tillsynsmyndighet är behörig myndighet enligt dataförordningen. Motsvarande bestämmelser finns i t.ex. 1 kap. 3 § lagen med kompletterande bestämmelser till EU:s förordning om digitala tjänster och 2 § lagen med kompletterande bestämmelser till EU:s dataförvaltningsförordning.

Vi kan dock konstatera att dataförordningen inte uttryckligen föreskriver att behöriga myndigheter ska utöva tillsyn. Begreppet tillsyn förekommer inte i de artiklar i förordningen som avser de behöriga myndigheternas ansvar och verksamhet. Däremot förekommer referenser till tillsynsmyndigheten inom dataskyddsområdet. Den övergripande uppgiften för behöriga myndigheter är enligt artikel 37.1 i förordningen att ansvara för tillämpningen och efterlevnaden av förordningen, något som enligt vår mening är en bredare uppgift än att utöva tillsyn. Den enda gången begreppet tillsyn används i anslutning till de behöriga myndigheternas uppgifter är i skäl 107 i förordningen, där det framgår att behöriga myndigheter ska ta hänsyn till det faktum att åtgärder för tillsyn och efterlevnadskontroll avseende en enhet som omfattas av en annan medlemsstats behörighet bör antas av den behöriga myndigheten i den andra medlemsstaten. I den engelska språkversionen av förordningen motsvaras tillsyn och efterlevnadskontroll av ”oversight and enforcement”.

Det tredje alternativet som vi har övervägt är att i författning definiera de uppgifter och befogenheter en behörig myndighet har. Detta alternativ tar fasta på kravet som ställs på medlemsstaterna i artikel 37.5 i förordningen att säkerställa att uppgifterna och befogenheterna för de behöriga myndigheterna är tydligt definierade. Genom

att i svensk författning föreskriva vilka uppgifter och befogenheter en behörig myndighet har lever Sverige upp till kravet i artikel 37.5. Vi har som sagt övervägt om begreppet tillsyn bör användas och att begreppet kan tolkas som att det omfattar flera av de uppgifter och befogenheter som framgår av artikel 37.5. Vi bedömer dock att en sådan lösning inte uppfyller kravet i förordningen på att uppgifterna och befogenheterna ska vara tydligt definierade.

Vår bedömning är därför att det tredje alternativet är mest lämpligt eftersom det på tydligast sätt lever upp till kravet artikel 37.5 i dataförordningen att uppgifter och befogenheter ska vara tydligt definierade. Begreppet behöriga myndigheter ska därför användas i kompletteringslagen och i kompletteringsförordningen. Vidare ska deras uppgifter och befogenheter uttryckligen anges i författning. Vår bedömning av hur det bör ske redovisas i avsnitt 4.5 och 4.6.

4.3.2 Det ska i kompletteringslagen anges att regeringen ska utse en eller flera behöriga myndigheter

Förslag: Det ska i kompletteringslagen föreskrivas att den eller de myndigheter som regeringen bestämmer ska vara behöriga myndigheter enligt EU:s dataförordning.

Om fler än en behörig myndighet utses ska regeringen utse en datasamordnare bland dem.

Som konstateras i avsnitt 4.1.1 har regeringen genom ett regeringsbeslut utsett PTS att vara behörig myndighet enligt dataförordningen till och med 2026. Efter denna tidpunkt har Sverige ingen utsedd behörig myndighet om inte ytterligare åtgärder vidtas. Enligt vår uppfattning är det inte en långsiktig lösning att regeringen med jämna mellanrum fattar beslut om att utse en eller flera myndigheter till behöriga myndigheter enligt förordningen. Behöriga myndigheter bör i stället utses i författning.

Som tidigare nämnts ska en behörig myndighet enligt artikel 37.1 i dataförordningen ansvara för tillämpning och genomförande av förordningen, vilket innebär att den ska säkerställa tillämpning och efterlevnad av förordningen. För att kunna säkerställa det ska en behörig myndighet vidta olika åtgärder. Dessa innefattar bl.a. åtgärder som har informationsspridande karaktär, utredningsåtgärder och

sanktioner. Det innebär att en behörig myndighet har befogenhet vidta åtgärder som är betungande för enskilda. Vi föreslår därför att uppgiften att vara behörig myndighet i enlighet med normgivningsmakten ska föreskrivas i lag. Däremot ska regeringen utse vilken eller vilka myndigheter som utses till behörig myndighet. Vi föreslår att det i kompletteringslagen föreskrivs att den eller de myndigheter regeringen bestämmer ska vara behörig myndighet enligt dataförordningen. Det ska vara möjligt för regeringen att utse fler än en behörig myndighet om behov uppstår.

Vilken eller vilka myndigheter som utses till behörig myndighet ska föreskrivas i kompletteringsförordningen. Eftersom våra förslag bygger på att PTS är behörig myndighet i Sverige ingår det i våra författningsförslag (se kapitel 1) att det i förordningen anges att PTS är behörig myndighet.

Om en medlemsstat utser fler än en behörig myndighet ska den enligt artikel 37.2 i dataförordningen utse en datasamordnare bland dem. Vi föreslår därför att det i kompletteringslagen föreskrivs att om regeringen utser fler än en behörig myndighet så ska även en datasamordnare utses bland dem.

Om det bara finns en behörig myndighet ska den utföra datasamordnarens uppgifter

Det övergripande syftet med en datasamordnare är enligt artikel 37.2 i dataförordningen att underlätta samarbetet mellan de behöriga myndigheterna och bistå enheter som omfattas av förordningen i alla frågor som rör dess tillämpning och efterlevnad. Om det enbart finns en behörig myndighet i en medlemsstat, såsom kommer att vara fallet i Sverige, finns det inget behov av att underlätta samarbetet mellan behöriga myndigheter. Datasamordnaren ska emellertid ha fler uppgifter enligt dataförordningen. Enligt artikel 37.6 ska en datasamordnare fungera som enda kontaktpunkt för alla frågor som rör tillämpningen av förordningen. Datasamordnaren ska också säkerställa att offentliga organs begäranden om att göra data tillgängliga på grund av ett exceptionellt behov enligt kapitel V i dataförordningen finns tillgängliga för allmänheten på nätet samt främja frivilliga avtal om datadelning mellan offentliga organ och datahållare. Dessutom ska datasamordnaren årligen informera kommissionen

om de avslag som det underrättats om enligt artiklarna 4.2, 4.8 och 5.11.

Enligt skäl 107 i dataförordningen bör den behöriga myndigheten åta sig de uppgifter som tilldelas datasamordnaren enligt förordningen om ingen datasamordnare har utsetts. Det innebär att PTS, som är ensam behörig myndighet i Sverige, ska utföra uppgifterna. PTS ska alltså, utöver de uppgifter som i dataförordningen tillskrivs en behörig myndighet, säkerställa att offentliga organs begäranden om att göra data tillgängliga på grund av ett exceptionellt behov enligt kapitel V finns tillgängliga för allmänheten på nätet och att frivilliga avtal om datadelning mellan offentliga organ och datahållare främjas. PTS ska också årligen informera kommissionen om de avslag som myndigheten har underrättats om enligt artiklarna 4.2, 4.8 och 5.11.

4.4 Aktörer som omfattas av den behöriga myndighetens jurisdiktion

Det är ett brett spektrum av aktörer som omfattas av den behöriga myndighetens jurisdiktion vad gäller att säkerställa tillämpning och efterlevnad av dataförordningen. Det rör sig om datahållare, användare, datamottagare, tredje parter, offentliga organ, tillverkare av uppkopplade produkter, leverantörer av tillhörande tjänster, säljare av en applikation som använder smarta kontrakt[5], rättsliga företrädare, företag som har utsetts till grindvakt enligt artikel 3 i EU:s förordning om digitala marknader[6] samt deltagare i dataområden.

I artikel 37.8 i dataförordningen föreskrivs att enheter som omfattas av tillämpningsområdet för förordningen ska omfattas av behörigheten för den medlemsstat där de är etablerade. Med enheter avses de aktörer som omfattas av förordningen och den svenska behöriga myndigheten är alltså behörig att vidta åtgärder avseende de enheter som är etablerade i Sverige. Vidare framgår av artikeln att om en enhet är etablerad i fler än en medlemsstat ska den anses omfattas av behörigheten för den medlemsstat där den har sitt huvudsakliga etableringsställe, dvs. där enheten har sitt huvudkontor eller

[5] I avsaknad av en sådan omfattas enligt artikel 36 i förordningen den person vars närings- eller yrkesverksamhet inbegriper användning av smarta kontrakt för andra inom ramen för genomförandet av ett avtal eller en del av det om att tillgängliggöra data.
[6] Europaparlamentets och rådets förordning (EU) 2022/1925 om öppna och rättvisa marknader inom den digitala sektorn och om ändring av direktiv (EU) 2019/1937 och (EU) 2020/1828 (förordningen om digitala marknader).

säte från vilket de huvudsakliga finansiella funktionerna och den operativa kontrollen utövas.

Enheter som omfattas av tillämpningsområdet för förordningen och som gör uppkopplade produkter tillgängliga eller erbjuder tillhörande tjänster i unionen, och som inte är etablerade i unionen, ska enligt artikel 37.11 i förordningen utse en rättslig företrädare i en av medlemsstaterna. Enheter som utser rättsliga företrädare anses enligt artikel 37.13 omfattas av den medlemsstats behörighet där dess rättsliga företrädare finns. Av samma artikel framgår dock att det faktum att enheten utser en rättslig företrädare inte påverkar enhetens ansvar eller rättsliga åtgärder som vidtas mot den. Sammantaget innebär detta att enheter i tredje land som utser rättslig företrädare i Sverige omfattas av Sveriges behörighet och omfattas av den svenska behöriga myndighetens jurisdiktion.

4.5 Uppgifter och befogenheter för behöriga myndigheter och hur de bör regleras i svensk rätt

4.5.1 Uppgifter och befogenheter enligt dataförordningen

Utöver det övergripande ansvaret för behöriga myndigheter att säkerställa tillämpning och efterlevnad av dataförordningen föreskriver förordningen ett antal mer detaljerade uppgifter och befogenheter för myndigheterna. Enligt artikel 37.5 ska medlemsstaterna säkerställa att uppgifterna och befogenheterna för de behöriga myndigheterna är tydligt definierade och omfattar följande:

a) Öka datakompetensen och medvetenheten bland de användare och enheter som omfattas av förordningen om deras rättigheter och skyldigheter enligt förordningen.

b) Hantera klagomål som härrör från påstådda överträdelser av förordningen, inbegripet vad gäller företagshemligheter, och i lämplig utsträckning undersöka föremålet för klagomålen och regelbundet inom rimlig tid informera de klagande, i tillämpliga fall i enlighet med nationell rätt, om hur utredningen fortskrider och om resultatet av den, särskilt om ytterligare utredning eller samordning med en annan behörig myndighet är nödvändig.

c) Utföra undersökningar om frågor som rör tillämpningen av förordningen, inbegripet på grundval av information som erhålls från en annan behörig myndighet eller offentlig myndighet.

d) Ålägga effektiva, proportionella och avskräckande ekonomiska sanktioner, som kan inbegripa viten och sanktioner med retroaktiv verkan, eller inleda rättsliga förfaranden för åläggande av böter.

e) Övervaka den tekniska och relevanta kommersiella utveckling som är relevant för tillgängliggörande och användning av data.

f) Samarbeta med behöriga myndigheter i andra medlemsstater och, i förekommande fall, med kommissionen eller Europeiska datainnovationsstyrelsen, för att säkerställa en konsekvent och effektiv tillämpning av förordningen, inbegripet utbyte av all relevant information på elektronisk väg, utan oskäligt dröjsmål, även avseende punkt 10 i artikel 37.

g) Samarbeta med de relevanta behöriga myndigheter som ansvarar för genomförandet av andra unionsrättsakter eller nationella rättsakter, inbegripet med myndigheter med behörighet på området data och elektroniska kommunikationstjänster, med den tillsynsmyndighet som ansvarar för att övervaka tillämpningen av EU:s dataskyddsförordning[7] eller med sektorsmyndigheter för att säkerställa att dataförordningen verkställs i överensstämmelse med annan unionsrätt och nationell rätt.

h) Samarbeta med de relevanta behöriga myndigheterna för att säkerställa att artiklarna 23–31, artikel 34 och 35 verkställs i överensstämmelse med annan unionsrätt och självreglering som är tillämplig på leverantörer av databehandlingstjänster.

i) Säkerställa att bytesavgifter avskaffas i enlighet med artikel 29.

j) Granska de begäranden om data som gjorts enligt kapitel V.

Utöver uppräkningen i artikel 37.5 framgår av förordningen att behöriga myndigheter har ytterligare uppgifter. Av artiklarna 4.2, 4.7, 4.8, 5.10 och 5.11 följer att datahållare ska underrätta en behörig

[7] Europaparlamentets och rådet förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

myndighet om datahållaren exempelvis avbryter eller vägrar att tillgängliggöra data, vilket innebär att den behöriga myndigheten ska ta emot sådana underrättelser. Vidare framgår av artikel 42 att behöriga myndigheter ska vara representerade i Europeiska datainnovationsstyrelsen, som inrättats av kommissionen som en expertgrupp enligt artikel 29 i EU:s dataförvaltningsförordning[8].

4.5.2 Utgångspunkter för den svenska regleringen av uppgifter och befogenheter

Med normgivningsmakten avses rätten att besluta rättsregler, dvs. regler som är bindande för enskilda och myndigheter och som gäller generellt. Normgivningsmakten regleras i huvudsak i 8 kap. regeringsformen (1974:152) (RF) men bestämmelser om normgivning finns även i andra kapitel i regeringsformen samt i tryckfrihetsförordningen (1949:105) och yttrandefrihetsgrundlagen (1991:1469).

Enligt 8 kap. RF är normgivningsmakten fördelad mellan riksdagen och regeringen och bygger på principen att de centrala delarna av normgivningen ska ligga hos riksdagen. Det område där riksdagen i första hand har normgivningskompetensen kallas det primära lagområdet. Det primära lagområdet framgår dels av 8 kap. 2–6 §§ RF, dels genom ett antal andra bestämmelser i regeringsformen, tryckfrihetsförordningen och yttrandefrihetsgrundlagen. Området omfattar bl.a. grundlagarna och riksdagsordningen, civilrättsliga föreskrifter, offentligrättsliga föreskrifter som är betungande för enskilda samt vissa typer av kommunalrättsliga föreskrifter. Av 8 kap. 2 § RF framgår att föreskrifter ska meddelas genom lag om de avser bl.a. enskildas personliga ställning och deras personliga och ekonomiska förhållanden inbördes samt förhållandet mellan enskilda och det allmänna under förutsättning att föreskrifterna gäller skyldigheter för enskilda eller i övrigt avser ingrepp i enskildas personliga eller ekonomiska förhållanden.

Riksdagen kan genom delegering till regeringen överlåta delar av sin normgivningskompetens inom det primära lagområdet. Den delen av det primära lagområdet där riksdagen däremot inte kan bemyndiga regeringen att meddela föreskrifter, dvs. inte kan delegera, brukar kallas det obligatoriska lagområdet. Hit hör bl.a. den civilrättsliga

[8] Europaparlamentets och rådets förordning (EU) 2022/868 om europeisk dataförvaltning och om ändring av förordning (EU) 2018/1724 (dataförvaltningsakten).

lagstiftningen, annan rättsverkan av brott än böter och föreskrifter om skatt och föreskrifter om konkurs eller utsökning. Delegering inom det obligatoriska lagområdet är emellertid möjlig om det gäller föreskrifter om anstånd med att fullgöra förpliktelser och lagars ikraftträdande och tillämpning.

Det område där delegering är möjlig kallas för det delegeringsbara området och regleras i 8 kap. 3–5 §§ RF. Ett bemyndigande av riksdagens ska ges i lag och rikta sig till regeringen. Om det gäller avgifter och vissa skatter kan det dock rikta sig direkt till kommuner.

I 8 kap. 7 § RF finns de huvudsakliga bestämmelserna om det område där regeringen utan delegering får meddela föreskrifter, dvs. regeringens primärområde. Hit hör föreskrifter om verkställighet av lag samt föreskrifter som inte enligt grundlag ska meddelas av riksdagen, den s.k. restkompetensen. Med verkställighetsföreskrifter avses dels tillämpningsföreskrifter av administrativt slag, dels föreskrifter som kompletterar en lag utan att tillföra den något väsentligt nytt. I verkställighetsföreskrifter får det inte ingå sådant som kan uppfattas som en ny skyldighet för enskilda eller som ett nytt ingrepp i enskildas personliga eller ekonomiska förhållanden. Till restkompetensen hör sådana offentligrättsliga föreskrifter som inte rör förhållandet mellan enskilda och det allmänna utan avser de statliga myndigheternas organisation, arbetsuppgifter och inre verksamhetsformer. Till restkompetensen hör också sådana föreskrifter som visserligen rör förhållandet mellan enskilda och det allmänna men som ur den enskildes synpunkt inte är betungande utan gynnande eller neutrala.

Normgivningsmakten påverkar var bestämmelser som avser de behöriga myndigheterna bör placeras i svenska författningar. De kan placeras i lag, som meddelas av riksdagen, eller i förordning som meddelas av regeringen. Vi kommer i det följande att redogöra för våra förslag avseende vilka uppgifter och befogenheter för behöriga myndigheter som ska placeras i kompletteringslagen och vilka som ska placeras i kompletteringsförordningen.

4.5.3 Bestämmelser om sanktioner ska anges i kompletteringslagen

För att en behörig myndighet ska kunna utföra det övergripande uppdraget att säkerställa att dataförordningen efterlevs krävs att myndigheten kan vidta åtgärder dels i form av att undersöka hur förordningen tillämpas samt utreda påstådda överträdelser, dels i form av att överträdelser av förordningens bestämmelser leder till konsekvenser. Att en behörig myndighet ska ha befogenhet att vidta åtgärder framgår av dataförordningen.

Enligt artikel 40.1 i förordningen ska medlemsstaterna fastställa regler om sanktioner för överträdelse av bestämmelserna i förordningen och vidta alla nödvändiga åtgärder för att säkerställa att de tillämpas. Sanktionerna ska vara effektiva, proportionella och avskräckande. I artikel 37.5 d föreskrivs att behöriga myndigheter ska ha i uppgift, samt ha befogenhet, att ålägga effektiva, proportionella och avskräckande ekonomiska sanktioner. Möjligheter för den behöriga myndigheter att vidta åtgärder, besluta om sanktioner inklusive sanktionsavgifter samt våra förslag i anslutning till detta behandlas i kapitel 5.

4.5.4 Rätt att begära de upplysningar och handlingar som behövs ska anges i kompletteringslagen

Förslag: Den som omfattas av EU:s dataförordning ska på begäran av en behörig myndighet lämna de upplysningar och handlingar som behövs för att säkerställa att EU:s dataförordning, kompletteringslagen och föreskrifter som har meddelats i anslutning till lagen följs.

Enligt artikel 37.14 i dataförordningen ska behöriga myndigheter ha befogenhet att från användare, datahållare eller datamottagare, eller deras rättsliga företrädare som omfattas av deras medlemsstats behörighet begära all information som krävs för att kontrollera efterlevnaden av förordningen. Möjligheten att hämta in upplysningar och handlingar är ett viktigt redskap för att kunna säkerställa efterlevnad av ett regelverk. De inhämtade uppgifterna ingår i underlaget för myndighetens granskning och beslut.

Att den behöriga myndigheten ska ha denna befogenhet följer direkt av förordningen avseende den krets av aktörer som anges i artikel 37.14. Enligt vår uppfattning bör dock befogenheten inte vara begränsad till dessa aktörer eftersom även andra aktörer som omfattas av förordningen kan ha information som är av betydelse för myndighetens utredning.

Ett krav att tillmötesgå en begäran om upplysningar eller handlingar är betungande för enskilda och ett sådant krav ska därför föreskrivas i lag. Vi föreslår att det i kompletteringslagen ska framgå att den behöriga myndigheten har rätt att begära in de upplysningar och handlingar som behövs för att säkerställa att dataförordningen, kompletteringslagen eller föreskrifter som meddelats i anslutning till lagen följs. Bestämmelsen bör formuleras så att det tydligt framgår att det är den som omfattas av dataförordningen som på begäran av en behörig myndighet ska lämna de upplysningar och handlingar som behövs. Vi ser inga hinder mot att bestämmelsen omfattar en bredare krets aktörer än de som anges i artikel 37.14. En uppgiftsskyldig ska enligt vårt förslag även kunna föreläggas vid vite att inkomma med de begärda uppgifterna eller handlingarna (se kapitel 5).

4.6 Uppgifter för behöriga myndigheter som bör föreskrivas i kompletteringsförordningen

4.6.1 Hantera och utreda klagomål avseende påstådda överträdelser

Förslag: Det ska i kompletteringsförordningen föreskrivas att behöriga myndigheter har i uppgift att hantera klagomål som härrör från påstådda överträdelser av EU:s dataförordning, inbegripet vad gäller företagshemligheter, och i lämplig utsträckning undersöka föremålet för klagomålen.

Enligt artikel 37.5 b i dataförordningen ska uppgifter och befogenheter för behöriga myndigheter omfatta att hantera klagomål som härrör från påstådda överträdelser av förordningen, inbegripet vad gäller företagshemligheter. Enligt bestämmelsen ska myndigheterna i lämplig utsträckning undersöka föremålet för klagomålet. Att ta emot och hantera klagomål är en naturlig uppgift för myndigheter

som har till uppgift att säkerställa att ett regelverk efterlevs. Inkomna klagomål hjälper myndigheten att få en bild av hur regelverket tillämpas i praktiken och att bedöma vilka åtgärder som bör vidtas om överträdelser kan konstateras. Denna del av artikeln preciserar vad en behörig myndighet ska och får göra inom ramen för det övergripande uppdraget att säkerställa tillämpning och efterlevnad av förordningen. Att detta är en uppgift för en behörig myndighet faller inom restkompetensen och vi föreslår därför att den anges i kompletteringsförordningen.

Behöriga myndigheter ska vidare enligt artikel 37.5 b regelbundet inom rimlig tid informera de som lämnar in klagomål, i tillämpliga fall i enlighet med nationell rätt, om hur utredningen fortskrider och om resultatet av den, särskilt om ytterligare utredning eller samordning med en annan behörig myndighet är nödvändig. Frågor om information till den som har lämnat in ett klagomål behandlas i avsnitt 4.6.2 och 4.10.3.

4.6.2 Information om hur en utredning fortskrider

Förslag: Det ska i kompletteringsförordningen föreskrivas att behöriga myndigheter regelbundet ska informera den som har lämnat in ett klagomål om hur utredningen fortskrider och om resultatet av den.

Enligt artikel 38.2 i dataförordningen ska den behöriga myndigheten i enlighet med nationell rätt underrätta klaganden om hur förfarandet fortskrider och om det beslut som fattats. Enligt artikel 37.5 b ska en behörig myndighet regelbundet inom rimlig tid informera de klagande, i tillämpliga fall i enlighet med nationell rätt, om hur utredningen fortskrider och om resultatet av den, särskilt om ytterligare utredning eller samordning med en annan behörig myndighet är nödvändig. Båda bestämmelserna hänvisar till nationell rätt. I detta avsnitt behandlas frågan om underrättelse om hur ärendet fortskrider. Frågan om underrättelse av beslut behandlas i avsnitt 4.10.3.

Bestämmelser om som gäller för svenska myndigheter i deras allmänna ärendehandläggning finns i regeringsformen, förvaltningslagen (2017:900), och offentlighets- och sekretesslagen (2009:400). Bestämmelserna i dessa lagar styr förfarandet vid ärendehandläggning

hos den svenska behöriga myndigheten. Enligt 6 § förvaltningslagen ska en myndighet se till att kontakterna med enskilda blir smidiga och enkla (serviceskyldigheten). Myndigheten ska lämna den enskilde sådan hjälp att han eller hon kan ta till vara sina intressen. Hjälpen ska ges i den utsträckning som är lämplig med hänsyn till frågans art, den enskildes behov av hjälp och myndighetens verksamhet. Enligt 9 § ska ett ärende handläggas så enkelt, snabbt och kostnadseffektivt som möjligt utan att rättssäkerheten eftersätts (skyndsamhetskravet). Av 10 § framgår att den som är part i ett ärende har rätt att ta del av allt material som har tillförts ärendet. Vidare framgår av 11 § att om en myndighet bedömer att avgörandet i ett ärende som har inletts av en enskild part kommer att bli väsentligt försenat, ska myndigheten underrätta parten om detta. Enligt 25 § ska en myndighet innan den fattar ett beslut i ett ärende, om det inte är uppenbart obehövligt, underrätta den som är part om allt material av betydelse för beslutet och ge parten tillfälle att inom en bestämd tid yttra sig över materialet (partsinsyn).

Enligt artikel 38.2 i dataförordningen ska den behöriga myndigheten i enlighet med nationell rätt underrätta den som har lämnat in klagomålet om hur förfarandet fortskrider och enligt artikel 37.5 b är kravet att myndigheten regelbundet inom rimlig tid ska informera den som har lämnat in klagomålet om hur utredningen fortskrider och resultatet av den. Bestämmelserna om kommunikation och partsinsyn i förvaltningslagen gäller för den som är part i ett ärende. Bestämmelserna i dataförordningen utgår inte från ett partsbegrepp i den mening som avses i svensk rätt, utan tar sikte på den som har lämnat in klagomålet. Det finns i svensk rätt inget hinder mot att den behöriga myndigheten underrättar den som har lämnat in klagomålet om hur utredningen fortskrider. Vår bedömning är emellertid att bestämmelserna i förvaltningslagen inte i tillräcklig utsträckning tillgodoser den rätt till information som bestämmelserna i dataförordningen föreskriver. Eftersom artikel 38.2 och artikel 37.5 b i förordningen hänvisar till underrättelse respektive informera i enlighet med nationell rätt bör det i svensk rätt införas en sådan bestämmelse avseende klagomål enligt dataförordningen.

Bestämmelsen är inte betungande för enskilda och kan meddelas med stöd av restkompetensen. Vi föreslår att den införs i kompletteringsförordningen. Enligt bestämmelsen ska den behöriga myndigheten regelbundet informera den som har lämnat in klagomålet om

hur utredningen fortskrider och om resultatet av den. Det blir upp till den behöriga myndigheten att i enlighet med bestämmelsen avgöra i vilken omfattning den som har lämnat in klagomålet ska informeras. Skyndsamhetskravet i 9 § förvaltningslagen motsvarar enligt vår uppfattning kravet i artikel 37.5 b att information ska ges inom rimlig tid. Det behöver därför inte uttryckligen anges i bestämmelsen.

4.6.3 Undersöka hur dataförordningen tillämpas

Förslag: Det ska i kompletteringsförordningen föreskrivas att behöriga myndigheter har i uppgift att utföra undersökningar om frågor som rör tillämpningen av EU:s dataförordning.

Av artikel 37.5 c i dataförordningen framgår att behöriga myndigheter ska ha i uppgift och befogenhet att utföra undersökningar om frågor som rör tillämpningen av förordningen, inbegripet på grundval av information som erhålls från en annan behörig myndighet eller offentlig myndighet. Att utföra undersökningar kopplade till det regelverk en behörig myndighet ansvarar för tillämpning och efterlevnad av får, i likhet med vad som gäller för hantering av klagomål, anses vara en naturlig del av uppdraget. Mot bakgrund av att uppgifter och befogenheter enligt artikel 37.5 tydligt ska definieras föreslår vi att det i kompletteringsförordningen, med stöd av restkompetensen, föreskrivs att en behörig myndighet har i uppgift att utföra undersökningar om frågor som rör tillämpningen av dataförordningen.

4.6.4 Granska begäran enligt kapitel V

Förslag: Det ska i kompletteringsförordningen föreskrivas att behöriga myndigheter har i uppgift att granska begäranden om data som gjorts enligt kapitel V i EU:s dataförordning.

I kapitel V i dataförordningen finns bestämmelser som innebär att offentliga organ kan begära data från företag om de har ett exceptionellt behov av data. Kapitel V behandlas i kapitel 7 i betänkandet.

I detta avsnitt behandlar vi enbart de bestämmelser som rör behöriga myndigheters granskning av begäran om data av offentliga organ med stöd av kapitel V i förordningen.

Av artikel 17.2 g i förordningen framgår att en begäran av ett offentligt organ ska överföras till datasamordnaren i den medlemsstat där det begärande offentliga organet är etablerat. Datasamordnaren ska utan oskäligt dröjsmål offentliggöra begäran på nätet under förutsättning att datasamordnaren inte anser att ett offentliggörande skulle utgöra en risk för den allmänna säkerheten. I avsaknad av en datasamordnare bör det offentliga organet skicka begäran till den behöriga myndigheten i den medlemsstat där organet är etablerat (se avsnitt 4.3.2). Det ställs i förordningen inget krav på att datasamordnaren eller den behöriga myndigheten måste göra en materiell prövning av innehåller i begäran. Av skäl 69 i förordningen framgår dock att den behöriga myndigheten efter mottagandet av en underrättelse om en begäran kan besluta att den ska bedöma om begäran är lagenlig och utöva sina uppgifter i samband med verkställandet och tillämpningen av förordningen. Det får förstås som att det är upp till den behöriga myndigheten att avgöra om den ska göra en bedömning av om en begäran är förenlig med förordningen eller inte.

En datahållare kan enligt artikel 18.2 avslå eller begära ändring av en begäran om datahållaren inte har kontroll över de data som begärs, om en liknande begäran för samma ändamål tidigare har lämnats in av ett annat organ och datahållaren inte har underrättats om att dessa data har raderats samt om begäran inte uppfyller de villkor som ställs på en begäran. Av artikel 18.5 framgår att om det offentliga organet, kommissionen, Europeiska centralbanken eller unionsorganet vill överklaga en datahållares vägran att tillhandahålla begärda data eller om datahållaren vill bestrida begäran och ärendet inte kan lösas genom en lämplig ändring av begäran, ska ärendet hänskjutas till den behöriga myndighet i den medlemsstat där datahållaren är etablerad. Att ärendet ska hänskjutas den behöriga myndigheten innebär enligt vår uppfattning att myndigheten ska avgöra ärendet.

När det gäller situationer då det föreligger ett exceptionellt behov av data finns särskilda bestämmelser om gränsöverskridande samarbete och ömsesidigt bistånd i artikel 22 i förordningen. Även i dessa situationer aktualiseras frågan om att granska en begäran om data. Om ett offentligt organ avser att begära data från en datahållare som är etablerad i en annan medlemsstat, ska den enligt artikel 22.3 först

underrätta den behöriga myndigheten i den medlemsstaten om den avsikten. Kravet gäller även när kommissionen, Europeiska centralbanken och unionsorgan begär data. Begäran ska granskas av den behöriga myndigheten i den medlemsstat där datahållaren är etablerad. Efter att den behöriga myndigheten har granskat begäran ska den utan onödigt dröjsmål antingen överföra begäran till datahållaren eller avslå begäran av vederbörligen motiverade skäl. Begäran av data med stöd av kapitel V i förordningen vid gränsöverskridande situationer behandlas ytterligare i kapitel 7 i betänkandet.

Att en behörig myndighet ska granska inkomna begäranden och i vissa fall vidta åtgärder enligt kapitel V i förordningen står klart. Som framgår ovan är kraven på en behörig myndighet vad gäller granskning av en begäran olika beroende på om det rör sig om en rent nationell situation eller en gränsöverskridande situation. Mot bakgrund av kravet i artikel 37.5 i dataförordningen att uppgifter och befogenheter för behöriga myndigheter tydligt ska definieras föreslår vi att det i kompletteringsförordningen föreskrivs att behöriga myndigheter har i uppgift att granska begäranden om data som gjorts enligt kapitel V i dataförordningen. En sådan uppgift kan meddelas av regeringen med stöd av restkompetensen.

4.6.5 Vidta åtgärder för att bytesavgifter avskaffas

Förslag: Det ska i kompletteringsförordningen föreskrivas att behöriga myndigheter har i uppgift att säkerställa att bytesavgifter avskaffas i enlighet med artikel 29 i EU:s dataförordning.

Enligt artikel 37.5 i dataförordningen ska en behörig myndighet ha i uppgift att och ha befogenhet att säkerställa att bytesavgifter avskaffas i enlighet med artikel 29 i förordningen. Enligt artikel 29.1 får leverantörer av databehandlingstjänster från och med den 12 januari 2027 inte ta ut några bytesavgifter av kunden för bytesprocessen. Med bytesprocessen avses i artikel 23 möjligheten att byta till en databehandlingstjänst som omfattar samma tjänstetyp och som tillhandahålls av en annan leverantör av databehandlingstjänster, byta till lokal IKT-infrastruktur eller att använda flera leverantörer av databehandlingstjänster samtidigt. Från och med den 11 januari 2024 till och med

12 januari 2027 får leverantörer av databehandlingstjänster enligt artikel 29.2 ta ut nedsatta bytesavgifter av kunden för bytesprocessen.

De sanktioner en behörig myndighet kan vidta i syfte att åstadkomma att bytesavgifter avskaffas är av sådan karaktär att de ska föreskrivas i lag (se vidare i kapitel 5). Att en behörig myndighet har i uppgift att säkerställa att sådana avgifter avskaffas kan däremot meddelas med stöd av restkompetensen och vi föreslår därför att uppgiften föreskrivs i kompletteringsförordningen.

4.6.6 Samarbeta med andra aktörer

Förslag: Det ska i kompletteringsförordningen föreskrivas att behöriga myndigheter har i uppgift att samarbeta med behöriga myndigheter i andra medlemsstater och, i förekommande fall, med Europeiska kommissionen eller Europeiska datainnovationsstyrelsen, för att säkerställa en konsekvent och effektiv tillämpning av EU:s dataförordning.

Det ska i kompletteringsförordningen föreskrivas att behöriga myndigheter har i uppgift att samarbeta med relevanta behöriga myndigheter som ansvarar för genomförandet av andra unionsrättsakter än EU:s dataförordning eller nationella rättsakter för att säkerställa att EU:s dataförordning verkställs i överensstämmelse med annan unionsrätt och nationell rätt.

Det ska i kompletteringsförordningen föreskrivas att behöriga myndigheter har i uppgift att samarbeta med relevanta behöriga myndigheter för att säkerställa att artiklarna 23–31, artikel 34 och 35 i EU:s dataförordning verkställs i överensstämmelse med annan unionsrätt och självreglering som är tillämplig på leverantörer av databehandlingstjänster.

Behöriga myndigheter ska enligt ett flertal artiklar i dataförordningen samarbeta med andra myndigheter, organ samt kommissionen. De ska enligt artikel 37.5 f i förordningen samarbeta med behöriga myndigheter i andra medlemsstater och, i förekommande fall, med kommissionen eller Europeiska datainnovationsstyrelsen, för att säkerställa en konsekvent och effektiv tillämpning av förordningen. Det innefattar utbyte av all relevant information på elektronisk väg, utan oskäligt dröjsmål. Enligt artikel 38.3 ska behöriga myndigheter dess-

utom samarbeta för att effektivt och snabbt hantera och avgöra klagomål, bl.a. genom att utan oskäligt dröjsmål utbyta all relevant information på elektronisk väg. För gränsöverskridande ärenden finns särskilda bestämmelser. Av artikel 37.15 framgår att om en behörig myndighet i en medlemsstat begär bistånd eller verkställighetsåtgärder från en behörig myndighet i annan medlemsstat ska den lämna en motiverad begäran. En behörig myndighet ska vid mottagandet av en sådan begäran utan oskäligt dröjsmål lämna ett svar med detaljerade uppgifter om de åtgärder som har vidtagits eller som avses att vidtas.

Av artikel 37.4 a framgår att när det gäller sektorsspecifika frågor som rör åtkomst till och användning av data i samband med tillämpningen av dataförordningen ska sektorsmyndigheternas behörighet respekteras. Enligt artikel 37.5 g ska samarbete ske med de relevanta behöriga myndigheter som ansvarar för genomförandet av andra unionsrättsakter eller nationella rättsakter, inbegripet med myndigheter med behörighet på området data och elektroniska kommunikationstjänster, med den tillsynsmyndighet som ansvarar för att övervaka tillämpningen av EU:s dataskyddsförordning eller med sektorsmyndigheter för att säkerställa att förordningen verkställs i överensstämmelse med annan unionsrätt och nationell rätt. I Sverige är Integritetsskyddsmyndigheten tillsynsmyndighet över dataskyddsförordningen.[9] Inom området elektronisk kommunikation är PTS regleringsmyndighet och tillsynsmyndighet enligt lagen (2022:482) om elektronisk kommunikation.[10] Myndigheten är även är tillsynsmyndighet över dataförmedlingstjänster enligt lagen med kompletterande bestämmelser till EU:s dataförvaltningsförordning.[11] Vilka övriga myndigheter, som ansvarar för sektorer, som den behöriga myndigheten kan komma att behöva samarbeta med kommer att skifta från fall till fall. Behovet av samarbete beror också på innehållet i den lagstiftning andra myndigheter tillämpar samt vilket behov av exempelvis information som den behöriga myndigheten enligt dataförordningen har.

Vidare ska samarbete ske med de relevanta behöriga myndigheterna för att säkerställa att artiklarna 23–31, artikel 34 och 35 i

[9] 3 § förordningen (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning.
[10] 1 kap. 5 § förordningen (2022:511) om elektronisk kommunikation.
[11] 3 § förordningen (2024:502) med kompletterande bestämmelser till EU:s dataförvaltningsförordning.

förordningen verkställs i överensstämmelse med annan unionsrätt och självreglering som är tillämplig på leverantörer av databehandlingstjänster.

Vi kan konstatera att det av diskussioner mellan behöriga myndigheter i medlemsstaterna i dagsläget råder olika syn på hur vissa av förordningens bestämmelser ska tolkas och tillämpas när det gäller hanteringen av gränsöverskridande ärenden. Det måste enligt vår uppfattning finnas utrymme för den svenska behöriga myndigheten att tillsammans med sina motsvarigheter i andra medlemsstater, inom ramen för det tolkningsutrymme dataförordningen ger, komma överens om hur gränsöverskridande ärenden ska hanteras i syfte att uppnå en effektiv och rättssäker hantering.

Enligt 23 § förvaltningslagen har en myndighet ett utredningsansvar och ska se till att ett ärende blir utrett i den omfattning som dess beskaffenhet kräver. En myndighet kan inom ramen för sitt utredningsansvar begära ett yttrande från en annan myndighet eller från någon enskild. Av 8 § förvaltningslagen följer att en myndighet inom sitt verksamhetsområde ska samverka med andra myndigheter. Att svenska myndigheter får, och i vissa fall ska, arbeta tillsammans med andra myndigheter framgår alltså redan av förvaltningslagen. Frågan är om detta stöd räcker för att en svensk behörig myndighet ska kunna utföra sitt uppdrag enligt dataförordningen. Att myndigheten ska samarbeta med andra framgår av förordningen och vår bedömning är att förordningens bestämmelser om samarbete, trots bestämmelserna i förvaltningslagen, bör ha motsvarigheter i svensk rätt. Detta mot bakgrund av att uppgifter och befogenheter för behöriga myndigheter enligt artikel 37.5 i förordningen ska vara tydligt definierade. Bestämmelser om att behöriga myndigheter har i uppgift att samarbeta med andra myndigheter, Europeiska kommissionen och Europeiska datainnovationsstyrelsen är sådana uppgifter som kan meddelas av regeringen med stöd av restkompetensen och ska därför föreskrivas i kompletteringsförordningen.

Samarbete med andra myndigheter och aktörer aktualiserar frågor om sekretess, dessa frågor behandlas i kapitel 9 i betänkandet.

4.6.7 Öka datakompetensen och medvetenheten om rättigheter och skyldigheter enligt dataförordningen

Förslag: Det ska i kompletteringsförordningen föreskrivas att behöriga myndigheter har i uppgift att öka datakompetensen och medvetenheten bland de användare och enheter som omfattas av EU:s dataförordning om deras rättigheter och skyldigheter enligt förordningen.

Den behöriga myndigheten ska enligt artikel 37.5 a öka datakompetensen och medvetenheten bland de användare och enheter som omfattas av förordningen om deras rättigheter och skyldigheter enligt förordningen. Med enheter avses aktörer som omfattas av förordningen. Datakompetens definieras inte i någon av förordningens artiklar men enligt skäl 19 i förordningen avses färdigheter, kunskap och förståelse som gör det möjligt för användare, konsumenter och företag, särskilt mikroföretag och små och medelstora företag som omfattas av förordningen, att dels bli medvetna om det potentiella värdet av de data de genererar, producerar och delar, dels bli motiverade att erbjuda och ge åtkomst till sina data i enlighet med relevanta rättsliga regler. Datakompetens bör enligt samma skäl 19 omfatta mer än kunskaper om verktyg och teknik och syfta till att ge medborgare och företag förmåga och egenmakt att dra nytta av en inkluderande och rättvis datamarknad. Av skäl 19 framgår också att myndigheten bör främja verktyg och anta åtgärder för att förbättra datakompetensen samt öka medvetenheten om deras rättigheter och skyldigheter enligt förordningen.

Det kommer enligt vår uppfattning att finnas ett behov av att hålla samman och publicera information om dataförordningen och utvecklingen kopplad till förordningen. Det kan komma att finnas behov av information om exempelvis delegerade akter som beslutas av kommissionen och om standarder som kan användas för att uppfylla krav i förordningen. Ett sätt för en behörig myndighet att informera om rättsutvecklingen vad gäller förordningen är att myndigheten löpande informerar om beslut som har fattats inom ramen för myndighetens uppdrag att säkerställa att förordningen efterlevs. Behovet av information från den behöriga myndigheten behandlas ytterligare i kapitel 8 i betänkandet.

Den uppgift som behöriga myndigheter ska ha enligt artikel 37.5 a i dataförordningen är av en utbildande och informationsgivande karaktär som inte är betungande för enskilda. Uppgiften kan meddelas med stöd av restkompetensen. Vi föreslår att i det kompletteringsförordningen i enlighet med artikel 37.5 a föreskrivs att behöriga myndigheter har i uppgift att öka datakompetensen och medvetenheten bland de användare och enheter som omfattas av dataförordningen om deras rättigheter och skyldigheter enligt förordningen.

4.6.8 Övervaka den tekniska och kommersiella utvecklingen

Förslag: Det ska i kompletteringsförordningen föreskrivas att behöriga myndigheter har i uppgift att övervaka den tekniska och relevanta kommersiella utveckling som är relevant för tillgängliggörande och användning av data.

Av artikel 37.5 e i dataförordningen framgår att behöriga myndigheter ska ha i uppgift att, samt ha befogenhet att, övervaka den tekniska och relevanta kommersiella utveckling som är relevant för tillgängliggörande och användning av data. Sådan övervakning är en förutsättning för att en behörig myndighet effektivt ska kunna säkerställa tillämpning och efterlevnad av förordningen. Frågor om tillgängliggörande och användning av data är i många avseenden horisontella och den tekniska och kommersiella utvecklingen kan, oavsett om den sker i en avgränsad sektor eller inte, komma att påverka sådant tillgängliggörande och sådan användning som omfattas av dataförordningen. Därför bör övervakningen av utvecklingen genomföras utifrån en bred ansats.

Uppgiften för behöriga myndigheter att övervaka den tekniska och relevanta kommersiella utvecklingen kan meddelas med stöd av restkompetensen. Vi föreslår därför att det i kompletteringsförordningen ska föreskrivas att behöriga myndigheter har i uppgift att övervaka den tekniska och relevanta kommersiella utveckling som är relevant för tillgängliggörande och användning av data.

4.7 Underrättelser om att hindra, avbryta eller vägra datadelning

Bedömning: Det krävs inga ytterligare bestämmelser i svensk rätt om att behöriga myndigheter ska ta emot underrättelser enligt artiklarna 4 och 5 i EU:s dataförordning.

I dataförordningens kapitel II finns bestämmelser om tillgängliggörande av data från uppkopplade produkter och tillhörande tjänster. I kapitlet finns ett antal krav på en datahållare att i vissa situationer underrätta den behöriga myndigheten om en åtgärd som datahållaren har vidtagit. Enligt artikel 4.2 får användare och datahållare genom avtal begränsa eller förbjuda åtkomst till, användning eller ytterligare delning av data, om sådan behandling skulle kunna undergräva säkerhetskraven för den uppkopplade produkten, i enlighet med unionsrätten eller nationell rätt, och leda till allvarliga negativa effekter på fysiska personers hälsa, säkerhet eller trygghet. Behöriga myndigheter får tillhandahålla användare och datahållare teknisk expertis i detta sammanhang. Om datahållaren vägrar att dela data enligt artikeln ska den underrätta den behöriga myndigheten.

Av artikel 4.6 ska datahållare komma överens med användare om proportionella tekniska och organisatoriska åtgärder som är nödvändiga för att bevara konfidentialiteten för delade data. Enligt artikel 4.7 ska en datahållare underrätta den behöriga myndigheten om att datahållaren har hindrat eller avbrutit datadelning mot bakgrund av att användaren underlåter att genomföra de överenskomna åtgärderna eller om det saknas en överenskommelse om åtgärder.

Om en datahållare kan visa att det är högst sannolikt att den kommer att lida allvarlig ekonomisk skada till följd av röjandet av företagshemligheter, trots de tekniska och organisatoriska åtgärder som vidtagits av användaren, får datahållaren under exceptionella omständigheter och från fall till fall enligt artikel 4.8 avslå en begäran om åtkomst till de specifika data som avses. Om datahållaren vägrar att dela data ska den underrätta den behöriga myndigheten.

När det gäller tillgängliggörande av data till tredje part finns i artikel 5.10 och 5.11 motsvarande bestämmelser som i artikel 4.7

och 4.8. Även i sådana fall ska datahållaren underrätta den behöriga myndigheten.

Det föreskrivs inte i förordningen att den behöriga myndighet som tar emot en underrättelse ska agera på den. Av artikel 4.9 a och artikel 5.12 a samt skäl 31 i förordningen framgår dock att om användaren eller en tredje part vill bestrida datahållarens beslut att vägra, hindra eller avbryta delningen av data kan användaren eller den tredje parten lämna in ett klagomål till den behöriga myndigheten. Myndigheten ska då utan oskäligt dröjsmål besluta om och på vilka villkor datadelning bör inledas eller återupptas.

Den behöriga myndigheten ska alltså inte agera på själva underrättelsen. Det rör sig därför om information som inkommer till myndigheten men det faktum att myndigheten tar emot informationen behöver i sig inte leda till en åtgärd mot enskild.

Det föreskrivs inte i artikel 37.5 i förordningen att behöriga myndigheter ska ta emot underrättelser enligt artiklarna 4 och 5 i förordningen. Det innebär att uppgiften att ta emot underrättelser inte behöver vara en tydligt definierad uppgift, såsom krävs av artikel 37.5. Att behöriga myndigheter kommer att ta emot underrättelser enligt artiklarna 4 och 5 följer direkt av bestämmelserna i dataförordningen. Det behövs därför ingen bestämmelse om detta i svensk rätt.

4.8 Rätt att lämna in klagomål till en behörig myndighet

Bedömning: Det krävs inga ytterligare bestämmelser i svensk rätt med anledning av rätten att lämna in klagomål till behöriga myndigheter enligt EU:s dataförordning.

Enligt artikel 38.1 i dataförordningen ska fysiska och juridiska personer ha rätt att enskilt eller, i förekommande fall, kollektivt lämna in ett klagomål till den relevanta behöriga myndigheten i den medlemsstat där de har sin hemvist, sin arbetsplats eller sin etableringsort, om de anser att deras rättigheter enligt förordningen har kränkts. Bestämmelsen påverkar inte något annat administrativt prövningsförfarande.

Det finns i förordningen ett flertal bestämmelser som uttryckligen föreskriver en möjlighet att lämna in klagomål till den behöriga

myndigheten, exempelvis artikel 4.3 a och artikel 5.12 a. Enligt artikel 20.5 kan ett organ som begär data vid exceptionellt behov som inte godtar den ersättningsnivå som datahållaren begär lämna in ett klagomål till den behöriga myndigheten i den medlemsstat där datahållaren är etablerad. Detsamma gäller enligt artikel 20.5 när en datahållare inte godtar att den begärande parten avser att överföra eller tillgängliggöra data till en annan part.

Fysiska och juridiska personer som har sin hemvist, arbetsplats eller sin etableringsort i Sverige kommer mot bakgrund av att regeringen har utsett PTS till behörig myndighet enligt förordningen ha rätt att lämna in ett klagomål till myndigheten. Detta oavsett som den aktör klagomålet är riktat mot är etablerad i Sverige eller i en annan medlemsstat. Om aktören är etablerad i annan medlemsstat aktualiseras förordningens bestämmelser om gränsöverskridande samarbete mellan medlemsstaternas behöriga myndigheter.

Att enskilda kan inleda ett ärende hos en myndighet genom en ansökan, anmälan eller annan framställning framgår av 19 § förvaltningslagen. Det finns i svensk lagstiftning inte något hinder för fysiska eller juridiska personer att lämna in klagomål till en behörig myndighet. Det behövs därför inte några ytterligare bestämmelser i svensk rätt som föreskriver en rätt att lämna in klagomål till en behörig myndighet.

För att det ska vara fråga om ett klagomål i dataförordningens mening, bedömer vi att det krävs att klagomålet innefattar ett påstående om att rättigheter enligt dataförordningen som tillkommer den som gett in klagomålet har kränkts. Allmänna tips eller anmälningar om att aktörer inte uppfyller sina skyldigheter enligt dataförordningen, men som inte inbegriper ett påstående av kränkning av rättigheter som tillkommer den som gett in klagomålet omfattas inte av rätten att ge in klagomål och därmed åtföljande rättigheter till tillgång till effektivt rättsmedel, m.m. (se vidare i avsnitt 4.9).

Rätten att lämna in klagomål som föreskrivs i artikel 38.1 i förordningen hänvisar till en medlemsstat. Det måste enligt vår uppfattning förstås som att rätten att lämna in klagomål enligt artikeln tillskrivs en fysisk eller juridisk person som har sin hemvist eller är etablerad i en medlemsstat.

4.9 Rätten till ett effektivt rättsmedel

4.9.1 Inledning

Av artikel 39.1 i dataförordningen följer att berörda fysiska och juridiska personer ska ha rätt till ett effektivt rättsmedel avseende rättsligt bindande beslut som fattats av behöriga myndigheter. Det finns därför anledning att ta ställning till vilka kompletterande bestämmelser som krävs i svensk lagstiftning för att säkerställa att kravet på tillgång till ett effektivt rättsmedel uppfylls.

Vidare framgår av artikel 39.2 att om en behörig myndighet underlåter att vidta åtgärder med avseende på ett klagomål ska berörda fysiska och juridiska personer, i enlighet med nationell rätt, antingen ha rätt till ett effektivt rättsmedel eller tillgång till omprövning av en opartisk myndighet som besitter lämplig sakkunskap. Även i detta avseende finns det anledning att överväga vilka författningsändringar som är nödvändiga för att svara mot dataförordningens krav.

4.9.2 Överprövning av förvaltningsrättsliga beslut

Besluts överklagbarhet

I svensk lagstiftning regleras besluts överklagbarhet på två sätt. Det är vanligt att specialförfattningar innehåller bestämmelser om överklagande som reglerar såväl forumfrågan som frågan om överklagbarhet, ofta i en och samma paragraf. Utöver detta finns en generell bestämmelse i förvaltningslagen om besluts överklagbarhet.

Av 41 § förvaltningslagen framgår att ett beslut får överklagas om beslutet kan antas påverka någons situation på ett inte obetydligt sätt. Det innebär att det är ett besluts faktiska verkningar som är avgörande för bedömningen av beslutets överklagbarhet. Bestämmelsen tillkom i och med den nu gällande förvaltningslagen och ger uttryck för de principer som utvecklats i Högsta förvaltningsdomstolens praxis. Syftet med införandet av den generella bestämmelsen om överklagbarhet var att öka förutsebarheten och motverka tillämpningssvårigheter, mot bakgrund av överklagandeinstitutets grundläggande betydelse för den enskildes rättsskydd (prop. 2016/17:180 s. 252).

Innan den nu gällande förvaltningslagen trädde i kraft saknades det generell reglering av besluts överklagbarhet. Syftet med överklagandeinstitutet är att ge den som på ett visst sätt påverkas av ett beslut en möjlighet att få beslutet upphävt eller ändrat för att på så sätt undvika de oönskade verkningar som beslutet annars skulle innebära. Enligt allmänna förvaltningsrättsliga principer har det ansetts gå att överklaga beslut som har en påvisbar effekt, men inte beslut som enbart i mycket begränsad utsträckning kan påverka någons faktiska situation (prop. 2016/17:180 s. 248). När det gäller kravet på påverkan som ställs för att ett beslut ska vara överklagbart uttalade regeringen i samband med införandet av bestämmelsen bl.a. att det bör vara fråga om påverkan av någorlunda kvalificerat slag (prop. 2016/17:180 s 253).

Utformningen av överklagandebestämmelser i specialförfattning varierar. I många fall innehåller bestämmelsen en uppräkning av vilka beslut enligt specialförfattningen som är överklagbara. I förarbetena till den nya förvaltningslagen uttalar regeringen bl.a. följande om sådana bestämmelser. Tillämpningen av sådana särskilda bestämmelser påverkas inte av regeringens förslag till allmän reglering i förvaltningslagen. Ibland innehåller överklagandebestämmelsen inte någon uttömmande uppräkning av överklagbara beslut. I stället anges allmänt t.ex. att ”beslut enligt denna lag” får överklagas. Detta innebär dock inte att alla tänkbara beslut enligt den lagen därmed görs överklagbara. Frågan om överklagbarhet i dessa fall avgörs i stället med ledning av allmänna förvaltningsrättsliga principer. Högsta förvaltningsdomstolens praxis är alltså för närvarande vägledande (jfr t.ex. RÅ 2007 ref. 7). Ett införande av en allmän reglering i förvaltningslagen om överklagbarhet är inte avsett att innebära någon ändring av detta förhållande. Det är i och för sig tänkbart att det i rättstillämpningen kan uppkomma fråga om denna typ av överklagandebestämmelser i specialförfattning innebär en sådan avvikelse från den nya förvaltningslagen som avses i bestämmelsen om denna lags subsidiaritet i förhållande till annan författning. Frågan är dock enligt regeringens uppfattning av mindre praktisk betydelse eftersom det även i ett sådant fall ytterst är Högsta förvaltningsdomstolens praxis kring den nya lagens allmänna bestämmelse som i det enskilda fallet blir vägledande för bedömningen i sak (prop. 2016/17:180 s. 254).

Några beslutstyper som inte ansetts överklagbara är t.ex. återförvisningsbeslut, eftersom sådana beslut inte innebär ett ställnings-

tagande i sakfrågan. Ren passivitet har inte tidigare ansetts kunna angripas genom överklagande, åtminstone inte generellt.

EU-rätten ställer krav på att beslut ska kunna överklagas. Av EU-domstolens praxis framgår att på EU-rätten grundade beslut ska kunna bli föremål för överprövning i domstol. Principen om ett effektivt domstolsskydd eller rättsmedel utgör en allmän unionsrättslig rättsgrundsats, som även kommit till uttryck i artiklarna 6 och 13 i Europakonventionen.

Enskildas rätt att överklaga

Ett beslut får enligt 42 § förvaltningslagen överklagas av den som beslutet angår, om det har gått honom eller henne emot.

För rätt att överklaga enligt tidigare gällande förvaltningslag (1986:223) krävdes dels att det beslut som angreps angick den som klagar, dels att beslutet gick denne emot. Bestämmelsen om kravet på saklegitimation tog sikte på enskildas rätt att överklaga, dvs. såväl fysiska personer som privaträttsliga juridiska personer, t.ex. aktiebolag och ideella föreningar. Bestämmelsen hade i sak samma innebörd som den föreskrift om rätt att överklaga som fanns i 1971 års förvaltningslag (prop. 1971:30 del 2 s. 398–399 och 592 och prop. 1985/86:80 s. 72). Det finns därför en omfattande och utvecklad rättspraxis i fråga om dess tillämpning.

Bestämmelsen i tidigare gällande förvaltningslag om rätt för enskilda att överklaga infördes ursprungligen i 1971 års förvaltningslag för att kodifiera den praxis som då fanns kring denna fråga. I propositionen som föregick den lagen anfördes att syftet med en allmän regel om rätt att överklaga främst borde vara att klargöra att det finns ett krav på saklegitimation vid överklagande. Den närmare bestämningen av kretsen av personer som uppfyller kravet fick liksom tidigare avgöras i rättstillämpningen (prop. 1971:30 del 2 s. 398–399).

Regeringen gjorde inför införandet av den nu gällande förvaltningslagen bedömningen att den nya förvaltningslagen bör innehålla en uttrycklig och grundläggande bestämmelse om enskildas rätt att överklaga som klargör att det finns ett krav på saklegitimation. Vidare bedömde regeringen det som lämpligast att utforma bestämmelsen i den nya lagen om rätt att överklaga så att den motsvarar det sakliga innehållet i 22 § i tidigare gällande förvaltningslag (prop. 2016/

17:180 s. 262 f.). Den omfattande rättspraxis som finns kopplad till den äldre regleringen är därför fortsatt vägledande.

Klagorätten hänger nära samman frågan om vem som är part i ett ärende. Klagorätt har i första hand den som är part.

Myndigheters rätt att överklaga

Rätten att överklaga gäller enskilda, dvs. såväl fysiska personer som privaträttsliga juridiska personer. Frågan om en myndighet kan överklaga en annan myndighets beslut regleras inte av förvaltningslagen och endast delvis genom bestämmelser i specialförfattningar. Vad som är gällande rätt följer i stället närmast uteslutande av rättspraxis. Enligt rättspraxis anses statliga och kommunala organ kunna uppträda som enskilda när de agerar som företrädare för ett rent privaträttsligt intresse, och inte fullgör en offentligrättsligt reglerad uppgift. När staten eller en kommun eller region handlar som en enskild har de därmed rätt att överklaga en myndighets beslut (se prop. 2016/17:180 s. 333).

Statliga myndigheter anses dock inte utan författningsstöd kunna överklaga beslut av en annan myndighet, när myndigheten i fråga inte företräder ett rent privaträttsligt intresse. Detta eftersom statliga myndigheter inte utgör självständiga juridiska personer utan agerar som företrädare för staten och de kan därför i princip inte föra talan mot varandra (prop. 2025/26:28 s. 180). Med andra ord anses en statlig myndighet som agerar i sin offentligrättsliga roll bara ha klagorätt om det finns författningsstöd för det. Kommuners och regioners rätt att överklaga förvaltningsbeslut regleras ibland genom speciallag och i andra fall avgörs överklaganderätten med ledning av regeln i 7 a § förvaltningsprocesslagen eller sedvanerätt.[12]

[12] Lundmark och Säfsten, Förvaltningslagen (26 aug. 2024, Version 1C, JUNO), kommentaren till 42 §.

4.9.3 Den behöriga myndighetens beslut får överklagas

Förslag: Det ska i kompletteringslagen framgå att ett beslut av en behörig myndighet som fattats med stöd av dataförordningen eller kompletteringslagen får överklagas till allmän förvaltningsdomstol.

En myndighet får överklaga en behörig myndighets beslut. Prövningstillstånd krävs för överklagande till kammarrätt.

Den behöriga myndighetens övergripande uppgift att säkerställa tillämpning och efterlevnad av dataförordningen innebär att myndigheten kommer att inleda ärenden mot aktörer som omfattas av förordningen. Myndigheten har möjlighet att fatta bindande beslut i sådana ärenden gentemot dessa aktörer. De sanktionsåtgärder vi föreslår att den behöriga myndigheten ska kunna vidta behandlas i kapitel 5 i betänkandet.

Bestämmelser om överklagande av ett beslut som har fattats av en myndighet finns i 41 § förvaltningslagen, som vi redogjort för ovan. Enligt artikel 39.1 i dataförordningen ska berörda fysiska och juridiska personer ha rätt till ett effektivt rättsmedel avseende rättsligt bindande beslut som fattats av behöriga myndigheter. Den behöriga myndighetens beslut för att säkerställa efterlevnad kommer innebära rättsverkningar för enskilda i förvaltningsrättslig mening och rikta sig gentemot en aktör som är part i ärendet. När det gäller möjlighet att överklaga beslut i ärenden om certifiering, se kapitel 6.

Rätten till ett effektivt rättsmedel mot myndighetsbeslut tillgodoses i svensk rätt normalt genom möjligheten att överklaga beslutet till allmän förvaltningsdomstol, dvs. till en förvaltningsrätt som första instans. När det gäller beslut som fattas enligt en EU-förordning framgår rätten att överklaga av 41 § förvaltningslagen. Någon särskild överklagandebestämmelse behövs därmed i och för sig inte i nationell lagstiftning när det gäller bindande beslut som den behöriga myndigheten fattar enligt dataförordningen. Däremot behövs det särskilda bestämmelser om rätten att överklaga den behöriga myndighetens beslut enligt kompletteringslagen, dvs. beslut om att utfärda förelägganden, meddela anmärkning och att ta ut sanktionsavgift. För att inte skapa otydlighet om hur olika beslut ska kunna överklagas så bör regleringen vara uttömmande i den nya lagen. Således bör även rätten att överklaga den behöriga myndighetens be-

slut enligt dataförordningen uttryckligen anges i den nya lagen. Förordningen kräver inte att överprövningen ska göras av en domstol. En effektiv och rättssäker ordning talar dock för att överprövning av den behöriga myndighetens beslut bör ske inom ramen för det befintliga systemet för överklagande av förvaltningsbeslut, dvs. med förvaltningsrätten som första instans.

Ett beslut får som vi redogjort för ovan enligt 42 § förvaltningslagen överklagas av den som beslutet angår, om det har gått honom eller henne emot. Klagorätt tillkommer alltså den som beslutet angår, om beslutet har gått denne emot. Kravet som ställs i dataförordningen innebär att de fysiska och juridiska personer som berörs av ett rättsligt bindande beslut som fattats av en behörig myndighet ska ha tillgång till ett effektivt rättsmedel. Ordningen i 42 § förvaltningslagen överensstämmer enligt vår bedömning med kravet på rättsmedel enligt artikel 39.1 i dataförordningen och bör således gälla även för beslut som den behöriga myndigheten fattar enligt förordningen och kompletteringslagen. Det finns en rad olika typer av aktörer som omfattas av dataförordningens bestämmelser. De beslut som den behöriga myndigheten kommer att fatta kommer enligt vår bedömning ha karaktären av beslut inom ramen för tillsyn och beslut efter överprövning av en begäran av data enligt kapitel V. Både i beslut som fattas inom ramen för tillsyn och i beslut avseende begäran om data finns en tydlig part som beslutet får rättsverkningar för. Det kan dock inte uteslutas att ett beslut skulle kunna ha rättsligt bindande följder även för andra än den som beslutet riktas mot. Dessa skulle i så fall också ha rätt att överklaga beslutet, enligt förvaltningslagens generella bestämmelse om klagorätt.

Dataförordningen omfattar även offentliga organ när de agerar i en privaträttslig kapacitet, t.ex. som användare. Rätten till överklagande bör därför gälla både för enskilda och offentliga organ. Vi föreslår vidare att sanktionsavgift ska få beslutas mot offentliga organ, inklusive statliga, regionala och kommunala myndigheter (se avsnitt 5.5.2). De ska t.ex. kunna åläggas sanktionsavgift för överträdelser av artikel 19, dvs. när de hanterarar data som begärts in för ett exceptionellt behov i strid med artikel 19 i dataförordningen. När en myndighet begär in och behandlar data enligt kapitel V agerar den i sin offentligrättsliga kapacitet. Det exceptionella behovet av data ska föreligga vid fullgörandet av lagstadgade skyldigheter av allmänt in-

tresse. Myndigheter bör ha rätt att överklaga den behöriga myndighetens beslut om ingripanden.

När statliga myndigheter utför en offentligrättsligt reglerad uppgift anses de inte utan författningsstöd ha rätt att överklaga ett beslut av en annan myndighet. Det bör därför framgå av kompletteringslagen att de får överklaga en behörig myndighets beslut. Motsvarande rätt bör gälla även för regionala och kommunala myndigheter.

Kompletteringslagen bör mot denna bakgrund innehålla en bestämmelse om överklagande som ger myndigheter en uttrycklig rätt att överklaga en behörig myndighets beslut.

Som huvudregel krävs prövningstillstånd vid överklagande till kammarrätten. Vi har inte funnit skäl att frångå denna ordning. Prövningstillstånd ska därför krävas vid överklagande till kammarrätt.

4.9.4 Den som har lämnat in ett klagomål får överklaga den behöriga myndighetens beslut att inte vidta åtgärder

Förslag: Det ska av kompletteringslagen framgå att en behörig myndighets beslut att inte vidta åtgärder med avseende på ett klagomål får överklagas hos allmän förvaltningsdomstol av den som gett in klagomålet.

Som vi redogjort för ovan i avsnitt 4.8 så följer det av artikel 38.1 i dataförordningen att fysiska och juridiska personer ska ha rätt att lämna in ett klagomål till den behöriga myndigheten om de anser att deras rättigheter enligt förordningen har kränkts. I skäl 108 förtydligas att fysiska och juridiska personer, för att hävda sina rättigheter vid överträdelser av dataförordningen, bör ha rätt att söka omprövning genom att inkomma med ett klagomål.

Om en behörig myndighet underlåter att vidta åtgärder med avseende på ett klagomål ska berörda fysiska och juridiska personer, i enlighet med nationell rätt, enligt artikel 39.2 antingen ha rätt till ett effektivt rättsmedel eller tillgång till omprövning av en opartisk myndighet som besitter lämplig sakkunskap.

Vi har ovan redogjort för besluts överklagbarhet. Ett beslut om att inte vidta åtgärder med anledning av ett klagomål har som utgångspunkt inte sådana rättsverkningar som krävs för att beslutet ska vara

överklagbart, jfr RÅ 2010 ref. 29.[13] Den som lämnar in ett klagomål är som utgångspunkt inte heller att betrakta som part i ett ärende, varför inte heller förutsättningarna i 42 § förvaltningslagen kan anses uppfyllda. För resonemang kring förvaltningslagens partsbegrepp kopplat till klagomålsärenden, se avsnitt 4.10.2.

I dataskyddsförordningen artikel 78.1 finns en bestämmelse som motsvarar den i artikel 39.1 i dataförordningen, där det framgår att ”utan att det påverkar något annat administrativt prövningsförfarande eller prövningsförfarande utanför domstol ska varje fysisk eller juridisk person ha rätt till ett effektivt rättsmedel mot ett rättsligt bindande beslut rörande dem som meddelats av en tillsynsmyndighet”. Av skäl 141 och 143 i ingressen till dataskyddsförordningen framgår att den registrerade bör ha rätt till ett effektivt rättsmedel vid den behöriga nationella domstolen mot ett beslut av en tillsynsmyndighet som har rättsliga följder för denna person. Som exempel nämns bl.a. beslut där tillsynsmyndigheten helt eller delvis avslår eller avvisar ett klagomål. Enligt Högsta förvaltningsdomstolen innebär detta att ett beslut vars innebörd är att Integritetsskyddsmyndigheten inte kommer att göra vad som begärts i ett klagomål måste betraktas som ett rättsligt bindande beslut som är överklagbart enligt artikel 78.1 i EU:s dataskyddsförordning (HFD 2023 ref 54).

I dataförordningen finns inte några uttalanden i skälen som motsvarar vad som framgår av skäl 141 och 143 i dataskyddsförordningen. I dataförordningen framgår i stället rätten till effektivt rättsmedel, eller rätt till omprövning av en opartisk myndighet, mot den behöriga myndighetens beslut att underlåta att vidta åtgärder med avseende på ett klagomål direkt av artikel 39.2. I bestämmelsen finns också en skrivning om att rätten till effektivt rättsmedel eller omprövning ska ges i enlighet med nationell rätt. Frågan är om en sådan rätt kan anses föreligga med stöd av förvaltningslagen. Det finns enligt vår bedömning flera omständigheter som medför att det är osäkert om en sådan rättighet kan anses föreligga. För det första krävs för att 41 § förvaltningslagen ska vara tillämplig, att ett beslut har påtagliga rättsverkningar, vilket inte ansetts vara fallet när det gäller beslut att inte vidta åtgärder med anledning av ett klagomål. För det andra är inte förutsättningarna för talerätt enligt 42 § för-

[13] Se även RÅ 1996 not. 190, där Regeringsrätten fann att ett beslut att avskriva ett tillsynsärende inte är av beskaffenhet att kunna bli föremål för en överprövning hos förvaltningsdomstol.

valtningslagen uppfyllda. Det är enligt vår uppfattning inte heller möjligt att genom en ren analogi till dataskyddsförordningen och med stöd av Högsta förvaltningsdomstolens avgörande i HFD 2023 ref 54 dra slutsatsen att förutsättningarna för överklagbarhet skulle vara uppfyllda. För det första är det fråga om två skilda rättsakter som meddelats med stöd av olika bestämmelser i grundfördragen.[14] För det andra saknar dataskyddsförordningen den hänvisning till nationell rätt som finns i dataförordningen.

Vi bedömer därför att det av tydlighetsskäl i kompletteringslagen behöver införas en bestämmelse om att en behörig myndighets beslut att inte vidta åtgärder med avseende på ett klagomål får överklagas av den som gett in klagomålet. Artikel 39.2 i dataförordningen lämnar två alternativ för omprövning. Antingen ska sådan ske genom tillgång till ett effektivt rättsmedel eller genom tillgång till omprövning av en opartisk myndighet som besitter lämplig sakkunskap. Vi bedömer att det första alternativet är det som ligger i linje med hur den svenska rättsordningen är utformad. Vi anser vidare att det inte finns någon lämplig myndighet att ge uppdraget som omprövningsinstans.[15] Det mest ändamålsenliga är att sådana beslut som det nu är fråga om prövas i allmän förvaltningsdomstol. Det ska därför anges i kompletteringslagen att en behörig myndighets beslut att inte vidta åtgärder med avseende på ett klagomål får överklagas till allmän förvaltningsdomstol.

Som vi redogjort för ovan regleras rätten att överklaga dels genom förvaltningslagens bestämmelser, dels genom bestämmelser i specialförfattningar och myndighetsinstruktioner. Även om det i en författning anges att ett beslut enligt författningen eller ett beslut av en viss myndighet kan överklagas, innebär det inte att alla sådana beslut är överklagbara. Överklagbarheten är begränsad till följd av allmänna principer som har utbildats i praxis (jfr RÅ 2007 ref. 7 och där angivna rättsfall). En myndighets faktiska handlande eller underlåtenhet att handla kan exempelvis inte överklagas. En annan förutsätt-

[14] Dataskyddsförordningen är beslutad med stöd av artikel 16 i fördraget om Europeiska unionens funktionssätt (FEUF) som reglerar skydd för fysiska personer. Dataförordningen är beslutad med stöd av artikel 114 FEUF, som ger unionen rätt att besluta om regler för att främja den inre marknaden.

[15] Kommissionen har i ett överträdelseärende mot Sverige bedömt att Riksdagens ombudsmän och Justitiekanslern inte kan anses vara domstolar i den mening som avses i artikel 47 i EU:s rättighetsstadga och att de därför inte kan anses utgöra rättsmedel enligt artikel 78.2 i förordningen i dataskyddsförordningen ((formell underrättelse – överträdelse nummer [2022]2022, C[2022]1665 final, den 6 april 2022).

ning för överklagande är att beslutet har någon inte alltför obetydlig verkan för parter eller andra. Normalt saknas också möjlighet att klaga över motiveringen till ett beslut (prop. 1997/98:101 s. 50 f.).

Frågan uppkommer då om vi genom att införa en bestämmelse i specialförfattning kan åstadkomma att sådana beslut som nu är i fråga kan överklagas, mot bakgrund av de konstateranden vi gjort ovan avseende avsaknad av påtagliga rättsverkningar och talerätt. Möjligheten att överklaga dessa beslut föreskrivs i en EU-förordning. Sådana förordningar gäller som utgångspunkt direkt i medlemsstaterna och framför nationell rätt. Vi bedömer mot denna bakgrund att den bestämmelse vi föreslår, tolkad i ljuset av dataförordningen och Sveriges åtaganden gentemot EU, medför att dataförordningens krav i artikel 39.2 ska anses uppfyllda och att sådana beslut som nu är i fråga ska kunna överklagas oavsett om beslutet anses ha rättsverkningar i förhållande till den som gett in klagomålet.

4.10 Underrättelse om beslut och handläggning

4.10.1 Inledning

Dataförordningen ställer krav på handläggningen av ärenden hos den behöriga myndigheten. Av artikel 38.2 i dataförordningen framgår att den behöriga myndighet till vilken ett klagomål har lämnats in i enlighet med nationell rätt ska underrätta den som har lämnat in klagomålet om hur förfarandet fortskrider och om det beslut som fattats. Artikeln innehåller alltså två krav. Det ena är ett krav på information om handläggningen och det andra är ett krav på beslutsunderrättelse. Underrättelse av beslut är en förutsättning för att det ska vara praktiskt möjligt att överklaga ett beslut. Vi har i avsnitt 4.9.4 föreslagit att det ska framgå av kompletteringslagen att den som har lämnat in ett klagomål enligt dataförordningen ska ha rätt att överklaga ett beslut att inte vidta åtgärder.

Allmänna bestämmelser som gäller för svenska myndigheter i deras ärendehandläggning finns i regeringsformen, förvaltningslagen, och offentlighets- och sekretesslagen. I förvaltningslagen finns bl.a. krav på att tillhandhålla service, på skyndsam handläggning och på information om beslut som myndigheten fattat. Många av bestämmelserna i förvaltningslagen bygger på att det finns en part i ärendet. Den som lämnar in ett klagomål enligt dataförord-

ningen kan emellertid inte enligt vår bedömning nödvändigtvis anses vara part i ärendet i förvaltningslagens mening eftersom eventuella åtgärder som kan vidtas av den behöriga myndigheten inte riktar sig mot den som lämnat in klagomålet. De riktar sig mot den som klagomålet avser. Det finns därför anledning att undersöka i vilken utsträckning som dataförordningens krav på information och beslutsunderrättelse till den som har lämnat in klagomålet föranleder behov av författningsändringar.

4.10.2 Regleringen i förvaltningslagen

Partsbegreppet i förvaltningsrätten

Ett av förvaltningslagens övergripande syften är att den ska värna enskildas rättssäkerhet. Av central betydelse för att uppnå detta syfte är att en part i ett ärende i princip ges tillgång till allt material som ligger till grund för beslutet i ärendet. En sådan rätt till insyn har sedan länge tillämpats inom svensk förvaltningsrätt och har även erkänts av EU-domstolen som en allmän EU-rättslig princip. Principen om partsinsyn har av Högsta förvaltningsdomstolen ansetts så central att den utgör en allmän rättsgrundsats, som i princip gäller oberoende av särskilt författningsstöd. Rätt till partsinsyn har ansetts föreligga även i ärenden som enligt 32 § tidigare gällande förvaltningslag faller utanför lagens tillämpningsområde och då 16 § tidigare gällande förvaltningslag alltså inte varit tillämplig (RÅ 1994 ref. 79 och RÅ 2001 ref. 27).

Varken tidigare eller nu gällande förvaltningslag innehåller någon särskild eller närmare definition av vad som avses med uttrycket part. I tidigare gällande förvaltningslag angavs att rätten till t.ex. partsinsyn (16 §), att lämna uppgifter muntligt (14 §), att bli kommunicerad (17 §) och att bli underrättad om beslut (21 §) avsåg den som var sökande, klagande eller annan part. Med sökande avses den som hos en myndighet ansöker om en åtgärd som är reglerad i den offentligrättsliga lagstiftningen. En klagande är den som överklagar ett förvaltningsbeslut. Det kan vara en sökande som fått avslag på sin framställning eller någon som drabbats av ett ingripande och vill att beslutet ska upphävas eller ändras. Uttrycket annan part inbegriper bl.a. den som är föremål för ett tillsynsärende och därmed intar ställning som s.k. förklarande part. Den som i någon annan egenskap har ett intresse

i saken anses normalt inte som part i första instans. Skulle dennes intresse i saken vara av sådan art att han eller hon tillerkänns klagorätt kan personen i fråga bli part i högre instans. Intressenten uppträder då som klagande i det ärende som inleds genom överklagandet. Däremot har den som tar ett initiativ till ett ärende genom en anmälan utan att ha någon närmare anknytning till ärendet normalt inte ställning som part (prop. 2016/17:180 s. 79).

I samband med införandet av nu gällande förvaltningslag gjorde regeringen bedömningen att den tolkning av partsbegreppet som gjorts i praxis visar att avsaknaden av en legaldefinition inte medför någon risk för att rättssäkerheten eftersätts, med hänvisning till bl.a. SOU 2010:29 s. 246–247 med de hänvisningar som görs där. Regeringen uttalade vidare att ett försök att i förvaltningslagen närmare reglera vem som ska anses som part tvärtom skulle kunna utgöra ett hinder för en generös tillämpning av allmänna regler om partsinsyn och kommunikation m.m. i situationer som inte direkt förutsetts av lagstiftaren samt att frågan om vem som ska anses som part i en viss typ av ärenden vid behov regleras i speciallagstiftningen. Regeringen slutsats var mot denna bakgrund att partsbegreppet kan och bör användas i förvaltningslagen på samma sätt som tidigare utan att det i lagtexten ges en mera exakt definition. Liksom hittills bör det alltså överlämnas till rättstillämpningen att utveckla närmare praxis kring detta. Avslutningsvis konstaterade regeringen att uttrycket part med fördel användas som samlande beteckning för det som i den nuvarande lagen anges som sökande, klagande eller annan part (prop. 2016/17:180 s. 79 f.).

Information om handläggning av ett ärende

Förvaltningslagen innehåller en bestämmelse om myndigheters serviceskyldighet, som gäller gentemot alla och envar. Bestämmelsen finns i 6 § förvaltningslagen, där det framgår att en myndighet ska se till att kontakterna med enskilda blir smidiga och enkla. Myndigheten ska lämna den enskilde sådan hjälp att han eller hon kan ta till vara sina intressen. Hjälpen ska ges i den utsträckning som är lämplig med hänsyn till frågans art, den enskildes behov av hjälp och myndighetens verksamhet. Den ska ges utan onödigt dröjsmål.

Utöver den allmänna serviceskyldigheten innehåller förvaltningslagen en rätt till partsinsyn. I 10 § förvaltningslagen framgår följaktligen att den som är part i ett ärende har rätt att ta del av allt material som har tillförts ärendet. Rätten att ta del av uppgifter gäller med de begränsningar som följer av 10 kap. 3 § offentlighets- och sekretesslagen.

I 11 § förvaltningslagen regleras situationer då ärendehandläggningen försenas. Där framgår att om en myndighet bedömer att avgörandet i ett ärende som har inletts av en enskild part kommer att bli väsentligt försenat, ska myndigheten underrätta parten om detta. I en sådan underrättelse ska myndigheten redovisa anledningen till förseningen. Skyldigheten gäller gentemot den som är part.

Förvaltningslagens bestämmelse om beslutsunderrättelse

I 33 § första stycket förvaltningslagen anges att en myndighet som meddelar ett beslut i ett ärende så snart som möjligt ska underrätta den som är part om det fullständiga innehållet i beslutet, om det inte är uppenbart obehövligt. I andra stycket samma paragraf anges bl.a. att om parten får överklaga beslutet ska han eller hon även underrättas om hur det går till. En underrättelse om hur man överklagar ska innehålla information om vilka krav som ställs på överklagandets form och innehåll och vad som gäller i fråga om ingivande och överklagandetid. Av tredje stycket framgår att myndigheten bestämmer hur underrättelsen ska ske. En underrättelse ska dock alltid vara skriftlig om en part begär det. Underrättelse får ske genom delgivning.

Förvaltningslagens bestämmelse om beslutsunderrättelse och fullföljdshänvisning är begränsad till att gälla gentemot den som är part i ärendet. Myndigheterna ska enligt paragrafen, oberoende av begäran, underrätta parter om innehållet i myndighetens beslut. Genom underrättelsen får parten möjlighet att inrätta sitt handlande efter beslutet. Ofta börjar överklagandetiden löpa i samband med underrättelsen och underrättelsen är därför också ofta en förutsättning för att överklagandetiden ska börja löpa. Fullföljdshänvisningen säkerställer att enskilda får den vägledning som de behöver för att kunna utnyttja sin rätt att överklaga.

Av 34 § förvaltningslagen framgår att bestämmelserna i 33 § samma lag om underrättelse om innehållet i beslut och hur ett överklagande

går till tillämpas också om någon som inte är part begär att få ta del av ett beslut som han eller hon får överklaga. Det finns inte, jämfört med vad som gäller enligt 33 § förvaltningslagen, någon skyldighet för myndigheten att på eget initiativ lämna underrättelse enligt 34 § förvaltningslagen, utan enbart att lämna sådan information på någons begäran.

4.10.3 Den som gett in ett klagomål ska underrättas om den behöriga myndighetens beslut

Förslag: Det ska i kompletteringslagen anges att 33 § förvaltningslagen ska gälla i förhållande till den som gett in ett klagomål till den behöriga myndigheten.

Bedömning: Skyldigheten att underrätta den som gett in ett klagomål om hur ärendet fortskrider tillgodoses genom den behöriga myndighetens serviceskyldighet och genom den behöriga myndighetens uppgift att regelbundet informera de klagande om hur utredningen fortskrider och om resultatet av den.

Information om hur ärendet fortskrider

Vi har i avsnitt 4.6.2 ovan bedömt att det bör anges i kompletteringsförordningen att den behöriga myndigheten ska informera den som lämnat in ett klagomål bl.a. om hur ärendet fortskrider.

Av 6 § förvaltningslagen följer som vi redogjort för ovan att myndigheter ska lämna enskilda sådan hjälp att han eller hon kan ta till vara sina intressen. I detta ingår att svara på frågor om hur handläggningen av ett ärende fortlöper.

Ett alternativ skulle vara att införa en bestämmelse i kompletteringslagen med innebörden att rätten till partsinsyn ska gälla även för den som gett in ett klagomål enligt dataförordningen till den behöriga myndigheten. Det finns enligt vår mening två skäl som talar emot detta. För det första ger 10 § förvaltningslagen en rätt till insyn, men inte någon skyldighet för myndigheten att proaktivt underrätta den som gett in klagomålet om hur ärendet fortskrider. För det andra ställer inte dataförordningen krav på att den som gett

in klagomålet ska ha sådan insyn i ärendet som den som är part i ett ärende normalt har. Vi bedömer därför att det saknas skäl att utsträcka rätten till partsinsyn till att även omfatta den som gett in enligt klagomål enligt dataförordningen.

Det finns också en möjlighet att ålägga den behöriga myndigheten en skyldighet att underrätta den som gett in ett klagomål om förseningar i handläggningen enligt 11 § förvaltningslagen. Vi bedömer dock att serviceskyldigheten sammantaget med den bestämmelse som vi föreslår i kompletteringsförordningen om att den behöriga myndigheten ska ha i uppgift att regelbundet informera den som gett in ett klagomål om hur utredningen fortskrider och om resultatet av den är tillräckligt för att svara mot kravet i artikel 38.2 på information om hur förfarandet fortskrider.

Beslutsunderrättelse

Av artikel 38.2 i dataförordningen framgår att den behöriga myndighet i enlighet med nationell rätt ska underrätta klaganden beslut som fattats.

Som framgått ovan så gäller 33 § förvaltningslagen enbart i förhållande till den som är part i ärendet. Även någon annan än den som är part i ärendet kan efter egen begäran enligt 34 § förvaltningslagen få ta del av ett beslut som han eller hon får överklaga. Vi har ovan föreslagit att det ska föras in en bestämmelse i kompletteringslagen om att en behörig myndighets beslut att inte vidta åtgärder med avseende på ett klagomål får överklagas. Den som gett in ett klagomål kommer med andra ord ha rätt att ta del av beslutet i ärendet med stöd av 34 § förvaltningslagen. Det föreligger dock ingen skyldighet för den behöriga myndigheten att på eget initiativ underrätta den som gett in klagomålet i ärendet om att beslut har fattats och hur beslutet kan överklagas. Det är enligt vår uppfattning inte en tillfredsställande ordning. Som framgår ovan så är det en förutsättning för att den som har rätt att överklaga ett beslut ska kunna bruka sin klagorätt, att denne underrättas om beslutet tillsammans med en fullföljdshänvisning. Vi föreslår därför att det kompletteringslagen förs in en bestämmelse om att 33 § förvaltningslagen ska gälla i förhållande till den som gett in ett klagomål till den behöriga myndigheten.

5 Sanktioner för att säkerställa efterlevnad av EU:s dataförordning

5.1 Inledning

Medlemsstaterna ska enligt artikel 40 i dataförordningen fastställa regler om sanktioner för överträdelser av bestämmelserna i förordningen och vidta alla nödvändiga åtgärder för att säkerställa att de tillämpas. Sanktionerna ska vara effektiva, proportionella och avskräckande. Enligt skäl 109 kan sanktioner bl.a. inkludera ekonomiska sanktioner, varningar, reprimander eller förelägganden om att affärsmodeller ska uppfylla de skyldigheter som föreskrivs i förordningen. I artikel 37.5 d anges att ekonomiska sanktioner kan inbegripa viten och sanktioner med retroaktiv verkan, eller möjligheten för en behörig myndighet att inleda rättsliga förfaranden för åläggande av böter. I övrigt innehåller förordningen inte några särskilda bestämmelser om sanktioner.

I skäl 109 anges även att medlemsstaterna vid åläggande av sanktioner ska ta hänsyn till rekommendationerna från Europeiska datainnovationsstyrelsen (EDIB) och på så sätt bidra till att största möjliga enhetlighet uppnås vid fastställandet och tillämpningen av sanktioner. I dagsläget finns det inte några sådana rekommendationer som kan beaktas inom ramen för vårt uppdrag att föreslå vilka regler om sanktioner som bör fastställas i Sverige.

Vilka sanktioner som kan bli aktuella är det alltså upp till medlemsstaterna att besluta om. Vi ska därför analysera vilka sanktioner som behövs och är lämpliga i Sverige för att uppfylla kravet på medlemsstaterna att fastställa regler om sanktioner vid överträdelser av förordningen och lämna nödvändiga författningsförslag.

Bestämmelser om sanktioner utgör myndighetsutövning mot enskild och ska anges i kompletteringslagen (se kapitel 4).

5.2 Utgångspunkter för sanktioner vid tillsyn

Det finns ingen legaldefinition av begreppet sanktion. En sanktion ska ha ett handlingsdirigerande eller bestraffande syfte. Sanktioner kan sägas omfatta alla former av påföljder som kan följa på ett rättsstridigt handlande. De sanktionsverktyg som används i den svenska rättsordningen är straff och sanktionsavgift samt vite, förbud och återkallelse av tillstånd. Straffrättsliga sanktioner, t.ex. böter, förutsätter att ett agerande är kriminaliserat. Administrativa sanktioner utgör inte straff även om de riktas mot en konstaterad överträdelse av en författningsbestämmelse. Viten har en framåtsyftande funktion. I Sverige finns inte något samlat regelverk om åläggande av sanktioner vid tillsyn. I stället finns regler om sanktioner i olika lagar som gäller för det specifika sakområdet. Sanktionerna kan skilja sig åt väsentligt.

I regeringens skrivelse En tydlig, rättssäker och effektiv tillsyn redogör regeringen för viktiga utgångspunkter vad gäller sanktioner vid tillsyn. I skrivelsen anges bl.a. följande. Sanktioner vid tillsyn bör vara proportionella i förhållande till de konstaterade bristerna och de olika möjligheterna till sanktioner som är tillgängliga för ett tillsynsorgan bör därför kunna användas vid såväl mindre som mer allvarliga brister i en verksamhet. Ingripandena kan då anpassas till den enskilda situationen. Ingripanden vid tillsyn har inte enbart ett bestraffande syfte. De ska även ha en framåtsyftande funktion och tillse att regler följs i framtiden. Samtidigt är det viktigt att tillsynsorganen kan ingripa mot regelöverträdelser där överträdelsen inte går att göra ogjord. Vid utformning av ingripandemöjligheterna vid tillsyn bör vidare behovet av att skapa större enhetlighet beaktas, särskilt inom närliggande tillsynsområden. Större enhetlighet gör det enklare för medborgare, tillsynsobjekt och tillsynsorgan att förstå innebörden av ett ingripande. Det skapar även bättre förutsättningar för samverkan mellan olika tillsynsorgan. När samma organisation utövar tillsyn enligt flera regelverk ökar möjligheterna att inom organisationen samordna tillsynen (skr. 2009/10:79 s. 41 f.).

Regeringens skrivelse tillkom för närmare sjutton år sedan och tar sikte på tillsyn av efterlevnad av i första hand nationella regler.

EU-rätten har sedan tillkomsten av skrivelsen utvecklats mot att ha ett större inflytande på den svenska rättsordningen. Vårt uppdrag är analysera vilka sanktioner som behövs för att uppfylla kravet på sanktioner vid överträdelse av dataförordningen, och lämna nödvändiga författningsförslag. Att det är fråga om en förordning som är direkt tillämplig sätter vissa ramar för vilka författningsändringar som vi kan och bör föreslå. Vi bedömer att de principer som beskrivs i regeringens skrivelse som allmän utgångspunkt är relevanta för vårt uppdrag att föreslå sanktioner för överträdelser av dataförordningen. Vi har därför beaktat dessa principer.

5.3 Överträdelser av bestämmelser i dataförordningen ska inte vara straffsanktionerade

Bedömning: Överträdelser av bestämmelser i dataförordningen ska inte vara straffsanktionerade.

Rättsliga åtgärder för åläggande av böter nämns i dataförordningen som ett exempel på sanktion som medlemsstaterna kan besluta om. Böter är i Sverige en straffrättslig sanktion för en kriminaliserad gärning. Kriminalisering som metod för att försöka hindra överträdelser av olika normer i samhället bör användas med försiktighet. Ett skäl till detta är att en alltför omfattande kriminalisering riskerar att undergräva straffsystemets brottsavhållande verkan, särskilt om rättsväsendet inte kan beivra alla brott på ett effektivt sätt. Ett annat skäl är att kriminalisering innebär påtagliga inskränkningar i medborgarnas valfrihet och ingripande tvångsåtgärder mot dem som begår brott. När det gäller överträdelser av reglerna i dataförordningen utgör straff inte en effektiv sanktion, eftersom det inte är relevant att identifiera en fysisk person som ansvarig för överträdelsen samt bevisa att denne haft uppsåt eller varit oaktsam på det sätt som krävs för straffbarhet. Vi bedömer att ekonomiska sanktioner som kan drabba företag eller organisationer som inte följer dataförordningen bör ha en tillräckligt avskräckande effekt och leda till att efterlevnaden av regelverket prioriteras högt.

Enligt vår uppfattning ska överträdelser av EU:s dataförordning inte vara kriminaliserade i Sverige.

5.4 Förelägganden och vite med anledning av bristande efterlevnad av förordningen ska kunna meddelas

5.4.1 Behöriga myndigheter ska kunna meddela de förelägganden som behövs

Förslag: Behöriga myndigheter ska kunna meddela de förelägganden som behövs för att EU:s dataförordning, kompletteringslagen eller föreskrifter som har meddelats i anslutning till lagen ska följas.

Det följer av artikel 40 i dataförordningen att en behörig myndighet ska ha befogenhet att besluta om sanktioner. Som exempel på sanktion som medlemsstaterna kan införa anges i skäl 109 förelägganden om att affärsmetoder ska uppfylla de skyldigheter som föreskrivs i dataförordningen.

Dataförordningen innehåller bestämmelser om skyldigheter för olika aktörer som innebär att de måste agera på ett visst sätt. Den behöriga myndigheten bör i enskilda fall ha möjlighet besluta om åtgärdsförelägganden för att kunna säkra efterlevnaden av bestämmelserna i dataförordningen. I allmänhet bör möjligheten att utforma förelägganden för att kunna styra beteendet hos tillsynsobjektet vara vitt och i princip ansluta till tillsynens omfattning (skr. 2009/10:79 s. 44).

I artikel 4.9 och 5.12 anges att användare respektive tredje part som vill bestrida en datahållares beslut att vägra, hindra eller avbryta datadelning får lämna in ett klagomål till den behöriga myndigheten, som då utan oskäligt dröjsmål ska fatta beslut om och på vilka villkor datadelning ska inledas eller återupptas. Sådana beslut bör kunna meddelas i form av förelägganden. Möjligheten bör dock inte begränsas till att omfatta särskilda bestämmelser eller skyldigheter, utan den behöriga myndigheten bör få besluta om de förelägganden som behövs för att säkerställa och främja efterlevnaden av förordningen och kompletteringslagen och eventuella föreskrifter inom ramen för sitt tillsynsuppdrag. Detta inbegriper åtgärder som behövs för att uppfylla skyldigheterna i dataförordningen. Det kan vara fråga om förbud att agera på ett visst sätt eller ett föreläggande om att agera på

ett visst sätt. Detta innefattar även skyldigheten att efterkomma en begäran om att inkomma med upplysningar och handlingar.

Det bör därför införas en bestämmelse i kompletteringslagen om att den behöriga myndigheten får utfärda de förelägganden som behövs för att säkerställa efterlevnaden av dataförordningen.

5.4.2 Förelägganden ska kunna förenas med vite

Förslag: Behöriga myndigheter ska kunna förena förelägganden med vite.

Viten anges som exempel på en ekonomisk sanktion som enligt artikel 37.5 d i dataförordningen kan åläggas för överträdelser av förordningen. Förordningen begränsar inte möjligheterna att ålägga ekonomisk sanktion till vissa typer av överträdelser. Möjligheten att förena ett föreläggande med vite ger den behöriga myndigheten ytterligare verktyg för att säkerställa efterlevnad av förordningen.

Att ha möjlighet att hämta in uppgifter från tillsynsobjektet eller en annan aktör är ett viktigt utredningsredskap i all slags tillsynsverksamhet. De inhämtade uppgifterna ingår i, och utgör ofta en viktig del av, underlaget för myndighetens granskning och beslut. Ett föreläggande om att inkomma med upplysningar och handlingar bör därför kunna förenas med vite. Regeringen har även uttryckt att ett föreläggande om att vidta en viss åtgärd eller att upphöra att en viss åtgärd i regel bör kunna förenas med vite (skr. 2009/10:79 s. 44). Vi bedömer mot denna bakgrund att det är viktigt att den behöriga myndigheten ges möjlighet att förena förelägganden med vite.

Dubbelprövningsförbudet kan aktualiseras när vite utdöms för ageranden som också kan leda till sanktionsavgift. Frågan behandlas i avsnitt 5.5.6.

Det saknas skäl till att kunna meddela vitesföreläggande mot staten

Myndigheter och andra offentliga organ kan komma att bli föremål för förelägganden vid överträdelser av dataförordningen. Ett vitesföreläggande kan som huvudregel inte riktas mot staten. Frågan om vite mot staten är inte reglerad i lagen (1985:206) om viten (viteslagen). I förarbetena till viteslagen överlämnas frågan om ett vitesföreläggande ska kunna riktas mot staten till rättstillämpningen. Dock anges att sådana viten bör komma i fråga främst i situationer där staten i så utpräglad grad uppträder som privaträttsligt subjekt, t.ex. på det marknadsrättsliga området, att det skulle vara onaturligt om vitesmöjligheten inte stod till buds. Vidare uttalas att det utanför det marknadsrättsliga området bör krävas att ett helt speciellt undantagsfall är för handen för att ett vitesföreläggande mot en statlig aktör ska vara godtagbart (se prop. 1984/85:96 s. 99 f.). Så kan det vara när staten, i situationer när ett vitesföreläggande skulle kunna vara aktuellt, agerar utanför sin rent offentligrättsliga kapacitet (se exempelvis prop. 2020/21:194 s. 66 och 67). Det antas generellt att en statlig myndighet i de flesta fall kommer att följa den behöriga myndighetens uppmaning på frivillig väg och att förelägganden därför endast undantagsvis behöver förenas med vite.

Myndigheter och andra offentliga organ har skyldigheter enligt dataförordningen och kan därmed komma att bli föremål för förelägganden, särskilt när de tar emot och behandlar data enligt kapitel V i dataförordningen. De kommer då att agera inom ramen för sin offentligrättsliga kapacitet. De kan dock omfattas av kapitel II som användare, i en avtalsförbindelse, och omfattas av kapitel III och IV om de agerar i egenskap av företag. De handlar då inte i sin offentligrättsliga kapacitet. Vi bedömer emellertid att staten sällan kommer att agera i egenskap av företag, dvs. i privaträttslig kapacitet, och därmed omfattas av dessa kapitel. Som redan nämnts bör en statlig aktör i regel efterkomma ett föreläggande även utan hot om vite. Sammantaget anser vi därför att det inte finns tillräckliga skäl för att den behöriga myndigheten ska kunna förena ett föreläggande mot staten med vite.

5.4.3 Vitets storlek och förfarandebestämmelser

Bedömning: Bestämmelser om vitets storlek och förfarandebestämmelser angående vite bör inte införas i kompletteringslagen.

Dataförordningen innehåller inte någon bestämmelse om vitets storlek (så som t.ex. är fallet i EU:s förordning om digitala tjänster[1]). Det är därmed upp till medlemsstaterna att bestämma hur ett vite ska beräknas och fastställas.

Viten som enligt lag eller annan författning får föreläggas av myndigheter regleras i Sverige i viteslagen. Hur vite ska fastställas föreskrivs i 3 § och 4 §. Förfaranderegler vad avser förelägganden av viten finns i viteslagen, förvaltningslagen (2017:900) och förvaltningsprocesslagen (1971:291). Vår bedömning är att det finns ett tillräckligt rättsligt ramverk för fastställande av vite och att det av den anledningen inte behövs några sådana bestämmelser i kompletteringslagen.

5.4.4 Interimistiska förelägganden

Förslag: Om det finns särskilda skäl får behöriga myndigheter besluta om förelägganden för tiden till dess saken slutligt har avgjorts.

I skäl 109 i dataförordningen, som handlar om att medlemsstaterna ska säkerställa att överträdelser av förordningen ska vara föremål för sanktioner som är ändamålsenliga, proportionella och avskräckande, uttalas att behöriga myndigheter när det är lämpligt bör använda sig av interimistiska åtgärder för att begränsa effekterna av en påstådd överträdelse medan utredningen av överträdelsen pågår. När de gör detta bör de beakta bl.a. överträdelsens art, allvar, omfattning och varaktighet med tanke på det allmänintresse som står på spel, omfattningen och typen av verksamhet som bedrivs samt överträdarens ekonomiska kapacitet. Det anges dock inte särskilt i artikel 37.5 att de behöriga myndigheterna ska ha denna befogenhet.

[1] Europaparlamentets och rådets förordning (EU) 2022/2065 av den 19 oktober 2022 om en inre marknad för digitala tjänster och om ändring av direktiv 2000/31/EG (förordningen om digitala tjänster).

Myndigheter som utses till behöriga myndigheter enligt dataförordningen ska kunna besluta om förelägganden (avsnitt 5.4.1). Förelägganden kan innefatta ett förbud att fortsätta att vidta åtgärder som utgör en överträdelse eller påbjuda att tillsynsobjektet ska ändra sitt agerande på ett visst sätt. Med hänsyn till vad som uttalas i skäl 109 och till att enskilda ageranden som står i strid med dataförordningen kan leda till allvarliga och oåterkalleliga skador bedömer vi att den behöriga myndigheten bör kunna besluta om sådana förelägganden med intermistisk verkan. Eftersom den behöriga myndigheten har mest information om det ärende som den utreder är det mest ändamålsenligt att myndigheten själv fattar beslut om interimistiska åtgärder. Brådskan vid fara för allvarlig skada talar också för att beslutet ska kunna fattas av den behöriga myndigheten i stället för av domstol. Det bör krävas särskilt starka skäl för ett sådant beslut. Normalt bör det handla det om att ett agerande som tydligt står i strid med dataförordningen och som riskerar att leda till väsentliga och oåterkalleliga skador för en enskild eller det allmänna. Att interimistiska åtgärder ska vara proportionerliga framgår av den allmänna proportionalitetsbestämmelsen i 5 § förvaltningslagen. Interimistiska förelägganden bör gälla omedelbart, om inget annat anges. Med andra ord gäller de tills ett slutligt och lagakraftvunnet beslut föreligger. Domstol kan efter överklagande inhibera ett interimistiskt beslut.

Förvaltningslagen innehåller inte någon bestämmelse som reglerar att, eller när, en myndighet får fatta intermistiska beslut under utredningens gång. För att tillsynsmyndigheter ska kunna fatta interimistiska beslut bör detta anges särskilt i lag. Vi föreslår därför att det införs en bestämmelse i kompletteringslagen om att behöriga myndigheter, om det finns särskilda skäl, får besluta om förelägganden för tiden till dess att frågan slutligt har avgjorts. Även sådana förelägganden ska kunna förenas med vite.

5.5 Sanktionsavgift och anmärkning ska kunna åläggas vid överträdelser av dataförordningen

5.5.1 Sanktionsavgift ska åläggas vid överträdelser av dataförordningen

Förslag: En behörig myndighet ska besluta att ta ut sanktionsavgift vid överträdelser av dataförordningen.

Val av ekonomisk sanktion

Enligt artikel 37.4 c i dataförordningen ska de behöriga myndigheterna ha befogenhet att ålägga ekonomiska sanktioner som kan inbegripa sanktioner med retroaktiv verkan och viten. Vi bedömer att medlemsstaterna har möjlighet att välja den form av ekonomisk sanktion som passar in i det nationella processuella systemet. I Sverige används administrativa sanktionsavgifter som påföljd för överträdelser av författningsbestämmelser som inte ingår i det straffrättsliga systemet. Enligt vår uppfattning är det är denna typ av ekonomisk sanktion som bör kunna åläggas, förutsatt att bestämmelserna uppfyller vissa kriterier som bör vara uppfyllda för att en överträdelse av en bestämmelse enligt svensk rätt ska kunna leda till sanktionsavgift, se vidare avsnitt 5.6.1. Vi föreslår därför att sanktionsavgift ska kunna komma i fråga för överträdelser av dataförordningen.

Vilka bestämmelser i dataförordningen om enligt vår bedömning ska kunna läggas till grund för sanktionsavgift när de överträds behandlar vi i avsnitt 5.6.3.

Behörig myndighet ska besluta om sanktionsavgift

Beslut om sanktionsavgift fattas som huvudregel av en tillsynsmyndighet eller av en domstol på ansökan av en tillsynsmyndighet. En domstol brukar anses vara mer lämpad att besluta om sanktionsavgift om det är aktuellt att pröva subjektiva rekvisit eller andra svårbedömda rekvisit. Generellt sett anses en tillsynsmyndighet lämpad att besluta om sanktionsavgift när reglerna är relativt enkla att tillämpa, beslutsfattandet är förhållandevis schabloniserat och sanktionsbestämmelserna bygger på strikt ansvar. En fördel med att tillsynsmyndig-

heten fattar beslut är att handläggningen kan bli snabbare eftersom inte flera myndigheter måste delta i hanteringen.

Den myndighet som har ansvar för att säkerställa efterlevnad av dataförordningen och som har utrett ärendet är enligt vår bedömning väl lämpad att själv fatta beslut om sanktionsavgift. Det är den behöriga myndigheten, PTS, som i första hand kommer att få kännedom om överträdelser av bestämmelserna, som också har bäst förutsättningar att utreda och bedöma om någon inte har följt det gällande regelverket. Det noteras även att PTS har befogenhet att besluta om sanktionsavgift enligt t.ex. 12 kap. lagen (2022:482) om elektronisk kommunikation (LEK) och 29 § lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-lagen). Vi föreslår därför att den behöriga myndigheten ska kunna besluta om sanktionsavgift.

Det ska i kompletteringslagen anges att sanktionsavgift ska tas ut vid överträdelser

Bestämmelsen om sanktionsavgift i kompletteringslagen skulle kunna föreskriva att behöriga myndigheter *får* besluta om sanktionsavgift för överträdelserna av dataförordningen. Det skulle indikera att de behöriga myndigheterna har utrymme att beakta enskilda omständigheter inklusive stor möjlighet att välja på vilket sätt den bör ingripa i det enskilda fallet. Samtidigt skulle en sådan formulering kunna ge sken av att det endast är fråga om en regel om befogenhet för behöriga myndigheter att besluta om en sanktionsavgift, och inte information om att en avgift enligt bestämmelsen faktisk bör tas om det inte finns skäl för en annan bedömning. I exempelvis propositionerna till lagarna som kompletterar förordningen om digitala tjänster respektive dataförvaltningsförordningen[2] föreslog regeringen, till skillnad mot utredningarna, att det i kompletteringslagen ska anges att sanktionsavgift *ska* tas ut vid överträdelser av de aktuella bestämmelserna i förordningarna (prop. 2023/24:160 s. 72 ff. respektive prop. 2023/24:73 s. 41 ff.). Att sanktionsavgift inte alltid ska beslutas anges i stället särskilt i en bestämmelse som föreskriver att och när den behöriga myndigheten helt eller delvis kan avstå från att ta ut sanktionsavgiften.

[2] Europaparlamentets och rådets förordning (EU) 2022/868 av den 30 maj 2022 om europeisk dataförvaltning och om ändring av förordning (EU) 2018/1724 (dataförvaltningsakten).

Vi bedömer att det å ena sidan kan framstå som ologiskt att ange att sanktionsavgift ska tas ut, samtidigt som det inte alltid ska ske. Å andra sidan skulle formuleringen att sanktionsavgift får tas ut kunna uppfattas som otydlig. Med den senare formuleringen skulle en bestämmelse i lagen som särskilt anger under vilka omständigheter den behöriga myndigheten får avstå ifrån att ta ut en sanktionsavgift vara överflödig. En sådan bestämmelse bidrar dock just till tydlighet vad avser enskilda fall när en sanktionsavgift kan sättas ned eller efterges, varför vi föreslår en sådan bestämmelse (se avsnitt 5.5.5). Att föreskriva att behöriga myndigheter ska besluta om sanktionsavgift stämmer även bättre överens med kravet i dataförordningen på att behöriga myndigheter ska ålägga effektiva och avskräckande ekonomiska sanktioner.

Vi föreslår därför att komplettringslagen bör utformas så att sanktionsavgift ska tas ut vid överträdelser.

Sanktionsavgift ska kunna beslutas för offentliga organ

Som redovisas i avsnitt 5.6.3 gör vi bedömningen att vissa skyldigheter för offentliga organ enligt artikel 19 i dataförordningen är av sådan art att sanktionsavgift ska kunna tas ut vid överträdelser. Skyldigheterna, som handlar om hur data som begärts in vid exceptionella behov ska hanteras, åligger bara offentliga organ i just den egenskapen. Därutöver kan offentliga organ göra sig skyldiga till överträdelser när de agerar på marknaden, särskilt i egenskap av användare.

Till skillnad från dataskyddsförordningen[3] (artikel 83.7) och AI-förordningen[4] (artikel 99.8) innehåller dataförordningen inte någon artikel som överlämnar till medlemsstaterna att fastställa bestämmelser om i vilken utsträckning en administrativ sanktionsavgift får påföras offentliga myndigheter och organ som är inrättade i medlemsstaten.

Mot denna bakgrund bedömer vi att sanktionsavgift ska kunna åläggas mot offentliga myndigheter och organ.

[3] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).
[4] Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens).

5.5.2 Sanktion i form av anmärkning kan vara tillräcklig

Förslag: Om det kan anses tillräckligt får behöriga myndigheter i stället för att besluta att ta ut en sanktionsavgift meddela en anmärkning.

Det är ofta ändamålsenligt att tillsynsorgan har författningsreglerade möjligheter till ingripanden vid mindre allvarliga överträdelser. Om det saknas möjlighet till mildare ingripanden kan detta leda till att inget ingripande sker trots en konstaterad brist, eftersom den som utövar tillsynen inte vill vidta en alltför ingripande åtgärd (skr. 2009/10:79 s. 43). Vidare kan det finnas skäl att besluta om en sanktion när en konstaterad överträdelse har upphört men det av olika skäl inte anses påkallat att besluta om sanktionsavgift, t.ex. om en aktör frivilligt vidtagit rättelse.

I skäl 109 i dataförordningen nämns varningar och reprimander som exempel på sanktioner som medlemsstaterna kan bestämma om. Sådana sanktioner är mindre ingripande än sanktionsavgifter. I Sverige används i olika författningar varning, erinran eller anmärkning som ingripande mot pågående eller avslutade överträdelser. Av dataskyddsförordningen (artikel 58.2 b) följer att tillsynsmyndigheten i vissa fall får utfärda en reprimand. Begreppet reprimand används dock enligt vår uppfattning inte i svenska författningar.

Varning reserveras vanligtvis för mer klandervärda ageranden som, om de upprepas, kan leda till återkallelse av ett tillstånd eller avregistrering (se t.ex. prop. 2010/11:15 s. 40 och Högsta förvaltningsdomstolens avgöranden i HFD 2016 ref. 2 I och II). Varning kan t.ex. utfärdas enligt lagen (2024:500) med kompletterande bestämmelser till EU:s dataförvaltningsförordning, bl.a. i situationer som kan leda till avregistrering. En erinran ses ofta som en mildare påföljd än en varning. Erinran förekommer i flera författningar så som fastighetsmäklarlagen (2021:516) och alkohollagen (2010:1622). I dessa författningar används erinran tillsammans med varning som ett förstahandsalternativ till påföljderna avregistrering respektive återkallelse av tillstånd.

Ett annat ingripande i svensk rätt är anmärkning. Anmärkning som ingripande är avsett att användas vid mindre allvarliga överträdelser (jfr skr. 2009/10:79 s. 43). Exempelvis har regeringen nyligen i propositionen till en ny cybersäkerhetslag föreslagit att en anmärk-

ning kan meddelas vid överträdelser om tillsynsmyndigheten inte finner skäl att ingripa på något annat sätt (prop. 2025/26:28).

Överträdelser av dataförordningen kan vara mer eller mindre allvarliga och det kan i det enskilda fallet föreligga omständigheter som gör att en sanktionsavgift inte anses proportionell. Om myndigheter endast får besluta om sanktionsavgift mot överträdelser finns det en risk för att de avstår från att ingripa vid överträdelser av dataförordningen som är mindre allvarliga. För överträdelser som har upphört kan inte heller sanktionen föreläggande användas. Vi bedömer därför att den behöriga myndigheten vid mindre allvarliga överträdelser eller om en överträdelse har upphört ska kunna besluta om en mindre ingripande sanktion än sanktionsavgift. Möjligheten bör finnas vid sådana överträdelser som kan bli föremål för sanktionsavgift. Detta skapar enligt vår bedömning goda förutsättningar för att sanktionssystemet i stort ska vara effektivt, proportionellt och avskräckande. Särskilt varningar används i regel för att ge tillsynsobjektet en möjlighet vidta rättelse av en pågående överträdelse för att undvika en annan sanktion såsom återkallelse av tillstånd. Överträdelser av dataförordningen kan inte leda till sådana konsekvenser. Pågående överträdelser kan även bli föremål för förelägganden. Det är därför inte relevant att använda begreppet varning i kompletteringslagen. Vi bedömer att begreppet anmärkning passar bäst att använda i kompletteringslagen eftersom sanktionen är särskilt avsedd att användas vid mindre allvarliga överträdelser.

Det bör därför anges i kompletteringslagen att en behörig myndighet, om det anses tillräckligt, får meddela anmärkning i stället för att ta ut en sanktionsavgift.

5.5.3 Sanktionsavgiftens storlek

Förslag: En sanktionsavgift ska uppgå till minst 5 000 kronor och högst 20 miljoner kronor.

En sanktionsavgift för en fysisk person som inte bedriver näringsverksamhet ska uppgå till minst 1 000 kronor och högst 10 000 kronor.

EU:s dataförordning innehåller inte några bestämmelser om sanktionsbelopp (till skillnad från bl.a. dataskyddsförordningen, förordningen om digitala tjänster och dataförvaltningsförordningen). Det åligger i stället medlemsstaterna att fastställa ramar för sanktionernas storlek. Vi ska därför föreslå vilket sanktionsbelopp som ska kunna utgå, eller i alla fall ramarna för vilka belopp som kan beslutas.

Sanktionsavgifters nivå är en viktig del av att utforma ett sanktionssystem. Utgångspunkten i dataförordningen är att sanktionerna ska vara effektiva, proportionella och avskräckande. Regeringen har uttalat att sanktionsavgifter bör kunna beräknas utifrån parametrar som gör det möjligt att i förväg förutse och fastställa avgiftens storlek (skr. 2009/2010:79 s. 46). Vi bedömer att det inte är möjligt att vara så precis i kompletteringslagen utan rättstillämpningen bör ges ett utrymme för att väga samman relevanta omständigheter. Det bör dock i komplettringslagen framgå vilka sanktionsbelopp det kan bli fråga om.

Sanktionsavgifter kan vara utformade på olika sätt. I regel handlar det om ett på förhand bestämt beloppsintervall (högsta och lägsta belopp) eller ett maxbelopp som är kopplat till omsättning.

För att bestämma vilka sanktionsbelopp som ska kunna bli aktuella enligt kompletteringslagen måste syftet med dataförordningen beaktas. Sanktionernas preventiva effekt har en viktig roll för att dataförordningen ska få genomslagskraft och bidra till att målen uppnås. Alltför låga sanktionsbelopp skulle inte vara tillräckligt avskräckande vad gäller överträdelser av skyldigheterna och inte heller ge tillräckligt incitament för aktörerna att uppfylla skyldigheterna i förordningen, särskilt inte vad gäller stora företag. Att sanktionsbeloppen ska vara proportionella kräver samtidigt att sanktionerna inte ska vara oproportionellt höga, t.ex. i jämförelse med sanktioner vid likartade överträdelser enligt svensk rätt. Det kommer att finnas skillnader mellan medlemsstaterna när det gäller storleken på sanktionsbelopp

som döms ut, vilket inte är önskvärt utifrån harmoniseringssynpunkt. Detta är dock en konsekvens av att EU-lagstiftaren har lämnat det till medlemsstaterna att bestämma sanktionsbelopp.

Vi har mot denna bakgrund beaktat bestämmelser om sanktionsavgifter i andra närliggande EU-förordningar och svensk lag. Vi redovisar även vilka beloppsgränser som några andra medlemsstater har föreslagit.

Sanktionsavgifter i annan lagstiftning

I EU:s dataskyddsförordning fastställs övre beloppsgränser för två olika kategorier av överträdelser. För mindre allvarliga överträdelser fastslås ett maxbelopp om 10 miljoner euro eller 2 procent av den globala årsomsättningen om det gäller ett företag, beroende på vilket belopp som är högst. För allvarligare överträdelser fastslås ett maxbelopp om 20 miljoner euro eller 4 procent av den globala årsomsättningen, beroende på vilket som är högst. I lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning anges att sanktionsavgifter ska bestämmas med tillämpning av förordningen. För myndigheter ska sanktionsavgiften bestämmas till högst 5 miljoner kronor eller högst 10 miljoner kronor beroende på vilken överträdelse som skett. Vi noterar att sanktionsnivåerna (maxbeloppen) för företag i dataskyddsförordningen är höga ur ett svenskt perspektiv, vilket kan ha att göra med att förordningen syftar till att säkerställa grundläggande rättigheter. För myndigheters del anges i förarbetena till den kompletterande lagen till dataskyddsförordningen att redan relativt sett lägre högsta sanktionsbelopp kan vara tillräckligt avskräckande (jfr prop. 2017/18:105 s. 141).

I förordningen om digitala tjänster fastslås att sanktionsavgiften för leverantörer av förmedlingstjänster ska bestämmas till högst 6 procent av den globala omsättningen. I lagen (2024:954) med kompletterande bestämmelser till EU:s förordning om digitala tjänster anges därför att sanktionsbeloppet ska bestämmas till högst 6 procent av omsättningen, och till lägst 5 000 kronor. Något högsta belopp fastställs alltså inte och sanktionsbeloppet kan bli mycket högt. Vi noterar att förordningen om digitala tjänster delvis syftar till att skapa en säkrare och rättvisare online-miljö för användare genom att hantera olagligt innehåll, öka transparensen och skydda användarnas

rättigheter, dvs. en form av skydd för enskilda bl.a. mot brott och trakasserier.

Dataförvaltningsförordningen innehåller inte någon bestämmelse om sanktionsavgifters storlek. I lagen (2024:500) med kompletterande bestämmelser till EU:s dataförvaltningsförordning anges att sanktionsavgiften ska uppgå till lägst 5 000 kronor och högst 10 miljoner kronor. Intervallet motiverades utifrån att dataförvaltningsförordningen omfattar både mycket små och stora globala företag och att det ger utrymme för effektiva, proportionella och avskräckande sanktioner även vid allvarliga överträdelser.

Konkurrensskadeavgift får enligt konkurrenslagen (2008:579) uppgå till högst 10 procent av det berörda företagets totala globala årsomsättning. Beräkningsgrunden följer direkt av EU-rätten, ursprungligen av förordning (EEG) nr 17/62.[5] Det noteras att överträdelser av konkurrensreglerna kan resultera i stora negativa ekonomiska effekter för konsumenterna och samhället.

Upphandlingsskadeavgift för upphandlande myndigheter eller enheter utgår enligt lagen (2016:1145) om offentlig upphandling, lagen (2016:1146) om upphandling inom försörjningssektorerna och lagen (2016:1147) om koncessioner till ett belopp mellan 10 000 kronor och 20 miljoner kronor. Beloppet får dock inte överstiga 10 procent av upphandlingens värde. Det högsta beloppet höjdes från den 1 januari 2024 från 10 miljoner kronor.[6]

Marknadsstörningsavgift enligt marknadsföringslagen (2008:486) liksom sanktionsavgift enligt lagen (1994:1512) om avtalsvillkor i konsumentförhållanden ska fastställas till lägst 10 000 kronor och högst 4 procent av näringsidkarens omsättning. Om uppgifter om årsomsättning saknas eller är bristfällig får årsomsättningen uppskattas och avgifter får då fastställas till ett belopp i kronor som motsvarar högst 2 miljoner euro. Beloppsnivåerna ändrades 2022 (från ett tidigare beloppstak om 10 miljoner kronor) med anledning av ändringsdirektiv (EU) 2019/2161, i vilket beloppsgränserna fastställs. Regelverken syftar till att skydda konsumenter.

Sanktionsavgift enligt penningtvättslagen (2017:630) kan för verksamhetsutövare som är juridiska personer uppgå till det högsta av

[5] Den ursprungliga tillämpningsförordningen till konkurrensreglerna i EG-fördraget (artiklarna 85 och 86).

[6] Lagen (2023:815), lagen (2023:816) respektive lagen (2023:817) om ändring av lagen (2016:1145) om offentlig upphandling, lagen (2016:1146) om upphandling inom försörjningssektorerna respektive lagen (2016:1147) om koncessioner.

två gånger den vinst som verksamhetsutövaren gjort till följd av överträdelsen, om beloppet går att fastställa, eller ett belopp i kronor motsvarande 1 miljon euro. Sanktionsavgiften får inte bestämmas till ett lägre belopp än 5 000 kronor.

Beloppsintervallet varierar mellan olika rättsområden. På miljöområdet och arbetsmiljöområdet är intervallet 1 000–1 miljon kronor. I lagarna på produktsäkerhetsområdet är intervallet normalt 5 000–5 miljoner kronor. Enligt både LEK (12 kap. 2 §) och NIS-lagen (30 §) är det lägsta sanktionsbeloppet 5 000 kronor och det högsta 10 miljoner kronor.

Vår genomgång av bestämmelser om sanktionsavgifters storlek i svenska lagar visar att tak för sanktionsavgifter bestäms antingen via beloppsintervall eller via en särskild procent av ett företags årsomsättning, i regel 4–6 procent. Sanktionsbelopp som beräknas i relation till omsättning förekommer enligt vår uppfattning främst i lagar som genomför direktiv eller kompletterar förordningar som föreskriver hur sanktionsbelopp ska beräknas. Lägsta möjliga sanktionsbelopp anges ofta, vilket motiveras av att sanktionsbeloppet inte bör vara alltför obetydligt.

Sanktionsavgifter i andra medlemsstater

I andra medlemsstaters förslag till bestämmelser som kompletterar dataförordningen, som vi kunnat ta del av, har olika beloppsgränser angetts.

I Finland föreslås att en sanktionsavgift som åläggs en juridisk person inte får överstiga 4 procent av den årliga omsättningen i EU under föregående räkenskapsår. Om sanktionsavgifter åläggs en fysisk person får böterna inte överstiga 1 000 euro eller 1 procent av personens senaste beskattade inkomst, beroende på vilket belopp som är högst.

I Tyskland föreslås olika beloppsgränser för överträdelser utifrån hur allvarliga de anses vara. För grindvakter får sanktionsavgiften uppgå till högst 5 miljoner euro, eller högst 4 procent av omsättningen i EU under föregående räkenskapsår, beroende på vilket belopp som är högst. För övriga överträdelser får sanktionsavgiften uppgå till högst 500 000 euro, högst 100 000 euro respektive högst 50 000 euro.

I Nederländerna föreslås att sanktionsavgiften ska uppgå till högst 1 030 000 euro eller 10 procent av årsomsättningen i EU, beroende på vilket belopp som är högst.

Vårt förslag

Vi noterar inledningsvis att medlemsstaterna kommer att tillämpa olika sätt att fastställa sanktionsavgifter och olika beloppsstorlekar. Detta kan leda till bristande harmonisering inom EU vad gäller sanktioner. EU har dock valt att inte fastställa regler om sanktioner i dataförordningen utan i stället uppdragit till medlemsstaterna att göra detta utifrån nationella sanktionsregler.

Sanktioner kan vara utformade på olika sätt. De kan avse på förhand bestämda belopp, ett beloppsintervall eller vara kopplade till ett företags årsomsättning. Överträdelser av de bestämmelser som ska kopplas till sanktionsavgiftssystemet kan även vara av mycket varierande art och karaktär. Bestämmelser om sanktioner bör därför utformas så att en sanktionsavgift kan tas ut med ett proportionellt belopp i varje enskilt fall.

Dataförordningen är horisontellt tillämplig och omfattar alltifrån mindre företag till stora globala företag. Även offentliga myndigheter och till och med konsumenter kan enligt förordningen göra sig skyldiga till överträdelser och därför komma i fråga för sanktionsavgift. Vidare föreligger det skillnader vad gäller överträdelsernas art. Överträdelserna kan bedömas som mer eller mindre allvarliga. Vi bedömer att ett system med ett bestämt avgiftsintervall är lämpligast. För att uppfylla kravet på effektiva, proportionella och avskräckande sanktioner bör beloppsintervallet vara förhållandevis stort.

Ett specifikt högsta belopp riskerar att drabba mindre företag mer än stora företag. Sanktionsavgifter som beräknas utifrån företagets omsättning ger den behöriga myndigheten utrymme att beakta såväl företagets storlek som överträdelsens art. Att omsättning inom EU bör beaktas vid fastställande av sanktioner anges även i artikel 40.3 f. När sanktionsavgifter enligt svenska lagar ska beräknas utifrån omsättning fastställs detta dock ofta direkt i en bakomliggande EU-rättsakt. Beräkningssättet ger utrymme för mycket höga sanktionsavgifter som i sig skulle kunna anses oskäliga. Vi bedömer att ett system med

ett bestämt beloppsintervall med ett bestämt lägsta och högsta sanktionsbelopp är lämpligast.

Det kan övervägas att föreskriva en kombination av högsta belopp och omsättningsrelaterat tak. Ett högsta belopp kan vid en sådan utformning syfta till att säkerställa att det maximala beloppet beräknat efter omsättning inte blir oskäligt eller oproportionellt högt (dvs. till skydd för företag med hög omsättning). Det kan även syfta till att säkerställa att det högsta beloppet blir tillräckligt avskräckande även för företag med mycket hög omsättning. Eftersom proportionaliteten kan beaktas inom ramen för ett (tillräckligt stort) beloppsintervall bör det snarare vara den andra situationen som ska säkerställas. I så fall bör sanktionsbeloppet bestämmas till en viss procent av omsättningen, eller till högst ett visst sanktionsbelopp, beroende på vilket belopp som är högst. På så vis blir takbeloppet snarare ett miniminibelopp för mycket stora företag. Vi bedömer dock inte att det är nödvändigt att även föreskriva ett högsta belopp som beräknas utifrån omsättning, om det högsta sanktionsbeloppet som väljs i sig kan anses tillräckligt avskräckande.

Beloppsintervallet behöver alltså vara stort, med ett förhållandevis högt sanktionstak, för att uppfylla kravet på effektiva, proportionella och avskräckande sanktioner. Intervallet behöver göra det möjligt att besluta om höga avgifter för allvarliga överträdelser och som är avskräckande även för stora företag. Det är svårt att uppskatta värdet av data och värdet kan variera stort från fall till fall. Det är därför svårt att utifrån marknadsförhållanden avgöra vilket högsta belopp som krävs för att sanktionsavgiften ska ha en tillräckligt handlingsdirigerande och avskräckande effekt. Syftet med dataförordningen är främst att främja en konkurrenskraftig inre marknad för data och skyldigheterna gäller ofta avtalsförhållanden mellan företag. Förordningen innehåller även bestämmelser till skydd för små och medelstora företag. För ageranden och åtgärder som utgör överträdelser av dataskyddsförordningen utgår sanktionsavgifter enligt det regelverket. Dataförordningen har dock inte ett motsvarande syfte, dvs. att skydda enskildas grundläggande rättigheter, som kan rättfärdiga sanktionsnivåer i höjd med sanktionsavgifter enligt det regelverket.

Dataförordningen bestämmelser gäller för många olika typer av aktörer, inklusive mycket stora företag. Vidare kan data representera stora värden, varför det kan finnas incitament att inte följa förord-

ningens krav. Vi bedömer därför att 20 miljoner kronor är ett belopp som ger möjlighet att ålägga effektiva, proportionella och tillräckligt avskräckande sanktionsavgifter (se dock nedan vad gäller sanktionsavgifter för fysiska personer som inte bedriver näringsverksamhet). Det kan konstateras att 20 miljoner kronor är ett relativt sett högt sanktionstak i svensk rätt. Vi bedömer dock att den nivån är ändamålsenlig och nödvändig för att ge utrymme för en tillräckligt avskräckande sanktionsavgift.

Sanktionsavgift ska kunna åläggas även vid överträdelser som framstår som mindre allvarliga. Sanktionsbeloppen kommer då kunna vara väsentligt lägre än det högsta möjliga sanktionsbeloppet. Det finns enligt vår mening goda skäl att bestämma ett särskilt lägsta sanktionsbelopp. Det ger förutsebarhet om att sanktionsavgiften inte ska vara helt obetydlig. Miniminivån får inte vara så hög att effekten blir orimlig för ett litet t.ex. nystartat företag. Med beaktande av detta och lägsta belopp i andra författningar bedömer vi att 5 000 kronor en rimlig lägsta nivå på sanktionsavgiften (se nedan om nedan fysiska personer som bedriver näringsverksamhet).

Sanktionsbelopp för myndigheter

Myndigheter och andra offentliga organ kan åläggas sanktionavgift för överträdelser av dataförordningens skyldigheter. Jämfört med vinstdrivande stora företag kan det finnas skäl att anta att även ett relativt sett lägre sanktionsbelopp kan ha en tillräckligt avskräckande och handlingsdirigerande effekt för myndigheter (jfr prop. 2017/ 18:105 s. 139 f.). Det saknas enligt vår bedömning skäl att ange ett särskilt högsta sanktionsbelopp för myndigheter. Det är upp till den behöriga myndigheten att fastställa vilket belopp som är proportionellt i det enskilda fallet.

Fysiska personer som inte bedriver näringsverksamhet.

Fysiska personer som inte bedriver näringsverksamhet är konsumenter. Konsumenter kan göra sig skyldiga till överträdelser av dataförordningen och de kan bli föremål för sanktionsavgifter. Sanktionsavgifter för enskilda i egenskap av konsumenter är generellt sett

ovanliga i svensk rätt, särskilt när det gäller marknadsrättsliga regelverk som i regel riktar sig mot företag.

Syftet med dataförordningen är främst att främja en konkurrenskraftig inre marknad för data. Det är företag som kontrollerar data och konsumenterna ges främst rätt att få åtkomst till data som genereras av uppkopplade produkter som de innehar för eget bruk. Konsumenter kommer sannolikt sällan bli aktuella för sanktionsavgifter. Betydelsen av att ålägga sanktioner för enskilda konsumenters överträdelser får antas vara begränsad, dvs. det finns en begränsad vinst med att kunna besluta om särskilt höga sanktionsavgifter för konsumenter.

Beloppsintervallet som föreslagits ovan är inte relevant för konsumenter, utan nivåerna för konsumenter bör vara väsentligt lägre. Detta bör framgå i kompletteringslagen. Vi föreslår att en sanktionsavgift för fysiska personer som inte bedriver näringsverksamhet ska uppgå till lägst 1 000 kronor och högst 10 000 kronor.

5.5.4 Kriterier som ska beaktas när sanktioner åläggs behöver inte införas i kompletteringslagen

Bedömning: Det behöver i kompletteringslagen inte särskilt föreskrivas vilka omständigheter som ska beaktas vid åläggande av sanktioner.

I artikel 40.3 dataförordningen anges att åtminstone följande kriterier ska beaktas när sanktioner åläggs.

a) Överträdelsen art, allvar, omfattning och varaktighet.

b) Varje åtgärd som den överträdande parten har vidtagit för att begränsa eller avhjälpa den skada som orsakats.

c) Eventuella tidigare överträdelser.

d) De ekonomiska fördelar som den överträdande parten har erhållit eller förluster som denna har undvikit, i den mån fördelarna eller förlusterna kan fastställas på ett tillförlitligt sätt.

e) Eventuella andra försvårande eller förmildrande omständigheter.

f) Den överträdande partens omsättning i EU under föregående räkenskapsår.

Vi noterar att bestämmelsens tillämpningsområde inte är uttryckligen begränsad till överväganden som avser just beslut om ekonomiska sanktioner. I propositionen till lagen (2024:500) med kompletterande bestämmelser till dataförvaltningsförordningen uttalade regeringen avseende motsvarande bestämmelse i den förordningen att den anser att dessa omständigheter är relevanta för bedömningen av sanktionsavgiftens storlek och att de bör ligga till grund för tillsynsmyndighetens bedömning av sanktionsavgiftens storlek (prop. 2023/24:73 s. 45). I kompletteringslagen till dataförvaltningsförordningen anges att kriterierna ska beaktas vid bestämmande av sanktionsavgift. Vi menar att omständigheterna som listas i artikel 40.3 är relevanta även vid bedömningen av vilken typ av sanktion som den behöriga myndigheten bör välja, vilket även är i linje med bestämmelsens ordalydelse. Exempelvis kan överträdelsens art eller förhållandet att rättelse har vidtagits även innebära att det finns skäl att stanna vid ett beslut om anmärkning eller att avstå ifrån att besluta om sanktionsavgift (se nedan). Det bör av den anledningen inte införas en bestämmelse som anger att omständigheterna som listas i artikel 40.3 ska beaktas just vid bestämmande av en sanktionsavgifts storlek.

Kriterierna som åtminstone ska beaktas fastställs direkt i dataförordningen som alltså är direkt tillämplig. Bestämmelser i en förordning bör bara införas i kompletterande nationell lagstiftning om det är nödvändigt. Omständigheterna är vidare sådana som normalt bör beaktas vid fastställande av sanktioner, enligt proportionalitetsprincipen som är fastställd i 5 § tredje stycket förvaltningslagen. Omständigheterna som enligt artikel 40.3 ska beaktas vid åläggande av sanktioner behöver enligt vår bedömning därför inte anges i kompletteringslagen.

5.5.5 Behöriga myndigheter får avstå från att besluta om sanktionsavgift

Förslag: Behöriga myndigheter ska kunna avstå från att ta ut en sanktionsavgift helt eller delvis om överträdelsen är ringa eller ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften.

Vi föreslår att sanktionsavgifter enligt dataförordningen ska kunna komma i fråga för många olika överträdelser av förordningen (se avsnitt 5.6.3).

Sanktionsavgifterna bygger på strikt ansvar, dvs. att avgiften tas ut oberoende av om överträdelsen har skett med uppsåt eller på grund av oaktsamhet. I regeringens skrivelse En tydlig, rättssäker och effektiv tillsyn anges att det för att uppnå en ökad tydlighet i regelverk om ingripanden vid tillsyn i vissa fall bör finnas en reglering av de situationer då tillsynsorganen inte behöver vidta någon åtgärd mot den objektsansvarige för en konstaterad brist. Det kan gälla situationer då det är mer lämpligt att låta bli att ingripa, t.ex. då överträdelsen är ringa eller då tillsynsobjektet har vidtagit rättelse. Rättelse bör dock inte utgöra en godtagbar grund för eftergift i allvarliga fall. När det gäller sanktionsavgifter har det vidare ifrågasatts om ett strikt ansvar, utan något utrymme att beakta förhållanden av subjektiv natur, är förenligt med Europakonventionen[7]. Det kan därför vara nödvändigt att ange att behöriga myndigheter i vissa undantagsfall inte behöver ta ut en sanktionsavgift, t.ex. om det vore oskäligt. Tillsynsorganets ställningstagande att underlåta att ingripa bör komma till uttryck i ett beslut, om inte annat för att den objektsansvarige ska få vetskap om att det aktuella tillsynsförfarandet har avslutats (skr. 2009/10:79 s. 49).

Enligt vår bedömning bör den behöriga myndigheten ha möjlighet att helt eller delvis avstå från att besluta om sanktionsavgift i enskilda fall av överträdelser av dataförordningen. Det kan röra sig om en bagatellartad överträdelse som inte skadat något allmänt eller enskilt intresse och där inte heller en anmärkning är påkallad. Vidare kan det i enskilda fall med hänsyn till omständigheterna vara oskäligt

[7] Europeiska konventionen den 4 november 1950 angående skydd för de mänskliga rättigheterna och de grundläggande friheterna.

att ta ut en sanktionsavgift. Sanktionsavgiften bör dock inte efterges eller sättas ner på grund av bristande rutiner eller påstådd bristande kännedom, tidsbrist eller dålig ekonomi.

Vi föreslår i avsnitt 5.5.1 att det i kompletteringslagen ska anges att en behörig myndighet *ska* besluta att ta ut en sanktionsavgift för överträdelser av olika skyldigheter i dataförordningen. För att tydliggöra att det finns ett utrymme för den behöriga myndigheten att avstå ifrån att ta ut, eller sätta ner, sanktionsavgiften i ett enskilt fall bör det införas en särskild bestämmelse om detta i kompletteringslagen. Bestämmelsen ska fastställa att den behöriga myndigheten kan avstå från att ta ut en sanktionsavgift helt eller delvis om överträdelsen är ringa eller ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften.

5.5.6 Förbud mot dubbelprövning

Förslag: Sanktionsavgift ska inte få beslutas om överträdelsen omfattas av ett föreläggande om vite och överträdelsen ligger till grund för en ansökan om utdömande av vitet.

Behöriga myndigheter ska enligt vårt förslag få meddela de föreläggande som behövs för att dataförordningen, kompletteringslagen och föreskrifter som har meddelats i anslutning till lagen ska följas. Föreläggandena förslås kunna förenas med vite. Myndigheten kan även besluta om sanktionsavgift.

Enligt den Europakonventionen och EU:s stadga om de grundläggande rättigheterna[8] finns en rätt att inte bli lagförd eller straffad två gånger för samma gärning, det så kallade dubbelprövningsförbudet. Ett vite har karaktär av straff och aktualiserar därmed tillämpning av förbudet mot dubbelprövning. Högsta domstolen har i sin praxis fastslagit att det inte enbart är ett slutligt avgörande som utgör ett hinder mot andra förfaranden, utan att även en pågående prövning utgör ett sådant hinder enligt svenska grundläggande processuella principer (se bl.a. NJA 2013 s. 502). I regelverk där det är möjligt att utfärda ett vitesföreläggande och ta ut en sanktionsavgift för samma överträdelse införs därför bestämmelser som syftar till att

[8] Europeiska unionens stadga om de grundläggande rättigheterna, 2010/C 83/02.

hindra dubbelprövning. Dessa brukar utformas på så sätt att sanktionsavgift inte får beslutas om överträdelsen även omfattas av ett vitesföreläggande och överträdelsen ligger till grund för en ansökan om utdömande av vitet, se exempelvis 12 kap. 3 § LEK (jfr prop. 2016/17:22 s. 228 och prop. 2021/ 22:136 s. 525). Möjligheten att besluta om en sanktionsavgift bör därför förutsätta att samma omständigheter som ligger till grund för avgiften inte omfattas av ett föreläggande om vite, om omständigheterna ligger till grund för en ansökan om utdömande av vitet. Detta bör enligt vår bedömning framgå av kompletteringslagen.

Eftersom en ansökan om utdömande av vite utgör hinder mot ett beslut om sanktionsavgift med omständigheter som grund bör den behöriga myndigheten noga överväga om en sådan ansökan är nödvändig när det samtidigt kan vara aktuellt att besluta om en sanktionsavgift. Det är inte särskilt troligt att den omvända situationen skulle uppstå, dvs. att en beslutad sanktionsavgift skulle utgöra hinder mot ett föreläggande eller utdömande av vite. Ett vitesföreläggande syftar till att få enskilda att vidta en åtgärd eller underlåta att göra något, dvs. att påverka ett framtida handlande. En sanktionsavgift syftar i stället till att straffa ett tidigare agerande. Ett vitesföreläggande som beslutas efter en sanktionsavgift kan därför inte omfatta samma händelse. Det är vidare att inte är sannolikt att den behöriga myndigheten skulle använda sig av ett vitesföreläggande, eller ansöka om utdömande av vite, för en överträdelse för vilken en sanktionsavgift har beslutats (jfr prop. 2021/22:136 s. 363 och 364). Risken för dubbelprövning i den beskrivna situationen är alltså mycket osannolik. Det är därför inte motiverat att införa en bestämmelse om förbud mot beslut om föreläggande, eller ansökan om utdömande av vite, när en sanktionsavgift har beslutats.

5.5.7 Bestämmelser om förfarandet vid beslut om sanktionsavgift

Förslag: En sanktionsavgift ska endast få beslutas om den som avgiften ska tas ut av har fått tillfälle att yttra sig inom två år från det att överträdelsen ägde rum. Beslutet om sanktionsavgift ska delges den som beslutet gäller.

En sanktionsavgift ska betalas till inom 30 dagar från det att beslutet om att ta ut avgiften fick laga kraft eller inom den längre tid som anges i beslutet.

Om sanktionsavgiften inte betalas i tid, ska den behöriga myndigheten lämna den obetalda avgiften för indrivning.

En beslutad sanktionsavgift faller bort till den del beslutet om avgiften inte har verkställts inom fem år från det att beslutet fick laga kraft.

Sanktionsavgiften tillfaller staten.

I och med att behöriga myndigheter ska besluta om sanktionsavgift kommer förvaltningslagen att gälla för förfarandet. Det behövs dock vissa ytterligare förfarandebestämmelser.

På grund av sanktionsavgiftens ingripande karaktär bör ett beslut om avgift delges den betalningsskyldige enligt delgivningslagen (2010:1932).

Det bör även finnas en bortre tidsgräns för när avgiften får beslutas. En sanktionsavgift bör endast få beslutas om den som avgiften ska tas ut av har fått tillfälle att yttra sig inom två år från det att överträdelsen ägde rum. Bevisbördan för att kommunikation har skett bör ligga på den behöriga myndigheten. Tidsfristen bör räknas från när överträdelsen ägde rum. I fråga om en överträdelse som skett löpande under viss tid är det tillräckligt att kommunikation sker inom två år från det att överträdelsen upphörde för att en sanktionsavgift ska kunna beslutas. En sanktionsavgift bör betalas till den behöriga myndigheten inom 30 dagar från det att beslutet om avgiften har fått laga kraft eller inom den längre tid som anges i beslutet. Om avgiften inte betalas i tid bör den behöriga myndigheten vara skyldig att lämna den obetalda avgiften för indrivning enligt lagen om indrivning av statliga fordringar m.m. I likhet med vad som i allmänhet gäller för sanktionsavgifter bör avgiften preskriberas till den del verkställighet inte har skett inom fem år. Slutligen ska sanktionsavgiften tillfalla staten.

Vi föreslår att dessa förfarandebestämmelser ska anges i kompletteringslagen.

Det följer av 3 kap. 1 § punkt 6 utsökningsbalken att en förvaltningsmyndighets beslut som innefattar betalningsskyldighet och som får överklagas som t.ex. förvaltningsbesvär utgör en exekutionstitel (prop. 2021/22:206 s. 36). Det saknas därför behov av att i komplet-

teringslagen särskilt ange att verkställighet får ske enligt utsökningsbalken.

5.6 Överträdelser av dataförordningen som kan bli föremål för sanktionsavgift

Dataförordningen innehåller många olika typer av skyldigheter för olika typer av aktörer. Förordningen specificerar inte närmare vilka överträdelser som bör bli föremål för vilken typ av sanktion, exempelvis ekonomiska sanktioner. Sanktionsavgifter kan ha en viktig avskräckande funktion och utgångspunkten i dataförordningen är att sanktionsavgifter ska kunna åläggas för överträdelser av skyldigheterna enligt förordningen. Sanktionsavgifter är dock en ingripande sanktion och det ställs i svensk rätt olika krav som ska vara uppfyllda för att en sanktionsavgift ska komma i fråga för regelöverträdelser. Utifrån ett rättssäkerhetsperspektiv finns det vidare skäl för att det i kompletteringslagen tydligt framgår vilka överträdelser som ska kunna bli föremål för sanktionsavgift.

I detta avsnitt redovisar vi vilka överträdelser av dataförordningen som enligt vår bedömning ska kunna leda till sanktionsavgift.

5.6.1 Kriterier för överträdelser som kan leda till sanktionsavgift

Sanktionsavgift utgör den mest ingripande formen av sanktioner, som har likheter med en straffrättslig sanktion. I regeringens skrivelse En tydlig, rättssäker och effektiv tillsyn anges följande om utformningen av sanktionsavgifter (skr. 2009/2010:79 s. 46):

> Utformningen av en sanktionsavgift vid tillsyn bör uppfylla de principer om sanktionsavgifters användningsområde och utformning som angavs i förarbetena till bestämmelsen om förverkande i 36 kap. 4 § brottsbalken (prop. 1981/82:142 s. 77). Enligt dessa principer bör sanktionsavgifter användas inom områden där regelöverträdelser är särskilt frekventa eller där det föreligger speciella svårigheter med att beräkna storleken av den vinst eller besparing som uppnås i det enskilda fallet. Avgifter bör vidare endast förekomma inom speciella och klart avgränsade rättsområden där det relativt lätt kan fastställas om en överträdelse skett eller inte. […]
>
> Om avgiftsskyldigheten ska bygga på ett strikt ansvar bör förutsättas att det finns starkt stöd för en presumtion om att överträdelser inte kan förekomma annat än som en följd av uppsåt eller oaktsamhet.

Vi gör bedömningen att bestämmelserna i dataförordningen generellt sett stämmer överens med följande kriterier.

- Det är svårt att beräkna storleken av vinst eller besparing som den berörda parten uppnår i det enskilda fallet.
- Bestämmelserna om skyldigheter innehåller inte något subjektivt rekvisit rörande uppsåt eller oaktsamhet (strikt ansvar) och det finns stöd för en presumtion om att bristande efterlevnad endast kan förekomma som följd av uppsåt eller oaktsamhet.
- Bestämmelserna är tillräckligt tydlig för att det relativt lätt kan fastställas om en bristande efterlevnad har skett eller inte. Svåra avvägningar och skälighetsbedömningar ska inte behöva göras.

Några bestämmelser i dataförordningen är dock utformade så att det inte tydligt framgår vad bestämmelsen i fråga faktiskt ställer för krav. Vissa bestämmelser ger vidare uttryck för formkrav eller skyldigheter av mer administrativ art. För sådana bestämmelser saknas det enligt vår mening förutsättningar och skäl att kunna ta ut en sanktionsavgift.

5.6.2 Hänvisningar i komplettringslagen till överträdelser i dataförordningen som kan bli föremål för sanktionsavgift

Som tidigare nämnts innehåller dataförordningen många olika typer av skyldigheter för olika typer av aktörer. Flera artiklar i dataförordningen föreskriver skyldigheter endast för en viss typ av aktör. Andra artiklar eller bestämmelser i en artikel innehåller i stället bestämmelser om skyldigheter för olika typer av aktörer.

Det bör tydligt framgå i kompletteringslagen vilka överträdelser av dataförordningens bestämmelser som kan bli föremål för sanktionsavgift. Det finns olika sätt att hänvisa till förordningens bestämmelser i kompletteringslagen. Utifrån intresset av tydlighet kan det finnas anledning att precisera vilken typ av aktör som kan komma i fråga för en sanktionsavgift i förhållande till varje enskild bestämmelse. Om hänvisningarna i lagen till dataförordningens artiklar görs för respektive typ av aktör innebär det bl.a. att vissa artiklar hänvisas till flera gånger i komplettringslagen. Utifrån ett EU-rättsligt perspektiv är denna lösning möjligen inte heller föredra, eftersom den

innebär en begränsning i förhållande till vilka skyldigheter som sanktioner kan aktualiseras, jämfört med vad som hade gällt om kretsen av aktörer inte preciserades i svensk lagstiftning. Vi bedömer dock att intresset av tydlighet överväger intresset av att lämna tillämpningen av förordningen så öppen som möjligt, varför vi föreslår att aktörskretsen preciseras i förhållande till de skyldigheter där överträdelser kan medföra sanktionsavgift.

Vidare föreslår vi att hänvisningar i lagtexten görs till berörda punkter i de olika artiklarna utan att närmare beskriva just vilket t.ex. agerande eller krav som avses. Ett alternativ vore att beskriva detta, dvs. exempelvis ange att sanktionsavgift ska utgå för underlåtelse att underrätta den behöriga myndigheten om den avslår en begäran om data enligt artikel 4.8. Att genomgående göra detta skulle ge upphov till en mycket omfattande lagtext. Eftersom förordningens bestämmelser är tillräckligt tydliga med avseende på vilka ageranden eller förfaranden som utgör skyldigheter är det enligt vår uppfattning tillräckligt att hänvisa till de aktuella bestämmelserna på det sätt som vi föreslår.

5.6.3 Överträdelser som kan leda till sanktionsavgift

Förslag: Sanktionsavgift ska kunna tas ut från följande aktörer vid överträdelse av följande artiklar i EU:s dataförordning, i den ursprungliga lydelsen:

- Tillverkare, försäljare, uthyrare, leasegivare eller leverantör av tillhörande tjänster, vid överträdelse någon av sina skyldigheter enligt artikel 3.1, 3.2 eller 3.3.
- Datahållare för överträdelser av någon av sina skyldigheter i artikel 4.1, 4.2, 4.4, 4.5, 4.7, 4.8, 4.13, 4.14, 5.1, 5.4, 5.6, 5.10 5.11, 8.1, 8.3, 8.4, 9.7 eller 18.1.
- Användare som överträder någon av sina skyldigheter enligt artikel 4.7, 4.10 eller 4.11.
- Tredje parter som överträder någon av sina skyldigheter enligt artikel 5.5, 6.1, 6.2, 11.2 eller 19.2.
- Datamottagare som överträder någon av sina skyldigheter enligt 11.2.

- Företag som har utsetts till grindvakt som överträder någon av sina skyldigheter enligt artikel 5.3.
- Offentliga organ som överträder någon av sina skyldigheter enligt artikel 19.
- Leverantörer av databehandlingstjänster som överträder sina skyldigheter enligt artikel 25.1, 25.2, 25.3, 26, 28, 29.1–6, 32.1, 32.3, 32.4 eller 32.5.
- Säljare av en applikation som använder smarta kontrakt eller, i avsaknad av en sådan, den person vars närings- eller yrkesverksamhet inbegriper användning av smarta kontrakt för andra inom ramen för genomförandet av ett avtal eller en del av det om att tillgängliggöra data, som överträder någon av sina skyldigheter enligt artikel 36.1 eller 36.2.
- Enheter och som gör uppkopplade produkter tillgängliga eller erbjuder tillhörande tjänster som inte utser rättslig företrädare enligt artikel 37.12.

Dataförordningen förutsätter att ekonomiska sanktioner ska kunna åläggas för överträdelser av förordningen (artikel 37.5 d). Förordningen föreskriver inte att just sanktionsavgifter ska kunna utgå för överträdelser av samtliga skyldigheter, utan det centrala är att sanktionerna är effektiva, proportionella och avskräckande (artikel 40.1). Som beskrivits ovan bör det ställas vissa krav på hur en skyldighet ska vara utformad för att en enligt svensk rätt överträdelse ska kunna leda till sanktionsavgift. Vi kan därför konstatera att det behöver göras en avvägning mellan intresset av att besluta om ekonomiska sanktioner vid överträdelser av förordningens bestämmelser och de krav som bör ställas på bestämmelse för att den ur rättssäkerhetssynpunkt ska vara lämplig att förena med en sanktionsavgift.

I detta avsnitt beskrivs förordningens bestämmelser om skyldigheter och om de enligt vår bedömning, med beaktande av de kriterier som beskrivits i avsnitt 5.6.1, bör kunna bli föremål för sanktionsavgift. Beskrivningen görs för respektive typ av aktör som dataförordningen är tillämplig på.

Tillverkare, försäljare, uthyrare eller leasegivare, eller leverantörer av tillhörande tjänster

I artikel 3.1 fastslås att, och när och hur, uppkopplade produkter ska utformas och tillverkas, och att tillhörande tjänster ska utformas och tillhandahållas, så att data, som standard är direkt tillgängliga för användaren. Bestämmelsen ställer alltså krav på aktörer som utformar uppkopplade produkter och tillhörande tjänster, dvs. tillverkare och leverantörer av tillhörande tjänster. I artikel 3.2 fastställs att försäljare, uthyrare eller leasegivare, som kan vara tillverkare, innan de ingår avtal om en uppkopplad produkt ska uppfylla den informationsskyldighet som följer av artikeln. Motsvarande informationsskyldighet gäller enligt artikel 3.3 för leverantörer av tillhörande tjänster.

Vi bedömer att sanktionsavgift ska kunna åläggas vid överträdelse av dessa skyldigheter, dvs. vid överträdelser av artikel 3.1, 3.2 eller 3.3.

Datahållare

Datahållare har många skyldigheter enligt dataförordningen. I kapitel IV fastslås skyldigheter att inte tillämpa oskäliga avtalsvillkor i avtal med företag. Avtalsvillkor som är oskäliga ska enligt artikel 13.1 inte vara bindande. Vi bedömer att bestämmelserna i kapitel IV främst är av civilrättslig karaktär och att tillämpning av oskäliga avtalsvillkor inte bör kunna bli föremål för sanktionsavgift.

Därutöver gäller skyldigheter enligt kapitel II (tillgängliggörande av data från uppkopplade produkter och tillhörande tjänster), kapitel III (tillgängliggörande av data enligt unionsrätten) och kapitel V (tillgängliggörande av data vid exceptionellt behov).

Artikel 4.1 är tillämplig om användaren inte har direkt åtkomst till data från den uppkopplade produkten eller den tillhörande tjänsten. Datahållaren är då skyldig att, på användarens begäran, utan oskäligt dröjsmål göra lätt åtkomliga data samt relevanta metadata som är nödvändiga för att tolka och använda dessa data, tillgängliga för användaren i enlighet med vad som anges i artikel 4.1. Om datahållaren vägrar att dela data enligt artikel 4 är den enligt artikel 4.2 skyldig att underrätta den behöriga myndigheten om detta.

I artikel 4.4 fastslås att datahållaren inte får göra det orimligt svårt för användaren att göra val eller utöva rättigheter enligt artikel 4.

Enligt artikel 4.5 får datahållare inte, för att kontrollera om en fysisk eller juridisk person kan anses vara en användare vid tillämpning av artikel 4.1, kräva att denna person lämnar någon information utöver vad som är nödvändigt. Datahållare får inte heller spara någon information om användarens åtkomst till de data som begärs utöver vad som är nödvändigt för ett korrekt utförande av användarens begäran och för säkerheten och underhållet av datainfrastrukturen.

Artikel 4.6 anger att företagshemligheter ska bevaras och att de endast får röjas om datahållaren och användaren före utlämnandet vidtar alla nödvändiga åtgärder för att bevara deras konfidentialitet. Datahållaren, eller om det inte är samma person, innehavaren av en företagshemlighet, ska identifiera de data som skyddas som företagshemligheter och ska komma överens med användaren om de proportionella tekniska och organisatoriska åtgärder som är nödvändiga för att bevara konfidentialiteten. För att möjliggöra datadelning är det viktigt att det ställs krav på datahållaren att vidta åtgärder som gör att den kan ge åtkomst till data utan att röja företagshemligheter. Bestämmelsen syftar bl.a. till att skydda datahållarens företagshemligheter. Vi bedömer att det saknas skäl att föreslå att datahållare ska kunna åläggas en sanktionsavgift för att den inte kommit överens om åtgärder enligt artikel 4.6.

Enligt artikel 4.7 får en datahållare hindra eller avbryta datadelning när det inte finns någon överenskommelse om nödvändiga skyddsåtgärder enligt punkt 6, eller om en användare underlåter att genomföra överenskomna åtgärder. En datahållare är då skyldig att underrätta den behöriga myndigheten om detta och även identifiera vilka åtgärder som inte har överenskommits eller genomförts och, i förekommande fall, för vilka företagshemligheter konfidentialiteten har äventyrats. Datahållaren ska även, utan dröjsmål, skriftligen lämna ett motiverat beslut om att begränsa eller avbyta datadelning till användaren.

Enligt artikel 4.8 ska en datahållare som är en innehavare av en företagshemlighet underrätta den behöriga myndigheten om den avslår en begäran om data med åberopande av att den högst sannolikt kommer att lida allvarlig ekonomisk skada till följd av röjandet av företagshemligheter, trots de åtgärder som vidtagits av användaren enligt artikel 4.6. Beslutet ska även i denna situation motiveras och skriftligen lämnas till användaren utan dröjsmål.

I artikel 4.13 fastslås att en datahållare endast får använda lätt åtkomliga data som är icke-personuppgifter på grundval av ett avtal med användaren. Datahållaren får heller inte använda sådana data för att få inblick i användarens ekonomiska situation, tillgångar och produktionsmetoder, eller användning av dessa, på något annat sätt som skulle kunna undergräva användarens kommersiella ställning. Av artikel 4.14 framgår att datahållare inte får göra produktdata, som är icke-personuppgifter, tillgängliga för tredje parter för kommersiella eller icke-kommersiella ändamål annat än för att fullgöra avtalet med användaren. Vid behov ska datahållare genom avtal förbinda tredje parter att inte dela vidare data som de har mottagit från dem.

I artikel 5.1 föreskrivs att datahållare, på begäran av en användare eller av en part som agerar för en användares räkning, är skyldiga att utan oskäligt dröjsmål för en tredje part tillgängliggöra lätt åtkomliga data, samt de relevanta metadata som är nödvändiga för att tolka och använda dessa data. Sådana data ska vara av samma kvalitet som den som är tillgänglig för datahållaren och ska tillhandahållas på ett enkelt och säkert sätt, kostnadsfritt för användaren, i ett heltäckande, strukturerat, allmänt använt och maskinläsbart format och, när så är relevant och tekniskt genomförbart, kontinuerligt och i realtid. Data ska göras tillgängliga av datahållaren för den tredje parten i enlighet med artiklarna 8 och 9.

Av artikel 5.4 följer att en datahållare, för att kontrollera om en fysisk eller juridisk person kan anses vara en användare eller en tredje part vid tillämpning av artikel 5.1, inte ska begära att användaren eller den tredje parten ska tillhandahålla någon information utöver vad som är nödvändigt. Datahållare får inte heller spara någon information om den tredje partens åtkomst till begärda data utöver vad som är nödvändigt för ett korrekt utförande av den tredje partens begäran och för säkerheten och underhållet av datainfrastrukturen.

I artikel 5.6 fastslås att datahållare inte får använda lätt åtkomliga data för att få inblick i den tredje partens ekonomiska situation, tillgångar och produktionsmetoder, eller användning av dessa, på något annat sätt som skulle kunna undergräva den tredje partens kommersiella ställning, såvida inte den tredje parten har gett sitt tillstånd till sådan användning och när som helst och på ett enkelt sätt kan återkalla det tillståndet.

Artikel 5.10 är tillämplig när det inte finns någon överenskommelse om nödvändiga åtgärder till skydd för företagshemligheter en-

ligt artikel 5.9, eller om den tredje parten underlåter att genomföra de åtgärder som överenskommits eller äventyrar företagshemligheternas konfidentialitet. Om datahållaren har hindrat eller avbrutit delning av data är den enligt artikel 5.10 skyldig att underrätta den behöriga myndigheten om detta, och även identifiera vilka åtgärder som inte har överenskommits eller genomförts och, i förekommande fall, för vilka företagshemligheter konfidentialiteten har äventyrats. Datahållaren ska även, utan dröjsmål, skriftligen lämna ett motiverat beslut om att begränsa eller avbyta datadelning till den tredje parten.

Artikel 8.1 gäller situationer där en datahållare inom ramen för förbindelser mellan företag är skyldig att göra data tillgängliga för en datamottagare enligt artikel 5 eller enligt annan tillämplig unionsrätt eller nationell lagstiftning som antagits i enlighet med unionsrätten. I artikeln anges att datahållaren ska komma överens med en datamottagare om villkoren för att göra data tillgängliga och ska göra detta på rättvisa, rimliga och icke-diskriminerande villkor och på ett öppet sätt i enlighet med kapitel III och kapitel IV.

Av enligt artikel 8.3 följer att datahållare är skyldiga att inte diskriminera mellan jämförbara kategorier av datamottagare när data görs tillgängliga. Om en datamottagare anser att diskriminering föreligger är datahållaren skyldig att på mottagarens motiverade begäran utan oskäligt dröjsmål ge datamottagaren information som visar att det inte har förekommit någon diskriminering.

Enligt artikel 8.4 får en datahållare inte, inbegripet på exklusiv grund, göra data tillgängliga för en datamottagare, om inte användaren begär detta enligt kapitel II.

I artikel 9.1 anges att ersättning som en datahållare och en datamottagare kommer överens om för att göra data tillgängliga i förbindelser mellan företag ska vara icke-diskriminerande och rimlig. Bestämmelsen är av avtalsrättslig karaktär. Att avgöra vad som utgör en icke-diskriminerande och rimlig ersättning kan förutsätta avvägningar och skälighetsbedömningar. Vi bedömer därför att sanktionsavgift inte bör vara aktuell vid överträdelser av denna bestämmelse.

Enligt artikel 9.7 är datahållaren skyldig att ge datamottagaren tillräckligt detaljerad information om grunden för beräkningen av ersättningen så att datamottagaren kan bedöma huruvida kraven i artikel 9.1–4 är uppfyllda.

Datahållare är vidare enligt artikel 18.1 skyldiga att ska utan oskäligt dröjsmål göra data tillgängliga enligt kapitel V.

Enligt vår bedömning ska en sanktionsavgift kunna tas ut av datahållare för överträdelser av någon av sina skyldigheter i artikel 4.1, 4.2, 4.4, 4.5, 4.7, 4.8, 4.13, 4.14, 5.1, 5.4, 5.6, 5.10 5.11, 8.1, 8.3, 8.4, 9.7 eller 18.1.

Användare

För användare gäller skyldigheter enligt artikel 4.6 och 4.7, 4.10 och 4.11. Bestämmelserna i artikel 4.6 och 4.7 syftar till att skydda datahållarens företagshemligheter. Enligt artikel 4.6 ska datahållaren och användaren komma överens om skyddsåtgärder. Liksom vad gäller datahållare bedömer vi att sanktionsavgift inte bör kunna utgå för att en överenskommelse inte har ingåtts. Användaren är enligt artikel 4.7 skyldig att följa åtgärder som överenskommits enligt artikel 4.6, eller, även om sådan överenskommelse saknas, att inte äventyra företagshemligheternas konfidentialitet.

Enligt artikel 4.10 får en användare inte använda de data som erhållits till följd av en begäran som avses i artikel 4.1 för att utveckla en konkurrerande uppkopplad produkt, och inte heller dela dessa data med en tredje part i det syftet. Användare får inte heller använda sådana data för att skaffa sig inblick i tillverkarens, eller datahållarens, ekonomiska situation, tillgångar och produktionsmetoder. Vidare är en användare enligt artikel 4.11 skyldig att inte använda tvångsmedel eller missbruka luckor i en datahållares tekniska infrastruktur för att få åtkomst till data.

Vid överträdelser av dessa skyldigheter i artikel 4.7, 4.10 eller 4.11 ska användare enligt vår uppfattning kunna påföras en sanktionsavgift. Det noteras att användare kan vara konsumenter. För det fall en användare agerar i strid med artikel 4.10 bör användaren inte anses vara konsument.

Grindvaktsföretag

Enligt artikel 5.3 gäller särskilda skyldigheter för företag som har utsetts till grindvakt enligt artikel 3 i förordningen om digitala plattformar.[9] Skyldigheterna innebär att grindvaktsföretag inte får anmoda

[9] Europaparlamentets och rådets förordning (EU) 2022/1925 av den 14 september 2022 om öppna och rättvisa marknader inom den digitala sektorn och om ändring av direktiv (EU) 2019/1937 och (EU) 2020/1828 (förordningen om digitala marknader).

en användare att göra data som användaren erhållit efter en begäran enligt artikel 4.1 tillgängliga för en av företagets tjänster enligt artikel 5.1. De får inte heller anmoda en användare att begära att datahållaren gör data tillgängliga för en av grindvaktsföretagets tjänster enligt artikel 5.1. Grindvaktsföretag får inte heller ta emot data från en användare som användaren har mottagit enligt begäran enligt artikel 4.1.

Om grindvaktsföretag agerar i strid med dessa skyldigheter ska de enligt vårt förslag kunna åläggas en sanktionsavgift.

Tredje parter

För företag eller fysiska personer som är en tredje part gäller skyldigheter i artikel 5.5, 6.1, 6.2 eller 11.2. Enligt artikel 5.5 får en tredje part inte använda tvångsmedel eller missbruka luckor i en datahållares tekniska infrastruktur för att få åtkomst till data. Enligt artikel 6.1 får en tredje part bara behandla data för de ändamål och på de villkor som överenskommits med användaren och ska radera dessa data när de inte längre är nödvändiga för det överenskomna ändamålet, såvida inte annat överenskommits med användaren när det gäller personuppgifter.

Artikel 6.2 fastställer särskilda skyldigheter, förbud och begränsningar för hur tredje parter får agera och använda data. Bl.a. får de inte tillgängliggöra data för ett grindvaktsföretag eller utveckla konkurrerande uppkopplade produkter.

Enligt artikel 11.2 ska en tredje part, under de omständigheter som avses i artikel 11.3, utan oskäligt dröjsmål tillmötesgå begäran från datahållaren eller innehavaren av en företagshemlighet eller användaren om att vidta sådana åtgärder som anges i artikeln. Åtgärderna handlar bl.a. om att radera data, avsluta produktion, tillhandahållande eller användning av varor, härledda data eller tjänster som framställts på grundval av kunskap som erhållits genom sådana data. Vidare får en tredje part, som tar emot data enligt kapitel V i förordningen, enligt artikel 19.2 inte använda mottagna data eller insikter om datahållarens ekonomiska situation, tillgångar och produktions- eller driftsmetoder för att utveckla eller förbättra en uppkopplad produkt eller tillhörande tjänst som konkurrerar med datahållarens

uppkopplade produkt eller tillhörande tjänst eller dela dessa data med en annan tredje part för något av dessa ändamål.

Vår bedömning är att en sanktionsavgift ska kunna tas ut av en tredje part som överträder någon av sina skyldigheter enligt artikel 5.5, 6.1, 6.2, 11.2 eller 19.2.

Datamottagare

För datamottagare gäller skyldigheterna i artikel 11.2 att bl.a. radera data, avsluta produktion och erbjudanden, lämna information och betala ersättning (punkterna a–d).

Vi bedömer att en sanktionsavgift ska kunna tas ut av en datamottagare som överträder någon av sina skyldigheter enligt 11.2.

Offentliga organ

För offentliga organ, kommissionen, Europeiska centralbanken och unionsorgan gäller bestämmelser i kapitel V om begäran och mottagande av data från företag vid exceptionellt behov (i det följande offentliga organ). Offentliga organ omfattas enligt artikel 37.5 av behörigheten för den medlemsstat där de är etablerade. Den behöriga myndigheten i Sverige är därmed endast behörig att vidta åtgärder mot myndigheter och andra offentliga organ som är etablerade i Sverige. Det finns enligt vår bedömning inte något som talar emot att myndigheter och andra organ ska kunna åläggas sanktionsavgift.

I artikel 19, med rubriken ”skyldigheter för offentliga organ, kommissionen, Europeiska centralbanken och unionsorgan”, fastslås att ett organ som tar emot data till följd av en begäran enligt artikel 14 inte får använda dessa data på ett sätt som är oförenligt med det ändamål för vilket de begärdes. Organen är skyldiga att ha genomfört tekniska och organisatoriska åtgärder som bevarar konfidentialiteten och integriteten avseende de data som begärs och säkerheten vid överföring av data, särskilt personuppgifter, och som skyddar de registrerades rättigheter och friheter. Organen är vidare skyldiga att radera mottagna data så snart de inte längre är nödvändiga för det angivna ändamålet, och att utan oskäligt dröjsmål informera datahållaren och enskilda personer eller organisationer som har tagit emot data enligt artikel 21.1 om att de har raderats. Denna skyldighet gäller

dock inte om det i enlighet med unionsrätt eller nationell rätt om allmänhetens tillgång till handlingar i samband med insynsskyldigheter, krävs att dessa data arkiveras. Vi noterar att det i Sverige finns krav på arkivering i arkivlagen (1990:782), som innebär att offentliga organ inte får radera uppgifter i strid med bestämmelserna.

Ett offentligt organ får enligt artikel 19.2 inte heller använda mottagna data eller insikter om datahållarens ekonomiska situation, tillgångar och produktions- eller driftsmetoder för att utveckla eller förbättra en uppkopplad produkt eller tillhörande tjänst som konkurrerar med datahållarens uppkopplade produkt eller tillhörande tjänst eller dela dessa data med en annan tredje part för något av dessa ändamål.

Röjande av företagshemligheter till ett offentligt organ ska enligt artikel 19.3 endast krävas i den mån det är absolut nödvändigt för att uppnå syftet med en begäran enligt artikel 15. Det offentliga organet ska före röjandet av företagshemligheter vidta alla nödvändiga och lämpliga tekniska och organisatoriska åtgärder för att bevara konfidentialiteten för företagshemligheterna, när så är lämpligt även användning av standardavtalsvillkor och tekniska standarder samt tillämpning av uppförandekoder. I artikel 19.4 anges att ett offentligt organ ska ansvara för säkerheten för de data som de tar emot.

Det följer av artikel 15 att begäran om data endast för göras om villkoren i artikel 15.1 är uppfyllda, dvs. att det föreligger ett exceptionellt behov. I artikel 17.1 och 2 föreskrivs krav på vad en begäran om data ska innehålla och hur den ska utformas. Det föreskrivs också att begäranden ska offentliggöras. Vad gäller kravet att inte begära information enligt artikel 15 i situationer när det inte föreligger ett exceptionellt behov anser vi inte att det bör kunna påföras sanktionsavgifter. Formkraven i artikel 17 är inte heller av sådan art att sanktionsavgifter bör komma i fråga. För det fall ett offentligt organ framställer en ogrundad begäran eller inte upprättar en korrekt sådan bör datahållaren inte vara skyldig att lämna ut begärda data.

Vi bedömer att en sanktionsavgift ska kunna påföras myndigheter och andra offentliga organ som inte uppfyller sina skyldigheter i artikel 19, dvs. de skyldigheter som föreligger när ett offentligt organ har mottagit data.

Leverantörer av databehandlingstjänster

För leverantörer av databehandlingstjänster gäller skyldigheter enligt artikel 25 punkterna 1–5, artikel 26, 28 och 29 punkterna 1–6 samt artikel 32 punkterna 1–5. Enligt artikel 25.1 är leverantörer av databehandlingstjänster skyldiga att i ett skriftligt avtal tydligt ange kundens rättigheter och leverantörens skyldigheter vad gäller ett byte av leverantör av databehandlingstjänster eller till lokal IKT-infrastruktur. Avtalet ska göras tillgängligt för kunden före undertecknandet av avtalet på ett sätt som gör det möjligt för kunden att lagra och återge avtalet. Avtalet ska innehålla åtminstone de villkor och den information som anges i artikel 25.2 punkterna a-i. Avtalet ska även innehålla de klausuler som anges i artikel 25.3. Om den obligatoriska maximala övergångsperiod som föreskrivs i artikel 25.2 a är tekniskt ogenomförbar ska leverantören av databehandlingstjänster enligt artikel 25.4 underrätta kunden inom 14 arbetsdagar efter det att begäran om byte gjorts och motivera varför det är tekniskt ogenomförbart samt ange en alternativ övergångsperiod om längst sju månader. I artikel 25.4 föreskrivs även att leverantörer av databehandlingstjänster ska säkerställa driftskontinuitet i enlighet med artikel 25.1 under hela den alternativa övergångsperioden. Enligt artikel 25.5 ska avtal, som avses i punkten 1 också innehålla klausuler som ger kunden rätt att förlänga övergångsperioden en gång med en tidsperiod som kunden anser lämpligare.

Enligt artikel 26 är leverantörer av databehandlingstjänster skyldiga att informera kunden enligt vad som anges i artikeln. Enligt artikel 28.1 ska en leverantör av databehandlingstjänster göra den information som anges i bestämmelsen tillgänglig på sina webbplatser och hålla informationen uppdaterad. De webbplatser som avses i punkt 1 ska förtecknas i avtal för alla databehandlingstjänster som erbjuds av leverantörer av databehandlingstjänster.

Artikel 29.1–3 reglerar att och när bytesavgifter ska avskaffas. Från den 12 januari 2027 får sådana inte tas ut, och från 11 januari 2024 får endast nedsatta bytesavgifter tas ut. Enligt artikel 29.4 är leverantörer av databehandlingstjänster skyldiga att, innan de ingår avtal med en kund, lämna tydlig information om eventuella standardavgifter och straffavgifter för uppsägning i förtid, samt om de nedsatta bytesavgifterna som kan komma att utkrävas. I artikel 29.5 anges att leverantörer av databehandlingstjänster, i förekommande fall, ska infor-

mera en kund om databehandlingstjänster som inbegriper mycket komplexa eller kostsamma byten eller för vilka det är omöjligt att byta utan betydande störningar i data, digitala tillgångar eller tjänstearkitektur. Enligt artikel 29.6 ska leverantörerna i tillämpliga fall göra den information som avses i punkterna 4 och 5 allmänt tillgänglig för kunderna via sin webbplats eller på något annat lättillgängligt sätt.

Kapitel VII innehåller en bestämmelse, artikel 32, om olaglig internationell statlig åtkomst till och överföring av icke-personuppgifter. Enligt artikel 32.1 ska leverantörer av databehandlingstjänster vidta alla adekvata tekniska, organisatoriska och rättsliga åtgärder för att förhindra internationell statlig åtkomst till och överföring av icke-personuppgifter som innehas i unionen, om en sådan överföring eller åtkomst skulle strida mot unionsrätten eller den berörda medlemsstatens nationella rätt. Enligt artikel 32.2 ska beslut eller domar från en domstol i ett tredjeland och beslut från en administrativ myndighet i ett tredjeland (tredjelandsmyndighet) där det krävs att en leverantör av databehandlingstjänster överför eller ger åtkomst till icke-personuppgifter endast ska erkännas eller genomföras om de grundar sig på en internationell överenskommelse. Artikel 32.3 reglerar situationen då en sådan internationell överenskommelse saknas. När en leverantör av databehandlingstjänster är adressat för ett beslut eller en dom från en tredjelansmyndighet om att överföra eller ge åtkomst till icke-personuppgifter, och efterlevnaden av beslutet eller domen skulle riskera att medföra att leverantören bryter mot unionsrätten eller den berörda medlemsstatens nationella rätt, ska tredjelandsmyndigheten motta eller få åtkomst till sådana data endast om de särskilda villkor som anges i punkt 3 första stycket är uppfyllda. I artikel 32.3 andra stycket anges att beslutets eller domens adressat får begära yttrande från det relevanta nationella organ eller den relevanta nationella myndighet som har behörighet för internationellt samarbete i rättsliga frågor, för att avgöra om villkor i första stycket är uppfyllda. Om adressaten anser att beslutet eller domen kan inkräkta på unionens eller dess medlemsstaters nationella säkerhets- eller försvarsintressen, ska den begära ett yttrande för att avgöra om begärda data rör sådana säkerhets- eller försvarsintressen. Om de villkor som fastställs i punkt 2 eller 3 är uppfyllda ska leverantören av databehandlingstjänster, enligt artikel 32.4, tillhandahålla den minsta mängd data som är tillåten som svar på en begäran, på grundval av en rimlig tolkning av aktuell begäran av leverantören eller det relevanta nationella behö-

riga organ myndighet som avses i punkt 3 andra stycket. Leverantören ska enligt artikel 32.5 informera kunden om att det finns en begäran från en myndighet i ett tredjeland om att få åtkomst till dess data innan begäran tillmötesgås, utom när begäran tjänar brottsbekämpande ändamål och detta är nödvändigt för att upprätthålla den brottsbekämpande verksamhetens effektivitet.

Det framgår inte tydligt i artikel 32.1 vilka åtgärder som är adekvata eller vilka unions- eller nationella rättsakter som avses. Vilka åtgärder som är adekvata kan variera från fall till fall. Vi bedömer emellertid att bestämmelsen är viktig för att förebygga olaglig dataöverföring och vi föreslår därför att sanktionsavgift ska kunna åläggas för överträdelse av skyldigheten att vidta adekvata åtgärder. Enligt vår bedömning bör sanktionsavgifter vidare kunna åläggas om åtkomst till eller överföring av data sker i strid med bestämmelserna i artikel 32.3 första stycket och artikel 32.4 (för mycket data överförs), eller kunden inte informeras i enlighet med vad som anges i artikel 32.5. Om dataöverföring sker trots att en internationell överenskommelse saknas är artikel 32.3 tillämplig och om för mycket data delas är artikel 32.4 tillämplig. Kravet i artikel 32.3 andra stycket på att begära yttrande när försvars- eller säkerhetsintressen föreligger innehåller ett rekvisit om att adressaten anser att så är fallet. Det är inte nödvändigtvis enkelt för adressaten att bedöma. Om olaglig dataöverföring sker, utan att yttrande har inhämtats, kan själva dataöverföringen bli föremål för sanktionsavgift. Vi bedömer därför att det inte finns skäl att kunna ålägga sanktionsavgift om yttrande inte begärs.

Vi bedömer att en sanktionsavgift ska kunna tas ut av en leverantör av databehandlingstjänster som inte uppfyller någon av sina skyldigheter enligt artikel 25.1, 25.2, 25.3, 26, 28, 29.1–6, 32.1, 32.3, 32.4 eller 32.5.

Deltagare i dataområden som erbjuder data eller datatjänster till andra deltagare

Artikel 33 i dataförordningen föreskriver bestämmelser för dataområden, som är ändamåls- eller sektorsspecifika eller sektorsöverskridande interoperabla ramar för gemensamma standarder och praxisformer för delning eller gemensam behandling av data för bl.a. utveckling av nya produkter och tjänster, vetenskaplig forskning

eller civilsamhällesinitiativ. Deltagare i dataområden som erbjuder data eller datatjänster till andra deltagare i ett dataområde är skyldiga att uppfylla de väsentliga krav som anges i artikel 33.1 a–d. I artikel 33.1 andra stycket förklaras att kraven kan vara av allmän karaktär eller avse specifika sektorer, samtidigt som sambandet med krav som härrör från annan unionsrätt eller nationell rätt beaktas fullt ut. I artikel 33.2 anges att kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 45 i dataförordningen för att komplettera förordningen genom att ytterligare specificera de väsentliga krav som fastställs i punkt 1.

I skäl 103 i förordningen beskrivs att europeiska dataområden är ändamåls- eller sektorsspecifika eller sektorsöverskridande interoperabla ramar för gemensamma standarder och praxisformer för delning eller gemensam behandling av data för bl.a. utveckling av nya produkter och tjänster, vetenskaplig forskning eller civilsamhällesinitiativ.

Vi noterar att begreppet ”dataområde” inte är närmare definierat på något tydligt sätt förordningen. Kommissionen presenterade i En EU-strategi för data målet att skapa ett gemensamt europeiskt dataområde som åtföljs av sektorsvisa dataområden.[10] Dataområden nämns i fler EU-rättsakter än dataförordningen, bl.a. dataförvaltningsförordningen och förordningen om ett interoperabelt Europa.[11] Den enda rättsakt vi har lyckats identifiera där en rättslig definition av ett dataområde finns är förordningen om det europeiska hälsodataområdet (EHDS).[12] I avsaknad av rättslig reglering uppfattar vi deltagande i dataområden som frivilligt. Arbete pågår med ett flertal sektorsvisa dataområden med stöd från programmet DIGITAL.[13]

Sammantaget bedömer vi att bestämmelsen i artikel 33.1 inte är tillräckligt tydlig vad avser vilka aktörer som kan göra sig skyldig till en överträdelse. Vi bedömer att det därför inte vore tillräckligt rättssäkert att ålägga sanktionsavgift för överträdelser enligt bestämmel-

[10] COM(2020) 66 final, s. 4–5.
[11] Europaparlamentets och rådets förordning (EU) 2024/903 av den 13 mars 2024 om åtgärder för en hög nivå av interoperabilitet inom den offentliga sektorn i hela unionen (förordningen om ett interoperabelt Europa).
[12] Europaparlamentets och rådets förordning (EU) 2025/327 av den 11 februari 2025 om det europeiska hälsodataområdet och om ändring av direktiv 2011/24/EU och förordning (EU) 2024/2847. Enligt artikel 1 inrättas genom förordningen det europeiska hälsodataområdet genom fastställande av gemensamma regler, standarder och infrastrukturer och en styrningsram i syfte att underlätta tillgången till elektroniska hälsodata för primäranvändning av elektroniska hälsodata och sekundäranvändning av dessa data.
[13] SWD(2024) 21 final.

sen. Om det i framtiden blir tydligare ur ett rättsligt perspektiv vad ett dataområde är, samt vilka aktörer som deltar i ett sådant område, kan det finnas skäl att göra en ny bedömning om det ska vara möjligt att utfärda sanktionsavgifter.

Säljare av applikationer som använder smarta kontrakt och andra som avses i artikel 36

Artikel 36 gäller för säljare av en applikation som använder smarta kontrakt eller, i avsaknad av en sådan, den person vars närings- eller yrkesverksamhet inbegriper användning av smarta kontrakt för andra inom ramen för genomförandet av ett avtal eller en del av det om att tillgängliggöra data. Enligt artikel 36.1 är de skyldiga att säkerställa att dessa smarta kontrakt efterlever de väsentliga krav som föreskrivs i artikel 36.1 punkterna a–e. I artikel 36.2 fastställs vidare att leverantörer som använder smarta kontrakt är skyldiga att utföra en bedömning av överensstämmelse i syfte att uppfylla de väsentliga krav som fastställs i punkt 1 och, när dessa krav är uppfyllda, utfärda en EU-försäkran om överensstämmelse

Sanktionsavgift ska enligt vår bedömning kunna tas ut av en leverantör som avses i artikel 36 och som överträder någon av sina skyldigheter enligt artikel 36.1 eller 36.2.

Enheter och som gör uppkopplade produkter tillgängliga eller erbjuder tillhörande tjänster

Enligt artikel 37.12 ska enheter som omfattas av tillämpningsområdet för dataförordningen, och som gör uppkopplade produkter tillgängliga eller erbjuder tillhörande tjänster i unionen, bemyndiga en rättslig företrädare som de behöriga myndigheterna ska vända sig till utöver eller i stället för enheten med avseende på alla frågor som rör denna enhet.

Sanktionsavgifter ska kunna tas ut om en enhet inte utser en rättslig företrädare i enlighet med artikel 37.12.

5.7 Bestämmelser som inte bör kunna ligga till grund för sanktionsavgifter

Som vi har redovisat ovan bedömer vi att några bestämmelser i dataförordningen som uppställer olika krav inte bör kunna bli föremål för sanktionsavgifter om de inte uppfylls. Detta gäller bestämmelserna i kapitel III om oskäliga avtalsvillkor som är av civilrättslig karaktär och som innebär att oskäliga avtalsvillkor inte är bindande. Även bestämmelsen om icke-diskriminerande och rimlig ersättning i artikel 9.1 är av avtalsrättslig karaktär. Dess tillämpning förutsätter en detaljerad bedömning av ersättning i det enskilda fallet. Tvister om ersättning kan komma att bli föremål för prövning av domstol eller tvistlösningsorgan. En datahållare som har begärt en ersättning som bedöms vara diskriminerande och orimlig bör bli återbetalningsskyldig. Vi menar sammantaget att sanktionsavgift inte bör kunna tas ut i dessa situationer.

Vidare menar vi att datahållare inte ska kunna åläggas sanktionsavgifter om de inte kommit överens om skyddsåtgärder enligt artikel 4.6, utan att den överträdelse som ska sanktioneras med sanktionsavgift är den som anges i artikel 4.7. I kapitel V i förordningen är det endast de krav och skyldigheter som anges i artikel 18 och 19 som bör kunna bli föremål för sanktionsavgift. Detta eftersom kraven i artikel 15–17 främst anger förutsättningar för när data får begäras eller anger formkrav för ansökan, vars icke-efterlevnad innebär att begäran inte måste efterföljas. Vidare anser vi inte att artikel 32.2 innebär en självständig skyldighet. Slutligen bedömer vi att bestämmelsen i artikel 33 om deltagare i dataområden som erbjuder data eller datatjänster i nuläget inte är tillräckligt tydlig med avseende på vilka som omfattas av bestämmelsen.

6 Certifiering av tvistlösningsorgan

6.1 Alternativ tvistlösning

Med alternativ tvistlösning avses tvistlösning som sker utanför domstol. Parter i en privaträttslig tvist där förlikning är tillåten är i princip fria att lösa tvisten utanför domstol och kan komma överens om villkoren för förfarandet. Det är också möjligt för dem att använda redan existerande förfaranden där villkoren, eller delar av villkoren, för förfarandet redan är fastslagna. För att vara ett relevant alternativ till ett domstolsförfarande bör ett tvistlösningsförfarande i allmänhet vara snabbt, billigt och enkelt utan att göra avkall på rättssäkerheten. Det ska också uppfylla krav på oberoende, opartiskhet, öppenhet och rättvisa förfaranderegler.

En vanlig form av tvistlösning i kommersiella tvister är skiljeförfarande. Bestämmelser om sådana förfaranden finns i lagen (1999:116) om skiljeförfarande. Parter kan avtala om att tvister mellan dem ska avgöras av en eller flera skiljemän (skiljeavtal). Parterna svarar för kostnaderna för förfarandet och skiljeförfarande har därför inte ansetts lämpligt för tvister mellan näringsidkare och konsument.[1]

Parter kan även komma överens om att anlita en neutral part för att få hjälp att träffa en förlikning (medling) eller enas om att inleda egna förlikningsförhandlingar. Med medling avses i allmänhet ett strukturerat förfarande genom vilket parterna söker lösa den uppkomna tvisten på frivillig väg med hjälp av en utomstående part. I Sverige finns bestämmelser om medling i lagen (2011:860) om medling i vissa privaträttsliga tvister.

Det är alltså i stor utsträckning möjligt att gemensamt bestämma tillvägagångsättet för att lösa en tvist i frågor som parter kan träffa förlikning om. Många av de tvister som kan uppstå mellan parter med anledning av dataförordningens bestämmelser är sådana tvister.

[1] Jfr 6 § lagen (1999:116) om skiljeförfarande.

Det är därför möjligt för parterna, om de inte vill få tvisten prövad i domstol, att komma överens om tillvägagångssättet för att lösa tvisten.

6.2 Dataförordningens bestämmelser om tvistlösningsorgan

Användare, datahållare och datamottagare samt kunder och leverantörer av databehandlingstjänster ska enligt artikel 10 i EU:s dataförordning ha tillgång till ett tvistlösningsorgan som certifierats enligt artikel 10.5 för att lösa vissa tvister. Den medlemsstat där tvistlösningsorganet är etablerat ska, på begäran av det organet certifiera detta organ, om organet kan visa att det uppfyller kraven som anges i artikel 10.5. Det står enligt skäl 52 i förordningen medlemsstaterna fritt att anta särskilda regler för certifieringsförfarandet, bl.a. för certifieringens upphörande eller återkallande. Förordningen ställer enligt samma skäl i förordningen inte krav på medlemsstaterna att inrätta tvistlösningsorgan.

Förordningen ställer inte krav på att ett tvistlösningsorgan måste vara certifierat för att det ska få hantera tvister enligt dataförordningen. Det bör därför stå parterna fritt att komma överens om att hänskjuta till en tvist till ett organ som inte är certifierat.

Tvistlösningsförfarandet är ett frivilligt förfarande och parterna bör enligt skäl 53 i förordningen fritt kunna välja ett tvistlösningsorgan, oavsett om det är i eller utanför de medlemsstater där de själva är etablerade. Av artikel 10.13 framgår att artikel 10 inte påverkar parters rätt att söka ett effektivt rättsmedel inför en domstol i en medlemsstat. Ett beslut av ett tvistlösningsorgan i en tvist är enligt artikel 10.12 bindande för parterna endast om parterna uttryckligen och innan tvistlösningsförfarandet inleds har samtyckt till att beslutet är bindande.

Tvistlösningsorganen får ta ut ta ut avgifter för att hantera tvister och i artikel 10.2 i förordningen föreskrivs vilken part som ska bära avgifterna. När det gäller tvister som hänskjutits enligt artiklarna 4.3, 4.9 och 5.12 ska datahållaren bära alla de avgifter som tas ut av tvistlösningsorganet om tvisten avgörs till förmån för användaren eller datamottagaren. Datahållaren ska också ersätta användaren eller datamottagaren för alla rimliga kostnader som denne har ådragit sig i sam-

band med tvistlösningen. Om tvistlösningsorganet avgör en tvist till förmån för datahållaren ska användaren eller datamottagaren däremot inte vara skyldig att ersätta några avgifter eller andra utgifter som datahållaren har betalat eller ska betala i samband med tvistlösningen. Detta under förutsättning att tvistlösningsorganet inte finner att användaren eller datamottagaren uppenbart har handlat i ond tro.

Tvister som ska kunna hänskjutas till tvistlösningsorgan

Möjligheten att hänskjuta tvister till ett certifierat tvistlösningsorgan är i förordningen särskilt föreskriven gällande vissa tvister.[2] Att användare, datahållare och datamottagare ska ha tillgång till ett certifierat tvistlösningsorgan gäller enligt artikel 10.1 för tvister enligt artiklarna 4.3, 4.9 och 5.12, samt för tvister avseende rättvisa, rimliga och icke-diskriminerande villkor för tillgängliggörande av data på ett öppet sätt i enlighet med kapitel III och IV i förordningen. I dessa artiklar anges att parterna får komma överens om att hänskjuta en tvist till ett tvistlösningsorgan. Det framgår även att detta inte ska påverka rätten till domstolsprövning.

Artikel 4.3 i förordningen gäller tvister mellan användare och datahållare och hänvisar till artikel 4.2. Enligt artikel 4.2 får användare och datahållare genom avtal begränsa eller förbjuda åtkomst till och användning av data eller ytterligare datadelning. Detta under förutsättning att sådan behandling skulle kunna undergräva säkerhetskraven för den uppkopplade produkten, i enlighet med unionsrätten eller nationell rätt, och leda till allvarliga negativa effekter på fysiska personers hälsa, säkerhet eller trygghet. Om en tvist uppstår avseende sådana avtalsbegräsningar eller förbud får parterna enligt artikel 4.3 komma överens om att hänskjuta ärendet till ett tvistlösningsorgan.

Artikel 4.9 hänvisar till punkterna 7 och 8 i artikel 4 som avser tvister som härrör från att en användare vill bestrida en datahållares beslut att vägra, hindra eller avbryta datadelning med hänvisning till skydd för företagshemligheter. Enligt artikel 4.9 får parterna komma överens om att hänskjuta ärendet till ett tvistlösningsorgan. Av artikel 5.12 framgår att tredje part som vill bestrida en datahållares beslut att vägra, hindra eller avbryta datadelning till skydd för företagshem-

[2] Detta bör inte hindra att även andra tvister hänskjuts till tvistlösning om detta avtalas mellan parterna och saken är av sådan art att förlikning är tillåten.

ligheter enligt punkterna 10 och 11 i artikel 5, får komma överens med datahållaren om att hänskjuta ärendet till ett tvistlösningsorgan.

Vidare ska användare, datahållare och datamottagare enligt artikel 10.1 i dataförordningen även ha tillgång till ett tvistlösningsorgan för att lösa tvister avseende rättvisa, rimliga och icke-diskriminerande villkor för tillgängliggörande av data på ett öppet sätt i enlighet med kapitel III och IV. Tvister enligt kapitel III avser tvister om avtalsvillkor enligt vilka datahållare gör data tillgängliga för datamottagare inom ramen för förbindelser mellan företag. Tvister enligt kapitel IV rör oskäliga avtalsvillkor som ensidigt åläggs ett annat företag i samband med dataledning mellan företag.

Enligt artikel 10.4 i förordningen ska kunder och leverantörer av databehandlingstjänster ha tillgång till ett tvistlösningsorgan för att lösa tvister som rör överträdelser av kundernas rättigheter och de skyldigheter leverantörerna har enligt artiklarna 23–31 i förordningen. I dessa artiklar saknas bestämmelser, motsvarande de i artiklarna 4.3, 4.9 och 5.12, om möjligheten komma överens om att hänskjuta ett ärende till ett tvistlösningsorgan. Artikel 10.3, som reglerar fördelningen av avgifter som tvistlösningsorganet tar ut, nämner inte artiklarna 23–31 i förordningen. Det är osäkert om en part ensidigt med stöd av förordningen kan hänskjuta en tvist enligt artikel 10.4 till ett tvistlösningsorgan eller om parterna måste komma överens om det. Det är också osäkert vilken part som i så fall ska bära eventuella avgifter. Vi kan konstatera att artikel 10.4 inte var med i kommissionens ursprungliga förordningsförslag. Artikeln måste därför ha tillkommit under förhandlingarna om förordningen. Möjligen kan detta ha lett till ett förbiseende vad gäller kravet på överenskommelse samt hur eventuella avgifter ska fördelas. Vi har dock inte mandat att fastställa hur förordningen i detta avseende ska tolkas och tillämpas. Det kommer i första hand att vara upp till de certifierade tvistlösningsorganen att tolka och tillämpa bestämmelserna.

Tillgång till certifierade tvistlösningsorgan ska enligt dataförordningen alltså finnas för att lösa tvister mellan å ena sidan datahållare och å andra sidan användare, tredje parter samt datamottagare. Därutöver ska leverantörer av databehandlingstjänster och deras kunder ha tillgång till tvistlösningsorgan för att lösa tvister mellan sig.

6.3 Certifiering av tvistlösningsorgan

Medlemsstaterna ska enligt artikel 10.5 i dataförordningen på begäran av ett tvistlösningsorgan, som är etablerat i medlemsstaten i fråga, certifiera detta organ om det kan visa att det uppfyller samtliga villkor som anges i artikeln.

Certifiering definieras inte i förordningen men en allmän beskrivning av certifiering är att det är ett intygande om att en produkt, en process eller en tjänst uppfyller specifika krav.[3] Certifiering kan ske på olika sätt, det kan t.ex. ske under ackreditering. I Sverige har myndigheten Swedac i uppdrag att vara nationellt ackrediteringsorgan, vilket innebär att myndigheten bl.a. kan ackreditera en organisation som i sin tur kan certifiera andra organ. Ackreditering regleras inom EU i förordningen om krav för ackreditering och marknadskontroll i samband med saluföring av produkter.[4] Den förordningens bestämmelser om ackreditering gäller både inom områden där ackreditering är ett krav och inom områden där ackreditering är frivilligt.[5]

I dataförordningen hänvisas inte till EU-förordningen om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och det finns inget krav på att certifieringen av tvistlösningsorgan måste utföras av ett ackrediterat organ. I dataförordningen föreskrivs inte heller på annat sätt vilken eller vilka aktörer som ska certifiera tvistlösningsorgan. Jämförelse kan göras med EU:s förordning om digitala tjänster[6] där det av artikel 21.3 framgår att samordnaren för digitala tjänster i den medlemsstat där ett tvistlösningsorgan är etablerat ska certifiera organet. Enligt 4 § andra stycket förordningen (2024:958) med kompletterande bestämmelser till EU:s förordning om digitala tjänster är Post- och telestyrelsen (PTS) samordnare för digitala tjänster och är därför också den aktör i Sverige som certifierar tvistlösningsorgan enligt EU:s förordning om digitala tjänster.

Enligt vår bedömning står det varje medlemsstat fritt att välja vilken eller vilka aktörer som certifierar tvistlösningsorgan enligt dataförordningen.

[3] https://www.swedac.se/amnesomraden/produkt-och-processcertifiering/ (hämtad 2025-11-12).
[4] Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och upphävande av förordning (EEG) nr 339/93.
[5] https://www.swedac.se/lag-ratt/eu-lagstiftning/ (hämtad 2025-11-12).
[6] Förordning (EU) 2022/2065 om en inre marknad för digitala tjänster och om ändring av direktiv 2000/31/EG (förordningen om digitala tjänster).

Villkor för certifiering och krav på verksamheten

I artikel 10.5 i dataförordningen fastställs de villkor ett tvistlösningsorgan ska uppfylla för att bli certifierat. Villkoren är följande.

- Tvistlösningsorganet ska vara opartiskt och oberoende, och ska fatta sina beslut i enlighet med tydliga, icke-diskriminerande och rättvisa förfaranderegler.
- Tvistlösningsorganet ska ha den sakkunskap som krävs, i synnerhet när det gäller rättvisa, rimliga och icke-diskriminerande villkor, inbegripet ersättning, och om att göra data tillgängliga på ett öppet sätt, vilket innebär att organet på ett effektivt sätt kan fastställa dessa villkor.
- Tvistlösningsorganet ska enkelt kunna nås genom elektronisk kommunikationsteknik.
- Tvistlösningsorganet ska kunna anta beslut på ett snabbt, effektivt och kostnadseffektivt sätt på minst ett av unionens officiella språk.

I artikel 10.9 i dataförordningen föreskrivs vidare att ett tvistlösningsorgan ska fatta sitt beslut i en fråga som hänskjutits till organet inom 90 dagar efter mottagandet av en begäran enligt artikel 10.1 och 10.4. Beslutet ska vara skriftligt eller på ett varaktigt medium och ska åtföljas av en motivering. Av skäl 52 i förordningen framgår att det i förordningen enbart är de villkor som tvistlösningsorgan måste uppfylla för att bli certifierade som fastställs. Bestämmelserna bör mot bakgrund av det enligt vår uppfattning enbart gälla certifierade organ. Kraven, t.ex. kravet att fatta beslut inom 90 dagar, bör inte förstås som ett generellt krav att alla tvister som avser dataförordningen som hanteras av ett tvistlösningsorgan måste hanteras inom denna tid. Bestämmelserna bör förstås som att kraven gäller om tvisten hanteras av ett certifierat organ.

Enligt artikel 10.6 i förordningen ska medlemsstaterna underrätta kommissionen om de tvistlösningsorgan som certifierats. Kommissionen ska offentliggöra en förteckning över dessa organ på en särskild webbplats som hålls uppdaterad.

6.3.1 Regeringen ska utse en statlig myndighet som certifierande myndighet

Förslag: Det ska i kompletteringslagen föreskrivas att ett tvistlösningsorgan som är etablerat i Sverige får ansöka om att bli certifierat enligt dataförordningen.

Regeringen ska utse en statlig myndighet som certifierar tvistlösningsorgan enligt dataförordningen (certifierande myndighet).

Ett tvistlösningsorgan som uppfyller villkoren i artikel 10.5 i dataförordning ska certifieras av den certifierande myndigheten.

Enligt artikel 10.5 i dataförordningen ska den medlemsstat där tvistlösningsorganet är etablerat på begäran av det organet certifiera detta organ under förutsättning att villkoren för certifiering är uppfyllda. Medlemsstater som saknar en ordning för att certifiera tvistlösningsorgan måste alltså inrätta en sådan ordning. Vår bedömning är att det är upp till respektive medlemsstat att avgöra lämplig ordning för certifiering av tvistlösningsorgan i medlemsstaten. I Sverige finns i dagsläget ingen generell certifieringsordning för tvistlösningsorgan. Det finns exempelvis inte en myndighet som har i uppdrag att certifiera tvistlösningsorgan utifrån olika regelverk. Det finns dock exempel på svenska myndigheter som certifierar eller godkänner tvistlösningsorgan inom vissa områden. Som nämns ovan ska PTS certifiera tvistlösningsorgan enligt EU:s förordning om digitala tjänster. Ett annat exempel är Kammarkollegiet som godkänner tvistlösningsnämnder enligt lagen (2015:671) om alternativ tvistlösning i konsumentförhållanden.[7]

Det skulle ur ett EU-rättsligt perspektiv vara möjligt för regeringen att fatta beslut om att certifiera tvistlösningsorgan. Enligt 4 § lagen om alternativ tvistlösning i konsumentförhållanden får exempelvis regeringen utse en förvaltningsmyndighet att vara nämnd för alternativ tvistlösning enligt lagen, om myndigheten uppfyller kraven för sådana nämnder. Regeringen har utsett Allmänna reklamationsnämnden (ARN) till en sådan nämnd. ARN fanns redan när lagen tillkom och hade bedrivit sin verksamhet under lång tid.

En liknande ordning, dvs. att regeringen fattar beslut om att certifiera tvistlösningsorgan, skulle vara möjlig även för dataförordningen.

[7] 8 b § förordningen (2007:824) med instruktion för Kammarkollegiet.

En sådan ordning kan t.ex. vara lämplig om en myndighet ska certifieras som tvistlösningsorgan. Vi bedömer emellertid att en svensk ordning för certifiering av tvistlösningsorgan enligt dataförordningen bör vara öppen även för andra organ än myndigheter. Sverige bör därför inrätta en certifieringsordning som möjliggör certifiering av privata aktörer och myndigheter. Vi anser att det inte det finns anledning att kräva att certifiering ska göras av ett ackrediterat organ och bedömer att den mest lämpliga ordningen är att en myndighet får i uppdrag att certifiera tvistlösningsorgan enligt dataförordningen, detta oavsett om det organ som ansöker om certifiering är en privat aktör eller en myndighet. Genom att ge en myndighet i uppdrag att certifiera tvistlösningsorgan säkerställer Sverige att sådan certifiering är möjlig, vilket dataförordningen kräver.

Vi föreslår att det i kompletteringslagen föreskrivs att ett tvistlösningsorgan som är etablerat i Sverige får ansöka om att bli certifierat enligt dataförordningen. Bestämmelsen krävs enligt vår uppfattning för att inrätta en ordning för certifiering av tvistlösningsorgan i Sverige. Vidare föreslår vi att regeringen ska utse en statlig myndighet som ska pröva ansökningar från tvistlösningsorgan som vill bli certifierade enligt dataförordningen. Myndigheten ska kallas certifierande myndighet och regeringen ska i kompletteringslagen bemyndigas att bestämma en statlig myndighet som ska vara certifierande myndighet.

Villkoren för att certifieras som tvistlösningsorgan finns i artikel 10.5 i dataförordningen. Vi föreslår att det ska framgå av kompletteringslagen att ett tvistlösningsorgan som uppfyller villkoren i artikel 10.5 i dataförordningen ska certifieras av den certifierande myndigheten. Certifiering kan ske om den certifierande myndigheten efter prövning av en ansökan om certifiering konstaterat att tvistlösningsorganet uppfyller villkoren i artikeln.

6.3.2 Post- och telestyrelsen ska vara certifierande myndighet

Förslag: Post- och telestyrelsen ska vara certifierande myndighet.

Enligt artikel 10.5 b i dataförordningen ska ett tvistlösningsorgan för att bli certifierat ha den sakkunskap som krävs, i synnerhet när det gäller rättvisa, rimliga och icke-diskriminerande villkor, inbegripet

ersättning. Tvistlösningsorganet ska också ha den sakkunskap som krävs om att göra data tillgängliga på ett öppet sätt, vilket innebär att organet på ett effektivt sätt kan fastställa dessa villkor. Kravet på sakkunskap är enligt vår uppfattning centralt i att avgöra vilken myndighet i Sverige som är bäst lämpad att certifiera tvistlösningsorganen. Den myndighet som ska pröva en ansökan om certifiering måste kunna bedöma om tvistlösningsorganet har den sakkunskap som krävs.

Vi har övervägt om Kammarkollegiet bör vara den myndighet som certifierar tvistlösningsorgan enligt förordningen. Enligt 6 § lagen om alternativ tvistlösning i konsumentförhållanden ska en tvistlösningsnämnd godkännas om nämnden uppfyller utpekade krav i direktivet om alternativ tvistlösning (tvistlösningsdirektivet).[8] Kraven för att godkännas som tvistlösningsorgan finns i kapitel II i direktivet. Kraven har många likheter med villkoren för att certifieras som tvistlösningsorgan enligt dataförordningen. I båda rättsakterna finns bl.a. krav på sakkunskap för att ett tvistlösningsorgan ska godkännas respektive certifieras. Kravet på sakkunskap i dataförordningen avser i synnerhet sakkunskap om villkor för tillgängliggörande av data. Av skäl 36 i tvistlösningsdirektivet framgår att kravet på sakkunskap i direktivet avser allmän kännedom om lagen samt tillräckliga allmänna kunskaper om juridiska frågor för att förstå tvistens rättsliga konsekvenser, det krävs inte yrkesmässiga juridiska kvalifikationer. Trots likheterna mellan villkoren i dataförordningen och kraven i tvistlösningsdirektivet bedömer vi att prövningen skiljer sig åt mellan de olika rättsakterna. När det gäller certifieringen av tvistlösningsorgan enligt dataförordningen kommer det enligt vår uppfattning vara av särskild vikt att kunna bedöma tvistlösningsorganets sakkunskap om tillgängliggörande av data.

Dataförordningen ställer omfattande krav på de myndigheter som utses till behöriga myndigheter i medlemsstaterna. Enligt artikel 37.9 i förordningen ska medlemsstaterna säkerställa att de behöriga myndigheterna har tillräckliga personalresurser, tekniska resurser och relevant sakkunskap för att de på ett effektivt sätt kunna utföra sina uppgifter i enlighet med förordningen. Behöriga myndigheter kommer

[8] Europaparlamentets och rådets direktiv 2013/11/EU av den 21 maj 2013 om alternativ tvistlösning vid konsumenttvister och om ändring av förordning (EG) nr 2006/2004 och direktiv 2009/22/EG (direktivet om alternativ tvistlösning).

att ha god kunskap om förordningen och om tillgängliggörande av data.

Vår sammanvägda bedömning är att det är en den myndighet som är behörig myndighet enligt förordningen som är bäst lämpad att bedöma om ett tvistlösningsorgan uppfyller villkoren för att bli certifierat.[9] En myndighet som inte är en behörig myndighet skulle behöva bygga upp kompetens som enbart gäller för certifieringen, vilket inte skulle vara en effektiv användning av resurser. En annan myndighet än en behörig myndighet kan för certifieringen inte dra nytta av kunskapen om förordningen som byggs upp i andra delar av verksamheten.

Regeringen har utsett PTS till behörig myndighet enligt dataförordningen (se kapitel 4). Vi föreslår därför att PTS också ska vara certifierande myndighet, dvs. den myndighet som i Sverige certifierar tvistlösningsorgan enligt förordningen.

6.3.3 En certifiering ska gälla tills vidare

Förslag: Certifiering av ett tvistlösningsorgan ska gälla tills vidare.

I dataförordningen regleras inte om certifiering av ett tvistlösningsorgan ska vara tidsbegränsat eller om certifieringen ska gälla tills vidare. Enligt skäl 52 i förordningen står det medlemsstaterna fritt att anta särskilda regler för certifieringsförfarandet, bl.a. för certifieringens upphörande eller återkallande. Vi har övervägt om certifiering av ett tvistlösningsorgan ska vara tidsbegränsad och gälla i exempelvis tre eller fem år. Ett skäl att tidsbegränsa en certifiering är att med jämna mellanrum låta det aktuella tvistlösningsorganet genom en ny ansökan visa att det fortfarande uppfyller kraven för certifiering i dataförordningen. Vår bedömning är dock att en certifiering inte bör vara tidsbegränsad. Skälen till detta är följande.

Enligt artikel 10.10 i förordningen ska tvistlösningsorganen utarbeta och offentliggöra årliga verksamhetsrapporter. Rapporterna ska innehålla en sammanställning av utgången av tvister, den genomsnittliga tid det har tagit att lösa tvister samt de vanligaste skälen

[9] Vi noterar att den tyska regeringen i sitt utkast till lag om genomförande av dataförordningen, publicerat den 7 februari 2025, föreslår att den behöriga myndigheten får i uppdrag att hantera ansökningar och att certifiera tvistlösningsorgan (2 och 5 §§)

till tvister. Rapporterna kommer att ge insyn i tvistlösningsorganens verksamhet.

Om det inte finns indikationer på att ett tvistlösningsorgan inte längre uppfyller villkoren för certifiering framstår det som onödigt att med jämna mellanrum kräva en ny ansökan om certifiering. Vår bedömning är att den insyn som de årliga rapporterna ger samt möjligheten för den certifierande myndigheten att återkalla en certifiering är tillräckliga för att säkerställa att ett tvistlösningsorgan uppfyller villkoren för certifiering över tid. Vi föreslår därför att en certifiering av ett tvistlösningsorgan ska gälla tills vidare. Den certifierande myndigheten bör dock kunna återkalla en certifiering (se avsnitt 6.3.5).

6.3.4 Den certifierande myndigheten får ta ut avgift för att pröva en ansökan om certifiering

Förslag: Den certifierande myndigheten får ta ut avgift för att pröva en ansökan om certifiering.

Det ska framgå av författning att myndigheten får ta ut avgift och att myndigheten får meddela föreskrifter om avgiftens storlek.

Avgiften ska beräknas utifrån principen om full kostnadstäckning.

Prövningen av en ansökan från ett tvistlösningsorgan om att certifieras kommer att vara förenad med kostnader hos myndigheten som gör prövningen. Myndigheten måste utreda om tvistlösningsorganet lever upp till villkoren för certifiering i dataförordningen. Det är frivilligt för ett tvistlösningsorgan att ansöka om certifiering enligt förordningen. Certifierade tvistlösningsorgan får ta ut avgift för sin verksamhet och det kan finnas ekonomisk vinning för organen att bli certifierade. Enligt vår uppfattning ska PTS, i egenskap av certifierande myndighet, få ta ut avgift från det ansökande tvistlösningsorganet för att pröva ansökan.

Storleken på avgiften ska fastställas av PTS. Bestämmelser om avgifter finns i avgiftsförordningen (1992:191). Av 9 § framgår att förordningens bestämmelser om avgifter som statliga myndigheter ska ta ut för prövning av ärenden gäller när det är särskilt föreskrivet. Vi föreslår att det i författning ska föreskrivas att myndigheten får ta ut avgift för prövning av ansökan om certifiering.

Enligt 5 § andra stycket avgiftsförordningen är huvudregeln att avgifter ska beräknas så att de helt täcker verksamhetens kostnader (full kostnadstäckning). Huvudregeln gäller om regeringen inte har föreskrivit något annat. Att certifieras enligt dataförordningen är som tidigare nämnts frivilligt för tvistlösningsorgan. Avsaknad av certifiering hindrar inte att ett tvistlösningsorgan hanterar tvister enligt förordningen. Det saknas skäl att frångå huvudregeln i avgiftsförordningen och avgiften för prövning av ansökan om certifiering ska av PTS därför beräknas utifrån full kostnadstäckning.

I förordningen (2016:602) om finansiering av Post- och telestyrelsens verksamhet finns bestämmelser om hur myndighetens verksamhet ska finansieras. I förordningen bestäms storleken på vissa avgifter som myndigheten får ta ut och för vissa avgifter fastställs ett högsta belopp för avgifternas storlek. PTS bemyndigas dessutom i 12 § i förordningen att meddela närmare föreskrifter om avgifterna. Myndigheten har meddelat bestämmelser om avgifternas storlek i Post- och telestyrelsens föreskrifter om avgifter (PTSFS 2024:3). Vi föreslår att denna ordning ska gälla även för avgifter för certifiering av tvistlösningsorgan enligt dataförordningen. Det ska i förordningen (2016:602) om finansiering av Post- och telestyrelsens verksamhet emellertid inte fastställas ett högsta belopp för avgiftens storlek. PTS ska fastställa avgiftens storlek utifrån huvudregeln att avgifterna ska täcka verksamhetens kostnader för prövning av ansökan.

6.3.5 En certifiering får återkallas

Förslag: Den certifierande myndigheten får återkalla en certifiering.

Ett beslut av den certifierande myndigheten att certifiera ett tvistlösningsorgan innebär att myndigheten anser att organet uppfyller kraven för certifiering i dataförordningen. Det ger parterna trygghet, som i och med certifiering inte själva behöver göra bedömningen. Förordningen innehåller inga bestämmelser om återkallelse av certifiering men av skäl 52 i förordningen framgår det står medlemsstaterna fritt att anta särskilda regler för certifieringsförfarandet, bl.a. för certifieringens upphörande eller återkallande.

Om ett certifierat tvistlösningsorgan inte längre uppfyller kraven i förordningen måste den behöriga myndigheten enligt vår uppfattning kunna återkalla certifieringen. Frånvaro av en sådan möjlighet kan påverka parternas förtroende för certifieringsordningen och de certifierade tvistlösningsorganen. Det framgår av skäl 52 i förordningen att det står medlemsstaterna fritt att anta regler för återkallande. Att i Sverige göra det möjligt att återkalla en certifiering står alltså inte i strid med förordningen.

Om den behöriga myndigheten efter en utredning finner att ett certifierat organ inte längre uppfyller kraven i dataförordningen ska myndigheten fatta beslut om att återkalla certifieringen.

6.3.6 Beslut att neka eller återkalla certifiering kan överklagas

Förslag: Beslut av den certifierande myndigheten att neka certifiering kan överklagas till allmän förvaltningsdomstol.

Beslut av den certifierande myndigheten att återkalla en certifiering kan överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs för överklagande till kammarrätt.

Om den certifierande myndigheten i sin prövning av en ansökan om certifiering finner att det aktuella tvistlösningsorganet inte lever upp till villkoren som ställs i dataförordningen kan myndigheten fatta beslut om att neka certifiering. Allmänna bestämmelser om överklagande av beslut av myndigheter finns i förvaltningslagen (2017:900). Enligt 41 § får ett beslut överklagas om beslutet kan antas påverka någons situation på ett inte obetydligt sätt. Ett beslut att neka certifiering har en sådan påverkan på det tvistlösningsorgan som har ansökt om certifieringen. Tvistlösningsorganet skulle i och för sig kunna överklaga ett sådant beslut med stöd av förvaltningslagen. Vår uppfattning är dock att det av tydlighetskäl uttryckligen ska framgå av kompletteringslagen att beslut att inte certifiera ett tvistlösningsorgan ska kunna överklagas.

Allmän förvaltningsdomstol är som huvudregel rätt domstol för enskilds överklagande av myndighetsbeslut enligt 40 § förvaltningslagen. Vår uppfattning är att ett beslut om certifiering som går sökanden emot är ett beslut som omfattas av huvudregeln och överklagande ska därför ske vid allmän förvaltningsdomstol.

För det fall myndigheten fattar beslut om att återkalla en certifiering ska även ett sådant beslut kunna överklagas. Ett sådant överklagande ska också ske vid allmän förvaltningsdomstol.

Som huvudregel krävs prövningstillstånd vid överklagande till kammarrätten. Vi har inte funnit skäl att frångå denna ordning. Prövningstillstånd ska därför krävas vid överklagande till kammarrätt.

6.4 Tillgång till alternativ tvistlösning

6.4.1 Möjligheter till tvistlösning utanför domstol i Sverige

Vi har i uppdrag att analysera befintliga möjligheter till tvistlösning genom tvistlösningsorgan. Analysen presenteras i detta avsnitt.

På konsumentområdet finns regler om nämnder för tvistlösning i tidigare nämnda lagen om alternativ tvistlösning i konsumentförhållanden. Lagen genomför tvistlösningsdirektivet. Lagen gäller för tvistlösning som initieras av en konsument avseende hans eller hennes anspråk mot en näringsidkare och innehåller bestämmelser om hur sådana nämnder utses och godkänns. Det krävs alltså inte att parterna kommer överens om att hänskjuta tvisten till en tvistlösningsnämnd, vilket annars som framgår ovan är den vanliga modellen. Kammarkollegiet har i uppdrag att godkänna tvistlösningsnämnder enligt lagen och kraven för godkännande berörs i avsnitt 6.3.2 ovan.

ARN är en förvaltningsmyndighet som prövar tvister mellan konsumenter och företag och är genom sin instruktion en nämnd för alternativ tvistlösning som avses i 4 § första stycket lagen om alternativ tvistlösning i konsumentförhållanden.[10] Ett beslut som fattas av ARN utgör en rekommendation om hur den aktuella tvisten ska lösa och är inte bindande. Företag kan dock ha åtagit sig att följa beslut av ARN, t.ex. genom medlemskap i en branschorganisation.[11] ARN tillämpar värdegränser för det krav konsumenten har på företaget. Gränserna skiljer sig åt mellan olika ärendekategorier.[12] Utöver ARN finns det i skrivande stund sex godkända tvistlösnings-

[10] 1 § förordningen (2015:739) med instruktion för Allmänna reklamationsnämnden.
[11] Ett exempel är Motorbranschens riksförbund, https://www.mrf.se/radgivningny/juridik/arn/ (hämtad 2025-11-12).
[12] https://www.arn.se/tvisteomraden/ (hämtad 2025-11-12).

nämnder i Sverige som har godkänts av Kammarkollegiet.[13] Exempel på sådana nämnder är Fastighetsmarknadens reklamationsnämnd och Nämnden för Rättsskyddsfrågor.

Utanför konsumentområdet finns det inte några särskilda bestämmelser om nämnder för tvistlösning (annat än i fråga om skiljenämnder). Det är emellertid inte ovanligt att privata nämnder prövar tvister mellan enskilda. Det förekommer exempelvis att parter i kommersiella förhållanden kommer överens om att inrätta en särskild nämnd i anslutning till ett specifikt projekt och åtar sig följa nämndens slutsatser under de förutsättningar som följer av deras överenskommelse. Det finns även organ som erbjuder skiljeförfarande och andra tvistlösningsformer som tjänster. Ett exempel på ett sådant organ är SCC Skiljedomsinstitut i Stockholm (SCC) som är ett skiljedomsinstitut för svenska och internationella tvister.[14] Det utgör en enhet inom Stockholms Handelskammare. SCC har vid kontakt med oss uppgett att institutet bedömer att det skulle kunna hantera i alla fall vissa av de tvister som kan uppstå mot bakgrund av dataförordningen.

Att myndigheter erbjuder tvistlösning förekommer även utanför konsumentområdet i Sverige. PTS kan exempelvis pröva tvister mellan företag enligt lagen (2022:482) om elektronisk kommunikation (LEK) och EU:s gigabitinfrastrukturförordning.[15] PTS är behörig att pröva tvister i alla frågor som har sin grund i skyldigheter som följer av LEK eller har beslutats med stöd av den lagen (prop. 2021/22:136 s. 348). Tvistlösningen kan t.ex. gälla tolkning av skyldigheter som beslutats för operatörer med betydande marknadsinflytande eller villkor för utlämnande av abonnentuppgifter. Tvistlösningen kan således avse två företag som genom tvistlösningen kan få stöd i tolkningen av ett beslut som fattats inom ramen för PTS regulatoriska verksamhet. Om det med hänsyn till den frågeställning som tvisten aktualiserat är lämpligare att den avgörs genom en åtgärd inom ramen för den allmänna tillsynen, får tillsynsmyndigheten besluta att inte ta upp tvisten för avgörande. Tvister enligt LEK är numera ovanliga.

[13] https://www.kammarkollegiet.se/vara-tjanster/alternativ-tvistlosning/ansok-om-att-bli-namnd-for-alternativ-tvistlosning/godkanda-namnder-for-alternativ-tvistlosning (hämtad 2025-11-12).
[14] https://sccarbitrationinstitute.se/sv/ (hämtad 2025-11-19).
[15] Europaparlamentets och rådets förordning (EU)2024/1309 av den 29 april 2024 om åtgärder för att minska kostnaderna för utbyggnad av gigabitnät för elektronisk kommunikation, om ändring av förordning (EU) 2015/2120 och om upphävande av direktiv 2014/61/EU (gigabitinfrastrukturförordningen). Förordningen ska tillämpas från och med den 12 november 2025.

Tvistlösning enligt lagen (2016:534) om åtgärder för utbyggnad av bredbandsnät, som ersätts av gigabitinfrastrukturförordningen, avser tolkning av skyldigheter som anges i lagen. Sedan lagen trädde i kraft 2016 har PTS hanterat ett tiotal tvister.

6.4.2 Tillgången till certifierade tvistlösningsorgan bör utvärderas längre fram

Det är i dagsläget inte möjligt för tvistlösningsorgan att bli certifierade enligt dataförordningen i Sverige. Vi lämnar i detta kapitel ett förslag till en ordning för sådan certifiering. Det har inte varit möjligt för oss att bilda en uppfattning om i vilken omfattning tvistlösningsorgan som är etablerade i Sverige kommer att vilja bli certifierade enligt förordningen. Det kan dock konstateras att många av de tvistlösningsorgan som i dag finns inte hanterar tvister inom samma härad som i framtiden kan uppstå mot bakgrund av dataförordningens bestämmelser. Ett flertal av organen hanterar en avgränsad kategori tvister om rör specifika områden eller specifika varor och tjänster. Det finns emellertid också tvistlösningsorgan som kan hantera många olika typer av tvister. Som framgår ovan bedömer SCC att de kan hantera i alla fall vissa av de tvister som kan uppstå mot bakgrund av dataförordningen.

Enligt vår uppfattning bör tillgången till certifierade tvistlösningsorgan utvärderas när dataförordningen har tillämpats en tid. Det kan noteras att regeringen gjorde en liknande bedömning vad gäller behovet av tvistlösning utanför domstol enligt EU:s förordning om digitala tjänster. Regeringen ansåg att en utvärdering av behovet bör göras när förordningen varit i kraft under en tid (prop. 2023/24:160 s. 99). Vi menar att utvärderingen av behovet enligt den förordningen också bör inkludera en utvärdering av behovet samt tillgången till certifierade tvistlösningsorgan enligt dataförordningen. Utredningen om kompletterande bestämmelser till EU:s förordning om en inre marknad för digitala tjänster redovisade i sitt slutbetänkande en genomgång av olika alternativ för det fall Sverige vill inrätta ett tvistlösningsorgan enligt EU:s förordning om digitala tjänster (SOU 2023:39 s. 169–174). Genomgången av alternativ är relevant också för ett eventuellt framtida inrättande av ett tvistlösningsorgan enligt dataförordningen.

7 Offentliga organ får begära data vid exceptionella behov

7.1 Inledning

Nationella offentliga organ och organ på EU-nivå kan med stöd av kapitel V i dataförordningen begära data från företag om organet i fråga har ett exceptionellt behov av dessa data, exempelvis för att hantera ett allmänt nödläge. Syftet med kapitlet är enligt skäl 70 i förordningen att säkerställa att dessa organ har den kunskap som krävs för att hantera, förhindra eller bidra till återhämtningen från allmänna nödlägen eller att bidra till fullgörandet av specifika uppgifter som uttryckligen föreskrivs i lag. I samband med att kommissionen presenterade sitt förslag till dataförordning konstaterade den att data är nödvändiga för framtagande av bättre policy och offentliga tjänster. Vidare konstaterades att offentliga organ vanligen får tillgång till data från den privata sektorn genom rapporteringskrav, offentlig upphandling eller frivillig datadelning. Kommissionen ansåg dock att sådana lösningar visade på tydliga begränsningar, bl.a. att de tar för lång tid. Kommissionen hänvisade till covid-19-pandemin och menade att pandemin bekräftade svårigheter att snabbt få tillgång till nödvändiga data för krishantering och att etablerade processer för att få tillgång till sådana data saknades.[1]

I Sverige finns ingen motsvarighet till kapitel V i dataförordningen. Även i Sverige har dock behovet av data för att hantera krissituationer identifierats. Coronakommissionen konstaterade t.ex. i sitt slutbetänkande att svenska myndigheter hade ett stort behov av data under covid-19-pandemin och att det ibland var svårt eller fanns hinder mot att få tillgång till data (SOU 2022:10 s. 551 ff.). Vidare har Utredningen om interoperabilitet vid datadelning konstaterat

[1] European Commission, Commission Staff Working Document, Impact Assessment Report, SWD (2022) 34 final s. 12.

att data behövs när kriser uppstår och att behov av nya datadelningar kan uppstå snabbt i en krissituation (SOU 2023:96 s. 63–64).

7.1.1 Kapitel V ersätter inte andra krav på datadelning

Kapitel V ska enligt artikel 16.1 i dataförordningen inte påverka de skyldigheter som fastställs i unionsrätten eller nationell rätt vad gäller rapportering eller att tillmötesgå begäranden om åtkomst till information eller visa eller kontrollera efterlevnaden av rättsliga skyldigheter.[2] Enligt skäl 66 i förordningen bör förordningen inte tillämpas på eller föregripa frivilliga arrangemang för utbyte av data mellan privata och offentliga enheter, inbegripet mikroföretags och små och medelstora företags tillhandahållande av data. Förordningen påverkar inte tillämpningen av unionsrättsakter som föreskriver att offentliga enheter ska begära information från privata enheter. Vidare framgår av skäl 66 att skyldigheter för datahållare att tillhandahålla data som motiveras av behov av icke-exceptionell art, i synnerhet när datauppsättningen och datahållarna är kända eller dataanvändningen kan ske regelbundet, såsom är fallet med rapporteringsskyldigheter och skyldigheter kopplade till den inre marknaden, inte bör påverkas av förordningen.

7.2 Vilka får begära data?

7.2.1 Offentliga organ enligt dataförordningen

De aktörer som kan begära data vid exceptionella behov är offentliga organ, kommissionen, Europeiska centralbanken samt unionsorgan. Offentliga organ definieras i artikel 2.28 i dataförordningen som medlemsstaternas nationella, regionala eller lokala myndigheter och medlemsstaternas offentligrättsliga organ, eller sammanslutningar som bildats av en eller flera sådana myndigheter eller ett eller flera sådana organ. Offentligrättsliga organ definieras inte i förordningen, däremot förekommer och definieras begreppet i ett flertal andra EU-

[2] Bestämmelsen är enklare att förstå i den engelska språkversionen av förordningen: This Chapter shall not affect the obligations laid down in Union or national law for the purposes of reporting, complying with requests for access to information or demonstrating or verifying compliance with legal obligations.

rättsakter. T.ex. definieras begreppet i artikel 2.4 i direktivet om offentlig upphandling[3] som organ som har samtliga följande egenskaper:

- De har särskilt inrättats för att tillgodose behov i det allmännas intresse, utan industriell eller kommersiell karaktär.
- De är juridiska personer.
- De finansieras till största delen av statliga, regionala eller lokala myndigheter, eller av andra offentligrättsliga organ, eller står under administrativ tillsyn av sådana myndigheter eller organ; eller de har ett förvaltnings-, lednings- eller kontrollorgan där mer än hälften av ledamöterna utses av staten, regionala eller lokala myndigheter, eller av andra offentligrättsliga organ.

Samma definition återfinns även i bl.a. artikel 2.18 i dataförvaltningsförordningen[4] och artikel 2.2 i öppna data-direktivet[5]. Definitionen innebär att även företag som uppfyller kriterierna ovan kan vara offentligrättsliga organ. Vår bedömning är att begreppet offentligrättsligt organ i dataförordningen bör ha samma innebörd som inom upphandlingsområdet. Det finns inga omständigheter som enligt vår mening talar emot en sådan tolkning.

När det kommer till organ på EU-nivå kräver kommissionen och Europeiska centralbanken ingen vidare förklaring. Unionsorgan definieras i artikel 2.27 i dataförordningen som de unionsorgan och unionsbyråer som inrättats genom eller enligt akter som antagits på grundval av fördraget om Europeiska unionen, EUF-fördraget eller fördraget om upprättandet av Europeiska atomenergigemenskapen. Exempel på unionsorgan är Europeiska datatillsynsmannen, EU:s smittskyddsmyndighet samt Europeiska kemikaliemyndigheten.

Myndigheter som utses till behöriga myndigheter enligt dataförordningen är offentliga organ. Av skäl 107 i förordningen framgår dock att behöriga myndigheter som ansvarar för tillämpningen och efterlevnaden av förordningen inte bör ha rätt att lämna in en begäran om tillgängliggörande av data mot bakgrund av ett exceptionellt behov. Detta för att undvika intressekonflikter.

[3] Europaparlamentets och rådets direktiv 2014/24/EU av den 26 februari 2014 om offentlig upphandling och om upphävande av direktiv 2004/18/EG.
[4] Europaparlamentets och rådets förordning (EU) 2022/868 av den 30 maj 2022 om europeisk dataförvaltning och om ändring av förordning (EU) 2018/1724 (dataförvaltningsakten).
[5] Europaparlamentets och rådets direktiv (EU) 2019/1024 av den 20 juni 2019 om öppna data och vidareutnyttjande av information från den offentliga sektorn.

7.2.2 Offentliga organ i Sverige

Uttrycket myndighet används i Sverige för organ som utövar offentlig makt och som är organiserade i offentligrättsliga former. I Sverige finns formellt statliga och kommunala förvaltningsmyndigheter (1 kap. 8 § regeringsformen). Även domstolarna är myndigheter. I Sverige finns också regionala myndigheter som formellt sett är kommunala myndigheter enligt regeringsformen. Svenska statliga, regionala och kommunala myndigheter är offentliga organ enligt definitionen i dataförordningen.

Ovan konstaterar vi att begreppet offentligrättsliga organ i dataförordningen bör ges samma innebörd som inom upphandlingsområdet. Upphandlingsregelverket inom EU har genomförts i svensk rätt genom bl.a. lagen (2016:1145) om offentlig upphandling (LOU). I LOU används begreppet offentligt styrt organ. Enligt 1 kap. 18 § LOU avses med offentligt styrt organ en juridisk person som tillgodoser behov i det allmännas intresse, under förutsättning att behovet inte är av industriell eller kommersiell karaktär och uppfyller något av följande villkor.

- Är till största delen finansierad av staten, en kommun, en region eller en upphandlande myndighet.
- Verksamheten står under kontroll av staten, en kommun, en region eller en upphandlande myndighet.
- I styrelsen eller motsvarande ledningsorgan är mer än halva antalet ledamöter utsedda av staten, en kommun, en region eller en upphandlande myndighet.

Definitionen innebär att statliga och kommunala bolag kan vara offentligt styrda organ. Bedömningen av om ett organ tillgodoser ett allmännyttigt behov som inte är av industriell eller kommersiell karaktär är inte alltid en enkel bedömning och det finns omfattande praxis på både EU-nivå och nationell nivå (prop. 2017/18:299 s. 32). Vår uppfattning är att mycket talar för att bolag som omfattas av definitionen av offentligt styrda organ i LOU är offentliga organ enligt definitionen i dataförordningen.[6] Att bedömningen för offentligt styrda organ måste göras från fall till fall kan tyckas vara otillfredsställande. Det är dock troligt att svenska aktörer redan har bedömt

[6] Se prop. 2017/18:299 s. 32 för liknande bedömning.

om de omfattas av definitionen i LOU eller inte, vilket alltså kan få bäring på möjligheterna att tillämpa kapitel V i dataförordningen.

Post- och telestyrelsen (PTS) är behörig myndighet enligt dataförordningen i Sverige. För att undvika intressekonflikter bör myndigheten i enlighet skäl 107 i förordningen inte ha rätt att begära data med stöd av kapitel V i förordningen.

7.2.3 Offentliga organ inom brott-, tull- och skatteområdet får inte begära data

Enligt artikel 16.2 i dataförordningen ska kapitel V inte tillämpas på offentliga organ, kommissionen, Europeiska centralbanken eller unionsorgan som bedriver verksamhet som syftar till att förebygga, förhindra, utreda, upptäcka eller lagföra brott eller administrativa överträdelser eller verkställa straffrättsliga påföljder, eller på tull- eller skatteförvaltning. Enligt skäl 68 i förordningen bör dessa aktörer förlita sig på sina befogenheter enligt unionsrätten eller nationell rätt för utövandet av sina uppgifter inom dessa områden. Av samma skäl framgår att förordningen därmed inte påverkar lagstiftningsakter om delning eller användning av data eller åtkomst till data inom dessa områden.

Offentliga organ som bedriver verksamhet för att exempelvis utreda eller upptäcka brott eller inom tull- eller skatteförvaltning, vilka i regel är myndigheter, kan därför inte begära data inom ramen för denna verksamhet med stöd av kapitel V i förordningen. De får i stället förlita sig på annat författningsstöd eller andra åtgärder om de har behov av att begära data.

7.3 Vad är lagstadgade skyldigheter av allmänt intresse?

7.3.1 Allmänt intresse i dataförordningen

Möjligheten att begära data gäller enligt artikel 14 i dataförordningen endast när aktören som begär data ska fullgöra sina lagstadgade skyldigheter av allmänt intresse. Vad som avses med allmänt intresse framgår inte tydligt av förordningen. Den begränsade vägledning som ges finns i skäl 65 i förordningen. Där framgår att det offentliga organet

bör visa att de data som begärs är nödvändiga för att utföra en specifik uppgift av allmänt intresse som uttryckligen föreskrivs i lag, såsom framställningen av officiell statistik eller begränsning av eller återhämtning från ett allmänt nödläge.

Begreppet allmänt intresse är ett EU-rättsligt begrepp som förekommer i ett flertal andra EU-rättsakter, exempelvis i EU:s dataskyddsförordning[7]. Det finns också praxis från EU-domstolen avseende allmänt intresse. Det går emellertid inte att ge en detaljerad definition av allmänt intresse eller dra en tydlig gräns för vad som är allmänt intresse och inte, men det omfattar bl.a. sådant som folkhälsa, säkerhet och samhällets övergripande funktion. En bedömning av om ett intresse är ett allmänt intresse måste göras utifrån sammanhanget.

7.3.2 Lagstadgade skyldigheter av allmänt intresse i Sverige

Allmänt intresse definieras alltså inte i dataförordningen. Begreppet förekommer emellertid i andra EU-rättsakter och har behandlats inom ramen för införandet av svenska kompletterande bestämmelser till dem. Vi bedömer att de resonemang som fördes avseende allmänt intresse vid införandet av kompletterande bestämmelser till dataskyddsförordningen är av intresse när det gäller dataförordningen.

I propositionen till de bestämmelserna uttalade regeringen att den ansåg att alla uppgifter som riksdag eller regering gett i uppdrag åt statliga myndigheter att utföra är av allmänt intresse. Om uppgifterna inte vore av allmänt intresse skulle myndigheterna inte ålagts att utföra dem. På motsvarande sätt ansåg regeringen att de obligatoriska uppgifter som ålagts kommuner och regioner att utföra är av allmänt intresse. Regeringen menade emellertid också att begreppet uppgifter av allmänt intresse inte bara omfattar sådant som utförs som en följd av ett offentligrättsligt och uttryckligt åliggande eller uppdrag. Som en följd av det kommunala självstyret har kommuner och regioner vidsträckt möjlighet att utföra frivilliga åtaganden. Befogenheten är emellertid enligt kommunallagen (2017:725) begränsad till angelägenheter av just allmänt intresse. Kommuner och regioner får driva näringsverksamhet, men bara om den drivs utan vinstsyfte och syftar till att tillhandahålla allmännyttiga anläggningar eller tjänster åt med-

[7] Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

lemmarna. Som exempel på sådana uppgifter av allmänt intresse som kommunerna utför på frivillig grund anförde regeringen tillhandahållande av bostäder och fritids- och idrottsanläggningar, åtgärder för att främja ortens näringsliv och annan kulturell verksamhet än bibliotek. Regeringen påpekade också att vissa myndigheter, t.ex. Lantmäteriet, har getts befogenhet av riksdagen eller regeringen att bedriva viss uppdragsverksamhet. Regeringen ansåg att även denna typ av verksamhet måste anses vara motiverad av ett allmänt intresse. Sammanfattningsvis ansåg regeringen att den verksamhet som en statlig eller kommunal myndighet bedriver, inom ramen för sin befogenhet, är av allmänt intresse (prop. 2017/18:105 s. 56–57).

Uttalandena från regeringen är enligt vår uppfattning en bra utgångspunkt även för bedömningen av allmänt intresse i dataförordningen. Skillnaderna mellan förordningarna måste dock beaktas. I dataskyddsförordningen föreskrivs inget uttryckligt krav på lagstadgade skyldigheter av allmänt intresse, vilket är ett krav i dataförordningen. I stället föreskrivs i artikel 6.1 e i dataskyddsförordningen att behandlingen ska vara nödvändig för att utföra en uppgift av allmänt intresse (eller som ett led i den personuppgiftsansvariges myndighetsutövning). Skillnaden mellan lagstadgad skyldighet av allmänt intresse och att utföra en uppgift av allmänt intresse är relevant för bedömningen av vad som avses i dataförordningen. Vår uppfattning är att formuleringen i dataförordningen ger uttryck för ett snävare tillämpningsområde än dataskyddsförordningen.

Av skäl 65 i dataförordningen framgår att det offentliga organet bör visa att begärda data är nödvändiga för att utföra en specifik uppgift av allmänt intresse som uttryckligen föreskrivs i lag, såsom framställningen av officiell statistik eller begränsning av eller återhämtning från ett allmänt nödläge. Uppräkningen är inte uttömmande. Av artikel 17.1 h i dataförordningen framgår att parten som begär data ska ange den rättsliga bestämmelse som tilldelar parten den specifika uppgift av allmänt intresse som är relevant för begäran om data. Det indikerar enligt oss att den specifika uppgiften ska vara tydligt definierad i författning.

Detta innebär enligt vår uppfattning bl.a. att sådant som omfattas av det frivilliga området i kommunallagen inte är aktuellt. Inte heller bör t.ex. uppgifter som ges till statliga myndigheter genom regeringsuppdrag omfattas. Det krävs emellertid inte att uppgiften är före-

skriven i lag. Den kan också föreskrivas i förordning eller i en EU-rättsakt.

Sammanfattningsvis bör en lagstadgad skyldighet av allmänt intresse i Sverige innebära att det är en specifik uppgift som har ålagts ett offentligt organ i svensk lag eller förordning eller i en EU-rättsakt.

7.4 Data kan begäras från företag

Enligt kapitel V i dataförordningen är det datahållare som ska göra data tillgängliga efter begäran. I artikel 2.13 i förordningen definieras en datahållare som ”en fysisk eller juridisk person som har en rätt eller skyldighet, i enlighet med dataförordningen, tillämplig unionsrätt eller nationell lagstiftning som antagits i enlighet med unionsrätten, att använda och tillgängliggöra data, inbegripet produktdata eller data från tillhörande tjänster som denne har hämtat eller genererat under tillhandahållandet av en tillhörande tjänst, om detta avtalats”. Enligt definitionen kan en datahållare alltså vara en fysisk eller juridisk person. När begreppet datahållare används i kapitel V omfattas emellertid inte hela kretsen av aktörer som annars omfattas av definitionen. I artikel 14 föreskrivs nämligen att det är datahållare som är andra juridiska personer än offentliga organ som ska göra data tillgängliga.

Det innebär att ett offentligt organ inte kan begära data från en fysisk person och att offentliga organ inte kan begära data av andra offentliga organ. De kan endast begära data från juridiska personer som inte är offentliga organ.

Enligt skäl 25 och 63 i förordningen omfattar begreppet datahållare i allmänhet inte offentliga organ men det kan, enligt skältexterna, omfatta offentliga företag. Texten antyder att offentliga organ i allmänhet inte är datahållare men att offentliga företag kan vara det. Som vi har konstaterat ovan kan definitionen av offentliga organ omfatta t.ex. kommunala bolag om kriterierna för ett offentligrättsligt organ är uppfyllda. Frågan som uppstår är om exempelvis en statlig myndighet kan begära data från ett offentligt företag eftersom sådana företag kan vara datahållare enligt förordningen.

Offentliga företag definieras inte i dataförordningen. Däremot finns en definition i kommissionens direktiv om insyn i de finansiella

förbindelserna mellan medlemsstater och offentliga företag[8]. I artikel 2 b i direktivet definieras offentliga företag som varje företag, över vilket de offentliga myndigheterna direkt eller indirekt kan utöva ett dominerande inflytande till följd av ägarskap, finansiell medverkan eller gällande regler. Ett företag som uppfyller kriterierna för ett offentligrättsligt organ bör enligt vår bedömning i vissa fall också kunna omfattas av definitionen av ett offentligt företag i kommissionens direktiv.

Det som är avgörande för bedömningen när det gäller möjligheterna att begära data med stöd av kapitel V i dataförordningen är om aktören är ett offentligt organ eller inte. Detta eftersom ett offentligt organ inte får begära data från ett annat offentligt organ. Definitionen av offentligt organ i artikel 2.28 i dataförordningen bör innebära att om ett företag uppfyller kriterierna för ett offentligrättsligt organ så är det ett offentligt organ. Om företaget är ett offentligt företag eller inte bör vara av underordnad betydelse. Det som avgör är alltså om företaget uppfyller villkoren för att var ett offentligt organ eller inte.

7.5 Data får endast begäras vid exceptionellt behov

Av artikel 14 i dataförordningen framgår att aktören som begär data ska visa att det föreligger ett exceptionellt behov av data för att fullgöra sina lagstadgade skyldigheter av allmänt intresse.

Vad som avses med ett exceptionellt behov framgår av artikel 15. Ett behov ska vara begränsat i tid och omfattning för att anses vara exceptionellt. Exceptionella behov är enligt skäl 63 i förordningen omständigheter som är oförutsebara och tidsbegränsade, till skillnad från andra omständigheter som kan vara planerade, schemalagda, periodiska eller ofta förekommande. Artikel 15 föreskriver två situationer då ett exceptionellt behov kan föreligga, vid allmänt nödläge (artikel 15.1 a) respektive i annat fall om ett organ identifierat specifika data, vars avsaknad hindrar det från att utföra en specifik uppgift av allmänt intresse som uttryckligen föreskrivs i lag (artikel 15.1 b).

[8] Kommissionens direktiv 2006/111/EG av den 16 november 2006 om insyn i de finansiella förbindelserna mellan medlemsstater och offentliga företag samt i vissa företags ekonomiska verksamhet.

7.5.1 Exceptionellt behov av data för att hantera ett allmänt nödläge

I artikel 15.1 a föreskrivs att data ska tillgängliggöras om de begärda data är nödvändiga för att hantera ett allmänt nödläge och det offentliga organet, kommissionen, Europeiska centralbanken eller unionsorganet inte i tid, på ett ändamålsenligt sätt och på likvärdiga villkor kan erhålla sådana data på alternativa sätt. Av skäl 64 i förordningen framgår att det är aktören som begär data som ska visa det inte går att erhålla data i tid på andra sätt. Det centrala begreppet är allmänt nödläge.

Vad är ett allmänt nödläge?

Allmänt nödläge definieras i artikel 2.29 i dataförordningen på följande sätt:

> en exceptionell situation under en begränsad tid, såsom ett hot mot folkhälsan, ett nödläge till följd av naturkatastrofer eller en större katastrof orsakad av människan, inbegripet en större cybersäkerhetsincident, med negativa konsekvenser för befolkningen i unionen, en medlemsstat eller en del av en medlemsstat, som medför en risk för allvarliga och bestående återverkningar på levnadsvillkoren eller den ekonomiska och finansiella stabiliteten, eller avsevärd och omedelbar värdeminskning av ekonomiska tillgångar i unionen eller berörda medlemsstater, och som fastställs och officiellt utlyses i enlighet med relevanta förfaranden i unionsrätten eller nationell rätt.

Enligt definitionen karaktäriseras ett allmänt nödläge alltså av att det är fråga om en exceptionell situation som råder under en begränsad tid, med negativa konsekvenser för befolkningen i unionen, en medlemsstat eller en del av en medlemsstat. Vidare medför det allmänna nödläget en risk för allvarliga och bestående återverkningar på levnadsvillkoren eller den ekonomiska och finansiella stabiliteten, eller avsevärd och omedelbar värdeminskning av ekonomiska tillgångar i unionen eller berörda medlemsstater. I skäl 64 i förordningen anges som exempel på allmänna nödlägen hot mot folkhälsan, nödsituationer till följd av naturkatastrofer, inbegripet sådana som förvärras av klimatförändringar och miljöförstöring, samt vid större katastrofer orsakade av människor, såsom större cybersäkerhetsincidenter. Flera av dessa exempel återfinns också i definitionen.

Vi noterar att olika språkversioner av förordningen inte stämmer överens vad gäller skrivningen ”fastställs och officiellt utlyses”. I den engelska språkversionen står det t.ex. ”determined or officially declared”. I den engelska språkversionen behöver nödläget alltså inte fastställas *och* utlysas. Det kan i stället fastställas *eller* utlysas. Syftet kan enligt oss inte vara att kraven på när ett allmänt nödläge anses föreligga ska skilja sig åt beroende på vilken språkversion av förordningen som tillämpas. Vi noterar också att det av skäl 64 i den svenska språkversionen av förordningen framgår att förekomsten av ett allmänt nödläge bör fastställas *eller* förklaras i enlighet med unionsrätten eller nationell rätt och på grundval av relevanta förfaranden, inbegripet berörda internationella organisationers förfaranden. Vår bedömning utifrån de olika språkversionerna av förordningen samt läsning av skäl 64 är att mycket talar för att ett allmänt nödläge kan anses råda enligt förordningen även om det enbart har fastställts *eller* utlysts.

Vi noterar också att begreppet allmänt nödläge även förekommer i Europakonventionen.[9] Enligt artikel 15.1 i konventionen får en hög fördragsslutande part under krig eller i annat allmänt nödläge som hotar nationens existens vidta åtgärder som innebär avvikelser från dess skyldigheter enligt den konventionen i den utsträckning som det är oundgängligen nödvändigt med hänsyn till situationens krav, under förutsättning att dessa åtgärder inte strider mot dess övriga förpliktelser enligt den internationella rätten. Artikeln har tillämpats av fördragsslutande parter bl.a. under covid 19-pandemin och vid terrorhot.[10] I dataförordningen finns inga hänvisningar till artikel 15.1 i konventionen och eftersom dataförordningen och konventionen har olika syften har allmänt nödläge inte nödvändigtvis samma innebörd.

I Sverige bygger inte lagstiftningen på att nödlägen ska utlysas

I svensk rätt finns ingen generell möjlighet att utlysa nödlägen som motsvarar utlysning av allmänna nödlägen i dataförordningen. Det finns heller ingen generell legaldefinition av allmänt nödläge eller nödläge. Bestämmelser om krig och krigsfara finns i 15 kap. regeringsformen. Bestämmelserna är primärt av konstitutionell karaktär. Om

[9] Europeiska konventionen den 4 november 1950 angående skydd för de mänskliga rättigheterna och de grundläggande friheterna.
[10] European Court of Human Rights, Derogation in time of emergency, februari 2022.

Sverige är i krigsfara eller om det råder sådana utomordentliga förhållanden som är föranledda av att det är krig utanför Sveriges gränser eller av att Sverige har varit i krig eller krigsfara, får regeringen med stöd av 3 § andra stycket lagen (1992:1403) om totalförsvar och höjd beredskap besluta om skärpt eller högsta beredskap. Till skillnad från vad som gäller för krig och krigsfara finns det inte något särskilt konstitutionellt ramverk för fredstida kriser. Utgångspunkten är i stället att sådana kriser får hanteras inom regeringsformens allmänna ramar och med stöd av de regler om exempelvis normgivning, beslutsprocesser och ansvarsfördelning mellan riksdag och regering som gäller under normala förhållanden (SOU 2023:75 s. 94).

De flesta andra länder i Europa har bestämmelser i grundlag även för fredstida kriser, som exempelvis naturkatastrofer, terroristangrepp, svåra epidemier eller svårartade ekonomiska kriser m.m. (SOU 2022:10 s. 276). Vissa länder i bl.a. Centraleuropa har tre typer av grundlagsreglerade nödtillstånd: krigstillstånd, undantagstillstånd, som ofta kopplas till hot mot den konstitutionella ordningen, samt naturkatastroftillstånd, vilket i vissa fall även omfattar industriolyckor och epidemier (SOU 2023:75 s. 141). Andra länder har två kategorier av nödtillstånd eller endast en. I Sverige är dock nödlägena i regeringsformen alltså begränsade till krig och krigsfara.[11]

Den särskilda lagstiftning som finns om fredstida kriser återfinns i huvudsak i författningar under grundlagsnivån. Kommittén om beredskap enligt regeringsformen konstaterade i sitt betänkande Stärkt konstitutionell beredskap (SOU 2023:75 s. 113–114) följande.

> Utgångspunkten är att svensk krisberedskap bygger på samhällets ordinarie verksamhet och på den vanliga förvaltningsstrukturen. Det innebär att det inte finns någon allmän ”krislag” som kan sätta i gång ett system av särskild verksamhet (jfr lagen om totalförsvar och höjd beredskap). Med några få undantag finns det inte heller någon särskild beredskapslagstiftning som har antagits av riksdagen och trätt i kraft men vars bestämmelser får börja att tillämpas först vid fredstida kriser, på det sätt som finns för krig eller krigsfara. I stället är det till stor del vanliga lagar och förordningar som ska tillämpas även vid fredstida kriser, som exempelvis polislagen (1985:387), hälso- och sjukvårdslagen (2017:30) och socialtjänstlagen (2025:400).
>
> Det har dock ansetts att det finns behov av viss speciallagstiftning även för svåra situationer i fredstid. Den lagstiftningen kan grovt sett

[11] Ett undantag är dock 8 kap. 13 § regeringsformen där det föreskrivs att riksdagen kan bemyndiga Riksbanken att meddela föreskrifter inom dess ansvarsområden enligt 9 kap. och dess övriga uppgifter i fråga om det finansiella systemet, kontanter och andra betalningsmedel, fredstida krissituationer och höjd beredskap och internationell verksamhet.

delas in i två kategorier eller typer. Dels finns det generell och övergripande lagstiftning som reglerar hur krisberedskapen ska vara uppbyggd, utan koppling till någon viss samhällssektor eller typ av kris. Sådan lagstiftning rör exempelvis vilket ansvar olika aktörer har inför och under en fredstida kris. Till stor del återfinns denna typ av lagstiftning i författningar som gäller både krisberedskap och beredskap för krigsförhållanden. Dels finns det mer specifik lagstiftning som reglerar vad som ska gälla på olika samhällsområden i händelse av kris, t.ex. inom skolväsendet eller vård och omsorg.

På samma sätt som när det gäller regler om krig och krigsfara finns det inte någon självklar samlingsbeteckning för all lagstiftning som på olika sätt rör fredstida kriser.

I svensk lagstiftning används andra begrepp än allmänt nödläge

I svensk rätt, när det gäller nödlägen som inte är i form av krig eller krigsfara, används olika begrepp i lagstiftning under grundlagsnivån för att beskriva svåra situationer i fredstid, bl.a. fredstida krissituation, extraordinär händelse, svår påfrestning på samhället, olycka, samhällsstörning och allvarlig händelse. Som framgår ovan kan den speciallagstiftning som gäller för svåra situationer i fredstid grovt sett kan delas in i dels generell och övergripande lagstiftning utan koppling till någon viss samhällssektor eller typ av kris, dels mer specifik lagstiftning som reglerar vad som ska gälla på olika samhällsområden i händelse av kris. Vi redogör i det följande för exempel på den begreppsbildning som inom svensk lagstiftning används för att beskriva svåra situationer i fredstid.

Fredstida krissituationer

Inom den statliga sektorn gäller förordningen (2022:524) om statliga myndigheters beredskap, som innehåller bestämmelser om uppgifter som statliga myndigheter under regeringen har inför och vid fredstida krissituationer och höjd beredskap. Av 1 § första stycket framgår att syftet med förordningen är att statliga myndigheter under regeringen genom sin verksamhet ska minska sårbarheten i samhället och utveckla en god förmåga att hantera sina uppgifter vid fredstida krissituationer och höjd beredskap. Enligt 6 § avses med fredstida krissituationer ”situationer som avviker från det normala, drabbar många människor, stora delar av samhället eller hotar grundläggande värden,

innebär en allvarlig störning eller överhängande risk för en allvarlig störning av viktiga samhällsfunktioner och kräver samordnande och skyndsamma åtgärder från flera aktörer".

Extraordinär händelse

Inom den kommunala sektorn gäller lagen (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap, som bl.a. syftar till att kommuner och regioner ska ha en god förmåga att hantera krissituationer i fred (1 §). Med extraordinär händelse avses i lagen enligt 4 § "en sådan händelse som avviker från det normala, innebär en allvarlig störning eller överhängande risk för allvarlig störning i viktiga samhällsfunktioner och kräver skyndsamma insatser av en kommun eller en region". Bestämmelsens utformning motsvarar vad som tidigare gällt enligt lagen (2002:833) om extraordinära händelser i fredstid hos kommuner och landsting. I propositionen som föregick den tidigare lagstiftningen uttalar regeringen bl.a. följande gällande extraordinära händelser (prop. 2001/02:184 s. 14).

> Det handlar om händelser där någon eller flera viktiga samhällsfunktioner som kommuner och landsting ansvar för hotas på ett omfattande sätt. Det kan exempelvis vara hot mot sjukvårdsverksamheten, energiförsörjningen, vatten- och avloppsnätet eller vägnätet. Tillämpningen av lagen aktualiseras vid större olyckshändelser som hotar liv, hälsa, miljö eller egendom. Typiska händelser som avses är väderrelaterade händelser av större omfattning, som t.ex. större översvämningar, ras som en följd av längre tids nederbörd och omfattande snöoväder. En större skogsbrand, som hotar bebyggelse eller liknande, och som kräver betydande insatser utöver räddningstjänsten, är ytterligare exempel på en extraordinär händelse. Normalt är dock inte enstaka bränder tänkta att omfattas av den föreslagna lagen. Det som särskiljer extraordinära händelser från andra händelser är de extraordinära händelsernas stora omfattning och att händelseförloppet är snabbt och svårt att överblicka och därmed kräver snabba beslut av de kommunala organen. Det är alltså händelser som ställer speciella krav på den kommunala organisationen.

När det gäller kravet på att händelsen ska avvika från det normala uttalar regeringen följande (prop. 2001/02:184 s. 14 f.).

> Växlingar i väderleken, större olyckor med mera kan påverka och störa kommunens eller landstingets verksamhet. Flertalet störningar av mer normal omfattning skall dock kunna hanteras inom ramen för annan lag-

> stiftning. De flesta händelser, även om de är störande och kommer plötsligt, bör enligt regeringens mening inte betraktas som extraordinära händelser. Vad som kan ses som normalt måste avgöras utifrån en helhetsbedömning i det enskilda fallet. Exempelvis torde mycket omfattande snöfall och sträng kyla uppfattas som mer normalt i de norra delarna av Sverige än i de södra. En extraordinär händelse behöver inte i sig vara oförutsägbar. Det som dock särskiljer extraordinära händelser från andra händelser är de extraordinära händelsernas stora omfattning och att händelseförloppet är snabbt och svårt att överblicka och därmed kräver snabba beslut av de kommunala organen, i vart fall i krisens inledningsskede. Det är enligt regeringens mening ur denna synvinkel som kravet på avvikelser från det normala bör ses.

Svåra påfrestningar

Även begreppet svåra påfrestningar förekommer i författningar. Elberedskapslagen (1997:288) innehåller bestämmelser om skyldighet att vidta beredskapsåtgärder inom elsektorn. Enligt 3 § avses med beredskapsåtgärder åtgärder som behövs för att förebygga, motstå och hantera sådana störningar i elförsörjningen som kan medföra svåra påfrestningar på samhället. Med beredskapsåtgärder avses i lagen också sådana åtgärder som krävs för att göra det möjligt att vidta de åtgärder som behövs vid höjd beredskap. Begreppet svåra påfrestningar används även i lagen (1992:1403) om totalförsvar och höjd beredskap. I 2 § föreskrivs att totalförsvarsresurser ska utformas så att de även kan användas vid internationella fredsfrämjande och humanitära insatser och stärka samhällets förmåga att förebygga och hantera svåra påfrestningar på samhället.

I förarbetena till den ovan nämnda lagen om extraordinära händelser i fredstid hos kommuner och landsting redogjorde regeringen för skillnaden mellan begreppen extraordinära händelser och svåra påfrestningar enligt följande (prop. 2001/02:184 s. 15).

> Med begreppet extraordinära händelser avses till övervägande del något annat än med begreppet svåra påfrestningar på samhället i fred. Med en svår påfrestning avses inte en enskild händelse i sig, exempelvis en olycka, ett sabotage osv., utan ett tillstånd som kan uppstå när en eller flera händelser utvecklar sig och eskalerar till att omfatta flera delar av samhället. Svåra påfrestningar kan sägas utgöra olika slag av extrema situationer med låg sannolikhet som skiljer sig i sak. Tillståndet är av sådan omfattning att det uppstår allvarliga störningar i viktiga samhällsfunktioner eller hotar grundläggande värden av olika slag i samhället och kräver att insatser från flera olika myndigheter och organ samordnas för att kunna

hantera situationen och därmed begränsa konsekvenserna. Med begreppet extraordinär händelse avses händelser av mindre geografisk omfattning, där en kommun eller ett landsting, eller ett par grannkommuner, har drabbats av en kris. Det är händelser som ligger mellan normaltillstånd och höjd beredskap. En extraordinär händelse kan undantagsvis utgöra en svår påfrestning på samhället i fred.

Fredstida krissituationer, extraordinära händelser och svåra påfrestningar kan motsvara ett allmänt nödläge

Vi kan konstatera att begreppen som används i svenska författningar inbegriper situationer och händelser som kan omfattas av definitionen av allmänt nödläge i dataförordningen.

Begreppen som används i de svenska författningarna kan avse situationer och händelser som gäller för en begränsad tid med negativa konsekvenser i unionen, en medlemsstat eller del av en medlemsstat. Vidare kan situationerna medföra en risk för allvarliga och bestående återverkningar på levnadsvillkoren eller den ekonomiska och finansiella stabiliteten, eller avsevärd och omedelbar värdeminskning av ekonomiska tillgångar.

Författningar ger stöd att fatta beslut om det råder kris eller nödlägen

En generell möjlighet att utlysa nödläge saknas alltså i Sverige. Vår bedömning är dock att mycket talar för att ett allmänt nödläge kan anses råda enligt förordningen även om det enbart har fastställts *eller* utlysts. Eftersom det saknas stöd för att utlysa nödlägen i Sverige är det utifrån svenska förhållanden möjligheten att fastställa ett allmänt nödläge som kvarstår.

Ovan redogör vi för vår bedömning att de begrepp som används i svenska författningar kan motsvara ett allmänt nödläge enligt dataförordningen. Vår bedömning är att om det i svensk författning föreskrivs att åtgärder kan vidtas under förutsättning att det råder kris eller nödlägen, så kan den aktuella krisen eller nödläget anses vara fastställd i och med att åtgärden vidtas. Detta eftersom kris eller nödläge är en förutsättning för att åtgärder ska kunna vidtas. Det talar för att krisen eller nödläget kan anses vara fastställd enligt dataförordningen, under förutsättning att övriga villkor för ett allmänt nödläge

i förordningen är uppfyllda. Det finns ett flertal exempel på författningar där det föreskrivs att regeringen, eller i vissa fall myndigheter, får fatta beslut som kan förstås som att de föranleds av någon form av nödläge. Några exempel redovisas nedan.

Med stöd av 2 kap. 15 § ordningslagen (1993:1617) får regeringen föreskriva att allmänna sammankomster och offentliga tillställningar inte får hållas inom ett visst område, om förbudet är nödvändigt med hänsyn till att Sverige är i krig eller krigsfara eller för att motverka epidemi eller för att förebygga eller bekämpa epizooti enligt epizootilagen (1999:657).

I 9 kap. smittskyddslagen (2004:168) finns bestämmelser som innebär att regeringen, den myndighet regeringen bestämmer och Folkhälsomyndigheten kan fatta vissa beslut avseende allmänfarliga respektive samhällsfarliga sjukdomar.

Enligt 2 kap. 2 § lagen om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap ska det i kommuner och regioner finnas en nämnd för att fullgöra uppgifter under extraordinära händelser i fredstid (krisledningsnämnd). Krisledningsnämndens ordförande bedömer när en extraordinär händelse medför att nämnden ska träda i funktion och beslutar i sådana fall att så ska ske. Enligt 2 kap. 4 § får krisledningsnämnden fatta beslut om att överta hela eller delar av verksamhetsområden från övriga nämnder i kommunen eller regionen i den utsträckning som är nödvändig med hänsyn till den extraordinära händelsens art och omfattning.

Om fara för liv, hälsa eller egendom eller för skada i miljön inte lämpligen kan hindras på något annat sätt får en räddningsledare vid en räddningsinsats enligt 6 kap. 2 § lagen (2003:778) om skydd mot olyckor bereda sig och medverkande personal tillträde till annans fastighet, avspärra eller utrymma områden, använda, föra bort eller förstöra egendom samt göra andra ingrepp i annans rätt, i den mån ingreppet är försvarligt med hänsyn till farans beskaffenhet, den skada som vållas genom ingreppet och omständigheterna i övrigt. Sådana ingrepp får också göras av en kommunal nämnd eller, i fråga om statlig räddningstjänst, av den myndighet som ansvarar för räddningstjänsten. Om länsstyrelsen eller annan statlig myndighet har tagit över ansvaret för den kommunala räddningstjänsten, får ingrepp göras av den myndigheten i stället för av den kommunala nämnden.

Beslut enligt exemplen ovan kan i vissa fall föranledas av en situation som är ett hot mot folkhälsan, ett nödläge till följd av naturkata-

strofer eller en större katastrof orsakad av människan eller en större cybersäkerhetsincident, i enlighet med definitionen av allmänt nödläge i dataförordningen. Enligt vår uppfattning bör beslutet i sig innebära att nödläget kan anses vara fastställt enligt förordningen och det kan därför vara ett allmänt nödläge. En bedömning måste emellertid göras från fall till fall.

Vår uppfattning är alltså att det inte är den begreppsapparat som används i nationella författningar som avgör om det rör sig om ett allmänt nödläge enligt dataförordningen eller inte. Den situation som råder måste i stället bedömas utifrån förordningens definition av allmänt nödläge. Om det uppstår en allvarlig situation där t.ex. en myndighet har en skyldighet enligt författning att vidta åtgärder och behöver data för detta, måste myndigheten i ett första läge avgöra om den situation som har uppstått kan anses vara ett allmänt nödläge enligt förordningen. Om situationen är sådan måste myndigheten också bedöma om det allmänna nödläget har fastställts, med utgångspunkt i den eller de författningar som ger stöd för att fatta beslut om att vidta åtgärder vid allvarliga situationer av olika slag. Ett beslut kan enligt vår uppfattning leda till att kravet på att ett allmänt nödläge ska fastställas är uppfyllt och anses ge uttryck för att det råder ett allmänt nödläge i dataförordningens mening.

Analysen ovan avser relevanta förfaranden i svensk rätt. Allmänna nödlägen kan enligt definitionen i dataförordningen fastställs eller officiellt utlysas även i enlighet med relevanta förfaranden i unionsrätten.

En möjlighet att utlysa allmänna nödlägen bör inte införas i Sverige mot bakgrund av dataförordningen

Eftersom kapitel V i dataförordningen utgår från en begreppsapparat som inte har motsvarighet i svensk rätt går det inte att komma ifrån att det kan uppstå osäkerhet kring när förordningens bestämmelser kan tillämpas. Enligt vår uppfattning vore det emellertid inte lämpligt att införa en möjlighet att utlysa allmänna nödlägen mot bakgrund av dataförordningen. En sådan möjlighet skulle väcka konstitutionella frågor som kräver noga överväganden avseende konsekvenserna. Det skulle vara olämpligt att införa en generell möjlighet att utlysa allmänna nödlägen enbart för att offentliga organ ska ges bättre tillgång till data. Ett allmänt nödläge innebär mer än att offentliga organ har

behov av data. Hanteringen av ett allmänt nödläge kräver fler insatser från offentliga organ än att de begär och använder data för att hantera nödläget. Om det av andra skäl finns anledning att införa en sådan ordning faller utanför vårt uppdrag. Vi noterar dock att utvecklingen inom beredskapsområdet på sikt kan få bäring på möjligheterna att tillämpa dataförordningens kapitel V i Sverige.[12]

7.5.2 Exceptionellt behov av data för andra ändamål än att hantera allmänt nödläge

Ett exceptionellt behov av data kan föreligga även i andra situationer än när de är nödvändiga för att hantera ett allmänt nödläge. Enligt artikel 15.1 b krävs dels att avsaknad av data hindrar organet från att utföra en specifik uppgift av allmänt intresse som uttryckligen föreskrivs i lag, dels att organet har uttömt alla andra till buds stående medel för att erhålla sådana data. Av artikel 15.1 b ii framgår att andra möjligheter att få tillgång till data som ska vara uttömda innefattar inköp av data på marknaden genom att erbjuda marknadspris, att organet förlitar sig på befintliga skyldigheter för att göra data tillgängliga eller antagande av nya lagstiftningsåtgärder som skulle kunna säkerställa att data finns tillgängliga i tid. Om organet exempelvis kan köpa de data det behöver på marknaden till marknadspris föreligger alltså inte ett exceptionellt behov.

I artikel 15.2 föreskrivs att artikel 15.1 b inte ska tillämpas på mikroföretag och små företag. Det innebär att om det exceptionella behovet av data grundar sig i ett annat behov än hantering av ett allmänt nödläge, så kan data inte begäras från sådana företag.

7.5.3 Vilka data som får begäras och hur snabbt företaget ska svara

Begärande parter kan med stöd av kapitel V i förordningen begära de data de behöver för att kunna fullgöra sina lagstadgade skyldigheter av allmänt intresse. Detta inkluderar de relevanta metadata som är nödvändiga för tolkningen och användningen av de data som begärs. Kapitel V begränsar t.ex. inte möjligheten att begära data till att en-

[12] Som exempel kan nämnas att regeringen har föreslagit att särskilda bestämmelser om normgivning i allvarliga fredstida krissituationer ska införas i regeringsformen, se prop. 2024/25:155.

dast omfatta exempelvis produktdata eller data från tillhörande tjänster (jfr definitionen av datahållare i artikel 2.13).

Av artikel 17.2 framgår att en begäran ska vara specifik avseende den typ av data som begärs och avse data som datahållaren har kontroll över vid tidpunkten för begäran. Vidare ska en begäran bl.a. innehålla ett åtagande om att säkerställa skyddet av företagshemligheter och i begäran ska också de tekniska och organisatoriska åtgärder som ska vidtas för att skydda de data som begärs fastställas.

En begäran ska som huvudregel gälla icke-personuppgifter. Om det exceptionella behovet inte har uppstått inom ramen för att hantera ett allmänt nödläge får, enligt artikel 15.1 b, endast data som är icke-personuppgifter begäras. Endast om icke-personuppgifter har visats vara otillräckligt för att tillgodose det exceptionella behovet av att använda data i enlighet med artikel 15.1 a, dvs. för att hantera ett allmänt nödläge, är det möjligt att begära personuppgifter. Om personuppgifter begärs ska det utan oskäligt dröjsmål anmälas till den tillsynsmyndighet som ansvarar för att övervaka tillämpningen av dataskyddsförordningen i den medlemsstat där det offentliga organet är etablerat. I Sverige ska anmälan göras till Integritetsskyddsmyndigheten.

En datahållare som mottar en begäran om att göra data tillgängliga ska enligt artikel 18.1 i förordningen tillgängliggöra dem utan oskäligt dröjsmål. Vad som avses med oskäligt dröjsmål specificeras inte i förordningen och får avgöras med hänsyn till omständigheterna i det enskilda fallet, exempelvis omfattningen av de data som begärs och vilka åtgärder datahållaren måste vidta för att i kunna tillgängliggöra dem.

Av artikel 18.2 framgår att en datahållare får avslå en begäran eller ansöka om ändring av en begäran. Om begäran gäller data som är nödvändiga för att hantera ett allmänt nödläge ska det ske utan oskäligt dröjsmål och under alla omständigheter senast fem arbetsdagar efter mottagandet av begäran. Om begäran gäller data för andra exceptionella behov än för att hantera ett allmänt nödläge ska begäran avslås eller ansökan om ändring ske senast 30 arbetsdagar efter mottagandet av en begäran. Datahållaren får avslå begäran eller ansöka om ändring om datahållaren inte har kontroll över de data som begärs eller om en liknande begäran för samma ändamål tidigare har lämnats in av ett annat offentligt organ eller kommissionen, Europeiska centralbanken eller ett unionsorgan, och datahållaren inte har underrättats

om att dessa data har raderats. För det senare ska datahållaren meddela den begärande parten vilken aktör som tidigare lämnat in en begäran för samma ändamål. Datahållaren kan också avslå eller begära ändring av begäran om begäran inte uppfyller inte de krav som ställs på en begäran.

Om den begärande parten vill överklaga en datahållares vägran att tillhandahålla begärda data eller om datahållaren vill bestrida begäran och ärendet inte kan lösas genom en lämplig ändring av begäran, ska ärendet hänskjutas till den behöriga myndighet som utsetts enligt artikel 37 i förordningen i den medlemsstat där datahållaren är etablerad.

7.6 Data får delas vidare

Enligt artikel 21.1 får ett offentligt organ, kommissionen, Europeiska centralbanken eller ett unionsorgan dela data som mottagits med stöv av kapitel V med enskilda personer eller organisationer i syfte att bedriva vetenskaplig forskning eller analys som är förenlig med det ändamål för vilket data begärdes. De får också dela data med nationella statistikbyråer och Eurostat för framställning av officiell statistik.

Kretsen av enskilda personer eller organisationer som data får delas med begränsas i artikel 21.2, där det föreskrivs att de ska agera utan vinstsyfte eller inom ramen för ett uppdrag av allmänt intresse som erkänns i unionsrätten eller nationell rätt. Detta omfattar inte organisationer på vilka kommersiella företag har ett betydande inflytande som sannolikt skulle kunna leda till förmånstillträde till forskningsresultaten.

Enskilda personer eller organisationer som tar emot data ska enligt artikel 21.3 fullgöra samma skyldigheter som är tillämpliga på offentliga organ, kommissionen, Europeiska centralbanken eller unionsorgan enligt artiklarna 17.3 och 19.

Det förefaller även som att offentliga organ, kommissionen, Europeiska centralbanken och unionsorgan får dela data mellan sig. Att så är fallet är dock inte självklart. Enligt artikel 22.1 ska offentliga organ, kommissionen, Europeiska centralbanken och unionsorgan samarbeta och bistå varandra för att genomföra kapitel V på ett konsekvent sätt. Ordalydelsen indikerar att aktörerna snarare ska hjälpa till med tolkning och förståelse av tillämpningen av kapitlet än att utbyta data som de har mottagit. I artikel 22.2 föreskrivs dock att

data som utbyts i samband med begärt bistånd och som tillhandahållits enligt artikel 22.1 inte får användas på ett sätt som är oförenligt med det ändamål för vilket de begärdes. Det indikerar att artikel 22.1 ska förstås som att samarbetet och biståndet innebär att aktörerna får dela data med varandra. Av artikel 17.1 f framgår också att en begäran om att tillgängliggöra data ska specificera eventuella andra offentliga organ eller kommissionen, Europeiska centralbanken eller unionsorgan och de tredje parter med vilka begärda data förväntas delas.

7.7 Data ska raderas när de inte längre behövs

Skyldigheter för offentliga organ, kommissionen, Europeiska centralbanken eller ett unionsorgan som tar emot data till följd av en begäran föreskrivs i artikel 19 i dataförordningen. Enligt artikel 19.1 ska dessa organ bl.a. radera data som de tar emot till följd av en begäran så snart de inte längre är nödvändiga för det angivna ändamålet. Detta gäller dock inte om dessa data ska arkiveras i enlighet med unionsrätt eller nationell rätt om allmänhetens tillgång till handlingar i samband med insynsskyldigheter. För det fall svenska offentliga organ begär och får data aktualiseras handlingsoffentligheten i Sverige och allmänhetens rätt till tillgång allmänna handlingar. Även arkivlagen (1990:782) och tillhörande författningar om bl.a. gallring aktualiseras. Arkivlagstiftningens huvudregel är att allmänna handlingar ska bevaras, men den medger ändå att handlingar får gallras under förutsättning att de inte längre behövs för att tillgodose arkivlagens bevarandeändamål avseende rätten att ta del av allmänna handlingar och behovet av information för rättskipningen, förvaltningen och forskningen. Eftersom det i Sverige finns nationella bestämmelser om arkivering måste svenska offentliga organ som begära och tar emot data med stöd av kapitel V i dataförordningen göra en bedömning om dessa data ska bevaras eller inte. Om organet bedömer att data ska bevaras enligt arkivlagstiftningen, så är det förenligt med artikel 21.1 i förordningen.

7.8 Ersättning

Bestämmelser om ersättning till datahållare som tillgängliggör data efter en begäran finns i artikel 20 i förordningen. Vilka företag som kan få ersättning skiljer sig åt beroende på om det exceptionella behovet som ligger till grund för begäran grundar sig i ett allmänt nödläge eller inte.

Om en begäran om att tillgängliggöra data har gjorts med stöd av artikel 15.1 b, dvs. i andra situationer än för att hantera ett allmänt nödläge, har datahållare enligt artikel 20.2 rätt till skälig ersättning. I bestämmelsen undantas inga företag från rätten till ersättning. Enligt artikel 20.1 ska emellertid datahållare som inte är mikroföretag och små företag kostnadsfritt tillgängliggöra de data som är nödvändiga för att hantera ett allmänt nödläge enligt artikel 15.1 a. Det innebär att resterande företag kostnadsfritt ska tillgängliggöra data. Däremot ska den aktör som har tagit emot dessa data enligt artikel 20.1 ge datahållaren offentligt erkännande om datahållaren begär det.

I Sverige finns ett grundlagsskydd mot expropriation och andra sådana förfoganden. Enligt 2 kap. 15 § regeringsformen är vars och ens egendom tryggad genom att ingen kan tvingas avstå sin egendom till det allmänna eller till någon enskild genom expropriation eller något annat sådant förfogande. Med uttrycket avses att en förmögenhetsrätt, dvs. äganderätt eller annan rätt med ett ekonomiskt värde, t.ex. nyttjanderätt, servitut eller vägrätt, tvångsvis överförs eller tas i anspråk (prop. 2009/10:80 s. 163). Den som tvingas avstå sin egendom ska vara tillförsäkrad full ersättning för förlusten. Det har inom ramen för utredningens arbete framförts att kostnaderna för att tillmötesgå en begäran om data kan vara höga även för stora företag och att alla företag borde få ersättning för de data de tillgängliggör, oavsett företagets storlek. Detta bl.a. mot bakgrund av rätten till ersättning vid expropriation i regeringsformen.

En begäran om att tillgängliggöra data med stöd av kapitel V i dataförordningen innebär inte att det företag som tillgängliggör data tvingas avstå dessa data. Företaget kommer att ha kvar alla data och kan fortsätta att använda dem. De data som inkommer till det offentliga organet är kopior. Vi bedömer därför att rätten till ersättning som föreskrivs i 2 kap. 15 § regeringsformen inte är tillämplig. Artikel 20.1 i dataförordningen är formulerad så att företag som inte är mikroföretag eller små företag kostnadsfritt ska tillgängliggöra data som

krävs för att hantera ett allmänt nödläge. Det innebär enligt vår uppfattning att det inte är möjligt att införa nationella bestämmelser som innebär att t.ex. medelstora och stora företag ska ha rätt till ersättning. Det finns i dagsläget frivilliga arrangemang mellan företag och myndigheter som innefattar tillgängliggörande av data. Sådana arrangemang kan innefatta ersättning till företag för att de tillgängliggör data för myndigheter och det finns enligt oss inget som hindrar att myndigheter eller andra offentliga organ frivilligt ersätter även stora företag för data de begär för att hantera ett allmänt nödläge med stöd av kapitel V i förordningen.

Ersättningen ska enligt artikel 20.2 täcka de tekniska och organisatoriska kostnader som uppstår till följd av tillmötesgåendet av begäran. Det inkluderar kostnader för anonymisering, pseudonymisering, aggregering och teknisk anpassning samt en rimlig marginal. Om det offentliga organet, kommissionen, Europeiska centralbanken eller unionsorganet begär det ska datahållaren tillhandahålla information om underlaget till kostnadsberäkningen och den rimliga marginalen. Om den begärande parten inte godtar den ersättning som datahållaren begär kan organet enligt artikel 20.5 i förordningen lämna in ett klagomål till den behöriga myndighet som utsetts enligt artikel 37 i den medlemsstat där datahållaren är etablerad.

Enligt artikel 20.4 ska datahållare inte ha rätt till ersättning för att göra data tillgängliga i enlighet med en begäran som gjorts enligt artikel 15.1 b, om den specifika uppgiften av allmänt intresse är framställning av officiell statistik och om inköp av data inte är tillåten enligt nationell rätt. Medlemsstaterna ska underrätta kommissionen om inköp av data för framställning av officiell statistik inte är tillåtet enligt nationell rätt. I Sverige finns inget förbud mot inköp av data för framställning av officiell statistik, vilket innebär att artikel 20.4 inte kommer att tillämpas i Sverige. Kravet i artikel 20.4 är formulerat så att medlemsstaterna ska meddela kommissionen om inköp av data för framställning inte är tillåtet enligt nationell rätt. Eftersom det i Sverige är tillåtet att köpa data för sådana ändamål ska Sverige enligt artikeln inte meddela kommissionen.

7.9 Data kan begäras från datahållare i en annan medlemsstat

I artikel 22.3 i förordningen föreskrivs att om ett offentligt organ avser att begära data från en datahållare som är etablerad i en annan medlemsstat, ska organet först underrätta den behöriga myndighet som utsetts enligt artikel 37 i förordningen i den medlemsstaten om sin avsikt. Samma krav gäller för begäranden från kommissionen, Europeiska centralbanken och unionsorgan. Begäran ska granskas av den behöriga myndigheten i medlemsstaten där datahållaren är etablerad.

Efter att den behöriga myndigheten har granskat en begäran ska den enligt artikel 22.4 vidta en av två åtgärder. Det ena åtgärderna är att överföra begäran till datahållaren och i tillämpliga fall ge den begärande parten råd om det eventuella behovet av att samarbeta med offentliga organ i den medlemsstat där datahållaren är etablerad, i syfte att minska den administrativa bördan för datahållaren när det gäller att tillmötesgå begäran. Den andra åtgärden är att avslå begäran av vederbörligen motiverade skäl. Detta måste förstås som att den behöriga myndighetens granskning av begäran syftar till att avgöra om den ska vidareförmedlas till datahållaren eller om den ska avslås. Enligt kommissionen ska den behöriga myndigheten granska begäran *ex ante*, dvs. i förväg.[13] Vår bedömning är att den granskning den behöriga myndigheten ska göra enbart är av formell karaktär. Myndigheten ska granska att den information som krävs enligt artikel 17.1 och 17.2 finns i begäran och att den är fullständig. Skälet till denna bedömning är att det av artikel 18.2 framgår att en datahållare får avslå en begäran som inte uppfyller villkoren i artikel 17.1 och 17.2. Det föreskrivs inga undantag från denna möjlighet, exempelvis att begäran har överförts från den behöriga myndigheten till datahållaren. Trots att begäran har granskats av den behöriga myndigheten kan datahållaren alltså avslå begäran om den inte uppfyller villkoren i artikel 17.1 och 17.2.

[13] Europeiska kommissionen, Frequently Asked Questions Data Act, version 1.2, s. 27.

7.10 För datadelning behövs tekniska resurser och organisatoriska förmågor

Dataförordningen ger svenska offentliga organ ett nytt verktyg för att begära data om det uppstår ett exceptionellt behov, t.ex. för att hantera allmänna nödlägen. Enligt våra utredningsdirektiv ska vi identifiera och föreslå vilka tekniska resurser, organisatoriska förmågor och digitala infrastrukturer som svenska offentliga organ behöver för att effektivt kunna ta emot, hantera, bearbeta och dela data som erhålls från företag vid exceptionella behov.

Datadelning är i dag en självklar del svenska offentliga organs verksamheter. De tar emot data samt tillgängliggör och skickar data till andra. Datadelningen sker mellan offentliga organ och företag och mellan offentliga organ. Offentliga organ tar emot data för att använda dem i sina verksamheter och datadelningen är i många fall en förutsättning för att kunna bedriva vissa verksamheter.

För att datadelning ska vara möjlig måste vissa förutsättningar finnas på plats. Det krävs tekniska resurser i form av bl.a. teknisk utrustning, it-system och teknisk expertkunskap. Det krävs också organisatoriska förmågor i form av bl.a. processer och resurshantering. Eftersom svenska offentliga organ redan tar emot och delar data finns dessa förutsättningar på plats. Enligt Utredningen om interoperabilitet vid datadelning använder myndigheter inom den offentliga förvaltningen olika tekniska lösningar för att dela data och för att samla in data, t.ex. API:er, överföring via e-post samt olika typer av e-tjänster som kräver inloggning och att uppgifter i vissa fall förs in manuellt (SOU 2023:96 s. 78). Ett och samma offentligt organ kan använda sig av olika tekniska lösningar inom sin verksamhet. Även om förmågorna för datadelning finns på plats hos offentliga organ kan de alltså ur tekniskt hänseende skilja sig åt.

Interoperabilitet och effektiv datadelning

För att datadelning ska vara effektiv krävs interoperabilitet. Det finns ett flertal olika definitioner av interoperabilitet och i allmänhet tar de sikte på förmågan hos informationssystem att fungera tillsammans vid utbyte av data (SOU 2023:96 s. 39). Ibland innehåller definitionerna också förmågor hos verksamheter och organisationer. I det Europeiska interoperabilitetsramverket (EIF) är utgångspunkten

att interoperabilitet består av fyra lager: rättslig, organisatorisk, semantisk och teknisk interoperabilitet.[14] Det får inte finnas rättsliga hinder mot datadelning och organisationer måste ha förmågan att säkerställa att deras verksamheter och processer kan dela och använda data. Semantisk interoperabilitet tar sikte på de data som utbyts och att de går att förstå genom hela utbyteskedjan. Teknisk interoperabilitet innebär att de tekniska förutsättningarna finns på plats för att kunna dela data.

Det är i dagsläget stora skillnader i nivån av interoperabilitet vid datadelning mellan offentliga organ och företag, samt mellan offentliga organ. I vissa fall kan data delas direkt mellan it-system hos två organisationer varvid den mottagande organisationen kan använda dem i sin verksamhet utan ytterligare bearbetning. I andra fall krävs manuella inslag när data delas och bearbetning av data krävs för att den organisation som tar emot dem ska kunna använda dem.

Förutsättningarna för offentliga organ att bedriva sina verksamheter förändras över tid. Det kan exempelvis ske förändringar i de sektorer de verkar i och rättsliga, organisatoriska och ekonomiska förutsättningar kan förändras. Förutsättningar som har direkt koppling till datadelning förändras också. Informationsflöden som tidigare har varit fysiska, t.ex. på papper, kan övergå till att bli digitala. Det kan tillkomma nya rapporteringskrav som innebär att företag ska rapportera nya uppgifter digitalt eller att rättsliga förutsättningar förändras som i praktiken leder till utökade möjligheter till datadelning. Den tekniska utvecklingen erbjuder ständigt nya möjligheter för hur data kan delas.

Arbete för ökad interoperabilitet pågår

Kapitel V i dataförordningen innebär att offentliga organ får ett nytt rättsligt verktyg att begära de data som de har ett behov av. Eftersom förutsättningarna för deras verksamheter förändras över tid har de redan i dagsläget erfarenhet av att anpassa sig. Offentliga organ har enligt vår bedömning tekniska resurser och organisatoriska förmågor på plats för att kunna hantera förändrade förutsättningar för datadelning och de har tillgång till digitala infrastrukturer.

[14] Europeiska kommissionen, Europeiska interoperabilitetsramen – genomförandestrategi, COM (2017) 134 final, bilaga 2. Se också artikel 6.2 i EU:s interoperabilitetsförordning.

Frågan är om kapitel V i dataförordningen och möjligheten att begära nya data, i vissa fall från nya aktörer, ställer särskilda krav på dessa resurser och infrastrukturer.

Arbete som kan leda till ökad interoperabilitet hos offentlig förvaltning pågår sedan tidigare, bl.a. inom Ena – Sveriges digitala infrastruktur, som är ett samlingsnamn för olika system, komponenter och standarder som gör det möjligt för den offentliga förvaltningen att dela digital information.[15] Digg ansvarar för samordningen av Ena och är också ansvarig för merparten av de sammanhängande gemensamma digitala lösningar som i dag finns i Ena. I samhället finns det flera lager av digitala infrastrukturer, med bredband, routrar och annan hårdvara i botten och olika mjukvaruapplikationer högst upp. Flera av Enas lösningar är inte synliga för användaren eftersom de utgör den underliggande digitala infrastrukturen som andra aktörer nyttjar för att skapa bättre digitala tjänster mot användare. Ena består av gemensamma lösningar som kan användas av alla offentliga aktörer och som underlättar för enskilda att få tillgång till effektiv samhällsservice.

Utöver att ansvara för samordningen av Ena är Digg bl.a. behörig myndighet och enda kontaktpunkt enligt artikel 17 förordningen om ett interoperabelt Europa.[16] Det innebär bl.a. att Digg samordnar alla frågor som rör förordningen och ger stöd till myndigheter i Sverige vid interoperabilitetsbedömningar, främjar utbytet och vidareutnyttjandet av interoperabilitetslösningar genom portalen för ett interoperabelt Europa samt representerar Sverige i styrelsen för ett interoperabelt Europa.[17] Exempel på andra myndigheter som bidrar till ökad interoperabilitet är Statistiska centralbyrån, som är ett behörigt organ enligt dataförvaltningsförordningen[18] och hjälper andra myndigheter som behöver tekniskt stöd för att kunna tillgängliggöra skyddade data för vidareutnyttjande genom att bidra med kunskap.[19] Enligt vår uppfattning kommer pågående utveckling inom interoperabilitetsområdet att underlätta för offentliga organ att ta emot, hantera, bearbeta och dela data som de begär från företag med stöd av kapitel V i dataförordningen.

[15] Regeringsbeslut, 2024-06-20, Fi2024/01455.
[16] 1 d § förordningen (2018:1486) med instruktion för Myndigheten för digital förvaltning.
[17] https://www.digg.se/kunskap-och-stod/eu-rattsakter/interoperabilitetsforordningen (hämtad 2025-11-14).
[18] 2 § 11 p. förordningen (2016:822) med instruktion för Statistiska centralbyrån.
[19] https://www.scb.se/om-scb/scbs-verksamhet/myndighetsstod-for-skyddade-data/ (hämtad 2025-11-14).

I sammanhanget bör också noteras att Utredningen om interoperabilitet vid datadelning har konstaterat att det saknas nationell styrning som gäller för hela den offentliga förvaltningen i syfte att data som delas ska vara interoperabla eller att den ska delas på ett interoperabelt sätt (SOU 2023:96). Den stora merparten av svenska offentliga organ enligt dataförordningen ingår i den offentliga förvaltningen. Utredningen föreslog en modell för nationell styrning vad gäller interoperabilitet och att en ny lag om den offentliga förvaltningens interoperabilitet ska införas. Förslaget bereds förnärvarande inom Regeringskansliet. I budgetpropositionen för 2026 framför regeringen att den avser att presentera ett lagförslag om den offentliga förvaltningens datadelning som beaktar Sveriges säkerhet samt föreslår att Digg och PTS får ökade anslag för arbete med den offentliga förvaltningens datadelning enligt kommande lagstiftning om interoperabilitet (prop. 2025/26:1 Utgiftsområde 22).

Vi har övervägt om det trots pågående interoperabilitetsarbete finns anledning att föreslå vilka tekniska resurser, organisatoriska förmågor och digitala infrastrukturer offentliga organ behöver när de begär data med stöd av kapitel V i dataförordningen. Vi bedömer emellertid att det inte är lämpligt att lämna sådana förslag. Datadelning som kommer att ske med stöd av kapitlet i förordningen är inte isolerad från offentliga organs datadelning i övrigt. Förutsättningarna som måste finnas få plats är desamma oavsett om datadelning sker med stöd av kapitel V eller annan författning. Utgångspunkten när data ska tillgängliggöras med stöd av kapitlet bör vara att de tekniska och organisatoriska resurser och digitala infrastrukturer som redan finns att tillgå bör användas. Detta under förutsättning att de erbjuder tillräckligt hög nivå av säkerhet. Vi har övervägt om vi bland de tekniska resurser, organisatoriska förmågor och digitala infrastrukturer som existerar i dagsläget bör föreslå att vissa av dem ska användas vid tillgängliggörande enligt kapitel V i förordningen. Det skulle innebära styrning som på sikt kan det leda till effektivare datadelning och att det blir enklare att upprätta nya datadelningar. Mot bakgrund av att offentliga organ i dagsläget bl.a. använder olika tekniska lösningar för datadelningen bedömer vi emellertid att konsekvenserna av att införa styrning som enbart avser datadelning med stöd av kapitlet i förordningen skulle bli för stora. Sådan styrning skulle kunna leda till höga och omotiverade kostnader, både hos offentliga organ och hos företag. För de offentliga organ och företag som inte använder

de tekniska och organisatoriska resurser samt digitala infrastrukturer som pekas ut genom styrning skulle anpassning krävas för det fall data begärs med stöd av kapitlet. Styrning i syfte att öka interoperabiliteten vid datadelning till och mellan offentliga organ kan visserligen vara nödvändig men styrningen bör inte vara isolerad till att enbart omfatta kapitel V i förordningen.

Regeringen avser som framgår ovan att presentera ett lagförslag om den offentliga förvaltningens datadelning. Arbete som kan leda till ökad interoperabilitet pågår som tidigare nämnts redan inom bl.a. Ena. Pågående och kommande arbete som syftar till att öka interoperabiliteten vid datadelning bör underlätta för offentliga organ att effektivt kunna ta emot, hantera, bearbeta och dela data som erhålls från företag med stöd av kapitel V i förordningen. Vi lämnar därför inga förslag om vad offentliga organ behöver i form av tekniska resurser, organisatoriska förmågor och digitala infrastrukturer som enbart avser kapitlet. Däremot lämnar vi nedan förslag som avser förberedelser och stöd till offentliga organ inom ramen för möjligheten att med stöd av kapitel V begära data för att hantera allmänna nödlägen.

7.11 Åtgärder för att underlätta datadelning i krissituationer

7.11.1 Exceptionella behov som grundar sig i ett allmänt nödläge bör prioriteras

Offentliga organ kan alltså begära data med stöd av kapitel V i förordningen om de har ett exceptionellt behov av data för att fullgöra sina lagstadgade skyldigheter av allmänt intresse. Sådana skyldigheter spänner över ett brett spektrum av uppgifter som har anförtrotts offentliga organ i Sverige. Om behovet grundar sig i att hantera ett allmänt nödläge gäller särskilda regler enligt förordningen.

Eftersom de data som kan begäras ska tillgodose ett exceptionellt behov som härrör från en lagstadgad skyldighet av allmänt intresse bör det falla inom ramen för det offentliga organets ordinarie verksamhet. Det kan visserligen krävas anpassningar om det offentliga organet begär data som den tidigare inte har tagit emot och använt. Att anpassningar krävs är emellertid inte ovanligt inom verksamheterna och offentliga organ har erfarenhet av det. Pågående och kommande arbete som syftar till att öka interoperabiliteten vid data-

delning bör underlätta för offentliga organ att effektivt kunna ta emot, hantera, bearbeta och dela data som erhålls från företag med stöd av kapitel V i förordningen.

Vi bedömer att inte finns skäl att föreslå åtgärder som avser begäran av data enligt kapitlet när det exceptionella behovet inte grundar sig att det offentliga organet ska hantera ett allmänt nödläge. När det gäller data för att hantera allmänna nödlägen gör vi emellertid en annan bedömning. Ett allmänt nödläge är enligt förordningen är en exceptionell situation, såsom ett hot mot folkhälsan, ett nödläge till följd av naturkatastrofer eller en större katastrof orsakad av människan, med negativa konsekvenser för befolkningen i unionen, en medlemsstat eller en del av en medlemsstat. Situationen medför en risk för allvarliga och bestående återverkningar på levnadsvillkoren eller den ekonomiska och finansiella stabiliteten eller avsevärd och omedelbar värdeminskning av ekonomiska tillgångar i unionen eller berörda medlemsstater. Tillgång till data kan underlätta hanteringen av sådana situationer, mildra konsekvenserna och underlätta återhämtning. När ett allmänt nödläge råder finns dessutom ett behov av att snabbt få tillgång till data. Samma tidskritiska aspekt finns inte om det exceptionella behovet grundar sig i något annat.

Enligt våra utredningsdirektiv ska vi föreslå vilka åtgärder som bör vidtas för att säkerställa att det hos de offentliga organen finns nödvändig kunskap för att ta emot, hantera, bearbeta och dela data från företag vid exceptionella omständigheter. Vi ska också föreslå hur effektiva samarbets- och kommunikationskanaler kan etableras och underhållas mellan företag och offentliga organ för att säkerställa snabb och säker datadelning vid exceptionella omständigheter. Mot bakgrund av de negativa konsekvenser ett allmänt nödläge kan få för samhället bedömer vi att åtgärder som syftar till att underlätta tillämpningen av kapitel V i förordningen för att hantera ett allmänt nödläge ska prioriteras.

7.11.2 Nuvarande ordning för krisberedskap är utgångspunkten för hantering av allmänna nödlägen

Samhällets krisberedskap kan beskrivas som förmågan att förebygga, motstå och hantera krissituationer. Förmågan byggs upp i den ordinarie verksamheten genom bl.a. utbildning, övning samt genom den organisation och de strukturer som skapas före, under och efter en kris (SOU 2023:50 s. 69). Utgångspunkten är att hela samhället gemensamt och inom sina respektive områden tar ansvar för och utvecklar krisberedskapsarbetet. I detta ligger också att enskilda människor utifrån sina egna förutsättningar tar ansvar för sin säkerhet. Arbetet sker på alla nivåer: lokalt, regionalt och nationellt, men också på EU-nivå och internationellt. Civilt försvar och krisberedskap regleras i lagar och förordningar. Fördelningen av ansvar och roller bygger även på följande grundläggande principer.

- Ansvarsprincipen – att den som har ansvar för en verksamhet i normala situationer också har motsvarande ansvar vid störningar i samhället. Aktörer har ett ansvar att agera även i osäkra lägen. Den utökade ansvarsprincipen innebär att aktörerna ska stödja och samverka med varandra.
- Närhetsprincipen – att samhällsstörningar ska hanteras där de inträffar och av de som är närmast berörda och ansvariga.
- Likhetsprincipen – att aktörer inte ska göra större förändringar i organisationen än vad situationen kräver. Verksamheten under samhällsstörningar ska fungera som vid normala förhållanden, så långt det är möjligt.

När en samhällsstörning inträffar finns det inte en särskild krisorganisation som tar över hanteringen, däremot kan verksamheten behöva gå upp i stabsläge eller aktivera en särskild krisledning. Alla som berörs av händelsen bidrar utifrån sitt ansvarsområde.

Aktörer med samordningsansvar

Vid större händelser berörs oftast flera delar av samhället, där olika aktörer har ansvar för sina respektive delar. För att samhället ska fungera under samhällsstörningen behöver de olika delarna fungera till-

sammans. Det gemensamma arbetet behöver samordnas, drivas och styras i en viss riktning för att vara effektivt. Det svenska beredskapssystemets arkitektur karakteriseras av en hierarkisk men decentraliserad struktur där ansvars-, närhets-, och likhetsprinciperna utgör grunden.

Myndigheten för samhällsskydd och beredskap (MSB) utgör den centrala samordnande myndigheten för krisberedskap och civilt försvar och har enligt sin instruktion i uppgift att stödja berörda myndigheters samordning av åtgärder vid en kris eller vid höjd beredskap. Myndigheten ska se till att berörda aktörer under sådana förhållanden, när det gäller krishantering och civilt försvar, får tillfälle att

- samordna åtgärder
- samordna information till allmänhet och medier
- effektivt använda samhällets samlade resurser och internationella förstärkningsresurser
- samordna stödet till centrala, regionala och lokala organ i fråga om information och lägesbilder.

Inom den statliga sektorn har 12 beredskapsmyndigheter enligt förordningen om statliga myndigheters beredskap ett definierat sektorsansvar. Dessa myndigheter är skyldiga att genomföra risk- och sårbarhetsbedömningar inom sina respektive ansvarsområden, vilka sedan sammanställs av MSB till en nationell helhetsbild.

Länsstyrelserna utgör en central komponent i det regionala beredskapssystemet genom att fungera som statens representant på regional nivå. Dessa myndigheter har enligt ett antal förordningar[20] ansvar för samordning av statliga myndigheters verksamhet inom länet vid krissituationer samt för stöd till kommunerna inom sitt geografiska ansvarsområde.

Kommunerna bär det primära ansvaret för räddningstjänst och lokal krishantering enligt lagen om skydd mot olyckor. MSB utövar tillsynsansvar gentemot kommunerna avseende denna verksamhet och tillhandahåller samtidigt råd, stöd och samordning på nationell nivå.

[20] Förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap, förordningen (2017:868) med länsstyrelseinstruktion, förordningen (2017:870) om länsstyrelsernas krisberedskap och uppgifter inför och vid höjd beredskap, samt förordningen (2022:525) om civilområdesansvariga länsstyrelser.

Samordningsverksamheten stöds av särskild teknisk infrastruktur, inbegripet radiokommunikationssystemet för skydd och säkerhet (RAKEL-systemet), den nationella kommunikationstjänsten Swedish Government Secure Intranet (SGSI) samt det webbaserade informationssystemet (WIS), vilka MSB förvaltar och tillhandahåller till berörda aktörer.

Systemet för krisberedskap bygger på etablerade processer för informationsdelning, lägesbildsframställning och resurstilldelning. MSB har möjlighet att ta fram förslag på prioritering och fördelning av förstärkningsresurser och driva samordningen av dessa samt samordning av varnings- och informationssystem till allmänheten. Vidare upprätthåller myndigheten beredskap med nationella stödresurser för assistans vid allvarliga olyckor och kriser.

MSB är vidare nationell cyberkrishanteringsmyndighet respektive CSIRT-enhet (Computer Security Incident Response Team) enligt EU:s NIS2-direktiv[21]. Denna struktur blir särskilt relevant för dataförordningens tillämpning vid cybersäkerhetsincidenter där snabb datainhämtning kan vara avgörande för nationell lägesbild och motåtgärder. MSB har även ansvar som gemensam nationell kontaktpunkt enligt samma direktiv, nationellt samordningscenter enligt EU:s CCCN-förordning[22] och är därutöver svensk teknisk kontaktpunkt gentemot OSSE:s verksamhet på cyberområdet.

MSB byter från och med den 1 januari 2026 namn till Myndigheten för civilt försvar. Det nya namnet syftar till att tydliggöra och markera myndighetens uppdrag inom civilt försvar.

Systemet för krisberedskap kan underlätta tillämpningen av kapitel V

Vi bedömer att nuvarande ordning för krisberedskap bör användas för att stödja svenska offentliga organ i deras förberedelser och i deras tillämpning av kapitel V i förordningen. Det finns redan en struktur på plats som kan underlätta för de offentliga organen att

[21] Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet).
[22] Europaparlamentets och rådets förordning (EU) 2021/887 av den 20 maj 2021 om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum.

så snabbt som möjligt få tillgång till nödvändiga data, som de tidigare inte har haft tillgång till, för att hantera ett allmänt nödläge.

7.11.3 Offentliga organ behöver stöd

Bedömning: Offentliga organ som kan begära data med stöd av kapitel V i dataförordningen behöver tillgång till stöd för att vara förberedda på att kunna begära samt använda data för att hantera ett allmänt nödläge.

Ett flertal offentliga organ i Sverige har uppgifter och uppdrag som innebär att de ska förbereda för eller hantera kriser av olika slag. För dessa organ kan ett exceptionellt behov av data för att hantera ett allmänt nödläge uppstå. Om behovet inte tillgodoses på annat sätt kan de välja att begära data med stöd av kapitel V i förordningen. Hur många företag i Sverige som i egenskap av datahållare är potentiella mottagare av begäran om att tillgängliggöra data går inte att fastslå eftersom det beror på många faktorer, bl.a. vilken typ av nödläge som råder samt vilka data som är nödvändiga för att hantera nödläget.

Vår bedömning är att offentliga organ bör förbereda sig för att kunna begära, ta emot och använda data om ett allmänt nödläge uppstår. När ett nödläge väl uppstår kommer behovet av data att snabbt behöva tillgodoses. Att inleda arbetet med förutsättningar för att ta emot och använda data först när nödläget uppstår riskerar att leda till att data inte kan komma till nytta tillräckligt snabbt.

Om offentliga organ på egen hand ska förbereda sig för att begära, ta emot och kunna använda data finns en överhängande risk att många lägger resurser på samma sak. Vi bedömer att det finns ett stort behov av stöd för att effektivisera processen genom att arbeta tillsammans.

Vi tror inte att det är rimligt att förvänta sig att offentliga organ kommer att bygga om sina it-system och sin digitala infrastruktur utifrån möjligheten att i framtiden eventuellt begära data för att kunna hantera ett allmänt nödläge. Organen behöver dock planera för hur de bör agera om de ska begära data när ett nödläge uppstår. För att detta arbete ska bli effektivt sett till hela den offentliga förvaltningen krävs enligt vår uppfattning stöd. Om arbetet med att förbereda, begära, ta emot, hantera samt använda data tar sin utgångspunkt i ett gemensamt stöd tror vi att arbetet kan bli mer effektivt än om varje

offentligt organ på egen hand måste arbeta med dessa frågor. Offentliga organ kan också behöva stöd i hur dataförordningens kapitel V ska tolkas och tillämpas.

En utmaning för offentliga organ kommer enligt vår bedömning att vara att få en fullgod bild av vilka data som finns att tillgå och som kan hjälpa till i hanteringen av ett allmänt nödläge, vilka datahållare som har sådana data samt i vilka format data är. Dataförordningen ställer inga krav på att datahållare ska informera offentliga organ om vilka data de innehar. Det finns enligt vår bedömning inte heller utrymme för medlemsstaterna att införa sådana krav. Även om det hade funnits en sådan möjlighet för medlemsstaterna anser vi att det hade varit en orimlig börda att lägga på datahållarna. Dessutom kan det finnas säkerhetsrisker med en så omfattande kartläggning av data som finns hos datahållare.

Datahållare behöver alltså inte informera offentliga organ om vilka data de innehar. Det kan dock finnas skäl för offentliga organ och datahållare att föra dialoger om data som potentiellt kan vara användbara när ett nödläge måste hanteras. Offentliga organ kan t.ex. bjuda in datahållare till sådana dialoger. Det finns fördelar med att sådana dialoger hålls i större forum i stället för att enskilda offentliga organ behöver arrangera dem.

För att underlätta för datahållare ser vi behov av att offentliga organ i förväg informerar om vad en begäran om att tillgängliggöra data vid exceptionella behov innebär. Även här blir stödet viktigt. Om offentliga organ i Sverige samordnar sig och begär data på samma eller likartat sätt är det också möjligt att lämna samlad information till datahållare. Det underlättar för datahållare att hitta informationen och bilda sig en uppfattning om vad de kan förvänta sig.

Ett företag som enligt en begäran från en myndighet ska tillgängliggöra data till ett offentligt organ kan få en begäran även från andra organ. Företaget kan exempelvis har olika verksamhetsgrenar, vilket kan innebära att olika data måste delas till olika myndigheter. Det kan också vara så att flera offentliga organ behöver samma datamängd från samma företag men för att hantera olika nödlägen eller för att hantera olika aspekter av samma nödläge. Det vore olyckligt om företag i sådana scenarion måste göra omfattande anpassningar utefter önskemål hos respektive offentligt organ. Som framgår ovan är vi medvetna om att offentliga organ bl.a. delar data genom olika tekniska lösningar. Förutsättningarna för att kunna använda data skiljer sig

åt mellan organen. Om offentliga organ utgår från ett gemensamt stöd i sitt arbete med att förbereda för att begära data med stöd av kapitel V i förordningen bör behovet av anpassningar hos de datahållare som ska tillgängliggöra data minska. Att helt komma bort från behovet av anpassningar tror vi emellertid inte är realistiskt.

7.11.4 Uppdrag till Myndigheten för samhällsskydd och beredskap att ge stöd till offentliga organ

Förslag: Regeringen ska ge Myndigheten för samhällsskydd och beredskap i uppdrag att ge stöd till svenska offentliga organ i deras arbete med att förbereda för att vid behov begära, ta emot och använda data med stöd av kapitel V i dataförordningen för att hantera allmänna nödlägen.

I uppdraget ska även ingå att identifiera om det finns behov av fortsatta åtgärder samt om uppdraget ska vara en permanent uppgift för myndigheten.

Uppdraget ska vara tidsbegränsat till ett år.

Ovan framgår att vi bedömer att offentliga organ som har möjlighet att begära data med stöd av kapitel V i dataförordningen behöver stöd för att vara förberedda på att kunna nyttja data för att hantera ett allmänt nödläge. Stödet bör bl.a. bestå i vägledning i hur organen kan underlätta för datahållare att så enkelt och säkert som möjligt tillgängliggöra data. Det bör ingå vägledning avseende hur tekniska resurser och organisatoriska förmågor kan användas för att underlätta tillämpning av kapitel V i förordningen. Vid behov kan utbildningar för offentliga organ hållas. Stödet syftar utöver att underlätta för offentliga organ och datahållare till att främja en hög nivå av säkerhet. Stödet bör också omfatta att löpande informera om vad datahållare kan förvänta sig om ett offentligt organ begär data, eftersom sådan information till datahållare förenklar för datahållarna och för de offentliga organen. Inom ramen för stödet bör dialog föras med datahållare eller representanter för datahållare om bl.a. de tekniska förutsättningarna för datadelning. Dialog kan också föras om ersättning för tillgänggörande av data och hur snabbt datahållare kan få ersättning för data som de tillgängliggör.

Uppdraget bör vara tidsbegränsat. Vi bedömer att rimlig tid som krävs för att genomföra uppdraget är ett år. I uppdraget bör också ingå att utreda om det finns behov av att uppdraget blir permanent, samt föreslå vilka eventuella åtgärder som i så fall krävs.

Stödet till de offentliga organens arbete med att förbereda och ta emot data enligt kapitel V i förordningen bör ledas av en statlig myndighet. Vi har övervägt om PTS bör få ett sådant uppdrag utöver sin roll som behörig myndighet. Det är dock inte lämpligt att den behöriga myndigheten ges ett sådant uppdrag. Som framgår av kapitel 4 i betänkandet ingår offentliga organ i den krets av aktörer som omfattas av den behöriga myndighetens uppdrag att säkerställa att dataförordningen följs. Det innebär att det finns risk för intressekonflikter om den myndighet som är behörig myndighet även ska ge stöd till vissa av dessa aktörer. PTS bör därför inte vara den statliga myndighet som ger stöd till offentliga organ.

Vi har även övervägt om Digg bör få uppdraget. Myndigheten ska enligt sin instruktion samordna och stödja den förvaltningsgemensamma digitaliseringen i syfte att göra den offentliga förvaltningen mer effektiv och ändamålsenlig[23] och bedriver arbete som har bäring på interoperabilitet och datadelning. Digg ska emellertid avvecklas och majoriteten av myndighetens uppgifter ska inordnas i PTS i januari 2027 (prop. 2025/26:1 Utgiftsområde 22). Som vi har konstaterat innebär risken för intressekonflikter att PTS inte bör få det uppdrag som vi föreslår.

Vidare har vi övervägt om MSB bör ges uppdraget. MSB har enligt sin instruktion ansvar för frågor om skydd mot olyckor, krisberedskap och civilt försvar, i den utsträckning inte någon annan myndighet har ansvaret.[24] Ansvaret avser åtgärder före, under och efter en olycka, kris, krig eller krigsfara. Myndigheten ska också bl.a. arbeta med och verka för samordning mellan berörda samhällsaktörer för att förebygga och hantera olyckor, kriser och konsekvenser av krig och krigsfara. Myndighetens ansvar beskrivs även i avsnitt 7.11.2.

Vi bedömer att MSB är bäst och väl lämpad för uppdraget att ge stöd till offentliga organ i deras arbete med att förbereda för att vid behov begära, ta emot och använda data med stöd av kapitel V i dataförordningen för att hantera allmänna nödlägen. Detta mot bakgrund

[23] 1 § förordningen (2018:1486) med instruktion för Myndigheten för digital förvaltning.
[24] 1 § förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap.

av att myndigheten redan i dag har samordningsuppdrag för att bl.a. förebygga och hantera olyckor och kriser. Myndigheten tillhandahåller t.ex. redan i dag vägledningar inom diverse områden och kan dra nytta av erfarenheterna från det arbetet. Vi föreslår därför att uppdraget ges till MSB.

Uppdraget bör utföras i samråd med Integritetsskyddsmyndigheten, eftersom det vid allmänna nödlägen är möjligt att begära personuppgifter med stöd av kapitel V i förordningen, samt med PTS.

7.11.5 Uppdrag till sektorsansvariga beredskapsmyndigheter att kartlägga förutsättningar

Förslag: Sektorsansvariga beredskapsmyndigheter ska ges i uppdrag att kartlägga tekniska och organisatoriska förutsättningar inom respektive beredskapssektor att begära, ta emot och använda data vid allmänt nödläge enligt kapitel V i dataförordningen.

Om förutsättningarna kan förbättras ska de sektorsansvariga myndigheterna lämna förslag till åtgärder som kan vidtas för att förbättra dem.

Uppdraget ska vara tidsbegränsat till ett år.

I förordningen om statliga myndigheters beredskap (beredskapsförordningen) finns bestämmelser om uppgifter för statliga myndigheter under regeringen inför och vid fredstida krissituationer och höjd beredskap. Av förordningens bilaga 1 framgår att 47 statliga myndigheter är beredskapsmyndigheter.

Enligt förordningen ska beredskapsmyndigheter bl.a. genomföra risk- och sårbarhetsanalyser samt ansvara för att egna informationshanteringssystem uppfyller sådana grundläggande och särskilda säkerhetskrav att myndighetens verksamhet kan utföras på ett tillfredsställande sätt. Enligt 20 § ska beredskapsmyndigheterna ha god förmåga att motstå hot och risker, förebygga sårbarheter, hantera fredstida krissituationer och genomföra sina uppgifter vid höjd beredskap. De ska även verka för att de övriga statliga myndigheter, kommuner, regioner, sammanslutningar och näringsidkare som är berörda utvecklar sin förmåga i dessa avseenden. I 20 § andra stycket sjunde punkten föreskrivs att beredskapsmyndigheterna särskilt ska beakta

behovet av säkerhet och kompatibilitet i de tekniska system som är nödvändiga för att myndigheterna ska kunna utföra sitt arbete.

Flera av beredskapsmyndigheterna ingår i beredskapssektorer. I varje beredskapssektor är en av beredskapsmyndigheterna sektorsansvarig myndighet. Enligt 24 § beredskapsförordningen ska en sektorsansvarig myndighet inom sin beredskapssektor leda arbetet med att samordna åtgärder inför och vid fredstida krissituationer och höjd beredskap. Den ska också driva på arbetet inom beredskapssektorn, stödja beredskapsmyndigheterna samt verka för att uppgifter och roller inom beredskapssektorn tydliggörs. Därutöver ska de verka för att de åtgärder som beredskapsmyndigheterna inom beredskapssektorn vidtar är samordnade med de åtgärder som andra beredskapsmyndigheter, inklusive länsstyrelser och civilområdesansvariga länsstyrelser, samt Försvarsmakten vidtar. En sektorsansvarig beredskapsmyndighet ska även verka för att samverkan med näringslivet sker i den utsträckning det behövs.

Det finns 12 beredskapssektorer och de sektorsansvariga myndigheterna är enligt förordningens bilaga 2 Försäkringskassan, PTS, Statens energimyndighet, Finansinspektionen, Skatteverket, Socialstyrelsen, Livsmedelsverket, Polismyndigheten, MSB, Trafikverket, Kommerskollegium och Tillväxtverket.

Som vi har konstaterat tidigare är det svenska beredskapssystemet relevant för möjligheten att begära data med stöd av kapitel V i dataförordningen när data behövs för att hantera ett allmänt nödläge. Beredskapsmyndigheterna behöver redan i dagsläget ha tillgång till data för att kunna utföra sina uppgifter och vi bedömer att dessa myndigheter i många fall är de myndigheter som kan komma att begära data med stöd av kapitel V i förordningen. Den datadelning som då ska komma till stånd underlättas av att förutsättningar kartläggs.

Ovan föreslår vi att MSB ska få ett tidsbegränsat uppdrag att ge stöd till offentliga organ vad gäller begäran av data med stöd av kapitel V i dataförordningen vid allmänna nödlägen. Stödet är av en allmän karaktär på så sätt att det ska rikta sig till samtliga offentliga organ som har uppgifter inom krishantering. Vi bedömer att detta stöd bör kompletteras med åtgärder hos beredskapsmyndigheterna i syfte att förbereda dem på möjligheten att begära data om behov uppstår.

Arbetet hos beredskapsmyndigheterna bör av effektivitetsskäl samordnas. Vi föreslår därför att de sektorsansvariga beredskapsmyn-

digheterna ges ett tidsbegränsat uppdrag avseende möjligheten att begära data med stöd av kapitel V i förordningen. Myndigheterna föreslås ges i uppdrag att kartlägga de tekniska och organisatoriska förutsättningarna för att kunna begära, och sedermera använda, data som begärs för att hantera ett allmänt nödläge. Som tidigare nämnts föreskrivs i 20 § andra stycket sjunde punkten beredskapsförordningen att beredskapsmyndigheterna särskilt ska beakta behovet av säkerhet och kompatibilitet i de tekniska system som är nödvändiga för att myndigheterna ska kunna utföra sitt arbete. Uppdraget ska därför innefatta bl.a. att kartlägga kompatibilitet i de tekniska systemen utifrån ett scenario där nya datamängder kan komma att begäras från företag med stöd av kapitel V. Vilka data och från vilka företag data kan komma att begäras kan skilja sig åt mellan olika beredskapssektorer. I uppdraget ska ingå att kartlägga förutsättningarna för att ta emot och använda nya datamängder i de tekniska systemen hos myndigheterna samt kartlägga tillgången till nödvändig digital infrastruktur för att begära och ta emot data samt vid behov dela data vidare. Enligt vår uppfattning är det troligt att data kan komma att begäras från andra offentliga organ än de som ingår i respektive beredskapssektor. Kartläggningen bör därför redovisas på ett sådant sätt att offentliga organ kan få inblick i de förutsättningar de har att beakta om de begär data. Om kartläggningen visar att förutsättningarna kan förbättras ska de sektorsansvariga beredskapsmyndigheterna lämna förslag till åtgärder som kan vidtas för att förbättra dem.

I avsnitt 7.11.4 bedömer vi att PTS, mot bakgrund av sin roll som behörig myndighet enligt dataförordningen inte bör få i uppdrag att ge stöd till offentliga organ vad gäller kapitel V i förordningen. Av skäl 107 i förordningen framgår att behöriga myndigheter inte bör ha rätt att begära data med stöd av kapitel V i förordningen. Detta för att undvika intressekonflikter. Uppdraget som vi föreslår här handlar om att kartlägga tekniska och organisatoriska förutsättningar inom bl.a. beredskapssektorn elektroniska kommunikationer och post. Datahållare som erbjuder elektroniska kommunikationstjänster innehar data som kan vara till stor nytta för att hantera ett allmänt nödläge. Myndigheter har uppgett att de under hanteringen av covid 19-pandemin hade stor hjälp av att följa bl.a. rörelsedata från telekomoperatörer (SOU 2022:10 s. 561). Ett exceptionellt behov av data från telekomoperatörer för att hantera ett allmänt nödläge kan alltså uppstå hos andra myndigheter än hos PTS. Det är enligt vår

uppfattning därför viktigt att den kartläggning vi föreslår sker även inom beredskapssektorn elektroniska kommunikationer och post. Eftersom PTS är sektorsansvarig myndighet är det naturligt att myndigheten leder det arbetet, även om myndigheten enligt skäl 107 i dataförordningen inte bör ha rätt att själv begära data. Eftersom uppdraget innebär kartläggning bedömer vi att det är förenligt med uppgiften att vara behörig myndighet, varför uppdraget också bör ges till PTS.

Uppdraget ska vara tidsbegränsat till ett år.

8 Åtgärder för att minska rättsliga och administrativa hinder

8.1 Inledning

Vi har i uppdrag att identifiera vilka administrativa och rättsliga hinder som svenska företag och offentliga organ kan möta vid tillämpningen av EU:s dataförordning och att föreslå åtgärder som bör vidtas för att minimera dessa hinder. I detta ingår att vi ska analysera och föreslå utbildnings- och informationsinsatser som behövs för att öka kunskapen om förordningens krav bland svenska företag och offentliga organ. Vi har även i uppdrag att föreslå hur tekniska och semantiska standarder och interoperabiliteten mellan system kan förbättras för att underlätta för svenska aktörer att uppfylla kraven i förordningen. Detta i syfte att underlätta för svenska företag och offentliga organ att förstå och enklare kunna efterleva dataförordningens bestämmelser, vilket ska bidra till att stärka företagens konkurrenskraft och den offentliga förvaltningens effektivitet.

Artikel 32 i dataförordningen föreskriver en möjlighet för leverantörer av databehandlingstjänster att begära särskilda yttranden från relevanta myndigheter eller organ i medlemsstaterna som har behörighet för internationellt samarbete i rättsliga frågor. Eftersom bestämmelsen syftar till att underlätta för leverantörerna av databehandlingstjänster att göra vissa bedömningar avseende datadelning till stater utanför EU har vi valt att behandla den frågan i detta kapitel.

8.2 Rättsliga hinder

8.2.1 Vad är rättsliga hinder?

Rättsliga hinder kan beskrivas som rättsregler som innebär att vissa åtgärder eller handlingar inte får vidtas. Det kan röra sig om regler i lagar, förordningar, föreskrifter, avtal och domstolsbeslut som sätter gränser för vad som är tillåtet. Rättsliga hinder kan vara alltifrån straffrättsliga regler som medför att vissa handlingar är olagliga och förbjudna till regler om formkrav som innebär att vissa åtgärder måste utföras på ett föreskrivet sätt.

Rättsliga hinder som uppstår när ett nytt regelverk införs bör föranleda behov att ändra befintliga författningar. Av förklarliga skäl kan vi bara föreslå ändringar av bestämmelser i svenska författningar. Vi har därför fokuserat på att utreda om det finns nationella regler som ger upphov till rättsliga hinder för företag och organisationer, för att identifiera om det finns behov av att föreslå författningsförändringar.

För myndigheter gäller särskilt att de behöver kunna agera i enlighet med förvaltningsrättsliga regler och reglerna i offentlighets- och sekretesslagen. Våra bedömningar avseende behov av författningsändringar i offentlighets- och sekretesslagen redovisar vi i kapitel 9. I detta avsnitt fokuserar vi på rättsliga hinder som rör företag.

Dataförordningen kommer att gälla parallellt med en stor mängd andra EU-rättsakter. Förordningen innehåller bestämmelser som uttryckligen behandlar hur dataförordningens bestämmelser ska samspela med vissa andra regelverk som har sin grund i EU-rätten. EU-domstolen har en tolkningsmetodik som innebär att konflikter löses ut genom att bruka de tolkningsprinciper som växt fram genom EU-domstolens praxis. Ur ett EU-rättsligt perspektiv bör det därför inte finnas rättsliga hinder mot parallell tillämpning av dataförordningen och andra rättsakter. Otydligheter kring vilka regler som ska gälla i det enskilda fallet utgör snarare ett administrativt hinder. Vi beskriver därför, utifrån detta perspektiv, i detta kapitel hur dataförordningen är tänkt att samspela med vissa andra närliggande EU-rättsakter som har genomförts i olika svenska lagar.

Företag och organisationer kan ha ingått avtal som innehåller villkor som står i strid med bestämmelserna i dataförordningen. Sådana avtalsrättsliga hinder är dock ofta en ofrånkomlig och avsedd konsekvens av införandet av nya lagar och förordningar. Det är ofrånkomligt

att avtalen måste anpassas utifrån bestämmelserna i dataförordningen. Att behöva se över avtal och t.ex. sina affärsmodeller innebär på så sätt administrativa hinder för aktörerna.

8.2.2 Svenska författningar hindrar inte tillämpningen av dataförordningen

Bedömning: Svenska författningar hindrar inte marknadsaktörerna från att tillämpa dataförordningen.

Vi har analyserat om det finns svenska författningar som hindrar marknadsaktörer från att tillämpa dataförordningens bestämmelser. Det skulle till exempel kunna röra sig om bestämmelser som står i strid med vad som föreskrivs i förordningen och som kan leda till att en åtgärd som ska vidtas enligt förordningen inte får vidtas eller att den inte får vidtas på det sätt som föreskrivs i förordningen.

Vi har utrett sådana hinder i horisontella svenska författningar och i sektorsspecifika författningar. Vi har emellertid inte identifierat några rättsliga hinder för företag eller organisationer att tillämpa dataförordningen. Vår bedömning är därför att svenska författningar som riktar sig till marknadsaktörer som omfattas av dataförordningen inte medför rättliga hinder mot att tillämpa förordningen. Vi har emellertid identifierat en risk för otydlighet när det gäller relationen mellan dataförordningen och 49 § upphovsrättslagen. Detta behandlas särskilt i kapitel 10.

Exempel på näraliggande regelverk som inte ska hindra tillämpningen av dataförordningen

Dataförordningen pekar ut vissa nationella rättsområden som inte ska påverkas av dataförordningen, om inte annat föreskrivs. Typiskt sett rör det sig om rättsområden som ligger nära reglerna i dataförordningen. I skäl 9 i förordningen anges t.ex. att dataförordningen inte påverkar nationell avtalsrätt, inbegripet regler om avtals ingående, giltighet eller verkan, eller konsekvenserna av hävning av ett avtal, såvida inte annat föreskrivs i förordningen. Vi har inte identifierat att svensk avtalsrätt uppställer krav som står i strid med förord-

ningen. I skäl 116 anges vidare att dataförordningen inte påverkar tillämpningen av konkurrensreglerna som särskilt baseras på artikel 101 och 102 EUF-fördraget, vilket konkurrenslagen (2008:579) gör. Att konkurrensreglerna inte ska påverkas av dataförordningen innebär att företagen vid t.ex. datadelning måste iaktta förbuden mot konkurrensbegränsande samarbeten och missbruk av dominerande ställning.

Därutöver nämns i dataförordningen uttryckligen att vissa regelverk som är harmoniserade inom EU genom implementering av olika direktiv, inte ska påverkas av dataförordningen. I skäl 31 konstateras att direktiv (EU) 2016/943 om företagshemligheter[1] föreskriver att anskaffande, utnyttjande eller röjande av en företagshemlighet ska anses som lagligt, bl.a. om sådant anskaffande, utnyttjande eller röjande krävs eller medges enligt unionsrätten eller nationell rätt. Dataförordningen kräver att datahållare röjer vissa data för användarna, eller för de tredje parter som väljs av en användare, även när dessa data uppfyller kraven för skydd i egenskap av företagshemligheter. Dataförordningen bör dock tolkas på ett sådant sätt att skyddet för företagshemligheter enligt direktivet om företagshemligheter bevaras. Detta direktiv är i Sverige genomfört genom lagen (2018:558) om företagshemligheter. Lagen innehåller bestämmelser om skadestånd, vitesförbud och straff för den som obehörigen angriper en företagshemlighet. Endast obehöriga angrepp på företagshemligheter omfattas av lagen. Röjande av företagshemligheter som sker i enlighet med dataförordningen bör inte utgöra ett obehörigt angrepp och lagen om företagshemligheter utgör således inte ett rättsligt hinder mot tillämpning av dataförordningen.

Vidare anges i skäl 9 i dataförordningen att förordningen kompletterar, och inte påverkar tillämpningen av, unionsrätt som syftar till att främja konsumenters intressen och säkerställa en hög nivå av konsumentskydd samt att skydda deras hälsa, säkerhet och ekonomiska

[1] Europaparlamentets och rådets direktiv (EU) 2016/943 av den 8 juni 2016 om skydd mot att icke röjd know-how och företagsinformation (företagshemligheter) olagligen anskaffas, utnyttjas och röjs.

intressen.[2] Sådana regler återfinns i bl.a. lagen (1994:1512) om avtalsvillkor i konsumentförhållanden, konsumentköplagen (2022:260) och lagen (2005:59) om distansavtal och avtal utanför affärslokaler. Dataförordningen innehåller inte bestämmelser om oskäliga avtalsvillkor i konsumentförhållanden, utan de regleras alltså i stället av de särskilda regelverken på konsumentområdet. I sammanhanget kan lagen (1984:292) om avtalsvillkor mellan näringsidkare nämnas. Enligt den lagen kan oskäliga avtalsvillkor mellan näringsidkare förbjudas av Patent- och marknadsdomstolen. Dataförordningen innehåller bestämmelser om oskäliga avtalsvillkor mellan företag (kapitel IV). Dessa får betraktas som speciallag i förhållande till lagen om avtalsvillkor mellan näringsidkare.

I skäl 12 i dataförordningen framgår att förordningen kompletterar, och inte påverkar tillämpningen, av unionsrätt som syftar till fastställande av tillgänglighetskrav för vissa produkter och tjänster, i synnerhet direktivet om tillgänglighetskrav för produkter och tjänster.[3] Direktivet är genomfört i lagen (2023:254) om vissa produkters och tjänsters tillgänglighet. Den lagen hindrar inte företagen att tillämpa dataförordningen.

Dataförordningen ska enligt artikel 1.8 vidare inte heller påverka tillämpningen av unionsrättsakter och nationella rättsakter som skyddar immateriella rättigheter.[4] I skäl 71 hänvisas vidare till direktivet om rättsligt skydd för databaser.[5] Regler på immaterialrättsområdet finns bl.a. i upphovsrättslagen. Som nämnts ovan behandlas dataförordningen och 49 § upphovsrättslagen i kapitel 10.

---

[2] I synnerhet rådets direktiv 93/13/EEG av den 5 april 1993 om oskäliga villkor i konsumentavtal; Europaparlamentets och rådets direktiv 2005/29/EG av den 11 maj 2005 om otillbörliga affärsmetoder som tillämpas av näringsidkare gentemot konsumenter på den inre marknaden och om ändring av rådets direktiv 84/450/EEG och Europaparlamentets och rådets direktiv 97/7/EG, 98/27/EG och 2002/65/EG samt Europaparlamentets och rådets förordning (EG) nr 2006/2004 (direktiv om otillbörliga affärsmetoder); samt Europaparlamentets och rådets direktiv 2011/83/EU av den 25 oktober 2011 om konsumenträttigheter och om ändring av rådets direktiv 93/13/EEG och Europaparlamentets och rådets direktiv 1999/44/EG och om upphävande av rådets direktiv 85/577/EEG och Europaparlamentets och rådets direktiv 97/7/EG.

[3] Europaparlamentets och rådets direktiv (EU) 2019/882 av den 17 april 2019 om tillgänglighetskrav för produkter och tjänster.

[4] Inbegripet Europaparlamentets och rådets direktiv 2001/29/EG av den 22 maj 2001 om harmonisering av vissa aspekter av upphovsrätt och närstående rättigheter i informationssamhället; Europaparlamentets och rådets direktiv 2004/48/EG av den 29 april 2004 om säkerställande av skyddet för immateriella rättigheter); samt Europaparlamentets och rådets direktiv (EU) 2019/790 av den 17 april 2019 om upphovsrätt och närstående rättigheter på den digitala inre marknaden och om ändring av direktiven 96/9/EG och 2001/29/EG.

[5] Europaparlamentets och rådets direktiv 96/9/EG av den 11 mars 1996 om rättsligt skydd för databaser.

8.3 Administrativa hinder

8.3.1 Vad är administrativa hinder?

Administrativa hinder kan vara regler, byråkratiska processer och krav som kan försvåra för företag, organisationer eller fysiska personer att genomföra olika typer av verksamheter. Sådana hinder kan leda till ökade kostnader och ineffektivitet. De kan även hindra innovation och tillväxt och innebära minskad konkurrenskraft för företag och organisationer. Administrativa hinder kan innefatta långa handläggningstider, omfattande rapporterings- eller dokumentationskrav eller krav på särskilda tillstånd. Hinder kan även uppstå till följd av mycket detaljerade regelverk eller av svårtolkade, komplexa eller överlappande regelverk, eftersom detta ger upphov till otydlighet. Vidare kan tillämpning av olika standarder som inte är kompatibla med varandra leda till administrativa hinder om det uppstår situationer där de som tillämpar de olika standarderna behöver samarbeta.

Sådana krav eller förhållanden ger upphov till en administrativ börda och ökade kostnader m.m. för företag, vilket kan ha negativa effekter för företagen och samhället i stort. Exempelvis kan konkurrenskraften motverkas. Det är dock inte nödvändigtvis fråga om hinder. I det följande använder vi därför även uttrycket administrativa utmaningar.

Sammantaget ställer dataförordningen upp många olika nya krav som berörda företag måste anpassa sina verksamheter efter. Det innebär bl.a. att avtals- och affärsmodeller måste ses över och anpassas och att rapporteringskrav ska iakttas. Detta innebär ofrånkomligen en administrativ börda och kostnader för aktörerna.

Dataförordningen utgör ett komplext regelverk som det inte är enkelt att få en överblick över eller förutse tillämpning eller tolkning av. Det föreligger bl.a. oklarheter kring hur begrepp ska tolkas och, inte minst, hur dataförordningen ska tillämpas parallellt med andra rättsakter. Detta trots att det i dataförordningen, som nämns ovan, framgår att förordningen inte ska påverka tillämpningen av diverse rättsakter. Särskilt inledningsvis kan dessa förhållanden, utöver de krav som dataförordningen i sig föreskriver, innebära väsentliga administrativa hinder för företag och organisationer som omfattas av förordningen. Dataförordningen är direkt tillämplig EU-rätt och det är således inte möjligt för medlemsstaterna att föreslå t.ex. förenklingar av regelverket som skulle innebära ett avsteg från dataförord-

ningens bestämmelser och krav. Åtgärder som vi kan överväga för att minska administrativa hinder eller utmaningar handlar därför primärt om myndigheters åtgärder som kan förtydliga dataförordningens innebörd och därigenom förenkla tillämpningen, liksom åtgärder som rör effektiv handläggning av ärenden.

Nationella lagstiftare bör inte tolka direkt tillämpliga EU-förordningar. Flera bestämmelser i dataförordningen syftar även till att underlätta för de berörda aktörerna att tillämpa förordningen. Ett exempel är standardisering och standardavtal på EU-nivå. Av detta följer begränsningar i vårt uppdrag, liksom i nationella myndigheters möjligheter att vidta förenklande åtgärder såsom riktlinjer och liknande. Den behöriga myndigheten kommer dock att ha en viktig roll att förklara och förtydliga reglernas innebörd.

Administrativa utmaningar till följd av EU:s dataförordning

Sammantaget ställer dataförordningen upp många olika krav som berörda företag måste anpassa sin verksamhet, vilket kan ge upphov till betydande administrativa kostnader. Exempelvis ställer dataförordningen krav på att data ska tillgängliggöras och delas på ett visst sätt. Företagen måste därför upprätta processer för att kunna dela data med andra aktörer enligt förordningen på ett säkert och kontrollerat sätt. Det kan innebära nya administrativa rutiner för att hantera förfrågningar om dataåtkomst och säkerställa att rätt data delas i rätt format enligt villkor som är förenliga med dataförordningen. Det kan även inkludera utbildning av personal om processerna så att de vet hur man hanterar förfrågningar korrekt och i tid. Dataförordningen ställer även krav på att data ska delas på ett säkert sätt och att företag måste införa tekniska och organisatoriska rutiner och säkerhetsrutiner för att skydda data mot obehörig åtkomst eller missbruk. Det kan kräva investeringar i nya it-system och nya interna processer. Sådana åtgärder kan kräva betydande investeringar och kostnader för löpande administration.

Vidare föreskriver dataförordningen regler om avtal och avtalsvillkor som bl.a. innebär vissa begränsningar av avtalsfriheten. Företag måste därmed anpassa eller ta fram nya avtal och avtalsmodeller avseende datadelning med kunder, leverantörer och samarbetspartners, som reglerar parternas rättigheter och skyldigheter i enlighet

med kraven i dataförordningen. Det kan kräva omfattande resurser i form av tid och juridisk kompetens. Att ta fram, förhandla och hantera nya eller anpassade avtal kan bli särskilt resurskrävande för företag som saknar juridisk expertis internt. För olika företag innebär dataförordningens nya krav sannolikt att de måsta anlita juridisk expertis för att ta fram nya avtalsmodeller som ska användas i olika situationer.

I dataförordningens ingress noteras bl.a. att det inom sektorer som kännetecknas av förekomsten av mikroföretag och små företag och medelstora företag ofta finns brist på digital kapacitet och färdigheter för att samla in, analysera och använda data (skäl 3). Vidare konstateras att små och medelstora företag samt företag från traditionella sektorer med mindre utvecklad digital kapacitet ofta har svårt att få åtkomst till relevanta data och att dataförordningen syftar till att underlätta åtkomsten till data för dessa enheter. Samtidigt omfattas dessa enheter av kraven i dataförordningen. Vissa särskilda bestämmelser om t.ex. rätt till ersättning och regeringslättnader gäller i syfte att säkerställa att skyldigheterna för små och medelstora företag är så proportionella som möjligt så att de inte blir alltför betungande (skäl 40). Vi kan dock sammantaget konstatera att dataförordningen medför särskilt stora administrativa utmaningar för små och medelstora företag som ofta saknar såväl digital kapacitet, kunskap i datafrågor och resurser i form av t.ex. juridisk expertis.

Åtgärder som exemplifieras ovan är sådana som krävs som en direkt konsekvens av att dataförordningen har börjat gälla. Det är företagen som ansvarar för att deras verksamheter och ageranden är förenliga med dataförordningens bestämmelser. Dataförordningen är direkt tillämplig och det finns inget utrymme för oss att föreslå förenklingar av regelverket. I det följande kommer vi därför inte att vidare beröra administrativa utmaningar och kostnader som direkt beror på att dataförordningen ställer ett visst krav.

8.4 EU:s roll för att minska administrativa utmaningar

8.4.1 Kommissionen

Enligt dataförordningen ska kommissionen vidta vissa särskilda åtgärder som syftar till att säkerställa harmonisering och efterlevnad av dataförordningen. Sådana åtgärder kan minska de administrativa utmaningarna för aktörer som omfattas av förordningen.

Enligt artikel 9.5 ska kommissionen anta riktlinjer för beräkningen av rimlig ersättning. Kommissionen ska beakta råd från Europeiska datainnovationsstyrelsen, som är behörig att lämna formella råd först sedan dataförordningen börjat gälla.

Kommissionen ska enligt artikel 41 i dataförordningen ta fram dels icke-bindande standardavtalsvillkor för åtkomst till och användning av data, inbegripet villkor om rimlig ersättning och skydd av företagshemligheter, dels icke-bindande standardavtalsklausuler för molnavtal. Syftet är att hjälpa parterna att utarbeta och förhandla fram avtal med rättvisa, rimliga och icke-diskriminerande avtalsenliga rättigheter och skyldigheter. Standardavtalsvillkoren bör enligt skäl 111 i första hand fungera som ett praktiskt verktyg som hjälper i synnerhet mikroföretag och små och medelstora företag att ingå avtal.

Kommissionen tillsatte under 2024 en expertgrupp[6] för att bistå kommissionen med denna uppgift. Baserat på en rapport från expertgruppen ska kommissionen anta en rekommendation. Expertgruppens slutliga rapport publicerades den 2 april 2025[7]. Rapporten innehåller olika standardavtalsvillkor och standardavtalsklausuler. Den 19 november 2025 publicerade kommissionen icke-bindande modelavtalsklausuler för tillgång till och användning av data och standardavtalsklausuler för molntjänstkontrakt.[8] Rekommendationen ska formellt antas av kommissionen först när alla språkversioner finns tillgängliga.

För de väsentliga krav avseende interoperabilitet som fastställs i artikel 33.1 har kommissionen befogenhet att anta delegerade akter för att ytterligare specificera de väsentliga kraven (med avseende på de krav som till sin natur inte kan ge den avsedda effekten om de

[6] Expert Group on B2B data sharing and cloud computing contracts (E03840).
[7] Final Report of the Expert Group on B2B data sharing and cloud computing contracts.
[8] Communication the to Commission, Approval of the draft Commission Recommendation on non-binding model contractual terms on data access and use and non-binding standard contractual clauses for cloud computing contracts (with Annexes), annexed hereto, C(2025) 7750 final.

inte specificeras närmare och för att korrekt återspegla den tekniska utvecklingen och marknadsutvecklingen (artikel 33.2). Enligt artikel 33.4 ska kommissionen begära att en eller flera europeiska standardiseringsorganisationer utarbetar harmoniserade standarder. Kommissionen får vidare, enligt artikel 33.5, genom genomförandeakter anta gemensamma specifikationer som omfattar något av eller alla de väsentliga kraven om villkoren i artikel 33.6 är uppfyllda.

Även avseende väsentliga krav för databehandlingstjänster som fastställs i punkterna 1 och 2 i artikel 35 får kommissionen, enligt artikel 35.4 och 35.5, begära att europeiska standardiseringsorganisationer utarbetar harmoniserade standarder, och genom genomförandeakter anta gemensamma specifikationer på grundval av öppna interoperabilitetsspecifikationer. I artikel 35.8 fastställs att kommissionen även genom genomförandeakter ska offentliggöra hänvisningar till harmoniserade standarder och gemensamma specifikationer för interoperabla databehandlingstjänster i ett centralt unionsregister.

Vad gäller smarta kontrakt ska kommissionen i enlighet med artikel 36.5 begära att en eller flera europeiska standardiseringsorganisationer utarbetar harmoniserade standarder som uppfyller de väsentliga krav som fastställs i artikel 36.1. Kommissionen får vidare, genom genomförandeakter, anta gemensamma specifikationer som omfattar något eller alla de väsentliga krav som fastställs i artikel 36.1, förutsatt att villkoren som anges i artikel 36.6 är uppfyllda.

Kommissionen uppger på websidan för dataförordningen att den kommer att fortsätta sitt engagemang med att samarbeta med företag, branschorganisationer och det civila samhället för att förtydliga bestämmelserna i förordningen och att utveckla praktiska verktyg för att stödja dess genomförande efter ikraftträdandet. Den pågående dialogen med berörda parter säkerställer att återkopplingen ligger till grund för framtida vägledning, håller genomförandet proportionerligt och bidrar till kommissionens bredare förenklingsagenda. Kommissionen har vidare för avsikt att inrätta en särskild juridisk helpdesk för dataförordningen för att ge företag direkt stöd i specifika frågor som rör tillämpningen av de nya reglerna.[9]

[9] https://digital-strategy.ec.europa.eu/en/policies/data-act (hämtad 2025-12-03).

8.4.2 Europeiska datainnovationsstyrelsen

Den europeiska datainnovationsstyrelsen (EDIB), som inrättats av kommissionen som en expertgrupp och i vilken behöriga myndigheter är företrädda, ska stödja en konsekvent tillämpning av dataförordningen. EDIB ska enligt artikel 42 i förordningen

a) ge råd till och bistå kommissionen när det gäller att utveckla en konsekvent praxis hos behöriga myndigheter avseende efterlevnaden av kapitlen II, III, V och VII

b) underlätta samarbete mellan behöriga myndigheter genom kapacitetsuppbyggnad och informationsutbyte, särskilt genom att fastställa metoder för ett effektivt informationsutbyte om efterlevnaden av rättigheterna och skyldigheterna enligt kapitlen II, III och V i gränsöverskridande fall, inbegripet samordning när det gäller fastställande av sanktioner

c) ge råd till och bistå kommissionen när det gäller i) huruvida det ska begäras att sådana harmoniserade standarder som avses i artiklarna 33.4, 35.4 och 36.5 utarbetas, ii) utarbetandet av de genomförandeakter som avses i artiklarna 33.5, 35.5, 35.8 och 36.6, iii) utarbetandet av de delegerande akter som avses i artiklarna 29.7 och 33.2, och iv) antagandet av de riktlinjer om fastställande av interoperabla ramar för gemensamma standarder och praxisformer för de gemensamma europeiska dataområdenas funktion som avses i artikel 33.11.

EDIB kommer således vara en arena för diskussioner mellan behöriga myndigheter och kommissionen i olika tillämpnings- och harmoniseringsfrågor. Styrelsen har en viktig roll när det gäller utvecklig av en konsekvent praxis och vid kommissionens framtagande av harmoniserade standarder, delegerade akter och riktlinjer.

8.5 Oklarheter kring hur dataförordningen samspelar med andra EU-rättsliga regelverk utgör administrativa hinder

Dataförordningen kommer sammantaget att gälla parallellt med en stor mängd andra EU-rättsakter. Förordningen innehåller bestämmelser som uttryckligen behandlar hur dataförordningens bestämmelser samspelar, och ska samspela, med andra regelverk som har sin grund i EU-rätten. Ur dataförordningens perspektiv finns det inte rättsliga hinder mot parallell tillämpning av dataförordningen och dessa andra regelverk. Bestämmelser i olika rättsakter kan dock vara motstridiga eller uppställa olika krav för olika situationer. Det gäller då att avgöra vilka regler som gäller i det enskilda fallet. Osäkerheter kring parallell tillämpning av regelverk skapar tillämpningsproblem och kan även hindra effektiv genomslagskraft av reglerna. Otydligheter kring vilka regler som ska gälla i det enskilda fallet utgör ett administrativt hinder för företagen. Företag behöver ofta juridisk och administrativ expertis för att tolka och följa olika regelverk parallellt.

Dataförordningen innehåller alltså bestämmelser som uttryckligen behandlar hur dataförordningens bestämmelser samspelar, och ska samspela, med vissa andra i förordningen utpekade rättsakter. Det gäller t.ex. dataskyddsförordningen[10] och sektorsspecifik reglering på dataområdet. Även om utgångspunkten för regleringen i dataförordningen tycks utgå från att regelverken samspelar väl, har flera aktörer under utredningens gång påtalat att det finns oklarheter kring hur olika rättsakter ska tillämpas parallellt. Dessutom använder olika rättsakter inte begrepp och termer på ett enhetligt sätt, vilken försvårar tillämpningen.

Dataförordningen är horisontellt tillämplig och det finns därför en mängd olika rättsakter som kommer att gälla parallellt för aktörerna. Det är inte möjligt eller ändamålsenligt att identifiera alla eventuella situationer där tillämpningsproblem kan uppstå. Nedan ger vi exempel på några områden där oklarheter vad gäller förhållandet mellan dataförordningen och andra regler kan innebära administrativa hinder.

[10] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

8.5.1 Samspelet mellan dataskyddsförordningens och dataförordningens bestämmelser

Av artikel 1.5 i dataförordningen följer att förordningen inte ska påverka reglerna om skydd för personuppgifter eller integritet i dataskyddsförordningen. Det anges vidare att, i den mån användare är registrerade, ska de rättigheter som fastställs i kapitel II i dataförordningen komplettera registrerades rättigheter till tillgång och rättigheter till dataportabilitet enligt artiklarna 15 och 20 i dataskyddsförordningen. Om dataförordningen står i strid med unionsrätten i fråga om skydd av personuppgifter eller integritet, eller med nationell lagstiftning som antagits i enlighet med sådan unionsrätt, har reglerna till skydd av personuppgifter eller integritet företräde.

Kommissionen understryker i sina Frequently Asked Questions att dataskyddsförordningen är fullt tillämplig på all behandling av personuppgifter som sker enligt dataförordningen. Dataförordningen reglerar inte skyddet av personuppgifter i sig utan har ett annat syfte. Syftet är att förbättra datadelning och möjliggöra en rättvis fördelning av värdet av data inom alla sektorer. Kommissionen konstaterar vidare att dataförordningen i vissa fall specificerar och kompletterar dataskyddsförordningen. Exempelvis gäller detta realtidsportabilitet av data från sakernas internet-objekt. I andra fall begränsar dataförordningen vidareutnyttjande av data av tredje part. Detta gäller t.ex. artikel 6 i dataförordningen om skyldigheter för tredje parter som tar emot data på användarens begära.[11]

Regelverken är alltså tänkta att tillämpas parallellt. Vid en eventuell konflikt gäller reglerna i dataskyddsförordningen före bestämmelserna i dataförordningen. Detta innebär inte att samspelet i praktiken är tydligt för berörda företag eller att tillämpningen är enkel.

8.5.2 Dataförordningen och datadelningsskyldigheter enligt andra rättsakter

Dataförordningen är en horisontell reglering som syftar till att förbättra rättvis tillgång till och användning av data inom alla sektorer av ekonomin. Kapitel III fastställer ett ramverk för villkor, ersättning och tekniska skyddsåtgärder som gäller närhelst en datainnehavare är skyldig enligt (annan) EU- eller nationell rätt att dela data med

[11] Frequently Asked Questions, Data Act, version 1.3, den 12 september 2005, s. 4.

en datamottagare. Dataförordningen och datadelningsskyldigheter i andra rättsakter ska således tillämpas parallellt och vi har uppfattat att detta ger upphov till otydligheter för aktörer som omfattas av sektorsspecifika regler.

Hur andra unionsrättsakter som reglerar rättigheter och skyldigheter avseende åtkomst till och användning av data ska samspela med dataförordningen beskrivs i artikel 41 och 44 i förordningen. Enligt artikel 41.1 ska dataförordningen inte påverka de specifika skyldigheterna att göra data tillgängliga mellan företag, mellan företag och konsumenter, och i undantagsfall mellan företag och offentliga organ, i unionsrättsakter som trädde i kraft senast den 11 januari 2024 (då dataförordningen trädde i kraft) och delegerade akter eller genomförandeakter som antagits på grundval av dessa. I artikel 44.2 föreskrivs vidare att dataförordningen inte påverkar sådan unionsrätt som, mot bakgrund av behoven inom en sektor, ett gemensamt europeiskt dataområde eller ett område av allmänt intresse, fastställer ytterligare krav. Detta gäller särskilt krav som avser tekniska aspekter på dataåtkomst, begränsningar av datahållares rätt att få åtkomst till eller använda vissa data som tillhandahålls av användarna och aspekter som går utöver åtkomst till och användning av data. I artikel 44.3 anges att dataförordningen, med undantag för kapitel V, inte påverkar tillämpningen av sådan unionsrätt och nationell rätt som föreskriver åtkomst till och godkännande av användning av data för vetenskapliga forskningsändamål.

Förhållandet till sektorspecifik reglering utvecklas i skälen i dataförordningen. I skäl 25 anges att förordningen inte hindrar sektorsspecifika regleringskrav enligt unionsrätten, eller nationell rätt som är förenlig med unionsrätten, som skulle utesluta eller begränsa datahållarens användning av vissa sådana data av tydligt definierade skäl grundade på offentlig policy. I skäl 27 anges att dataförordningen bör bygga vidare på senare tids utveckling inom enskilda sektorer, såsom uppförandekoden för delning av jordbruksdata genom avtal. Unionsrätt eller nationell rätt kan antas för att hantera sektorsspecifika behov och mål. Även i skäl 115 noteras att dataförordningen inte bör påverka tillämpningen av regler som avser behov som är specifika för enskilda sektorer eller områden av allmänt intresse. Sådana regler kan innefatta ytterligare krav som avser de tekniska aspekterna av åtkomsten till data, såsom gränssnitt för dataåtkomst, eller hur dataåtkomsten kan tillhandahållas, exempelvis direkt från en produkt

eller via dataförmedlingstjänster. Sådana regler kan också omfatta begränsningar av datahållares rätt till åtkomst till eller användning av användardata, eller andra aspekter utöver dataåtkomst och dataanvändning, såsom styrningsaspekter eller säkerhetskrav, inbegripet cybersäkerhetskrav. Dataförordningen bör inte heller påverka tillämpningen av mer specifika regler i samband med utvecklingen av gemensamma europeiska dataområden eller, med förbehåll för de undantag som anges i förordningen, unionsrätt och nationell rätt som föreskriver åtkomst till och godkännande av användning av data för vetenskapliga forskningsändamål.

I kommissionens Frequently Asked Questions förklarar kommissionen hur dataförordningen och datadelningsskyldigheter enligt andra regelverk ska samspela enligt följande. Det konstateras att artikel 44 i dataförordningen reglerar två viktiga aspekter för samverkan mellan dataförordningen och annan EU-lagstiftning som innehåller regler om åtkomst till och användning av data. Att dataförordningen enligt artikel 44.1 inte påverkar skyldigheter för datadelning som trädde i kraft före den 11 januari 2024 eller tidigare innebär att tidigare skyldigheter har företräde framför skyldigheter enligt dataförordningen. Om det införs EU-rättsakter med regler om datadelning efter den 11 januari 2024 och före den 12 september 2025 (då dataförordningen blev tillämplig) bör enligt kommissionen bästa möjliga ansträngningar göras för att säkerställa en anpassning, men det finns ingen rättslig skyldighet att göra det. Vidare förklarar kommissionen att artikel 44.2 tillåter att dataförordningen kompletteras med sektorsspecifika regler, när sådana behövs, avseende praktiska och tekniska modaliteter, såsom säkerhet, standardisering eller tekniska aspekter, eller med särskilda begränsningar för datahållares rätt att få tillgång till eller använda data från användare. Utvecklingen av sådana sektorsspecifika regler bör dock, enligt kommissionens, i största möjliga utsträckning hanteras med försiktighet och vara förenlig med principerna i dataförordningen, för att på så sätt undvika onödig komplexitet. Dataförordningens principer gäller för alla aspekter som rör ”åtkomst till data” som inte är särskilt reglerade genom sådana sektorsspecifika regler.[12]

Av detta följer att frågan om vilka regler som ska ha företräde avgörs dels av när de trädde i kraft, dels om de utgör regler som är avser sektorsspecifika behov.

[12] Frequently Asked Questions, Data Act, version 1.3, den 12 september 2005, s. 5.

Förordningen om det europeiska hälsodataområdet

En sektorsspecifik reglering som redan har trätt i kraft är förordningen om det europeiska hälsodataområdet (EHDS-förordningen).[13] EHDS-förordningen ger nya möjligheter att dela invånares hälsodata inom EU för gränsöverskridande vård och forskning m.m. Den publicerades den 5 mars 2025 och trädde i kraft den 26 mars 2025. Förordningen börjar tillämpas från och med 26 mars 2027 men olika bestämmelser kommer att börja tillämpas stegvis. Medlemsländerna kan genomföra flera etapper på frivillig basis, men de flesta av skyldigheterna kommer att börja gälla först fyra år efter det att förordningen trädde i kraft. Enligt förordningen ska kommissionen även anta olika genomförandetakter.

I EHDS-förordningen anges att det europeiska hälsodataområdet (EHDS) bygger på viktiga befintliga övergripande EU-ramar, bl.a. dataförordningen, dataskyddsförordningen, dataförvaltningsförordningen[14] och NIS 2-direktivet[15]. I artikel 1.3 i EHDS-förordningen anges att förordningen inte ska påverka andra unionsrättsakter om tillgång till, delning av eller sekundäranvändning av, elektroniska hälsodata eller unionskrav som rör behandlingen av data som innehåller elektroniska hälsodata, t.ex. dataförordningen.

I artikel 75.11 i EHDS-förordningen stadgas att medlemsstaterna och kommissionen ska sträva efter att säkerställa interoperabilitet mellan ehälsodataområdet och andra relevanta gemensamma europeiska dataområden som avses i dataförvaltningsförordningen och dataförordningen.

I förordningen anges även att organ för tillgång till hälsodata får bistå offentliga myndigheter när de får tillgång till elektroniska hälsodata i enlighet med artikel 14 i dataförordningen, och får tillhandahålla stöd till en offentlig myndighet när den erhåller data under de omständigheter som avses i artikel 15 i dataförordningen, i enlighet med reglerna i den förordningen, genom att ge tekniskt stöd till behandlingen av dessa data eller kombinera dem med andra data för

[13] Europaparlamentets och rådets förordning (EU) 2025/327 av den 11 februari 2025 om det europeiska hälsodataområdet och om ändring av direktiv 2011/24/EU och förordning (EU) 2024/2847.
[14] Europaparlamentets och rådets förordning (EU) 2022/868 av den 30 maj 2022 om europeisk dataförvaltning och om ändring av förordning (EU) 2018/1724 (dataförvaltningsakten).
[15] Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet).

gemensam analys. I skäl 61 uppges att offentliga myndigheter måste kunna agera bortom det exceptionella behov som avses i kapitel V i dataförordningen. Organ för tillgång till hälsodata bör dock tillåtas att ge stöd till offentliga myndigheter när de behandlar eller kopplar samman data. EHDS-förordningen ger offentliga myndigheter möjlighet att få tillgång till information som de behöver för att fullgöra sina uppgifter enligt förordningen men utvidgar inte uppdraget för sådana offentliga myndigheter.

8.5.3 Olika definitioner av begrepp i olika rättsakter skapar administrativa hinder

Företag och andra aktörer som omfattas av dataförordningen omfattas i stor utsträckning av andra regleringar på angränsande områden, exempelvis inom området data och datadelning men även t.ex. av rättsakter som ställer krav på produkter. Flera aktörer har under utredningens gång påtalat att sådana samtidigt tillämpliga regelverk innehåller olika definitioner av lika eller likartade begrepp och termer. Användningen av olika begrepp och definitioner i olika regelverk utgör ett administrativt hinder för företag eftersom det skapar oklarheter kring hur regler ska tolkas och tillämpas. Företagen kan behöva lägga resurser på att förstå skillnaderna, vilket ökar risken för fel och leder till dubbelarbete, särskilt vid rapportering till olika myndigheter. Det kan även försvåra digitalisering och effektivisering av interna processer, vilket i sin tur medför ökade administrativa kostnader.

Under utredningens gång har påtalats att olika rättsakter som ska tillämpas samtidigt innehåller olika definitioner kring produkter. Exempelvis finns i produktsäkerhetsförordningen en definition av ”produkt”, dataförordningen ger en definition av en ”uppkopplad produkt”; cybersäkerhetsakten har en definition av ”IKT-produkt” och cyberresiliensförordningen definierar ”produkt med digitala element” och så vidare.[16] Alla dessa rättsakter ställer i huvudsak krav

[16] Förordning (EU) 2023/988 om allmän produktsäkerhet, ändring av förordning (EU) nr 1025/2012 och direktiv (EU) 2020/1828 och om upphävande av direktiv 2001/95/EG och direktiv 87/357/EEG; Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten); respektive Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen).

på produkter som ska släppas ut på EU-marknaden och ska tillämpas samtidigt.

Vidare definieras ”data” i förordningen om en ram för det fria flödet av andra data än personuppgifter i EU[17] som andra uppgifter än personuppgifter. I dataförordningen avses med ”data” i stället varje digital återgivning av handlingar, fakta eller information och varje sammanställning av sådana handlingar, fakta eller information, även i form av ljudupptagningar, bildupptagningar eller audiovisuella upptagningar.[18]

Inkonsekvens vad gäller definitioner försvårar som beskrivits ovan företagens tillämpning av olika regler. Vi konstaterar att det vore önskvärt med en översyn av definitioner och begrepp i olika rättsakter så att enhetlighet uppnås. Detta är dock åtgärder som måste vidtas på EU-nivå.

8.5.4 Slutsats om administrativa hinder som beror på otydligheter om hur olika regelverk samspelar

Sammantaget konstaterar vi att det finns ett stort antal rättsakter inom området data och datadelning men även andra rättsakter som ställer krav på produkter m.m. som kommer att vara parallellt tillämpliga för aktörer som bedriver verksamhet inom EU. Att användningen av olika begrepp kan skilja sig mellan regelverken försvårar tillämpningen och medför administrativa hinder för företagen och andra aktörer. Vi har dock inte identifierat åtgärder på nationellt plan som kan undanröja eller minska dessa administrativa hinder.

Det är dock tydligt att frågan om olika regelverks förhållande till varandra skapar osäkerhet och utgör ett väsentligt administrativt hinder. I den mån det är möjligt bör myndigheter som tillämpar de olika regelverken, t.ex. tillsynsmyndigheter på områdena, bidra till ökad tydlighet i detta avseende.

[17] Europaparlamentets och rådets förordning (EU) 2018/1807 av den 14 november 2018 om en ram för det fria flödet av andra data än personuppgifter i Europeiska unionen.
[18] Dataförvaltningsförordningen innehåller snarlik definition av data, dock med vissa skillnader (artikel 2.1).

8.6 Tekniska och semantiska standarder samt interoperabilitet mellan system

8.6.1 Inledning

Interoperabilitet är en förutsättning för att datadelning ska vara effektiv. Utredningen om interoperabilitet vid datadelning konstaterade att det finns ett flertal olika definitioner av interoperabilitet och att de i allmänhet tar sikte på förmågan hos informationssystem att fungera tillsammans vid utbyte av data (SOU 2023:96 s. 39). Ibland innehåller definitionerna också förmågor hos verksamheter och organisationer. I artikel 2.40 i dataförordningen definieras interoperabilitet som förmågan hos två eller fler dataområden eller kommunikationsnät, system, uppkopplade produkter, applikationer, databehandlingstjänster eller komponenter att utbyta och använda data för att utföra sina funktioner. För att datadelning ska vara effektivt krävs att data får och kan delas, men det krävs också att data sedan kan förstås och användas. För att interoperabilitet ska uppnås krävs att rättsliga, organisatoriska, semantiska och tekniska förutsättningar finns på plats.[19]

För att uppnå interoperabilitet kan exempelvis gemensamma standarder och vokabulärer användas. Tekniska lösningar som är kompatibla med varandra ökar förutsättningarna för interoperabilitet. Även metadata ökar förutsättningarna eftersom de underlättar för den som ska använda data att förstå data.

I en enkätstudie genomförd inom EU:s publika konsultation avseende den då överenskomna dataförordningen framkommer flera hinder för delning av data mellan företag. Tekniska hinder, såsom format och brist på standarder, identifierades som ett väsentligt hinder. Vi har också inom ramen för vårt arbete fått till oss att interoperabilitet är en utmaning när det kommer till tillämpningen av dataförordningen. Det beror bl.a. på att gemensamma standarder saknas, exempelvis inom sektorer, eller att gemensamma standarder inte används av alla. Avsaknad av interoperabilitet leder till att anpassningar krävs när data ska delas. Det kan krävas anpassningar hos den som delar data och den som ska ta emot och använda data. Detta leder följaktligen till ökade kostnader.

[19] I det Europeiska interoperabilitetsramverket är utgångspunkten att interoperabilitet består av fyra lager: rättslig, organisatorisk, semantisk och teknisk interoperabilitet.

8.6.2 Dataförordningens bestämmelser om interoperabilitet

Dataförordningen innehåller bestämmelser som syftar till att öka interoperabiliteten. Dessa tar sikte på databehandlingstjänster och dataområden. Enligt artikel 30 ska vissa leverantörer av databehandlingstjänster, beroende på vilken tjänst de erbjuder, säkerställa kompatibilitet med gemensamma specifikationer som bygger på öppna interoperabilitetsspecifikationer[20] eller harmoniserade standarder[21] för interoperabilitet. Krav på öppna interoperabilitetsspecifikationer och harmoniserade standarder för interoperabla databehandlingstjänster och hur dessa fastställs föreskrivs i artikel 35.

Vidare föreskrivs i artikel 33.1 att deltagare i dataområden som erbjuder data eller datatjänster till andra deltagare ska uppfylla ett antal väsentliga krav för att underlätta interoperabiliteten mellan data, datadelningsmekanismer och datadelningstjänster samt mellan gemensamma europeiska dataområden. Kommissionen får med stöd av artikel 33.2 anta delegerade akter som ytterligare specificerar de väsentliga kraven. Av artikel 33.5 framgår också att kommissionen begära att en eller flera europeiska standardiseringsorganisationer utarbetar harmoniserade standarder som uppfyller de väsentliga kraven. Att kommissionen har sådan befogenhet framgår också av artikel 10.1 i förordningen om europeisk standardisering.[22] Enligt den bestämmelsen får kommissionen, inom ramen för de befogenheter som fastställs i fördraget, begära att en eller flera europeiska standardiseringsorganisationer utarbetar en europeisk standard eller en europeisk standardiseringsprodukt inom en viss tidsfrist. Europeiska standarder och europeiska standardiseringsprodukter ska vara marknadsdrivna, ta hänsyn till allmänintresset och de politiska mål som tydligt angetts i kommissionens begäran och ska bygga på samförstånd.

Enligt artikel 42 i dataförordningen ska EDIB stödja en konsekvent tillämpning av förordningen. Vissa av EDIB:s uppgifter innefattar interoperabilitet, eftersom den bl.a. ska ge råd till och bistå

[20] En öppen interoperabilitetsspecifikation är enligt definitionen i artikel 2.41 en teknisk specifikation på informations- och kommunikationsteknikområdet som är resultatinriktad på att uppnå interoperabilitet mellan databehandlingstjänster.
[21] Harmoniserad standard är enligt definitionen i artikel 2.43 i dataförordningen densamma som enligt artikel 2.1 c i Europaparlamentets och rådets förordning (EU) nr 1025/2012 av den 25 oktober 2012 om europeisk standardisering och om ändring av rådets direktiv 89/686/EEG och 93/15/EEG samt av Europaparlamentets och rådets direktiv 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG och 2009/105/EG samt om upphävande av rådets beslut 87/95/EEG och Europaparlamentets och rådets beslut 1673/2006/EG.
[22] Se föregående not.

kommissionen när det gäller om det ska begäras att harmoniserade standarder utarbetas, utarbetande av genomförandeakter och antagandet av riktlinjer om fastställande av interoperabla ramar för gemensamma standarder och praxisformer för de gemensamma europeiska dataområdenas funktion.

8.6.3 Interoperabilitetsarbetet bör bedrivas på EU-nivå

De aktörer som ska dela data eller ta emot och använda data enligt dataförordningen kommer att behöva göra detta utifrån sina nuvarande förutsättningar. Förordningen innehåller bestämmelser som innebär att data ska delas. Den tar också höjd för att det kommer att krävas ytterligare specifikationer och gemensamma standarder som ökar interoperabiliteten och därigenom leder till förbättrade möjligheter att dela, ta emot och använda data. Dessa specifikationer och gemensamma standarder finns i stora delar emellertid ännu inte på plats. Med det sagt finns det en mängd specifikationer och standarder som i många fall visserligen kan användas men det saknas utpekanden av dem i enlighet med förordningen. Det riskerar oundvikligen att leda till osäkerhet, särskilt hos datahållare som ska uppfylla kraven i förordningen. Det riskerar också att leda till att datahållare behöver göra investeringar för att leva upp till kraven i förordningen. Om t.ex. standarder i ett senare skede kommer på plats kan datahållare hamna i en situation där de behöver göra ytterligare en investering för att anpassa sig till dessa standarder. Det finns därför ett behov av skyndsamhet när det gäller att genom specifikationer och standarder peka ut hur data ska delas i syfte att uppnå en hög nivå av interoperabilitet, inte bara att data ska delas. Om arbetet tar för lång tid kan det som framgår ovan riskera att leda till högre kostnader än vad som annars hade varit fallet. Dessutom finns en risk att medlemsstater vidtar nationella åtgärder, i ett försök att öka interoperabiliteten på nationell nivå, som senare kan visa sig inte vara förenliga med de åtgärder som vidtas på EU-nivå. En sådan situation är enligt vår uppfattning inte önskvärd eftersom även den riskerar att leda till bl.a. ökade kostnader. Dessutom är det inte självklart att medlemsstaterna kan vidta sådana åtgärder. I förordningen fastställs harmoniserade regler om datadelning inom EU och eventuella nationella initiativ om hur data ska delas riskerar att leda till fragmentering.

Interoperabilitetsarbetet med anledning av dataförordningen ska bedrivas på EU-nivå. Kommissionen och EDIB spelar en stor roll i arbetet. Detsamma gäller standardiseringsorganisationerna. Medlemsstaterna spelar emellertid också en viktig roll när det kommer till att bidra i arbetet och tillvarata de intressen som aktörer som omfattas av dataförordningen har. Mot bakgrund av EDIB:s uppgifter kommer PTS, i egenskap av behörig myndighet i Sverige, också att spela en roll i det interoperabilitetsarbete som bedrivs på EU-nivå. I avsnitt 8.7.2 redogör vi för vår uppfattning om vilken roll PTS bör ha i detta arbete.

8.7 Post- och telestyrelsens roll för att minska administrativa hinder

Vi har alltså i uppdrag att föreslå åtgärder som bör vidtas för att minimera administrativa hinder. I detta ingår att vi ska analysera och föreslå utbildnings- och informationsinsatser som behövs för att öka kunskapen om förordningens krav bland svenska företag och offentliga organ. Vi bedömer att det främst är den behöriga myndigheten, PTS, som kan föreslås vidta åtgärder för att minska de administrativa hindren för företagen.

8.7.1 Vilka typer av åtgärder kan minska administrativa hinder?

I allmänhet finns det en rad åtgärder som det allmänna typiskt sett kan vidta eller verka för. Genom att förenkla regler och göra dem mer enhetliga minskar risken för missförstånd och felaktig tolkning. Vi konstaterar åter att dataförordningen är direkt tillämplig och att det därför inte är aktuellt för oss att överväga eller föreslå förenklingar för att minska administrativa hinder. Även standardisering av regler mellan olika myndigheter inom ett land eller i olika länder, kan minska komplexiteten. Vad gäller dataförordningen är själva syftet att främja effektiv datadelning. Redan förhållandet att EU beslutat om enhetliga regler i en förordning om åtkomst till och delning av data är ett steg mot att skapa just enhetliga regler för datadelning inom unionen. Vidare innehåller förordningen bestämmelser om standardisering, varför standardisering inte bör föreslås på nationell nivå. För att säkerställa att regler inte skapar onödiga hinder kan myndigheter

ibland genomföra utvärderingar i syfte att vid behov förenkla eller avveckla regler som inte fungerar som det är tänkt. Enligt artikel 49 dataförordningen ska kommissionen senast den 12 september 2028 genomföra en utvärdering av dataförordningen och lämna en rapport om de viktigaste resultaten till Europaparlamentet, rådet och Europeiska ekonomiska och sociala kommittén. Artikeln nämner vidare vissa frågor och områden som särskilt ska vara föremål för utvärdering. Att överväga särskilda nationella utvärderingsåtgärder avseende själva förordningen är därmed inte aktuellt. Däremot finns det skäl att utvärdera konsekvenserna av förordningen (se avsnitt 12.9).

PTS har som behörig myndigheter enligt dataförordningen i uppdrag att öka medvetenheten bland de aktörer som omfattas av förordningen om deras rättigheter och skyldigheter. Utöver den roll som PTS har genom att utöva tillsyn är främjandet ett viktigt led för att förordningen ska efterlevas och få åsyftad genomslagskraft. Att tillhandahålla tydlig information och instruktioner om komplexa regelverk är viktigt för reglernas genomslagskraft. PTS roll som informationspunkt är enligt vår uppfattning viktig, se avsnitt 8.7.2.

Behovet av information och stöd är särskilt stort i det inledande skedet där det föreligger osäkerheter kring hur dataförordningen ska tillämpas i olika situationer. Efterlevnaden av tillämpliga regler är berörda aktörers egna ansvar. Myndigheter bör generellt sett inte lämna rättslig rådgivning i enskilda fall utan rådgivande och upplysande verksamhet bör begränsas till att förklara innebörden av olika regelverk som de har ansvar för, på ett tydligt sätt. Myndigheter kan inte heller via sådan verksamhet lämna besked till enskilda som de är bundna av i sin egen tillsyn. Införandet av nya komplexa regler kan dock ställa mycket stora krav på företag som omfattas av reglerna. Det gäller särskilt för mindre företag med begränsade resurser.

Ett särskilt verktyg för att förenkla tillämning av nya regelverk är s.k. regulatoriska sandlådor eller regulatorisk testverksamhet. Det handlar i grunden om att testa nya eller innovativa lösningar i en kontrollerad miljö för att se hur de fungerar i praktiken och om de uppfyller ett visst regelverk. Nyttan av regulatoriska sandlådor är särskild stor när det gäller komplexa regelverk. Det behöver inte bara handla om nya tekniska produkter eller tjänster, utan det kan även handla om att exempelvis testa om avtalsvillkor, processer eller nya affärsmodeller är förenliga med regelverket i fråga. I stället för att direkt implementera t.ex. nya avtalsvillkor i stor skala (med risk att

överträdelser kan anses föreligga), kan aktörerna använda en sandlåda för att testa villkoren i en begränsad och övervakad miljö. Dataförordningen är ett mycket komplext regelverk och vi menar därför att det skulle vara lämpligt att PTS ges i uppdrag att inrätta regulatorisk testverksamhet. Detta förslag presenteras nedan i avsnitt 8.7.6.

8.7.2 PTS roll som informations- och kontaktpunkt

Myndigheter kan ta fram vägledningar och förklaringar, t.ex. dokument med ”vanliga frågor och svar” som förklarar begrepp och reglers innebörd, vilket underlättar för företag att göra rätt och agera mer effektivt. Sådana uppgifter ligger inom ramen för PTS roll att främja kunskapen om dataförordningen. Främjandearbete kan även ske genom att myndigheter lämnar tydlig information på sina webbplatser och genomför riktade informationsmöten och upplysningskampanjer. Sådana åtgärder underlättar för berörda aktörer att göra rätt och kunna tillgodogöra sig sina rättigheter.

Som vi konstaterat är utrymmet för PTS att ta fram egna vägledningar om tillämpningen av dataförordningen begränsat eftersom dataförordningen är en direkt tillämplig rättsakt vars innebörd avgörs i rättstillämpningen, t.ex. inom armen för ett tillsynsärende, och där tolkningen ytterst avgörs av EU-domstolen. En viktig uppgift för PTS som främjandemyndighet är dock att fungera som en enhetlig och transparant informationspunkt. Här kan exempelvis webbplatsen vara en viktig ingångspunkt. Det är inte enkelt att navigera bland och hitta all relevant EU-rättslig information, och det är inte heller lätt att följa vilka riktlinjer och liknade åtgärder som tas fram. PTS kan enligt vår uppfattning därför med fördel lägga resurser på att tillhandahålla relevant och uppdaterad information via en enhetlig informationspunkt på myndighetens webbplats, lämpligen en särskild portal eller plattform.

På en sådan informationspunkt kan tillämpliga rättsakter och vägledande dokument av kommissionen eller EDIB publiceras. I den mån det bedöms som lämpligt, kan material från EU översättas. I takt med att PTS fattar egna tillsynsbeslut kan dessa, liksom information om domar och beslut från EU-domstolarna och viktiga beslut eller avgöranden i andra medlemsstater, samlat publiceras via informationspunkten.

PTS kan vidare anordna olika informationsmöten och workshops. Dataförordningen är dock brett tillämplig vilket innebär att det finns vitt skilda målgrupper som i olika grad har skyldigheter respektive rättigheter enligt förordningen. Informationsinsatser i förhållande till stora företag respektive små förtag kan skilja sig åt, och inte minst konsumenter kan ha särskilda behov av information. Det förhållandet att dataförordningen omfattar så olika typer av aktörer och branscher, på olika sätt, innebär att det kommer att vara utmanande för myndigheten att vidta informationsåtgärder som är tillräckligt relevanta för olika målgrupper. Diskussioner kan förslagsvis föras och utbildningar hållas inom t.ex. olika branschorganisationer eller samarbetsforum som är väl insatta i medlemmarnas behov. Det finns även en rad olika utbildningsföretag som sannolikt kommer att erbjuda utbildningar om dataförordningen.

PTS har sammantaget uppgifter inom flera områden som innefattar främjande av nya rättsakter, och det får förutsättas att myndigheten kommer att prioritera och utforma insatser på ett ändamålsenligt sätt. Vi ser inga skäl att föreslå vilka mer exakta informationsinsatser som bör prioriteras av PTS. Dock förordar vi att PTS särskilt fokuserar på information till konsumenter och mindre företag.

8.7.3 PTS roll för att öka datakompetensen

Behöriga myndigheter ska ha i uppdrag att öka datakompetensen. Vad som avses med datakompetens förklaras i skäl 19 i dataförordningens ingress. Med datakompetens avses färdigheter, kunskap och förståelse som gör det möjligt för användare, konsumenter och företag, särskilt mikroföretag och små och medelstora företag som omfattas av förordningen, att dels bli medvetna om det potentiella värdet av de data de genererar, producerar och delar, dels bli motiverade att erbjuda och ge åtkomst till sina data i enlighet med relevanta rättsliga regler. Datakompetens bör omfatta mer än kunskaper om verktyg och teknik och syfta till att ge medborgare och företag förmåga och egenmakt att dra nytta av en inkluderande och rättvis datamarknad. Det anges vidare särskilt att de behöriga myndigheterna bör främja verktyg och anta åtgärder för att förbättra datakompetensen bland de användare och enheter som omfattas av dataförordningen samt öka medvetenheten om deras rättigheter och skyldigheter.

PTS ska alltså vidta åtgärder som främjar datakompetensen enligt vad som anges i förordningen. Det bör enligt vår mening innefatta både att öka olika aktörers generella medvetenhet om nyttan och värdet av data och datadelning och om att öka kunskap om verktyg och teknik, inklusive frågor om interoperabilitet.

PTS har erfarenhet av arbete på dataområdet genom bl.a. rollen som samordnare enligt förordningen om digitala tjänster och som tillsynsmyndighet enligt dataförvaltningsförordningen. Från och med den 1 januari 2027 ska Myndigheten för digital förvaltning, (Digg) inordnas i PTS. Digg:s uppgifter innefattar bl.a. att arbeta för att främja tillgängliggörande och vidareutnyttjande av data från den offentliga förvaltningen. Digg tillhandahåller t.ex. riktlinjer och verktyg som ska underlätta utvecklingen av effektiva och interoperabla API:er. Inordningen av Digg i PTS bör enligt vår bedömning stärka den behöriga myndighetens förmåga att främja kunskapen om data, datadelning och interoperabilitetsfrågor.

Det är upp till PTS som behörig myndighet att, med beaktande av kraven i dataförordningen, kompletteringslagen och kompletteringsförordningen, utforma sin främjandeverksamhet även vad gäller att öka datakompetensen.

8.7.4 PTS processer för handläggning av ärenden

PTS kommer att behöva utveckla interna processer och rutiner för handläggningen av ärenden enligt dataförordningen. PTS kan med fördel på sin webbplats tydligt beskriva relevanta regler kring klagomålshantering, inklusive hur de olika nationella behöriga myndigheterna hanterar klagomål sinsemellan. Det skulle sannolikt underlätta för användare, datahållare och andra som fattas av dataförordningen om PTS tar fram och publicerar formulär för t.ex. klagomål, anmälan om rättslig företrädare, anmälan av att datadelning har begränsats enligt artikel 4.7 och 5.10 i dataförordningen (s.k. handbroms avseende företagshemligheter) och andra specifika situationer. För att underlätta för berörda aktörer kan det även vara bra om det finns en lista över kontaktpunkter i andra medlemsstater.

PTS har bl.a. inom ramen för uppdraget att vara samordnare enligt EU:s förordning om digitala tjänster utvecklat en e-tjänst där användare kan lämna in klagomål och ett ärendehandläggningssystem för

handläggningen av inkomna klagomål. Vi bedömer att en sådan ordning med fördel kan gälla även för hantering av ärenden enligt dataförordningen.

8.7.5 PTS samarbete med andra myndigheter och kommissionen

Den behöriga myndigheten ska enligt dataförordningen samverka med svenska tillsynsmyndigheter inom andra rättsområden och sektorsmyndigheter. PTS kommer även som behörig myndighet delta i samarbeten inom ramen för EDIB. Genom att ingå i det samarbetet ges myndigheten god möjlighet att diskutera t.ex. tolknings- och tillämpningsfrågor med andra behöriga myndigheter och med kommissionen. PTS kommer även ha möjlighet att ta en aktiv roll med prioritering av frågor som är särskilt viktiga i förhållande till företag i Sverige. I den mån samarbetet leder till formella ställningstaganden eller liknande kan PTS agera proaktivt i att informera marknadernas aktörer om detta, vilket kan bidra till att undanröja eller minska administrativa utmaningar för företagen.

Inom ramen för samarbetet med andra myndigheter och kommissionen, särskilt inom ramen för EDIB, kan PTS enligt vår mening med fördel aktivt bidra i arbetet som avser interoperabilitet. Som en följd av inordnandet av Digg i PTS kommer PTS också vara behörig myndighet och enda kontaktpunkt enligt EU-förordningen om ett interoperabelt Europa och därmed representera Sverige i Styrelsen för ett interoperabelt Europa. I syfte att aktivt bidra i interoperabilitetsarbetet kan PTS inbjuda till dialog med aktörer som omfattas av förordningen samt med myndigheter och andra organisationer som arbetar med tekniska specifikationer och standarder inom områden som omfattas av förordningen.

8.7.6 Vägledning genom regulatorisk testverksamhet

Förslag: PTS ska ges i uppdrag av regeringen att inrätta regulatorisk testverksamhet för att lämna fördjupad vägledning om tillämpningen av dataförordningen.

Uppdraget ska vara tidsbegränsat till två år.

Dataförordningen är ett nytt regelverk och det råder osäkerhet om hur dataförordningen ska tillämpas. Osäkerheten bottnar bl.a. i att många bestämmelser lämnar utrymme för tolkning, såsom ofta är fallet med EU-reglering. Denna rättsliga osäkerhet riskerar att hämma dataförordningens genomslag och de effekter som den är avsedd att få. Osäkerheten riskerar även att leda till att otillräckliga eller felaktiga åtgärder vidtas av de aktörer som träffas av dataförordningens bestämmelser. PTS kommer i sin roll som behörig myndighet att spela en stor roll i att utveckla hur förordningen ska tolkas och tillämpas. Detta kommer primärt att ske genom beslut inom ramen för tillsynsverksamheten, dvs. genom bedömningar i efterhand av olika ageranden (ex post). Myndigheten kommer inte kunna ge förhandsbesked till en aktör som vänder sig till myndigheten med frågar om t.ex. en ny lösning är förenlig med kraven i förordningen.

Som framgår ovan anser vi att PTS i egenskap av behörig myndighet kommer att spela en viktig roll i att sprida information om dataförordningen och tolkningen och tillämpningen av den. Som ett led i att underlätta för aktörer att tolka och tillämpa förordningen föreslår vi att PTS får ett regeringsuppdrag att införa regulatorisk testverksamhet för att lämna fördjupad vägledning om tillämpningen av dataförordningen. Detta skulle ge PTS en möjlighet att i rollen som behörig myndighet anlägga ett utforskande och lärande perspektiv som inte är möjlig inom ramen för formell tillsyn. Med regulatorisk testverksamhet avser vi fördjupad vägledning till en eller flera aktörer inom ett avgränsat område eller i relation till en specifik aktivitet om hur dataförordningen i förhållande bör tolkas och tillämpas. Ett sådant arbetssätt understödjer syftet med dataförordningen, dvs. att skapa en rättvis, konkurrenskraftig och innovativ europeisk datamarknad. Det ger även PTS en möjlighet att bygga ökad kunskap om förordningen genom ett utforskande arbetssätt tillsammans med av förordningen berörda aktörer.

Dataförordningen innehåller inte några bestämmelser om regulatorisk testverksamhet. Uttrycklig reglering av regulatoriska sandlådor finns dock t.ex. i AI-förordningen. Att sådana regler finns är inte en förutsättning för att PTS ska kunna inrätta regulatorisk testverksamhet. Integritetskyddsmyndigheten (IMY) bedriver regulatorisk testverksamhet inom området dataskydd sedan 2022. Det är IMY som tagit initiativ till verksamheten, och dataskyddsförordningen innehåller inte någon bestämmelse om att sådan verksamhet ska genom-

föras. Arbetssättet används även av andra dataskyddstillsynsmyndigheter i Europa. Vi har i samtal med företrädare för IMY fått bilden av att myndigheten har positiva erfarenheter av verksamheten.

Det finns enligt vår uppfattning många bestämmelser i dataförordningen som lämnar utrymme för tolkning i enskilda fall. I förordningen finns t.ex. bestämmelser som föreskriver att data ska tillgängliggöra i ett allmänt använt format, utan att specificera vilka kraven är för att ett format ska anses vara allmänt använt.[23] Vår avsikt med detta exempel ska inte uppfattas som en instruktion till PTS om vad som ska avhandlas inom ramen för testverksamheten, det syftar enbart till att illustrera att det finns bestämmelser i förordningen som lämnar utrymme för tolkning och som kan leda till osäkerhet bland de aktörer som ska tillämpa bestämmelserna. Vilka ”ämnen” som blir föremål för sådan verksamhet kan bestämmas utifrån förslag som företag och andra aktörer kan lämna in till myndigheten.

Genom att inrätta regulatorisk testverksamhet kan, som vi lyft ovan, marknadens aktörer och den behöriga myndigheten tillsammans utforska dataförordningen. Det är viktigt att kraven på att delta i sandlådan inte ställs på en sådan hög nivå att t.ex. mindre företag inte har möjlighet att delta och att urvalet av deltagande aktörer sker på objektiva och rättvisa grunder. PTS bör informera om inriktning för den regulatoriska testverksamheten.

En viktig aspekt av testverksamheten är att den ska syfta till att främja kunskapen om dataförordningen även för aktörer som inte deltar i testverksamheten. Det är viktigt att de som deltar i testverksamheten inte ges fördelar som t.ex. kan snedvrida konkurrensen. Resultaten av projekt inom ramen för testverksamheten bör därför skyndsamt publiceras.

Arbetet inom ett projekt i den regulatoriska testverksamheten bör bedrivas i dialogbaserad form. Det bör inte finnas behov för PTS att begära in stora mängder handlingar från marknadsaktörerna som deltar i ett projekt. Vårt förslag är att PTS ska få ett regeringsuppdrag att bedriva regulatorisk testverksamhet. Uppdraget är tidsbegränsat. Enligt vår uppfattning föreligger inte något behov av sekretess i testverksamheten. Hade ett sådant behov förelegat är det tveksamt om det hade varit lämpligt att föreslå en ny sekretessbestämmelse eftersom det rör sig om ett regeringsuppdrag som är tidsbegränsat. Det

[23] Se t.ex. artikel 3.1 och artikel 4.1.

bör vara tillräckligt att PTS överväger vilka handlingar och uppgifter som krävs för att kunna genomföra projekt samt hur informationshanteringen utformas på ett lämpligt sätt. Det är också viktigt att dataskyddsregelverket respekteras, i den mån som personuppgiftsbehandling aktualiseras. Vi är medvetna om att avsaknad av sekretess kan innebära begränsningar i vilka frågor som kan hanteras inom ramen för ett projekt. Vi bedömer emellertid att det finns många frågor avseende dataförordningen som PTS och marknadsaktörerna tillsammans kan utforska utan att det finns behov av sekretess.

I uppdraget till PTS bör ingå att myndigheten, baserat på erfarenheterna av att genomföra testverksamheten, bedömer om verksamheten ska bli en permanent uppgift för myndigheten samt vilka eventuella författningsändringar som i så fall är nödvändiga, inklusive avseende sekretess. I den mån andra myndigheters tillsynsområde berörs kan sådana bjudas in att delta i den regulatoriska testverksamheten. PTS bör inom ramen för regeringsuppdraget dra nytta av IMY:s erfarenheter av att bedriva regulatorisk sandlåda inom dataskyddsområdet.

Uppdraget bör vara tidsbegränsat till två år.

8.8 Myndighet eller organ för att underlätta bedömningar enligt artikel 32.3

Tredjeländer kan anta lagar och andra författningar som syftar till att direkt överföra eller ge statlig åtkomst till icke-personuppgifter som finns inom EU. Artikel 32 i dataförordningen syftar till att hindra olaglig internationell statlig åtkomst till och överföring av icke-personuppgifter. Bestämmelsen är tillämplig på leverantörer av databehandlingstjänster, t.ex. leverantörer av moln- och edgetjänster, och ska säkerställa att leverantörernas kunder som väljer att lagra sina icke-personuppgifter i EU, skyddas från att deras uppgifter olagligen åtkoms av eller överförs till regeringar utanför EU (skäl 101). I artikel 32.3 stadgas att leverantörer av databehandlingstjänster i vissa fall bara får efterleva domar eller beslut från myndigheter i stater utanför EU om vissa förutsättningar är uppfyllda. För att underlätta för leverantörerna av databehandlingstjänster att göra de bedömningar som föreskrivs, kan eller ska de begära yttranden från ”det relevanta

nationella organ eller den relevanta nationella myndighet som har behörighet för internationellt samarbete i rättsliga frågor”.

Dataförordningen anger inte att medlemsstaterna särskilt ska utse en myndighet eller ett organ som kan lämna yttranden artikel 32.2. Vårt uppdrag enligt vara kommittédirektiv innefattar inte heller att föreslå att regeringen utser en sådan myndighet eller sådant organ. Inom ramen för utredningen har vi dock utrett om det finns någon myndighet eller något organ som i Sverige har ett uppdrag som liknar uppgiften att bistå enskilda enligt artikel 32.2.

8.8.1 Innebörden av artikel 32.3

Artikel 32.2 aktualiseras om leverantörer av databehandlingstjänster är föremål för beslut eller dom från en domstol eller administrativ myndighet i ett tredjeland som ställer krav på att de ger åtkomst till icke-personuppgifter som omfattas av dataförordningen och som innehas i unionen. Enligt bestämmelsen ska sådana domar eller beslut som utgångspunkt endast erkännas eller genomföras om de grundar sig på en internationell överenskommelse, t.ex. fördrag om ömsesidig rättslig hjälp, som gäller mellan det begärande tredjelandet och EU eller en medlemsstat. I annat fall kan det uppstå situationer där en begäran om överföring av eller åtkomst till icke-personuppgifter inom ramen för tredje lands lagstiftning står i strid med en skyldighet att skydda sådana data enligt unionsrätten eller enligt den berörda medlemsstatens nationella rätt (skäl 101).

Om en sådan överenskommelse om ömsesidig rättslig hjälp saknas är artikel 32.3 tillämplig. Enligt bestämmelsens första stycke får leverantören av databehandlingstjänster bara ge åtkomst till eller överföra data enligt domen eller beslutet om vissa villkor är uppfyllda. Villkoren innebär att leverantören av databehandlingstjänster måste kontrollera att tredjelandets rättssystem omfattar krav på att beslutets skäl och proportionalitet anges, att domstolsavgörandet eller beslutet är specifikt till sin karaktär och att den motiverade invändningen från mottagaren är föremål för prövning av en behörig tredjelandsdomstol som har befogenhet att vederbörligen beakta de relevanta rättsliga intressena för leverantören av sådana data. Villkoren i artikel 32.3 första stycket handlar alltså om tredje landets rätts-

system. Att ge åtkomst till eller överför data om villkoren inte är uppfyllda utgör en överträdelse av artikel 32.3 (se avsnitt 5.6.3).

Leverantörer av databehandlingstjänster ska enligt artikel 32.3 andra stycket i en sådan situation, dvs. för att bedöma om villkoren i första stycket är uppfyllda, ha möjlighet att begära ett yttrande från ”det relevanta nationella organ eller den relevanta nationella myndighet som har behörighet för internationellt samarbete i rättsliga frågor”. Särskilt gäller detta när den anser att beslutet kan avse företagshemligheter och andra kommersiellt känsliga data samt innehåll som skyddas av immateriella rättigheter eller att överföringen kan leda till återidentifiering. Det relevanta nationella organet eller den relevanta nationella myndigheten får i sin tur samråda med kommissionen.

Vidare anges i artikel 32.3 andra stycket att leverantören av databehandlingstjänster, om den anser att beslutet eller domen från det tredje landet kan inkräkta på unionens eller dess medlemsstaters nationella säkerhets- eller försvarsintressen, ska begära ett yttrande från det relevanta nationella organet eller den relevanta nationella myndigheten för att avgöra om begärda data rör unionens eller dess medlemsstaters nationella säkerhets- eller försvarsintressen. Om adressaten inte har fått något svar inom en månad, eller om yttrandet av ett sådant organ eller en sådan myndighet visar att de villkor som anges i artikel 32.3 första stycket inte är uppfyllda, får adressaten avslå begäran om överföring eller åtkomst till icke-personuppgifter av dessa skäl.

8.8.2 Relevanta myndigheter eller organ enligt dataförordningen

Såsom förordningstexten är skriven utgår förordningen ifrån att det i medlemsstaterna finns en eller flera befintliga nationella myndigheter eller organ som har uppdrag som innebär att de kan lämna sådana yttranden som avses och att de hjälpa den enskilde att bedöma om villkoren i första stycket är uppfyllda eller unionens eller medlemsstatens säkerhets- eller försvarsintressen berörs. Det finns inte någon bestämmelse i förordningen som kräver att medlemsstaterna ska säkerställa att en sådan myndighet eller ett sådant organ kan lämna yttrande enligt artikel 32.3 andra stycket. (jfr t.ex. vad som gäller angående certifiering av tvistlösningsorgan i artikel 10). Det

nämns inte heller något mer i skälen om sådana myndigheter eller organ (jfr skäl 101 och102).

Vi noterar att det i artikel 31 i dataförvaltningsförordningen finns en bestämmelse som motsvarar artikel 32 i dataförordningen. Även enligt dataförvaltningsförordningen ska en bedömning göras avseende sådana villkor som anges i artikel 32.3 första stycket i dataförordningen. Dataförvaltningsförordningen föreskriver dock inte någon ordning för att kunna begära yttranden från en relevant myndighet eller ett relevant organ. I dataskyddsförordningen, artikel 45.1, föreskrivs att personuppgifter får överföras till ett tredjeland eller en internationell organisation om kommissionen har beslutat att det tredjelandet, ett territorium eller en eller flera specificerade sektorer i tredjelandet, eller den internationella organisationen i fråga säkerställer en adekvat skyddsnivå vad gäller skydd för personuppgifter. Kommissionen ska vid denna bedömning särskilt beakta de förhållandens som nämns i artikel 45.2, inklusive förhållanden i det tredjelandets rättssystem. Kommissionen får genom en genomförandetakt besluta att ett visst tredjeland uppfyller kraven på adekvat skyddsnivå (artikel 45.3). Hittills har kommissionen fattat ett antal sådana beslut (adequacy decisions) beträffande olika stater och organisationer.[24] Detta förfaringssätt underlättar naturligtvis för företagen att bedöma om dataöverföring får ske.

I sina Frequently Asked Questions[25] svarar kommissionen på frågan om vilka organ en leverantör av databehandlingstjänster kan konsultera innan den beslutar om huruvida den ska bevilja åtkomst till eller överföra uppgifter efter en begäran från myndigheter i tredje land. Kommissionen uppger att leverantören av databehandlingstjänsten, för att identifiera en relevant myndighet eller ett relevant organ som avses i artikel 32 i dataförordningen, måste kontrollera vilken administrativ enhet i dess medlemsstat som normalt ansvarar för genomförandet av avtal om ömsesidig rättslig rättshjälp (s.k. MLAT, Mutual Legal Assistant Treaty).[26] Kommissionen anger vidare att leverantören av databehandlingstjänster, när det är oklart, också kan konsultera medlemsstatens datasamordnare. Vi tolkar detta som att kommissionen anser att leverantören av databehand-

[24] Se Data protection adequacy for non-EU countries.
[25] Frequently Asked Questions, Data Act, version 1.3, den 12 september 2025, s. 42 f.
[26] Som exempel på relevanta organ anges Bureau de l'entraide pénale internationale, som är en enhet inom det franska justitieministeriet och Bundesjustizamt som är en central punkt för internationellt samarbete i Tyskland.

lingstjänster ska kunna konsultera datasamordnaren för att kunna identifiera den relevanta myndigheten eller det relevanta organet i medlemsstaten i fråga. Sammantaget verkar det alltså inte, i vart fall inte för alla medlemsstater, vara självklart vilken eller vilka myndigheter eller organ som ska kunna lämna yttranden enligt artikel 32.2.

8.8.3 Vilken myndighet eller vilket organ i Sverige kan bistå med yttranden?

För Sveriges del är det inte uppenbart vilken eller vilka myndigheter eller organ som skulle kunna lämna yttrande enligt artikel 32.2. Det finns olika rättsvårdande myndigheter och organ i Sverige som arbetar med internationellt rättsligt samarbete enligt internationella regelverk. T.ex. arbetar Åklagarmyndigheten med internationellt rättsligt samarbete som innebär att myndigheten hjälper utländska åklagare i brottsutredningar som äger rum utomlands. Det kan gälla förhör med personer som finns i Sverige, husrannsakan eller utlämning av en misstänkt person. På motsvarande sätt kan det krävas hjälp från utlandet i svenska brottsutredningar.

Enligt de flesta avtal och konventioner om internationellt straff- och civilrättsligt samarbete ska stater utse en s.k. centralmyndighet som ska fungera som kontaktpunkt i samarbetet. Justitiedepartementets enhet för brottmålsärenden och internationellt rättsligt samarbete (BIRS) är Sveriges centralmyndighet för detta samarbete. Funktionen går under benämningen Centralmyndigheten. Centralmyndigheten tar emot, granskar och vidarebefordrar framställningar till och från Sverige i ärenden om bl.a. rättslig hjälp i brottmål, utlämning för brott, överförande av straffverkställighet, överförande av lagföring för brott, bevisupptagning i civila mål och ärenden samt ansökningar om rättshjälp. En stor del av Centralmyndighetens arbete går ut på att ge service och rådgivning till svenska och utländska rättsliga myndigheter för att underlätta det internationella rättsliga samarbetet. Centralmyndigheten lämnar vidare upplysningar till svenska och utländska myndigheter om innehållet i både svensk och utländsk rätt. Centralmyndigheten handlägger även regeringens ärenden som rör det internationella rättsliga samarbetet i brottmål. Främst gäller detta ärenden om utlämning av personer till en annan stat, om överförande av straffverkställighet till Sverige samt ärenden om rättslig hjälp i brottmål. Ärendena kan också avse överförande av lagföring

eller tillstånd att väcka åtal i vissa fall för brott begångna utomlands.[27] Om särskilda beslut ska fattas är det regeringen som fattar dessa.

Vi kan konstatera att Centralmyndigheten inte har ett uppdrag som liknar den roll som avses i artikel 32.2, dvs. att bistå enskilda med bedömningar av rättssystem i länder utanför EU, med vilka det inte finns en internationell överenskommelse som hanterar ömsesidig rättshjälp. Centralmyndigheten hanterar främst ärenden mellan myndigheter, och inte ärenden som initieras av enskilda. Stor del av ärendena hanteras vidare i enlighet med regler på området för internationellt rättsligt samarbete som har sin bakgrund i internationella överenskommelser. Med andra ord rör ärendena inte situationer som inte täcks av sådana internationella överenskommelser. Verksamheten att ta emot, granska och vidarebefordra framställningar till och från Sverige i straff- och civilrättsliga ärenden kan beskrivas som en ”brevlåda”. I den mån Centralmyndigheten fattar beslut är det regeringen som fattar beslutet. Det skulle enligt vår bedömning inte vara lämpligt att ett yttrande enligt artikel 32.3 ska utgöra ett regeringsbeslut.

Samtidigt tycks det vara funktioner av typen centralmyndighet för internationell rättslig rättshjälp som avses i artikel 32.2. Vi har inte heller kunnat identifiera någon annan myndighet eller något annat organ som har en liknande roll att bistå enskilda med rättsliga bedömningar om tredje länders rättssystem eller liknande.

I artikel 32.3 andra stycket föreskrivs alltså vidare att leverantören av databehandlingstjänster, om den anser att beslutet eller domen från det tredje landet, kan inkräkta på unionens eller dess medlemsstaters nationella säkerhets- eller försvarsintressen, ska begära ett yttrande från det relevanta nationella organet eller den relevanta nationella myndigheten för att avgöra om begärda data rör unionens eller dess medlemsstaters nationella säkerhets- eller försvarsintressen. Bestämmelsen anger att yttrande ska inhämtas, till skillnad från vad som gäller yttranden angående bedömningen av villkoren i första stycket som får inhämtas. Samtidigt ska yttrande inhämtas först om leverantören av databehandlingstjänster själv anser att försvars- eller säkerhetsintressen berörs. Här kan man tänka sig att myndigheter som Försvarsmakten eller Säkerhetspolisen, mot bakgrund av sina respektive instruktioner och kompetensområden, skulle kunna

[27] Se Faktablad *Internationellt rättsligt samarbete – Centralmyndighetens roll*, Justitiedepartementet, Ju 14.01, Mars 2014.

bistå med bedömningen. Uppgiften att på kort tid lämna ett formellt yttrande till enskild framstår dock som främmande för myndigheterna.

I Sverige kommer datasamordnarens uppgifter att ligga på Post- och telestyrelsen som enda behöriga myndighet. Vår bedömning är dock att det skulle vara svårt för myndigheten att hänvisa leverantören av databehandlingstjänster till en särskild myndighet. Den uppgiften för en behörig myndighet eller datasamordnare är inte heller något som föreskrivs i dataförordningen, utan nämns endast i kommissionens Frequently Asked Questions.[28]

8.8.4 Det är oklart vilken myndighet i Sverige som ska underlätta vid tillämpning av artikel 32.3

Vi har inte lycktas identifiera någon eller några myndigheter eller organ som i dagsläget bedriver verksamhet som motsvarar den uppgift som beskrivs i artikel 32.3 i dataförordningen. Vad gäller yttranden som rör bedömning av tredje länders rättssystem framstår det som att Centralmyndigheten, som är en del av Justitiedepartementet, är den myndighet vars verksamhet ligger närmast beskrivningen av en nationellt relevant myndighet eller ett organ i artikel 32.3 i dataförordningen. För bedömning av säkerhets- eller försvarsintressen skulle Försvarsmakten eller Säkerhetspolisen kunna vara relevanta myndigheter.

Om det vid tillämpningen av förordningen visar sig att leverantörer av databehandlingstjänster inte får den hjälp som föreskrivs i artikel 32.3 i dataförordningen genom att vända sig till svenska myndigheter bör regeringen överväga att utse en eller flera myndigheter relevanta myndigheter enligt artikeln.

8.9 Sammanfattning om åtgärder för att minska administrativa hinder

Vi har i detta kapitel konstaterat att förhållandet att dataförordningen är en direkt tillämplig EU-förordning innebär begegränsningar vad gäller utrymmet på det nationella planet att vidta åtgärder som

[28] Frequently Asked Questions, Data Act, version 1.3, den 12 september 2025, s. 43.

kan minska administrativa hinder som beror på dataförordningen. Det är t.ex. inte ändamålsenligt att föreslå särskilda initiativ till förenklings- eller standardiseringsåtgärder. Samtidigt har vi konstaterat att dataförordningen utgör ett mycket komplext regelverk och att det föreligger osäkerheter kring hur förordningen ska tolkas m.m. Behovet av information och förtydliganden är därför stort. Den instans som kan underlätta för företagen när det gäller administrativa hinder är i första hand den behöriga myndigheten, PTS. Det är tydligt i dataförordningen att den behöriga myndigheter ska ha i uppdrag att öka kunskaperna om dataförordningen och datakunskapen. Vi har därför påtalat vikten av att PTS tillhandahåller information om dataförordningen, exempelvis på sin webbplats, och vidtar de informationsåtgärder som myndigheten ser behov av. Vi föreslår särskilt att PTS får i uppdrag att inrätta regulatorisk testverksamhet.

Utöver vad som diskuterats i detta kapitel har vi inte identifierat några andra myndigheter eller organ som bör få ett särskilt uppdrag i syfte att minska i detta kapitel de administrativa utmaningar som vi lyfter. I sammanhanget kan dock noteras att vi i kapitel 7 bl.a. föreslår att MSB ska få ett stödjande uppdrag när det gäller tillämpning av kapitel V i förordningen.

9 Sekretess och dataskydd

9.1 Inledning

I det här kapitlet redovisas först våra överväganden när det gäller sekretess hos den behöriga myndigheten och vid det informationsutbyte som blir ett resultat av samarbete och samverkan mellan den behöriga myndigheten och andra myndigheter. I kapitlet redovisas våra överväganden kring om det krävs författningsändringar för att myndigheterna ska kunna utföra det informationsutbyte som aktualiseras inom ramen för samverkan enligt dataförordningen. Därefter redovisar vi våra bedömningar avseende dataskydd och stödet för behandling av personuppgifter hos den behöriga myndigheten och andra berörda myndigheter liksom hos offentliga organ som begär data med stöd av kapitel V i dataförordningen.

9.2 Dataförordningen ställer krav på konfidentialitet, informationsutbyte och datadelning till offentliga organ

9.2.1 Dataförordningens krav på konfidentialitet

Dataförordningen ställer krav på konfidentialitet. Det framgår av artikel 37.16 att behöriga myndigheter ska respektera principen om konfidentialitet och om yrkes- och affärshemligheter och ska skydda personuppgifter i enlighet med unionsrätten eller nationell rätt. Det får därför anses ingå i vårt uppdrag att analysera vilken sekretess som gäller hos den behöriga myndigheten för uppgifter som hanteras inom ramen för dess verksamhet enligt dataförordningen, samt vilket skydd som gäller för personuppgifter. Vidare föreskriver artikel 19 att mottagande offentliga organ ska bevara konfidentialiteten för uppgifter som hämtas in med stöd av kapitel V i förordningen.

En i sammanhanget viktig utgångspunkt är att en begränsning av offentlighetsprincipen ska anges i en särskild lag eller i en annan lag som den särskilda lagen hänvisar till (2 kap. 2 § tryckfrihetsförordningen). Detta gäller även när begränsningen har sitt ursprung i en EU-rättsakt. En bestämmelse i en EU-rättsakt måste alltså motsvaras av en tillämplig bestämmelse eller hänvisning i offentlighets- och sekretesslagen (2009:400) (OSL) för att kraven i tryckfrihetsförordningen ska vara uppfyllda. Dataförordningens krav på konfidentialitet kan därför inte läggas till grund för att begränsa den grundlagsstadgade rätten till insyn i offentlig verksamhet. I den mån dataförordningens krav på konfidentialitet i den behöriga myndighetens verksamhet inte kan anses uppfyllt genom befintlig reglering av sekretess så behöver vi föreslå ändringar i offentlighets- och sekretesslagen.

Det framgår också av artikel 37.16 i dataförordningen att all information som utbyts inom ramen för en begäran om bistånd och som tillhandahålls enligt artikel 37 endast får användas med avseende på det ärende för vilket den har begärts. Denna begränsning behöver beaktas av den behöriga myndigheten eller av offentliga organ när de utför sina uppdrag, men kan inte läggas till grund för sekretess enligt 15 kap. 1 a § OSL, vilket vi berör nedan.

9.2.2 Informationsutbyte mellan behöriga myndigheter, andra myndigheter och kommissionen

Dataförordningen innehåller en rad bestämmelser om att myndigheter ska samarbeta och samverka såväl internationellt som nationellt. Det finns t.ex. ett allmänt krav på att de behöriga myndigheterna ska samarbeta med varandra när de utövar sina uppgifter enligt artikel 37.5 (artikel 37.2). Vidare ska de behöriga myndigheterna kunna samarbeta med relevanta behöriga myndigheter som ansvarar för genomförandet av andra unionsrättsakter eller nationella rättsakter, inbegripet med myndigheter med behörighet på området data och elektroniska kommunikationstjänster, med den tillsynsmyndighet som ansvarar för att övervaka tillämpningen av dataskyddsförordningen[1] eller med sektorsmyndigheter. Detta i syfte att säkerställa

[1] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

att dataförordningen verkställs i överensstämmelse med annan unionsrätt och nationell rätt (artikel 37.5 g). Slutligen ska de behöriga myndigheterna kunna samarbeta med de relevanta behöriga myndigheterna för att säkerställa att artiklarna 23–31, artikel 34 och 35 verkställs i överensstämmelse med annan unionsrätt och självreglering som är tillämplig på leverantörer av databehandlingstjänster (artikel 37.5 h). Om en datasamordnare har utsetts ska denna underlätta detta samarbete och på begäran bistå de behöriga myndigheterna (artikel 37.5 andra stycket).

Vissa av bestämmelserna om samarbete förutsätter informationsutbyte mellan myndigheter och några bestämmelser innehåller ett uttalat krav på att information ska kunna utbytas. Förordningen ställer t.ex. krav på att medlemsstaterna ska säkerställa att de behöriga myndigheterna kan samarbeta med behöriga myndigheter i andra medlemsstater och, i förekommande fall, med kommissionen eller Europeiska datainnovationsstyrelsen (EDIB), för att säkerställa en konsekvent och effektiv tillämpning av förordningen, inbegripet utbyte av all relevant information på elektronisk väg, utan oskäligt dröjsmål (artikel 37.5 f). Ett annat exempel är att om en behörig myndighet i en medlemsstat begär bistånd eller verkställighetsåtgärder från en behörig myndighet i annan medlemsstat ska den lämna en motiverad begäran. En behörig myndighet ska vid mottagandet av en sådan begäran utan oskäligt dröjsmål lämna ett svar med detaljerade uppgifter om de åtgärder som har vidtagits eller som avses att vidtas (artikel 37.15). Behöriga myndigheter ska också samarbeta för att effektivt och snabbt hantera och avgöra klagomål, bl.a. genom att utan oskäligt dröjsmål utbyta all relevant information på elektronisk väg (artikel 38.3).

Åtminstone initialt är det endast Post- och telestyrelsen (PTS) som kommer att vara behörig myndighet i Sverige. Samverkan mellan olika behöriga myndigheter i Sverige aktualiseras därför inte. De uppgifter som ankommer på datasamordnaren enligt dataförordningen kommer därför, i den mån de är relevanta, att ankomma på PTS. Inom ramen för uppdraget som behörig myndighet kommer PTS att delta i det gränsöverskridande samarbetet med de behöriga myndigheterna i andra medlemsstater och med kommissionen genom EDIB.

Dataförordningens bestämmelser förutsätter att den behöriga myndigheten ska kunna samverka även med andra nationella myn-

digheter, som är behöriga att utöva tillsyn på närliggande områden, och med sektorsmyndigheter. Det anges särskilt att samverkan kan behöva ske med tillsynsmyndigheten för dataskyddsförordningen.

9.2.3 Datadelning till och mellan offentliga organ

Offentliga organ har enligt kapitel V i förordningen möjlighet att begära data från företag på grundval av ett exceptionellt behov (artikel 14 och 15). Sådana data kan enligt artikel 17.4 utbytas med andra offentliga organ, kommissionen, Europeiska centralbanken eller unionsorgan i syfte att fullgöra de uppgifter som avses i artikel 15. Enligt samma artikel kan sådana data också göras tillgängliga för en tredje part om den som först begärt data med stöd av kapitel V genom ett offentligt tillgängligt avtal har delegerat tekniska inspektioner eller andra funktioner till denna tredje part.

Ett offentligt organ, kommissionen, Europeiska centralbanken eller ett unionsorgan ska enligt artikel 21 ha rätt att dela data som mottagits enligt kapitel V med enskilda personer eller organisationer i syfte att bedriva vetenskaplig forskning eller analys som är förenlig med det ändamål för vilket data begärdes. Data ska även kunna delas med nationella statistikbyråer och Eurostat för framställning av officiell statistik.

9.3 Sekretess i den behöriga myndighetens verksamhet

9.3.1 Allmänt om offentlighet och sekretess i den svenska rättsordningen

Allmänheten har en grundlagsstadgad rätt att med stöd av offentlighetsprincipen få insyn i offentlig verksamhet, vilket kommer till uttryck i rätten att ta del av allmänna handlingar. För att göra undantag från rätten att ta del av allmänna handlingar krävs stöd i lag. Sådant stöd finns främst i bestämmelserna om sekretess och tystnadsplikt i OSL.

Sekretess innebär ett förbud mot att röja en uppgift, vare sig det sker muntligen, genom utlämnande av en allmän handling eller på något annat sätt (3 kap. 1 § OSL). Sekretess gäller både i förhållande

till enskilda personer och andra myndigheter (8 kap. 1–2 §§ OSL). Sekretess gäller också i förhållande till utländska myndigheter och mellanfolkliga organisationer (8 kap. 3 § OSL). Om en uppgift omfattas av sekretess får den inte lämnas ut om inte annat anges i OSL eller i lag eller förordning som OSL hänvisar till (8 kap. 1 § OSL).

Sekretess gäller inte bara i förhållande till allmänheten utan även mellan myndigheter. En myndighet ska på begäran av en annan myndighet lämna uppgift som den förfogar över, om inte uppgiften är sekretessbelagd eller det skulle hindra arbetets behöriga gång (6 kap. 5 § OSL). Om en sekretessbrytande bestämmelse är tillämplig finns alltså en skyldighet att lämna ut uppgifter till andra myndigheter.

9.3.2 Befintlig sekretess är tillräcklig för att uppfylla kravet på konfidentialitet

Bedömning: Det behövs inte några nya bestämmelser om sekretess för att uppfylla dataförordningens krav på konfidentialitet hos den behöriga myndigheten. Det finns inte heller i övrigt behov av nya bestämmelser om sekretess med anledning av uppdraget som behörig myndighet enligt dataförordningen.

Sekretess för uppgifter om enskilda vid nationell tillsyn

PTS kommer i egenskap av behörig myndighet att övervaka efterlevnaden av dataförordningen och kompletteringslagen, det vill säga utöva tillsyn. Inom ramen för sin tillsynsverksamhet kommer PTS att hantera uppgifter om enskildas ekonomiska förhållanden. Det kan exempelvis röra sig om uppgifter om på vilket sätt uppkopplade produkter, tillhörande tjänster och databehandlingstjänster fungerar. Sådana uppgifter om enskilda kan även ges in från behöriga myndigheter i andra medlemsstater, t.ex. om ett ärende lämnas över till PTS. Vidare kan PTS komma att ta emot uppgifter om enskilda från andra svenska tillsynsmyndigheter. De uppgifter som PTS inhämtar kan vara känsliga för t.ex. uppgiftslämnaren och även de som trätt i affärsförbindelse med denne. Det finns mot denna bakgrund anledning att beröra vilken sekretess som kan aktualiseras för dessa uppgifter.

I 30 kap. 23 § OSL föreskrivs att sekretess gäller, i den utsträckning regeringen meddelar föreskrifter om det, i en statlig myndighets verksamhet som består i utredning, planering, prisreglering, tillståndsgivning, tillsyn eller stödverksamhet med avseende på produktion, handel, transportverksamhet eller näringslivet i övrigt

1. för uppgift om en enskilds affärs- eller driftförhållanden, uppfinningar eller forskningsresultat, om det kan antas att den enskilde lider skada om uppgifterna röjs, och
2. för uppgift om andra ekonomiska eller personliga förhållanden än som avses i 1 för den som har trätt i affärsförbindelse eller liknande förbindelse med den som är föremål för myndighetens verksamhet.

Paragrafen reglerar sekretess i statlig tillsynsverksamhet, m.m. Paragrafen ger inte i sig själv upphov till någon sekretess, utan förutsätter att regeringen föreskriver om sekretess.

Relevanta föreskrifter har meddelats i offentlighets- och sekretessförordningen (2009:642) (OSF). Av 9 § OSF framgår att sekretess enligt 30 kap. 23 § OSL gäller, i den utsträckning som anges i bilagan till förordningen. Enligt bilagan gäller sekretess i verksamhet som består i utredning, tillståndsgivning och tillsyn hos PTS, med begränsningen att sekretessen inte gäller i beslut i ärenden.

Sekretessen gäller inom verksamhet som innefattar utredning, planering, prisreglering, tillståndsgivning, tillsyn eller stödverksamhet. Med tillståndsgivning och tillsyn åsyftas det område som i 1937 års sekretesslag beskrevs med ordet kontroll. Ordet tillsyn ska inte ges en alltför snäv tolkning utan får anses omfatta alla de fall där en myndighet har en övervakande eller styrande funktion i förhållande till näringslivet. Under begreppet tillsyn faller också sådan rådgivning som sker som ett led i en myndighets tillsynsverksamhet (prop. 1979:80:2 Del A s. 235). Den statliga verksamheten som omfattas av bestämmelsen om sekretess ska ha avseende på näringslivet.

Sekretessens föremål är enligt punkt 1 i 30 kap. 23 § OSL uppgifter om enskilds affärs- eller driftförhållanden, uppfinningar eller forskningsresultat. Ordet enskild syftar inte bara på den som är direkt föremål för den verksamhet som avses i paragrafen utan också den som står i affärsförbindelse eller annan sådan förbindelse med denne.

En förutsättning för sekretess enligt punkt 1 är att det kan antas att den enskilde lider skada om uppgiften röjs. Sekretessen är med andra ord reglerad med ett rakt skaderekvisit, dvs. det råder presumtion för offentlighet. Skyddet enligt punkt 2 är starkare än det som ges i punkt 1 genom att något skaderekvisit inte uppställs, vilket innebär att absolut sekretess gäller för uppgifter som omfattas av den punkten.

Vi bedömer att befintlig reglering av sekretess i PTS tillsynsverksamhet är tillräcklig för att kraven i dataförordningen på upprätthållande av konfidentialitet inom behöriga myndigheters verksamhet ska anses uppfyllda.

Sekretess vid planering

När det gäller skyddet för det allmännas intressen, dvs. myndigheters verksamhet, finns i 17 kap. 1 § OSL skydd för uppgift om planläggning eller andra förberedelser för bl.a. inspektion, om det kan antas att syftet med granskningsverksamheten motverkas om uppgiften röjs. Det är oklart om tillsynsverksamheten kommer att ha en sådan karaktär att ett röjande av sådana uppgifter skulle motverka granskningsverksamheten. I den mån så är fallet kan den aktuella bestämmelsen tillämpas. Bestämmelsen utgör enligt vår mening tillräckligt skydd för allmänna intressen inför planerade tillsynsåtgärder.

Sekretess i internationellt samarbete

Sekretess gäller enligt 15 kap. 1 a § första stycket OSL för uppgift som en myndighet har fått från ett utländskt organ på grund av en bindande EU-rättsakt eller ett av EU ingånget eller av riksdagen godkänt avtal med en annan stat eller med en mellanfolklig organisation, om det kan antas att Sveriges möjlighet att delta i det internationella samarbete som avses i rättsakten eller avtalet försämras om uppgiften röjs. Motsvarande sekretess gäller enligt andra stycket i samma paragraf för uppgift som en myndighet har inhämtat i syfte att överlämna den till ett utländskt organ i enlighet med en sådan rättsakt eller ett sådant avtal som avses i första stycket.

Av specialmotiveringen till bestämmelsen framgår bl.a. följande. I paragrafen regleras sekretess för uppgifter som har lämnats till

eller inhämtats av en myndighet på grund av en bindande EU-rättsakt eller ett av EU ingånget eller av riksdagen godkänt internationellt avtal. Av första stycket framgår att sekretess under vissa förutsättningar gäller för en uppgift som en myndighet har fått på grund av reglerat internationellt samarbete med en annan stat eller mellanfolklig organisation. Uttrycket ”har fått från ett utländskt organ” innebär att uppgifter som en myndighet har fått från såväl utländska myndigheter som andra utländska organ omfattas av sekretessbestämmelsen. Att uppgiften finns hos myndigheten ”på grund av” en bindande EU-rättsakt eller ett av EU ingånget eller av riksdagen godkänt avtal innebär att endast sådana uppgifter som myndigheten har fått som en direkt följd av rättsakten eller avtalet träffas av bestämmelsen. Uppgifter som finns hos myndigheten av andra skäl än just på grund av rättsakten eller avtalet i fråga omfattas därmed inte. Med ”bindande EU-rättsakt” avses sådana rättsakter som gäller till följd av Sveriges medlemskap i EU, dvs. anslutningsfördragen samt förordningar, direktiv och beslut som antas av EU:s institutioner. Det bör observeras att inte bara lagstiftningsakter, utan även delegerade akter och genomförandeakter kan ha en bindande verkan. Uppgiftens innehåll, art eller karaktär saknar betydelse för bestämmelsens tillämplighet, till skillnad från vad som gäller i fråga om utrikessekretess enligt 15 kap. 1 § OSL. Bestämmelsen är vidare tillämplig även i fråga om uppgifter om enskilda, om de finns hos myndigheten på grund av ett reglerat internationellt samarbete. Så kan exempelvis vara fallet om uppgiften inkommit från en utländsk myndighet och härrör från en utredning, en upphandling eller ett annat ärende där (prop. 2012/13:192 s. 43 f.).

En förutsättning för att sekretess ska gälla är att ett röjande av uppgiften kan antas försämra Sveriges möjlighet att delta i det internationella samarbete som avses i EU-rättsakten eller avtalet. Termen ”försämras” ska inte uppfattas som att det råder en lägre tröskel för att ett utlämnande ska kunna nekas, jämfört med om termen ”skadas” i stället hade använts i bestämmelsen. Tvärtom indikerar termen ”försämras” att det är en viss typ av skada som ska kunna antas uppstå för att skaderekvisitet ska vara uppfyllt. Termen används även i bl.a. 19 kap. 4 och 9 §§ samt 42 kap. 2 § OSL. Tolkningen av termen i de sammanhangen kan användas till vägledning för tolkningen av termen här. Uttrycket ”möjlighet att delta i” syftar i detta sammanhang främst på möjligheten att få del av information i enlighet med

EU-rättsakten eller avtalet, dvs. dra nytta av samarbetet. Bestämmelsen innebär att myndigheten i det enskilda fallet är skyldig att göra en självständig bedömning av vilka konsekvenser ett röjande kan antas få för det fortsatta samarbetet. Myndigheten måste då beakta om och i så fall på vilket sätt frågan om sekretess regleras i rättsakten eller avtalet. Det kan i detta sammanhang noteras att s.k. användningsbegränsningar, dvs. bestämmelser som till synes uttömmande reglerar för vilka ändamål viss information får användas av den mottagande myndigheten, inte bör tolkas som ett sådant krav på sekretess som aktualiserar en tillämpning av den nya sekretessbestämmelsen (prop. 2012/13:192 s. 46).

Av andra stycket i 15 kap. 1 a § OSL framgår att motsvarande sekretess gäller även för uppgifter som myndigheten har samlat in på annat sätt, t.ex. inom landet eller direkt från enskilda, om uppgiften inhämtats enbart i syfte att överlämnas till ett utländskt organ i enlighet med en sådan rättsakt eller ett sådant avtal som avses i första stycket, dvs. i enlighet med en bindande EU-rättsakt eller ett av EU ingånget eller av riksdagen godkänt avtal med en annan stat eller en mellanfolklig organisation. En förutsättning för att en sådan internationell handräcknings- eller biståndsskyldighet över huvud taget ska kunna aktualiseras är att utlämnande av uppgifter till utländska organ i sig är förenligt med svensk rätt. Andra stycket anger endast att om en sådan skyldighet gäller, och uppgifter samlas in enbart för att vidarebefordras i enlighet med denna, gäller sekretess för uppgifterna, om det kan antas att Sveriges möjlighet att delta i det internationella samarbete som avses i rättsakten eller avtalet försämras om uppgiften röjs. Bestämmelsen är däremot inte tillämplig på uppgifter som samlats in av myndigheten av något annat skäl, t.ex. inom ramen för handläggningen av ett eget tillsynsärende (prop. 2012/13:192 s. 45).

Vi har ovan redogjort för bestämmelser i dataförordningen som förutsätter eller i vissa fall ställer krav på utbyte av information mellan behöriga myndigheter i olika medlemsstater. Det rör sig om såväl mer allmänt ställda krav på samarbete som specifika krav på utbyte av information på elektronisk väg. Utöver uppgifter som rör enskilda kommer PTS att ta emot och hantera uppgifter från kommissionen i samband med arbetet i EDIB, t.ex. i mötesanteckningar om kommissionens och de behöriga myndigheternas arbete med förordningen.

Sådana uppgifter kan röra tolkning av dataförordningens bestämmelser, sanktionsnivåer och olika planerade åtgärder.

Det finns också ett krav på konfidentialitet i den behöriga myndighetens verksamhet, vilket innebär att det kan finnas en berättigad förväntan hos andra medlemsstater på att information som utbyts mellan behöriga myndigheter i olika medlemsstater som en konsekvens av dataförordningen inte ska bli föremål för utlämnande till allmänheten. Bakgrunden till införandet av sekretessbestämmelsen i 15 kap. 1 a § OSL var att sekretessen till skydd för allmänna intressen bedömdes som otillräcklig, vilket riskerade att försämra Sveriges möjligheter att delta i det internationella samarbetet. Det kan mot denna bakgrund finnas skäl att tillämpa sekretess för bestämmelser som utbyts inom ramen för samverkan och samarbete enligt dataförordningen, och då aktualiseras bl.a. 15 kap. 1 a § OSL.

Dataförordningen är en bindande EU-rättsakt. Bestämmelsen i 15 kap. 1 a § OSL kan tillämpas för uppgifter som inhämtas såväl från utländska myndigheter som andra utländska organ. Uppgiften ska ha inkommit till PTS som en direkt följd av dataförordningen, dvs. de krav på samarbete och utbyte av uppgifter som ställs i den förordningen. Uppgiftens innehåll, art eller karaktär saknar betydelse för bestämmelsens tillämplighet, men en förutsättning för att tillämpa sekretess enligt den aktuella bestämmelsen i OSL är att ett röjande av uppgiften kan antas försämra Sveriges möjlighet att dra nytta av det internationella samarbete som avses i dataförordningen.

Samarbete mellan behöriga myndigheter i olika medlemsstater är nödvändigt för en effektiv tillsyn enligt dataförordningen, inte minst eftersom avtal som innefattar datadelning som omfattas av förordningen ofta träffas mellan företag i olika länder. Det kan inte uteslutas att Sveriges möjlighet att samarbeta på det sätt som föreskrivs dataförordningen skulle försämras om uppgifter inte skyddas i Sverige. I så fall bör 15 kap. 1 a § OSL kunna tillämpas. PTS måste i det enskilda fallet göra en självständig bedömning av vilka konsekvenser ett röjande kan antas få för det fortsatta samarbetet. I sammanhanget kan noteras att kravet på konfidentialitet i dataförordningen får uppfattas som förhållandevis allmänt hållet.

Sekretess gäller vidare enligt 30 kap. 24 § OSL hos en statlig myndighet, i sådan verksamhet som avses i 23 §, för uppgift om en enskilds ekonomiska eller personliga förhållanden som myndigheten förfogar över på grund av EU-samarbetet. Bestämmelsen innehåller

inte något skaderekvisit, dvs. absolut sekretess gäller för dessa uppgifter. Bestämmelsen förutsätter dock att den aktuella rättsakten innehåller en klausul om att uppgifterna inte får lämnas vidare i det aktuella fallet (jfr prop. 2006/07:110 s. 38).

Kravet på konfidentialitet i artikel 37.16 dataförordningen är allmänt hållet. Det finns inte några uttryckliga begränsningar avseende konfidentialitet i förhållande till specifika uppgifter som kan bli föremål för inhämtande eller utbyte. Detta kan behöva beaktas vid överväganden om vilka uppgifter som omfattas av sekretess enligt bestämmelsen i 30 kap. 24 § OSL.

9.3.3 Det behövs inte något ytterligare stöd för att lämna ut sekretessbelagda uppgifter från den behöriga myndigheten

Bedömning: De möjligheter som finns att med stöd av OSL lämna ut sekretessbelagda uppgifter är tillräckliga.

Samarbete mellan den behöriga myndigheten och andra myndigheter i Sverige

I Sverige kommer PTS att vara ensam behörig myndighet enligt dataförordningen. Samarbete mellan myndigheter som är behöriga myndigheter enligt dataförordningen aktualiseras därför inte av våra förslag.

Samarbete kan dock aktualiseras med myndigheter som ansvarar för genomförandet av andra unionsrättsakter eller nationella rättsakter, inbegripet med myndigheter med behörighet på området data och elektroniska kommunikationstjänster, med den tillsynsmyndighet som ansvarar för att övervaka tillämpningen av dataskyddsförordningen eller med sektorsmyndigheter för att säkerställa att förordningen verkställs i överensstämmelse med annan unionsrätt och nationell rätt (jfr artikel 37.5 g i dataförordningen).

I Sverige är Integritetsmyndigheten (IMY) tillsynsmyndighet för dataskyddsförordningen. Inom området elektronisk kommunikation är PTS regleringsmyndighet och tillsynsmyndighet enligt lagen (2022:482) om elektronisk kommunikation. PTS är även till-

synsmyndighet över dataförmedlingstjänster och dataaltruismorganisationer enligt lagen (2024:500) med kompletterande bestämmelser till EU:s dataförvaltningsförordning. Myndigheten för digital förvaltning (Digg) och Statistiska centralbyrån (SCB) är behöriga organ enligt dataförvaltningsförordningen med uppgift bl.a. att hjälpa andra myndigheter att ge tillgång till skyddade data för vidareutnyttjande.

Vad gäller sektorsmyndigheter anges i artikel 37.4 a i dataförordningen att sektorsmyndigheternas behörighet ska respekteras när det gäller sektorsspecifika frågor som rör åtkomst till och användning av data. Det finns en rad olika sektorsmyndigheter som hanterar eller kommer att hantera sådana frågor. Som exempel kan nämnas myndigheter som kommer att tillämpa förordningen om det europeiska hälsodataområdet[2]. Vi noterar vidare att behov av samverkan med Konsumentverket, med behörighet inom konsumentområdet, skulle kunna uppstå.

Det är inte möjligt att uttömmande identifiera vilka andra myndigheter som den behöriga myndigheten kan behöva samverka med utifrån bestämmelserna i dataförordningen. Vilken myndighet som kan vara aktuell beror på vad frågan avser och t.ex. vilken sektor som berörs. Det går därför inte att kartlägga vilken sekretess som kan aktualiseras för uppgifter som behöver utbytas mellan den behöriga myndigheten och andra myndigheter med anledning av dataförordningen. Vi bedömer dock att samarbete med andra myndigheter i de allra flesta fall inte nödvändigtvis föranleder behov av att utbyta uppgifter i enskilda ärenden. I ärendespecifika fall bör det många gånger räcka med att PTS lämnar tillräckligt med information till sektorsmyndigheten för att den myndigheten ska kunna göra en egen bedömning om t.ex. ett ärende ska inledas eller inte. Om ett ärende inleds kan den andra myndigheten begära de uppgifter som den myndigheten anser är nödvändiga för utredningen direkt från den eller de aktörer ärendet gäller.

Det kan inte uteslutas att det kan bli nödvändigt för PTS i egenskap av behörig myndighet enligt dataförordningen att lämna ut sekretessreglerade uppgifter för att uppfylla dataförordningens krav på samarbete mellan myndigheter. Det är dock svårt att förutse vilka uppgifter som kan komma i fråga för utlämnande. De sekretess-

[2] Europaparlamentets och rådets förordning (EU) 2025/327 av den 11 februari 2025 om det europeiska hälsodataområdet och om ändring av direktiv 2011/24/EU och förordning (EU) 2024/2847.

bestämmelser som vi redogjort för ovan är med något undantag utformade med skaderekvisit, vilket innebär att sekretess inte gäller automatiskt för uppgifterna, utan att utlämnande många gånger kan vara möjligt efter en skadeprövning.

I många fall finns även sekretessbestämmelser som kan vara tillämpliga hos den mottagande myndigheten. Det gäller exempelvis alla myndigheter som omfattas av 9 § offentlighets- och sekretessförordningen. I IMY:s verksamhet gäller enligt 32 kap. 1 § OSL sekretess i ärende om tillstånd eller tillsyn som enligt lag eller annan författning ska handläggas av myndigheten och i ärende om sådant bistånd som avses i Europarådets konvention om skydd för enskilda vid automatisk databehandling av personuppgifter, för uppgift om en enskilds personliga eller ekonomiska förhållanden, om det kan antas att den enskilde eller någon närstående till denne lider skada eller men om uppgiften röjs. Vår bedömning är att det ofta finns sekretessbestämmelser som är tillämpliga för den myndighet till vilken utlämnande aktualiseras, viket i så fall kan tas i beaktande i skadeprövningen (jfr bl.a. JO beslut den 9 september 2014, dnr 3032 2011, s. 22).

Det kan inte uteslutas att det finns uppgifter som omfattas av sekretess som kan komma att bli föremål för det uppgiftsutbyte som föranleds av dataförordningen. I den mån uppgifter som omfattas av sekretess ska lämnas ut krävs det att det finns stöd i OSL, eller i annan lag eller förordning som OSL hänvisar till, för utlämnandet.

I OSL finns det inte några specifika sekretessbrytande regler som är tillämpliga i förhållande till den sekretessreglering som aktualiseras i den behöriga myndighetens verksamhet. Enligt 10 kap. 2 § OSL kan en myndighet lämna sekretessbelagda uppgifter till enskilda eller andra myndigheter om det är nödvändigt för att den utlämnande myndigheten ska kunna fullgöra sin verksamhet. Bestämmelsen ska tillämpas restriktivt. Bestämmelsen tar sikte på den utlämnande myndighetens verksamhet. Den bör med andra ord kunna tillämpas i de fall då PTS i egenskap av behörig myndighet behöver lämna ut en uppgift för att uppfylla sina åtaganden enligt dataförordningen.

Uppgifter som omfattas av sekretess kan också lämnas ut till en annan myndighet med stöd av 10 kap. 27 § OSL, om det är uppenbart att intresset av att uppgiften lämnas ut har företräde framför det intresse som sekretessen ska skydda (exempelvis den enskildes

intressen). Det har ansetts att sekretessregler inte bör hindra myndigheterna från att utväxla uppgifter i situationer där intresset av att uppgifterna lämnas ut bör ha företräde framför det intresse som sekretessen ska skydda. I förarbetena till den tidigare gällande sekretesslagen uttalas att bestämmelsen särskilt ger utrymme för informationsutbyte när det är fråga om myndigheter med samma sakliga behörighet men med skilda lokala kompetensområden, eller myndigheter som har närbesläktade funktioner och som båda har rättslig befogenhet att direkt begära in de utväxlade uppgifterna (prop. 1979/80:2 Del A s. 326 f.). Det är inte något villkor att en uttrycklig begäran från annan myndighet föreligger, utan en myndighet kan lämna ut uppgifter med stöd av generalklausulen på eget initiativ (prop. 1979/80:2 Del A s. 327). Vidare uttalades i förarbetena till sekretesslagen att möjligheterna att utväxla uppgifter mellan myndigheter får utnyttjas mer sparsamt och med större försiktighet om informationen inte är sekretesskyddad hos den mottagande myndigheten. Detta gäller särskilt i fråga om uppgifter som är hemliga med hänsyn till enskilds intressen (prop. 1979/80:2 Del A s. 77).

Till sammanhanget hör att det av 15 kap. 1 a § tredje stycket OSL följer att om sekretess gäller enligt första eller andra stycket så föreligger hinder mot tillämpning av vissa sekretessbrytande bestämmelser. Vid bedömningen av om sådan sekretess gäller i förhållande till en annan myndighet måste det i normalfallet beaktas om uppgiften även hos den mottagande myndigheten omfattas av ett sekretesskydd. Om det i det enskilda fallet inte kan antas att ett utlämnande till exempelvis de rättsvårdande myndigheterna skulle försämra det framtida samarbetet, är skaderekvisitet inte uppfyllt. I en sådan situation gäller inte sekretess i förhållande till den andra myndigheten och bestämmelsen i tredje stycket aktualiseras därmed inte. Om det däremot i det enskilda fallet kan antas att Sveriges möjligheter att delta i ett avtalsreglerat samarbete försämras om en uppgift lämnas ut till exempelvis regeringen, innebär tredje stycket att ett utlämnande inte kan ske med stöd av den sekretessbrytande bestämmelsen i 10 kap. 15 § OSL.

Vår bedömning är att dataförordningen endast i mycket begränsad omfattning innebär krav på att PTS i egenskap av behörig myndighet ska lämna ut sekretessbelagda uppgifter till andra myndigheter. Det kommer sannolikt inte ske med regelbundenhet. När utlämnandet krävs för att PTS ska fullgöra sina uppgifter som behörig myndighet enligt förordningen kan både 10 kap. 2 och 27 §§ OSL aktuali-

seras och ge stöd för utlämnande utifrån en bedömning i det enskilda fallet.

Sekretess hindrar enligt 10 kap. 28 § OSL inte att en uppgift lämnas till en annan myndighet, om uppgiftsskyldighet följer av lag eller förordning. Bestämmelsen i artikel 37.5 g i dataförordningen om att samverkan ska ske med andra tillsyns- och sektorsmyndigheter är riktad mot medlemsstaterna och innebär inte en tydlig uppgiftsskyldighet. Det finns inte heller någon annan bestämmelse om uppgiftsskyldighet som är specifikt tillämplig för utlämnanden av uppgifter som föranleds av dataförordningen.

Regeringen har bedömt att det kopplat till förordningen om digitala tjänster[3] funnits behov av en uppgiftsskyldighet till stöd för utbyte av uppgifter som föranleds av den förordningen. Relevant bestämmelse finns i förordningen (2024:958) med kompletterande bestämmelser till EU:s förordning om digitala tjänster, där det i 9 § framgår att en tillsynsmyndighet på begäran ska lämna en uppgift till en annan tillsynsmyndighet om myndigheten som begär uppgiften behöver den i egenskap av samordnare för digitala tjänster eller för att utöva tillsyn enligt EU:s förordning om digitala tjänster, lagen (2024:954) med kompletterande bestämmelser till EU:s förordning om digitala tjänster eller föreskrifter som har meddelats i anslutning till lagen. Uppgiftsskyldigheten är begränsad till att gälla mellan myndigheter som utövar tillsyn enligt regelverket eller är samordnare för digitala tjänster. En viktig skillnad jämfört med situationen enligt dataförordningen är att det inte kommer att finnas fler än en behörig myndighet eller någon samordnare i Sverige. Behovet av utbyte av uppgifter är därför inte jämförbart med vad som gäller enligt regelverket om digitala tjänster.

I 4 § förordningen (2024:502) med kompletterande bestämmelser till EU:s dataförvaltningsförordning[4] anges att IMY och Konkurrensverket på begäran ska lämna en uppgift till tillsynsmyndigheten om uppgiften behövs för att tillsynsmyndigheten ska kunna utföra sitt tillsynsuppdrag enligt EU:s dataförvaltningsförordning och lagen (2024:500) med kompletterande bestämmelser till EU:s dataförvaltningsförordning. Motsvarande uppgiftsskyldighet gäller enligt 5 § i samma förordning från tillsynsmyndigheten gentemot IMY, om

[3] Europaparlamentets och rådets förordning (EU) 2022/2065 om en inre marknad för digitala tjänster och om ändring av direktiv 2000/31/EG (förordningen om digitala tjänster).
[4] Europaparlamentets och rådets förordning EU) 2022/868 av den 30 maj 2022 om europeisk dataförvaltning och om ändring av förordning (EU) 2018/1724 (dataförvaltningsakten).

uppgiften behövs för att den myndigheten ska kunna bedriva tillsyn enligt dataskyddsförordningen och lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning. I departementspromemorian som föregick propositionen anges att många myndigheter anser att generalklausulen är svår att tillämpa och inte ger den effektivitet i arbetet som är nödvändig då ett löpande informationsutbyte förutsätter en sekretessprövning på förhand (Ds. 2023:24 s. 214). Det får antas att det är just behovet av ett löpande informationsutbyte av sekretessreglerade uppgifter som föranledde behovet av uppgiftsskyldigheten som är kopplad till dataförvaltningsförordningen.

Sammanfattningsvis bedömer vi att dataförordningen endast i begränsad omfattning innefattar krav på att PTS som behörig myndighet ska lämna ut sekretessbelagda uppgifter till andra myndigheter. När utlämnandet krävs för att PTS ska fullgöra sina uppgifter som behörig myndighet utifrån de krav som förordningen ställer, kan både 10 kap. 2 § och 27 § OSL aktualiseras och ge stöd för utlämnande utifrån en bedömning i det enskilda fallet. Det enda konkreta skälet för att införa ett mer generellt stöd för PTS att lämna ut sekretessbelagda uppgifter till andra myndigheter genom att föreslå en ny uppgiftsskyldighet är enligt vår uppfattning att PTS inte skulle behöva göra bedömningar av om utlämnande kan ske i det enskilda fallet. Uppgiften kan i och för sig vara betungande, men främst om detta är något som kommer att ske regelbundet och ofta. Så kommer sannolikt inte vara fallet. Det är också svårt att utforma en bestämmelse om uppgiftsskyldighet eftersom det är otydligt för vilka uppgifter och gentemot vilka myndigheter skyldigheten att lämna uppgifter skulle gälla.

Utlämnande av uppgifter till behöriga myndigheter i andra medlemsstater

Av 8 kap. 3 § 1 OSL följer att sekretess inte hindrar att uppgifter röjs för en utländsk myndighet, om utlämnandet sker i enlighet med särskild föreskrift i lag eller förordning. En EU-förordning är direkt tillämplig och bestämmelsen i 8 kap. 3 § OSL gör det därför möjligt att lämna uppgift till en utländsk myndighet om det sker med stöd i dataförordningen. Dataförordningen innehåller olika bestämmelser om uppgiftsutbyte. I artikel 37.15 anges att en behörig myn-

dighet i en medlemsstat som begär bistånd eller verkställighetsåtgärder från en behörig myndighet i annan medlemsstat ska lämna en motiverad begäran och att den mottagande behöriga myndigheten utan oskäligt dröjsmål lämna ett svar med detaljerade uppgifter om de åtgärder som har vidtagit eller som avses att vidtas. I artikel 38.3 föreskrivs att behöriga myndigheter ska samarbeta för att effektivt och snabbt hantera och avgöra klagomål, bl.a. genom att utan oskäligt dröjsmål utbyta all relevant information på elektronisk väg. Det kan i sammanhanget behöva övervägas om den bestämmelse i dataförordningen som aktualiserar utlämnande av uppgifter är utformad med en sådan tydlighet att det kan anses vara fråga om en uppgiftsskyldighet gentemot mottagaren.

Vi bedömer att det inte krävs något ytterligare stöd i för att den behöriga myndigheten i Sverige ska kunna utbyta uppgifter med behöriga myndigheter i andra medlemsstater.

9.4 Sekretess hos offentliga organ som begär in data vid exceptionella behov

9.4.1 Befintlig sekretess är tillräcklig för uppgifter som inhämtas med stöd av kapitel V

Bedömning: Det behövs inga författningsändringar om sekretess eller till stöd för utlämnande av uppgifter med anledning av kapitel V i dataförordningen.

Enligt artiklarna 14 och 15 i dataförordningen har datahållare en skyldighet att göra vissa data tillgängliga om ett offentligt organ, kommissionen, Europeiska centralbanken eller ett unionsorgan visar att det föreligger ett exceptionellt behov av att använda dessa data för att fullgöra sina lagstadgade skyldigheter av allmänt intresse. Data enligt kapitel V kan komma att begäras in av en mängd olika myndigheter och offentliga organ, såväl statliga som kommunala myndigheter och organ. Det är inte möjligt för utredningen att överblicka vilka bestämmelser till skydd för företagens uppgifter om drifts- och affärsförhållanden eller till skydd för det allmännas intresse som kan aktualiseras. Det är vidare oklart i vilken uträckning

begärda data kommer att omfatta uppgifter om enskilds drift- och affärsförhållanden.

Begäran om data ska vara proportionerlig och begränsad till att omfatta data som är nödvändiga för det specifika ändamålet. I regel bör sådana data inte nödvändigtvis utgöra känsliga affärsuppgifter eller personuppgifter. I den uträckning de gör det kan uppgifter om enskildas affärs- och driftsförhållanden, vars röjande kan antas leda till skada för företagen i fråga, omfattas av sekretess. Olika aktörer har lyft fram hur viktigt det är att de kan förlita sig på att känsliga affärsuppgifter inte kan lämnas ut till motparter eller allmänheten och att de inte används på ett sätt som skadar företaget.

Bestämmelser om sekretess i OSL är normalt utformade för att skydda enskilda eller allmänna intressen inom ramen för typer av verksamheter som olika myndigheter eller offentliga organ vanligen har i uppdrag att bedriva. I en situation när ett offentligt organ kommer att begära in data vid ett allmänt nödläge ska det offentliga organets uppgift i situationen ha sin utgångspunkt i ett uppdrag som framgår av lag (se vidare i kapitel 7).

Enligt artikel 15.1 b i dataförordningen kan data även begäras när ett offentligt organ agerar på grundval av unionsrätten eller nationell rätt och har identifierat att avsaknaden av specifika data hindrar organet från att utföra en specifik uppgift av allmänt intresse som uttryckligen föreskrivs i lag, såsom framställning av officiell statistik eller begränsning av eller återhämtning från ett allmänt nödläge, och organet har uttömt alla andra till buds stående medel för att erhålla sådana data.

Kopplat till offentliga organs verksamhetsreglering finns i de flesta fall de bestämmelser om sekretess som bedömts som nödvändiga i förhållande till uppdraget. Dataförordningens bestämmelser om offentliga organs möjlighet att begära data enligt kapitel V innebär enligt vår mening inte att de offentliga organen får i uppgift att bedriva någon ny form av verksamhet, utan snarare att organen ges ytterligare ett verktyg för att uppfylla sina befintliga uppdrag när förutsättningarna i förordningen för att begära data är uppfyllda. Vi bedömer att det mot denna bakgrund får förutsättas att lagstiftaren redan tagit ställning till vilken sekretess som är nödvändig i de offentliga organens redan befintliga verksamhet och att det saknas skäl för oss att ompröva dessa ställningstaganden. Vi föreslår därför inte några

nya bestämmelser om sekretess för uppgifter som inhämtas med stöd av artikel 14 och 15 i dataförordningen.

9.4.2 Det behövs inte något ytterligare stöd för att dela data enligt kapitel V

Enligt artikel 17.4 ska data som begärts in med stöd av artikel 15 kunna utbytas med andra offentliga organ eller kommissionen, Europeiska centralbanken eller unionsorgan, i syfte att fullgöra de uppgifter som avses i artikel 15, eller att göra dessa data tillgängliga för en tredje part om det eller den genom ett offentligt tillgängligt avtal har delegerat tekniska inspektioner eller andra funktioner till denna tredje part. I artikel 21 i dataförordningen anges vidare att ett offentligt organ, kommissionen, Europeiska centralbanken eller ett unionsorgan ska ha rätt att dela de data som erhållits med andra enheter eller personer när det är nödvändigt för genomförandet av forskningsverksamhet eller analysverksamhet som de själva inte kan utföra, under förutsättning att sådan verksamhet är förenlig med det ändamål för vilket data begärdes. Sådana data får också under samma omständigheter delas med de nationella statistikbyråerna och Eurostat för utveckling, framställning och spridning av officiell statistik.

I artikel 19 i dataförordningen föreskrivs uttryckligen att de mottagande offentliga organen ska bevara konfidentialiteten för inhämtade uppgifter. I bestämmelsen anges även att uppgifterna inte får användas för annat än avsett bruk och, om nationella regler inte hindrar detta, att de ska raderas efter användning.

Vi bedömer att de sekretessbrytande bestämmelserna i 8 kap 3 §, 10 kap. 2 §, 10 kap. 27 § och 10 kap. 28 § är tillräckliga för att möjliggöra sådan delning av data som föreskrivs enligt artikel 17.4 och artikel 21 i dataförordningen.

9.5 Dataskydd

9.5.1 Allmänt om dataskydd

Inom EU är dataskyddsförordningen det övergripande regelverket för behandling av personuppgifter. Med behandling avses varje åtgärd som vidtas med personuppgifter, exempelvis insamling, bear-

betning eller utlämnande. En personuppgift är varje upplysning som direkt eller indirekt avser en identifierad eller identifierbar fysisk person (registrerad). I dataskyddsförordningen finns bestämmelser om när och hur personuppgifter får behandlas. I Sverige kompletteras dataskyddsförordningen av lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning och förordningen (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning. Dessutom finns ett flertal svenska författningar eller enskilda bestämmelser i författning som reglerar en viss behandling av personuppgifter, exempelvis patientdatalagen (2008:355).

Regleringen i dataskyddsförordningen utgår från att varje behandling av personuppgifter måste vila på en rättslig grund. I dataskyddsförordningen räknas dessa rättsliga grunder upp i artikel 6.1. Behandling är enligt denna bestämmelse laglig endast om och i den mån som åtminstone ett av följande villkor är uppfyllt:

a) Den registrerade har lämnat sitt samtycke till att dennes personuppgifter behandlas för ett eller flera specifika ändamål.

b) Behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås.

c) Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige.

d) Behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person.

e) Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.

f) Behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter, särskilt när den registrerade är ett barn.

Behandling av s.k. särskilda kategorier av personuppgifter, dvs. personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter,

religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning, är som utgångspunkt förbjuden att utföra. För att sådan personuppgiftsbehandling ska vara tillåten måste något av de undantag som framgår av artikel 9 i dataskyddsförordningen vara uppfyllt. Ett sådant undantag innefattar behandling som är nödvändig av hänsyn till ett viktigt allmänt intresse, på grundval av unionsrätten eller medlemsstaternas nationella rätt, vilken ska stå i proportion till det eftersträvade syftet, vara förenligt med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen (artikel 9.2 g i dataskyddsförordningen). Bestämmelsen har genomförts i svensk rätt genom 3 kap. 3 § lagen med kompletterande bestämmelser till EU:s dataskyddsförordning. Enligt paragrafen får känsliga personuppgifter behandlas av en myndighet med stöd av artikel 9.2 g i EU:s dataskyddsförordning om uppgifterna har lämnats till myndigheten och behandlingen krävs enligt lag, om behandlingen är nödvändig för handläggningen av ett ärende, eller i annat fall, om behandlingen är nödvändig med hänsyn till ett viktigt allmänt intresse och inte innebär ett otillbörligt intrång i den registrerades personliga integritet.

Utöver att behandlingen ska vara laglig enligt artikel 6.1 och att det måste finnas ett tillämpligt undantag för behandling av särskilda kategorier av personuppgifter enligt artikel 9.2 så behöver principerna för behandling av personuppgifter enligt kapitel 5 i dataskyddsförordningen och övriga krav på behandling av personuppgifter enligt dataskyddsförordningen och kompletterande svensk lagstiftning vara uppfyllda, för att personuppgiftsbehandlingen ska vara tillåten.

9.5.2 Relationen mellan dataförordningen och dataskyddsförordningen

Dataförordningen syftar till ett ökat tillgängliggörande av data vilket kommer att leda till ett ökat antal behandlingar av data. Ett flertal av bestämmelserna i dataförordningen utesluter inte att personuppgifter ingår i de data som omfattas av krav på att t.ex. delas, vilket

innebär att de data som kan komma att behandlas kan vara såväl personuppgifter som icke-personuppgifter.

Enligt skäl 7 i dataförordningen bör ingen bestämmelse i förordningen tillämpas eller tolkas så att den minskar eller begränsar rätten till skydd av personuppgifter eller rätten till integritet eller konfidentialitet vid kommunikation. I artikel 1.5 i dataförordningen föreskrivs att dataförordningen inte påverkar tillämpningen av unionsrätt och nationell rätt om skydd av personuppgifter, integritet och konfidentialitet vid kommunikation samt terminalutrustningens integritet, som ska tillämpas på personuppgifter som behandlas i samband med de rättigheter och skyldigheter som fastställs i dataförordningen, i synnerhet dataskyddsförordningen, förordningen om behandling av personuppgifter av unionens institutioner, organ och byråer[5] och direktivet om integritet och elektronisk kommunikation[6]. Tillsynsmyndigheternas befogenheter och behörighet enligt dessa regelverk och registrerades rättigheter ska inte heller påverkas. I den mån användare är registrerade ska de rättigheter som fastställs i kapitel II i dataförordningen enligt artikel 1.5 komplettera registrerades rättigheter till tillgång och rättigheter till dataportabilitet enligt artiklarna 15 och 20 i dataskyddsförordningen. I kapitel 8 i betänkandet konstaterar vi att dataskyddsförordningen och dataförordningen är tänkta att tillämpas parallellt. Om dataförordningen står i strid med unionsrätt om skydd av personuppgifter eller integritet, eller står i strid med nationell lagstiftning som antagits i enlighet med sådan unionsrätt, har den relevanta unionsrätten eller den nationell rätten om skydd av personuppgifter eller integritet företräde framför dataförordningen. Detta innebär att om personuppgifter behandlas till följd av dataförordningen så ska sådan behandling vara förenlig med dataskyddsförordningen och nationell lagstiftning. Den personuppgiftsansvarige måste ha rättsligt stöd för behandlingen.

Dataförordningen utgör enligt skäl 7 i förordningen inte i sig en rättslig grund för datahållares insamling eller behandling av personuppgifter. Förordningen bör enligt samma skäl heller inte tolkas som att den medför någon ny rättighet för datahållare att använda person-

[5] Europaparlamentets och rådet förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG.
[6] Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation).

uppgifter som genereras genom användning av en uppkopplad produkt eller tillhörande tjänst. Om data som genereras av de uppkopplade produkterna eller tillhörande tjänsterna helt eller delvis utgörs av personuppgifter måste datahållaren alltså säkerställa att det finns stöd för den personuppgiftsbehandling som sker.

Enligt dataförordningen kan bl.a. användare och offentliga organ begära att data tillgängliggörs av datahållare. I de fall datahållare är skyldiga att tillgängliggöra data som är eller innehåller personuppgifter enligt förordningen kan behandlingen som det innebär att tillgängliggöra personuppgifterna vara nödvändig för att fullgöra en rättslig förpliktelse, vilket är en rättslig grund för behandling enligt artikel 6.1 c i dataskyddförordningen (se mer nedan). Av skäl 7 i förordningen framgår också att om användaren inte är den registrerade så skapar dataförordningen inte någon rättslig grund för att tillhandahålla åtkomst till personuppgifter eller för att göra personuppgifter tillgängliga för en tredje part. Exempel på en sådan situation kan vara om data innehåller personuppgifter om anställda som arbetsgivaren (företaget som äger de uppkopplade produkterna eller har avtalet om de tillhörande tjänsterna) vill föra över till tredje part med stöd av förordningen.

9.5.3 Stöd för den behöriga myndighetens behandling av personuppgifter med anledning av dataförordningen

Bedömning: PTS har stöd i dataskyddsförordningen och kompletterande nationell lagstiftning för den behandling av personuppgifter som är nödvändig för att utföra sitt uppdrag som behörig myndighet.

PTS är behörig myndighet enligt dataförordningen och behöver behandla personuppgifter inom ramen för verksamheten för att kunna utföra sina befogenheter på ett korrekt, rättssäkert och effektivt sätt. Det kan bl.a. röra sig om personuppgifter om personer som lämnar in klagomål till myndigheten och personuppgifter om personer som arbetar vid marknadsaktörer.

Den behandling som är nödvändig hos PTS för att myndigheten ska kunna utföra sitt uppdrag som behörig myndighet syftar till att för att utföra en uppgift av allmänt intresse. Vissa delar av uppdraget

som behörig myndighet innefattar myndighetsutövning, där behandling av personuppgifter också är nödvändig. Den behöriga myndighetens behandling av personuppgifter som är nödvändig för att fullgöra sitt uppdrag kan utföras med stöd av artikel 6.1 e dataskyddsförordningen. I den utsträckning som behandling av särskilda kategorier av personuppgifter är nödvändig så finns stöd i 3 kap. 3 § lagen med kompletterande bestämmelser till EU:s dataskyddsförordning.

PTS omfattas inte av någon registerförfattning som närmare anger under vilka förutsättningar och för vilka ändamål personuppgiftsbehandling får ske. PTS ska dock följa de skyldigheter som framgår av dataskyddsförordningen och av kompletterande bestämmelser i nationell dataskyddsreglering.

PTS är personuppgiftsansvarig för den personuppgiftsbehandling som myndigheten utför, vilket bl.a. innebär att myndigheten måste kunna visa att personuppgiftsbehandlingen är författningsenlig och att den registrerades rättigheter skyddas genom att vidta lämpliga tekniska och organisatoriska åtgärder (se artikel 24 i dataskyddsförordningen).

9.5.4 Stöd för behandling av personuppgifter som begärs med stöd av kapitel V

Bedömning: Det finns inte behov av några författningsändringar avseende dataskydd för att möjliggöra datadelning enligt kapitel V i dataförordningen.

Inledning

Svenska offentliga organ kan med stöd av kapitel V i dataförordningen begära data från datahållare om organet har ett exceptionellt behov av dessa data. Förordningens kapitel V behandlas i kapitel 7 i betänkandet.

Offentliga organ kan enligt artikel 15 i förordningen begära personuppgifter endast om det exceptionella behovet grundar sig i att begärda data är nödvändiga för att hantera ett allmänt nödläge. Om det exceptionella behovet grundar sig på något annat framgår av artikel 15.1 b i förordningen att ett offentligt organ endast får begära

icke-personuppgifter. Vi kommer därför att i detta avsnitt enbart att beröra situationen när det exceptionella behovet hos offentliga organ grundar sig i att de data som begärs är nödvändiga för att hantera ett allmänt nödläge.

Rättslig grund

När en datahållare ska tillmötesgå en begäran om att tillgängliggöra data som utgör eller innehåller personuppgifter krävs det att en eller flera behandlingar av personuppgifterna utförs. Om personuppgifterna ska avidentifieras så utgör själva avidentifieringen en behandling, likaså om personuppgifterna ska pseudonymiseras. Själva tillgängliggörandet av personuppgifterna i pseudonymiserad form är också en behandling av personuppgifter. Datahållaren måste ha en rättslig grund för denna behandling.

Det framgår av skäl 7 i dataförordningen att förordningen i sig inte utgör rättslig grund för datahållares insamling eller behandling av personuppgifter och att förordningen inte bör tolkas som att den medför någon ny rättighet för datahållaren att använda personuppgifter som genereras genom användning av en uppkopplad produkt eller tillhörande tjänst.[7] Det får förstås som att en datahållare inte kan samla in eller nyttja genererade personuppgifter enbart med åberopande av dataförordningen. Detsamma gäller det offentliga organet som begär uppgifterna – insamlingen av de begärda personuppgifterna kan inte ske med åberopande enbart av dataförordningens bestämmelser.

Enligt artikel 6.1 c i dataskyddsförordningen är behandlingen laglig om den är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige. Enligt den kompletterande svenska bestämmelsen, 2 kap. 1 § lagen med kompletterande bestämmelser till EU:s dataskyddsförordning, får personuppgifter behandlas med stöd av artikel 6.1 c i EU:s dataskyddsförordning om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna fullgöra en rättslig förpliktelse som följer av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning. Vår bedömning är att den rättsliga

[7] Möjligheten att begära data med stöd av kapitel V i förordningen är emellertid inte begränsad till data som genereras genom användning av kopplade produkter och tillhörande tjänster, även andra data kan begäras.

grunden i artikel 6.1 c i dataskyddsförordningen är tillämplig när en datahållare ska tillmötesgå en begäran från ett offentligt organ enligt kapitel V. Detta eftersom den rättsliga förplikten att tillmötesgå begäran föreskrivs dataförordningen.

Enligt artikel 19.1 b i dataförordningen ska ett offentligt organ som tar emot data till följd av en begäran ha genomfört tekniska och organisatoriska åtgärder som bevarar konfidentialiteten och integriteten avseende de data som begärs och säkerheten vid överföring av data, särskilt personuppgifter, och som skyddar de registrerades rättigheter och friheter.

Kapitel V ställer inte krav på offentliga organ att begära data, kapitlet föreskriver endast en sådan möjlighet. Ett svenskt offentligt organ som avser att begära personuppgifter med stöd av kapitel V måste därför säkerställa att det finns en rättslig grund som stöd för behandlingen av personuppgifter. Vi bedömer att kapitel V i dataförordningen i sig inte utgör en rättsligt grund för behandling av personuppgifter eftersom det inte går att finna stöd för sådan behandling i någon av grunderna i artikel 6.1 i dataskyddsförordningen. Utöver de allmänna bestämmelserna om behandling av personuppgifter kan det för myndigheter och andra verksamheter finnas speciallagstiftning som reglerar behandlingen av personuppgifter.

När det gäller myndigheters personuppgiftsbehandling utförs denna oftast för att behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning. Regeringen bedömt att alla uppgifter som riksdag eller regering gett i uppdrag åt statliga myndigheter att utföra är av allmänt intresse, samt att obligatoriska uppgifter som ålagts kommuner och regioner att utföra är av allmänt intresse (prop. 2017/18:105 s. 57–58).

Vissa registerförfattningar begränsar eller specificerar vilka personuppgifter som får behandlas av en myndighet och för vilka ändamål. Det har inom ramen för vårt uppdrag inte varit möjligt att identifiera registerförfattningar som aktualiseras med anledning av kapitel V i dataförordningen. Varje offentligt organ måste själv säkerställa att det har stöd för den behandling av personuppgifter som organet utför. En utgångspunkt för vårt arbete är dock att kapitel V inte innebär att offentliga organ får utökade uppgifter utan bygger på befintliga uppdrag och bidrar med ett ytterligare verktyg för att fullgöra dessa uppdrag.

Den uppgift som det offentliga organet har tilldelats genom lagstiftning, som kan läggas till grund för en begäran av data enligt kapitel V, måste enligt vår uppfattning har varit föremål för överväganden, exempelvis hur uppgiften ska utformas och vilket eller vilka offentliga organ den ska tilldelas. Det bör också ha övervägts vilka personuppgifter som kan komma att behandlas inom ramen för fullgörandet av uppgiften samt vilket stöd för behandlingen av personuppgifterna som krävs. Behovet av att kunna behandla personuppgifter för att utföra uppgiften bör därför redan vara tillgodosett. Vi bedömer mot denna bakgrund att det inte finns behov av att föreslå författningsändringar med anledning av den behandling av personuppgifter som kan aktualiseras på grund av en begäran om data med stöd av kapitel V i förordningen.

Pseudonymisering

Enligt artikel 17.2 e i dataförordningen ska en begäran om data enligt kapitel V som huvudregel gälla icke-personuppgifter. En begäran får avse personuppgifter endast om icke-personuppgifter har visats vara otillräckligt för att tillgodose det exceptionella behovet av att använda data i enlighet med artikel 15.1 a. Begäran ska då avse personuppgifter i pseudonymiserad form och fastställa de tekniska och organisatoriska åtgärder som ska vidtas för att skydda dessa data.

Pseudonymisering är en säkerhetsåtgärd som innebär att personuppgifterna ersätts med något annat, t.ex. en kod, och det krävs kompletterande uppgifter för att det ska vara möjligt att hänföra uppgiften till en specifik person. Pseudonymiserade personuppgifter omnämns inte specifikt i definitionen av personuppgift i artikel 4.1 i dataskyddsförordningen. Pseudonymisering definieras i artikel 4.5 i förordningen som ”behandling av personuppgifter på ett sätt som innebär att personuppgifterna inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används, under förutsättning att dessa kompletterande uppgifter förvaras separat och är föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte tillskrivs en identifierad eller identifierbar fysisk person”. En nyligen meddelad dom från EU-domstolen klargör att pseudonymiserade uppgifter inte per definition utgör personuppgifter. Det går dock inte heller enligt domstolen att rakt av avfärda pseudony-

miserade uppgifter som icke-personuppgifter.[8] Enbart den omständigheten att det existerar kompletterande uppgifter som gör det möjligt att identifiera den registrerade innebär inte i sig att pseudonymiserade uppgifter under alla omständigheter och för alla personer ska anses utgöra personuppgifter.[9] Domstolen uttalar följande om bedömningen huruvida pseudonymiserade uppgifter ska anses utgöra personuppgifter när den personuppgiftsansvarige har överfört uppgifterna till en mottagare, bl.a. i samband med en eventuell senare överföring till tredje man. I den mån det inte är uteslutet att en tredje man med rimlig sannolikhet kan hänföra de pseudonymiserade uppgifterna till den registrerade utgör uppgifterna personuppgifter. Detta kan ske genom att tredje man till exempel jämför de pseudonymiserade med andra uppgifter som den tredje mannen förfogar över. Den registrerade anses då vara identifierbar vad gäller såväl denna överföring som all senare behandling av dessa uppgifter som nämnda tredje man utför.[10] Det kan antas att bedömningen ska göras på samma sätt vid utlämnandet från den personuppgiftsansvarige till ett offentligt organ som begärt personuppgifter med stöd av kapitel V i dataförordningen. Domstolen klargör sammanfattningsvis att pseudonymiserade uppgifter inte ska anses utgöra personuppgifter under alla omständigheter och för alla personer, eftersom pseudonymisering, beroende på omständigheterna i det enskilda fallet, faktiskt kan hindra andra personer än den personuppgiftsansvarige från att identifiera den registrerade.[11]

Om ett offentligt organ begär personuppgifter ska organet enligt artikel 17.1 g i dataförordningen specificera om datahållaren kan tillämpa anonymisering av personuppgifterna innan data görs tillgängliga. Det framgår också av artikel 18.4 att om de data som begärs innehåller personuppgifter ska datahållaren anonymisera personuppgifterna på korrekt sätt, såvida det inte för att tillmötesgå begäran om att göra data tillgängliga för ett offentligt organ krävs att personuppgifterna lämnas ut. I sådana fall ska datahållaren pseudonymisera personuppgifterna.

[8] Dom av den 4 september 2025, *Europeiska datatillsynsmannen mot Gemensamma resolutionsnämnden*, C-413/23 P, EU:C:2025:645, p. 71–73, där domstolen uttalar att ”själva förekomsten av sådana upplysningar utgör emellertid hinder för att uppgifter som har pseudonymiserats under alla omständigheter kan anses vara anonyma uppgifter som inte omfattas av förordningens tillämpningsområde”.
[9] *Europeiska datatillsynsmannen mot Gemensamma resolutionsnämnden*, p. 82.
[10] *Europeiska datatillsynsmannen mot Gemensamma resolutionsnämnden*, p. 85.
[11] *Europeiska datatillsynsmannen mot Gemensamma resolutionsnämnden*, p. 86.

Sammantaget innebär detta att om ett offentligt organ begär data som utgör eller innehåller personuppgifter ska dessa som huvudregel avidentifieras på ett sätt som medför att det inte längre är fråga om personuppgifter i dataskyddsförordningens mening av datahållaren. Om det offentliga organet har bedömt att personuppgifterna är nödvändiga ska de pseudonymiseras. Om personuppgifter begärs ska det offentliga organet enligt artikel 17.2 utan oskäligt dröjsmål anmäla det till den tillsynsmyndighet som ansvarar för att övervaka tillämpningen av dataskyddsförordningen i den medlemsstat där det offentliga organet är etablerat, dvs. i Sverige IMY.

9.5.5 Behandling av personuppgifter i den certifierande verksamheten hos PTS

Bedömning: Det finns inte behov av författningsändringar för att nödvändig behandling av personuppgifter ska kunna utföras i den certifierande verksamheten hos PTS.

Vi föreslår att PTS ska vara den myndighet i Sverige som certifierar tvistlösningsorgan enligt dataförordningen, dvs. vara certifierande myndigheten. Verksamheten omfattar att ta emot och pröva ansökningar om certifiering från tvistlösningsorgan. Det ingår också för PTS att följa upp verksamheten hos certifierade tvistlösningsorgan. För att kunna utföra verksamheten krävs att PTS kan behandla personuppgifter.

Certifiering av tvistlösningsorgan blir därmed en uppgift av allmänt intresse i dataskyddsförordningens mening som dessutom innefattar myndighetsutövning. Den personuppgiftsbehandling som är nödvändig för att fullgöra uppgiften kan därför ske med stöd av artikel 6.1 e i dataskyddsförordningen, i den utsträckning som behandlingen är nödvändig för att fullgöra uppgiften och under förutsättning att övriga krav på personuppgiftsbehandlingen är uppfyllda. Behandling av särskilda kategorier av personuppgifter bedöms inte bli aktuell. Om sådan behandling skulle bli nödvändig för att kunna fullgöra uppgiften att certifiera tvistlösningsorgan, finns stöd för sådan personuppgiftsbehandling i 3 kap. 3 § lagen med kompletterande bestämmelser till EU:s dataskyddsförordning.

9.5.6 Behandling av personuppgifter hos domstolarna

Bedömning: Det finns inte behov av författningsändringar för att nödvändig behandling av personuppgifter ska kunna utföras hos domstolarna när ett beslut enligt dataförordningen eller den kompletterande lagstiftningen överklagas.

Beslut av PTS i egenskap av behörig myndighet samt i egenskap av certifierande myndighet kan överklagas till allmän förvaltningsdomstol. När ett beslut överklagas kommer behandling av personuppgifter att vara nödvändig hos domstolarna. Bestämmelser om behandling av personuppgifter finns i domstolsdatalagen (2015:728). Lagen kompletterar dataskyddsförordningen vid behandling av personuppgifter i de allmänna domstolarnas, de allmänna förvaltningsdomstolarnas och hyres- och arrendenämndernas rättskipande och rättsvårdande verksamhet. Enligt 6 § får personuppgifter behandlas om det behövs för handläggning av mål och ärenden. Behandling av särskilda kategorier av personuppgifter kan ske med stöd av 3 kap. 3 § lagen med kompletterande bestämmelser till EU:s dataskyddsförordning.

Det krävs enligt vår bedömning inte några ytterligare bestämmelser för att nödvändig behandling av personuppgifter ska kunna ske hos domstolarna till följd av överklagande av ett beslut enligt dataförordningen eller den kompletterande lagstiftningen.

10 Dataförordningen påverkar rätten av sitt eget slag

10.1 Dataförordningens undantag från rätten av sitt eget slag i databasdirektivet

EU:s direktiv om rättsligt skydd för databaser (databasdirektivet)[1] innehåller bestämmelser om bl.a. upphovsrättsligt skydd för databaser. Enligt artikel 1.2 avses med databas en samling av verk, data eller andra självständiga element som sammanställts på ett systematiskt och metodiskt sätt och som var för sig är tillgänglig genom elektroniska medier eller på något annat sätt.

I artikel 7.1 i direktivet föreskrivs att medlemsstaterna ska tillerkänna en databasproducent som vid anskaffning, granskning eller presentation visar sig innehålla en kvantitets- eller kvalitetsmässigt sett väsentlig investering, rätten att förbjuda utdrag och/eller återanvändning av hela eller en kvalitativt eller kvantitativt sett väsentlig del av databasens innehåll.[2] Rättigheten för databasproducenten heter på svenska rätten av sitt eget slag men i ett flertal andra språkversioner av direktivet används begreppet *sui generis*-rättighet.

Artikel 43 i dataförordningen föreskriver att rätten av sitt eget slag i artikel 7 i databasdirektivet inte ska tillämpas när data erhålls från eller genereras av en uppkopplad produkt eller en tillhörande tjänst som omfattas av förordningen. Det innebär att dataförordningen inför en begränsning av tillämpningsområdet av artikel 7 i direktivet. Direktivet ändras emellertid inte genom förordningen.

[1] Europaparlamentets och rådets direktiv 96/9/EG av den 11 mars 1996 om rättsligt skydd för databaser.

[2] Bestämmelsen är i den engelska språkversionen av direktivet enligt vår uppfattning enklare att förstå: Member States shall provide for a right for the maker of a database which shows that there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents to prevent extraction and/or re-utilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database.

Av skäl 112 i dataförordningen framgår att syftet med artikel 43 är att undanröja risken för att innehavare av data i databaser som erhålls eller genereras med hjälp av fysiska komponenter, såsom sensorer, i en uppkopplad produkt och en tillhörande tjänst eller andra maskingenererade data, åberopar rätten av sitt eget slag och därigenom i synnerhet hindrar ett effektivt utövande av användarnas rätt till åtkomst till och användning av data och deras rätt att dela data med tredje parter enligt förordningen. Det bör därför enligt samma skäl klargöras att rätten av sitt eget slag inte gäller för sådana databaser. Vidare framgår av skältexten att detta inte påverkar den eventuella tillämpningen av rätten av sitt eget slag enligt artikel 7 i databasdirektivet på databaser som innehåller data som inte omfattas av dataförordningen, förutsatt att kraven om skydd enligt punkt 1 i artikel 7 i direktivet är uppfyllda.

10.2 Rätten av sitt eget slag i Sverige

I Sverige har artikel 7 i databasdirektivet genomförts i 49 § upphovsrättslagen (1960:729) (URL), i det s.k. katalogskyddet. I 49 § första stycket URL föreskrivs att den som har framställt en katalog, en tabell eller ett annat dylikt arbete i vilket ett stort antal uppgifter har sammanställts eller vilket är resultatet av en väsentlig investering har uteslutande rätt att framställa exemplar av arbetet och göra det tillgängligt för allmänheten.

Det rör sig alltså om en bestämmelse i svensk lag som genomför en bestämmelse i ett EU-direktiv. Katalogskyddet fanns emellertid i svensk rätt innan databasdirektivet började gälla. Vid det svenska genomförandet av databasdirektivet konstaterades att skyddsföremålet för katalogskyddet är samlingar med ett stort antal uppgifter, t.ex. telefonkataloger, tidtabeller och sammanställningar av valuta- och börskurser (prop. 1996/97:111 s. 19–20). För att direktivet skulle bli helt genomfört ansågs att katalogskyddets föremål behövde ändras till att uttryckligen avse alla arbeten som är resultatet av en väsentlig investering, i enlighet med artikel 7 i databasdirektivet (prop. 1996/97:111 s. 19–20). Första stycket i 49 § URL ändrades följaktligen så att det inte endast är kataloger, tabeller och liknande arbeten som innehåller ett stort antal uppgifter som skyddas, utan även liknande arbeten som är resultatet av en väsentlig investering.

Vid genomförandet framhölls att databaser som är resultatet av en väsentlig investering har angivits som skyddsföremål (artikel 7.1) och att databaser som inte representerar en väsentlig investering inte kan göra anspråk på skydd (prop. 1996/97:111 s. 53–54). Rätten ger inte något skydd för de särskilda verk, uppgifter eller annat material som har samlats i databasen och får återanvändas av andra utan hinder av rätten av sitt eget slag (prop. 1996/97:111 s. 53–54). Det är endast databasen som sådan som är skyddad, med andra ord hela eller en väsentlig del av innehållet i databasen.

Katalogskyddet tar alltså sikte på katalog eller en annan produkt som innehåller en stor mängd information, inklusive databaser. Katalogskyddet omfattar alltså mer än databaser, till skillnad från artikel 7 i databasdirektivet som enbart avser databaser.

10.3 Dataförordningen påverkar upphovsrättslagens tillämpningsområde

Artikel 43 i dataförordningen föreskriver att artikel 7 i databasdirektivet inte ska tillämpas när data erhålls från eller genereras av en uppkopplad produkt eller en tillhörande tjänst som omfattas av förordningen. Dataförordningen föreskriver alltså en begränsning i tillämpningsområdet för databasdirektivet. En EU-förordning är bindande för medlemsstaterna och gäller direkt och likadant i alla medlemsstater. Den blir en del av den nationella lagstiftningen och får inte genomföras på annat sätt i nationell rätt. Eftersom EU-direktiv, till skillnad från EU-förordningar, ska genomföras i medlemsstaterna genom nationella bestämmelser ska begränsningen i dataförordningen i praktiken gälla för den nationella bestämmelse som genomför databasdirektivet. I svensk rätt är det 49 § URL.

Utifrån principen om EU-rättens företräde har dataförordningen företräde framför nationella bestämmelser. 49 § URL genomför artikel 7 i databasdirektivet såsom artikeln skulle förstås och tillämpas innan dataförordningens tillkomst. Paragrafen är alltså avsedd att omfatta databaser även när data erhålls från eller genereras av en uppkopplad produkt eller en tillhörande tjänst som omfattas av dataförordningen, under förutsättning att villkoren för att rätten av sitt eget slag är uppfyllda. Undantaget i artikel 43 i förordningen påverkar tillämpningsområdet för 49 § URL. Eftersom dataförordningen har

företräde, ska 49 § URL inte tillämpas på sådana situationer som omfattas av undantaget i artikel 43 dataförordningen.

Ur ett EU-rättsligt perspektiv är den uppkomna situationen inte tillfredsställande och den kan leda till svårigheter att förstå och tillämpa 49 § URL korrekt. Även om artikel 43 i dataförordningen har företräde förutsätter det att läsaren av 49 § URL har kännedom om artikeln. Någon form av åtgärd bör därför enligt vår bedömning vidtas.

10.3.1 Ändring i upphovsrättslagen

Förslag: I 49 § upphovsrättslagen (1960:729) ska en upplysningsbestämmelse införas som upplyser om att det av artikel 43 i EU:s dataförordning framgår att rätten av sitt eget slag enligt artikel 7 i direktiv 96/9/EG inte ska tillämpas när data erhålls från eller genereras av en uppkopplad produkt eller en tillhörande tjänst som omfattas av förordningen, särskilt med avseende på artiklarna 4 och 5 i förordningen.

Två lösningsalternativ

Utifrån principen om EU-rättens företräde går det att argumentera för att det skulle räcka med att konstatera att 49 § URL ska förstås och tillämpas i enlighet med de begränsningar som framgår av artikel 43 i dataförordningen. Det ställer dock krav på att den som ska tillämpa 49 § URL känner till artikel 43 i förordningen för att tillämpningen ska bli korrekt. Vi anser att det av tydlighetsskäl bör införas någon form av bestämmelse i 49 § URL som hänvisar till eller bygger på artikel 43 i förordningen eftersom det främjar korrekt tillämpning av paragrafen. Att inte vidta någon åtgärd bedömer vi inte som tillfredsställande. Vi har identifierat två möjliga lösningsalternativ.

Alternativet som vi förordar: Upplysningsbestämmelse

Det första alternativet är att införa en upplysningsbestämmelse i 49 § URL. En sådan bestämmelse upplyser om att det av artikel 43 i dataförordningen framgår att rätten av sitt eget slag enligt artikel 7 i databasdirektivet inte ska tillämpas när data erhålls från eller genereras av en uppkopplad produkt eller en tillhörande tjänst som om-

fattas av dataförordningen. Detta alternativ hjälper läsaren av lagtexten att förstå att det i en EU-rättsakt finns en bestämmelse som påverkar tillämpningen, utan att för den skull innebära att det blir fråga om att genomföra förordningen i svensk lagstiftning på ett sätt som utifrån ett EU-rättsligt perspektiv inte är tillåtet. Vi anser mot denna bakgrund att detta lösningsalternativ är att föredra. Vi föreslår därför att det införs en upplysningsbestämmelse i 49 § URL som upplyser om artikel 43 i dataförordningen.

Upplysningsbestämmelsen bör utformas i enlighet med hur artikel 43 i förordningen är formulerad. Detta för att inte riskera tolkning av artikeln. Vi är medvetna om att en texttrogen upplysningsbestämmelse i sig riskerar att uppfattas som otydlig. Artikel 43 i dataförordningen hänvisar till rätten av sitt eget slag i artikel 7 i databasdirektivet. I 49 § URL förekommer inte begreppet rätten av sitt eget slag och paragrafen, eller upphovsrättslagen i övrigt, hänvisar inte till databasdirektivet. Det finns därför risk att innebörden av upplysningsbestämmelsen inte blir enkel att förstå. Eftersom vi inte vill riskera tolkning av artikel 43 i förordningen anser vi emellertid att undantagsbestämmelsen bör formuleras på detta sätt. En sådan upplysningsbestämmelse bidrar till mer tydlighet avseende tillämpningen av 49 § URL än vad som hade varit fallet om bestämmelsen inte införs.

Det andra alternativet som vi har övervägt: Undantagsbestämmelse

Ett alternativ till att införa en upplysningsbestämmelse är att införa en undantagsbestämmelse. En sådan undantagsbestämmelse skulle begränsa tillämpningsområdet för 49 § URL, i syfte att säkerställa att paragrafen inte tillämpas på sådana situationer som omfattas av undantaget i artikel 43 i dataförordningen.

Att konstruera en ändamålsenlig undantagsbestämmelse är i detta fall förenat med vissa utmaningar. Som nämns ovan förekommer inte begreppet rätten av sitt eget slag i ordalydelsen i 49 § URL och hänvisning till databasdirektivet saknas. Databaser förekommer inte heller i ordalydelsen i paragrafen. Det framgår dock av lagens förarbeten att databaser omfattas. En undantagsbestämmelse skulle enligt vår uppfattning behöva formuleras som ett undantag till första stycket i 49 § URL och formuleras på ett sådant sätt att den kan förstås tillsammans med första stycket. Undantagsbestämmelsen skulle t.ex.

kunna formuleras som att första stycket inte ska tillämpas på databaser när data erhålls från eller genereras av en uppkopplad produkt eller en tillhörande tjänst som omfattas av EU:s dataförordning. En risk med att frångå formuleringen i artikel 43 i dataförordningen är dock att Sverige genomför förordningen i nationell rätt som ger andra rättsliga effekter än de som uppstår vid en direkt tillämpning av artikel 43 i dataförordningen. En annan möjlighet är att formulera undantagsbestämmelsen helt i enlighet med artikel 43 i dataförordningen. Det finns dock en risk att undantagsbestämmelsen då blir svår att förstå när den läses tillsammans med första stycket i 49 § URL.

Vi utesluter inte att det är möjligt att införa en undantagsbestämmelse i 49 § URL men bedömer att riskerna för otydlighet vad gäller förståelsen av undantaget talar för att en upplysningsbestämmelse, sammantaget med att EU-förordningar inte får genomföras i nationell lagstiftning, är att föredra.

11 Ikraftträdande och övergångsbestämmelser

Förslag: Lagen respektive förordningen med kompletterande bestämmelser till EU:s dataförordning samt övriga föreslagna författningsändringar ska träda i kraft den 1 juli 2026.

Enligt artikel 50 i dataförordningen ska förordningen börja tillämpas den 12 september 2025. Vissa delar av förordningen ska dock börja tillämpas vid en senare tidpunkt. De skyldigheter som följer av artikel 3.1 i förordningen ska tillämpas på de uppkopplade produkter och de tillhörande tjänster som släpps ut på marknaden efter den 12 september 2026. Tidpunkten för när vissa typer av avtal har ingåtts kan också påverka när förordningens bestämmelser ska tillämpas.

Den 12 september 2025 har vid överlämnandet av detta betänkande passerat. Det är därför angeläget att våra författningsförslag träder i kraft så fort som möjligt. Med hänsyn till remissförfarandet, det sedvanliga beredningsarbetet inom Regeringskansliet och riksdagsbehandlingen bedömer vi att den 1 juli 2026 är en realistisk tidpunkt. Bestämmelserna om att vissa delar av dataförordningen under vissa förutsättningar ska tillämpas vid en senare tidpunkt än den 12 september 2025 påverkar inte tillämpningen av de författningsförslag vi lämnar.

Vi bedömer att det inte finns behov av övergångsbestämmelser.

12 Förslagens konsekvenser

12.1 Inledning

Vi ska enligt våra utredningsdirektiv i enlighet med kommittéförordningen (1998:1474) och förordningen (2024:183) om konsekvensutredningar (konsekvensutredningsförordningen) bedöma och beskriva förslagens ekonomiska och samhällsekonomiska konsekvenser, samt konsekvenser i övrigt för enskilda, företag och det allmänna. Av 2 § konsekvensutredningsförordningen framgår att särskilda utredare ska redovisa en konsekvensutredning när de lämnar in förslag till regeringen eller Regeringskansliet om att regeringen ska föreslå eller besluta om nya eller ändrade lagar och förordningar. Särskilda utredare ska även för andra förslag som lämnas i ett betänkande redovisa en konsekvensutredning. Våra utredningsdirektiv och konsekvensutredningsförordningen tar alltså sikte på de förslag som lämnas av den särskilda utredaren.

Våra förslag kompletterar dataförordningen och vi redovisar i detta kapitel konsekvenser av förslagen. Europeiska kommissionen redovisade i anslutning till förslaget till dataförordning sin konsekvensutredning avseende förslaget.[1] Att dataförordningen kommer att leda till konsekvenser, inklusive ekonomiska konsekvenser, för ett stort antal företag, konsumenter och myndigheter står klart. Vi har emellertid inte bedömt konsekvenserna av själva förordningen eftersom det faller utanför vårt uppdrag.

I detta kapitel redovisar vi konsekvenserna av våra förslag.

[1] European Commission, Staff Working Document, Impact Assessment, SWD (2022) 34 final s. 68 ff.

12.2 Konsekvenser om inga åtgärder vidtas (nollalternativet)

I dataförordningen ställs krav på medlemsstaterna att vidta vissa åtgärder, exempelvis att utse en eller flera behöriga myndigheter. Att inte vidta de åtgärder som krävs skulle innebära att Sverige i egenskap av medlemsstat inte lever upp till sina skyldigheter. När det gäller behörig myndighet kan konstateras att regeringen visserligen har gett Post- och telestyrelsen (PTS) i uppdrag att vara behörig myndighet. Det räcker emellertid inte för att myndigheten ska kunna vidta alla de åtgärder som krävs för att säkerställa att förordningen efterlevs. Våra förslag avseende den behörig myndigheten är nödvändiga för att myndigheten ska kunna utföra uppgiften som behörig myndighet.

Vi lämnar också förslag om stöd till offentliga organ avseende tillämpning av kapitel V i dataförordningen samt uppdrag till sektorsansvariga beredskapsmyndigheter. Förslagen har ingen motsvarighet i, och krävs inte av, dataförordningen. De syftar till att i förlängningen underlätta tillämpningen av kapitel V i förordningen och förbättra förutsättningarna för offentliga organ att begära data med stöd av bestämmelserna i kapitlet. Förslagen är inte nödvändiga för att Sverige ska leva upp till kraven som ställs på medlemsstaterna men de kommer att underlätta tillämpningen av förordningen för beredskapsmyndigheter och övriga offentliga organ. Ökat stöd till offentliga organ kommer enligt vår bedömning även att underlätta för datahållare.

Sammantaget innebär nollalternativet, dvs. att inte vidta de åtgärder som krävs enligt dataförordningen, dels att Sverige inte lever upp till sina åtaganden, dels att aktörer som omfattas av förordningen kan drabbas negativt.

12.3 Förslagens konsekvenser för företag

Det har inte varit möjligt för oss att få fram statistik över hur många svenska företag som omfattas av dataförordningen. Vi har t.ex. inte lyckats identifiera statistik över hur många tillverkare av uppkopplade produkter eller leverantörer av tillhörande tjänster som finns i Sverige. Det finns statistik över företag inom olika branscher men inte statistik över hur många av företagen i en bransch som tillverkar exempelvis uppkopplade produkter. Inom vissa branscher kan

antalet företag som tillverkar sådana produkter vara högre eller lägre än i andra och i vissa branscher kan i princip alla tillverkare tillverka uppkopplade produkter. Det har heller inte varit möjligt för oss att få fram statistik som kan hjälpa oss att bedöma hur många företag det finns i Sverige som är datahållare enligt dataförordningen eller som kommer att vara datamottagare. Skälet till att vi lyfter detta är att antalet företag som omfattas av förordningen också omfattas av våra förslag avseende den behöriga myndigheten. Det får påverkan på vilka resurser som krävs för uppdraget att utöva tillsyn över dataförordningen och den kompletterande lagen.

En central utgångspunkt i utredningens arbete bör enligt våra utredningsdirektiv vara att skapa en balans mellan effektiv tillsyn och administration och minimering av den administrativa bördan för företag och myndigheter. Enligt direktiven ska vi också beakta vikten av att underlätta för svenska företag, särskilt små och medelstora företag, att följa de nya reglerna utan att skapa onödiga hinder för innovation och tillväxt. Våra förslag innebär inga ytterligare krav på företag utöver de som ställs i dataförordningen. Vi har aktivt arbetat för att förslagen inte ska leda till ökade kostnader för företag utöver de som följer av förordningen. Dataförordningen ger dock inte utrymme för att göra undantag från eller på annat sätt förenkla bestämmelserna i förordningen. Det går emellertid inte att bortse från att den verksamhet som PTS bedriver i egenskap av behörig myndighet kan komma att leda till kostnader hos ett företag om det t.ex. inkommer ett klagomål till myndigheten avseende det aktuella företaget. Det framgår dock av dataförordningen att behöriga myndigheter ska hantera och utreda klagomål samt vidta åtgärder vid överträdelser.

Våra förslag innebär att dataförordningen kompletteras med svenska bestämmelser. Vissa av dessa bestämmelser krävs för att den behöriga myndigheten ska kunna utföra de uppgifter och befogenheter som förväntas enligt dataförordningen. Myndigheten ska exempelvis kunna fatta beslut om sanktioner. För att det ska vara möjligt krävs bestämmelser i lag. Företag kan omfattas av dataförordningen utifrån olika roller. De kan t.ex. vara datahållare, datamottagare, tredje part, leverantörer av databehandlingstjänster eller kunder av databehandlingstjänster. Samma företag kan också, beroende på situationen, omfattas av förordningen utifrån flera roller, exempelvis som datahållare i en situation och datamottagare i en annan. Möjligheten

för PTS att kunna fatta beslut om sanktioner och sanktionsavgifter vid överträdelser av förordningen innebär att myndigheten kan säkerställa att företag lever upp till sina skyldigheter enligt förordningen och underlättar för företag att tillvarata sina rättigheter. Att leva upp till dataförordningens krav kan vara förenat med kostnader för företag. Avsaknad av möjligheter för den behöriga myndigheten att kunna vidta adekvata åtgärder för att säkerställa att förordningen efterlevs riskerar att leda till att företag inte lever upp till kraven för att undvika kostnaderna. Det ska inte gynna ett företag att inte leva upp till förordningens krav och risken att kunna drabbas av sanktionsavgifter bedömer vi främjar en sund konkurrens.

Dataförordningen är ett komplext regelverk och som vi konstaterar i kapitel 8 i betänkandet uppfattar vi att det råder osäkerhet om hur vissa bestämmelser ska tolkas och tillämpas. Som vi har nämnt tidigare anser vi att en viktig uppgift för PTS i egenskap av behörig myndighet är att löpande informera om dataförordningen och utvecklingen som har bäring på förordningen. Dataförordningen påverkar företag och för flera av dem kommer anpassningar att krävas. Ett aktivt informationsarbete av PTS kan underlätta för företagen.

När det gäller förslaget att ge PTS i uppdrag att inrätta regulatorisk testverksamhet kommer projekt inom ramen för testverksamheten att gynna företag eftersom projekten kommer att öka förståelsen för bestämmelserna i dataförordningen. Projekten kan i sig också ge en ökad inblick i hur förordningen påverkar företag. Endast ett eller ett fåtal företag kommer att ingå i respektive projekt. Det finns en risk att det kan leda till att de företag som ingår i ett projekt får en konkurrensfördel gentemot andra aktörer i sin bransch. Det är därför viktigt att resultatet av arbetet i ett projekt inom ramen för testverksamheten skyndsamt publiceras offentligt så att alla kan ta del av det. Detta i syfte att motverka risken för att påverka konkurrensförhållanden.

12.4 Konsekvenser för statliga myndigheter och domstolarna

12.4.1 Konsekvenser för Post- och telestyrelsen

Bedömning: Förslagen innebär utökade och nya arbetsuppgifter för PTS. Det medför initialt ett ökat finansieringsbehov motsvarande

- 9 miljoner kronor för 2026 och 18 miljoner kronor för 2027 för verksamheten som behörig myndighet,
- 4,5 miljoner kronor för det första året och 3 miljoner för det andra året för uppdraget att bedriva regulatorisk testverksamhet, och
- 500 000 kronor för 2026 och 300 000 kronor för 2027 för verksamheten som certifierande myndighet.

Finansieringen bör ske genom att myndighetens anslag ökas.

Våra förslag innebär till viss del till utökade och nya arbetsuppgifter för PTS. Myndigheten är visserligen redan utsedd till behörig myndighet enligt dataförordningen av regeringen men våra förslag syftar till att säkerställa att myndigheten i sin roll som behörig myndighet har de uppgifter och befogenheter som krävs enligt förordningen.

Vidare föreslår vi att PTS ska få i uppdrag att inrätta regulatorisk testverksamhet och att myndigheten ska vara den certifierande myndighet i Sverige som certifierar tvistlösningsorgan enligt förordningen. Dessa uppgifter omfattas inte av regeringens beslut att utse myndigheten till behörig myndighet.

Konsekvenser för PTS i egenskap av behörig myndighet

PTS har som behörig myndighet enligt dataförordningen den övergripande uppgiften att säkerställa tillämpning och efterlevnad av förordningen. Det innefattar bl.a. hantering av klagomål och att vidta utredningsåtgärder, undersöka hur förordningen tillämpas, informera om förordningen samt samarbete med nationella myndigheter, myndigheter i andra medlemsstater samt EU-organ.

Arbetet med att bygga upp verksamheten hos PTS har redan påbörjats eftersom myndigheten redan är utsedd till behörig myndighet. PTS har erfarenhet av att bedriva tillsynsverksamhet. Myndigheten är t.ex. tillsynsmyndighet enligt lagen (2024:500) med kompletterande bestämmelser till EU:s dataförvaltningsförordning[2] och tillsynsmyndighet enligt lagen (2022:482) om elektronisk kommunikation[3]. Erfarenheten av att bedriva tillsyn bör underlätta myndighetens uppbyggnad av verksamheten som behörig myndighet enligt dataförordningen.

Vi tror även att det finns fler synergier. Behöriga myndigheter enligt dataförordningen ska enligt artikel 42 i förordningen vara företrädda i Europeiska datainnovationsstyrelsen (EDIB), som har inrättats av kommissionen som en expertgrupp enligt artikel 29 i dataförvaltningsförordningen. Eftersom PTS är behörig myndighet enligt dataförvaltningsförordningen är myndigheten redan företrädd i EDIB. Myndigheten har därigenom redan erfarenhet av arbetet i EDIB, vilket torde underlätta för myndigheten att sätta sig in i arbetet som avser dataförordningen. Vidare har regeringen, som tidigare nämnts, aviserat att Myndigheten för digital förvaltning (Digg) ska avvecklas och att merparten av myndighetens uppgifter ska inordnas i PTS. Digg har i dag uppgifter som på olika sätt har relevans för PTS inom ramen för uppgiften att vara behörig myndighet enligt dataförordningen. Digg är t.ex. behörigt organ enligt dataförvaltningsförordningen[4] och behörig myndighet och enda kontaktpunkt enligt förordningen om ett interoperabelt Europa[5]. Vi bedömer att erfarenheterna och kunskapen inom Digg kommer att underlätta för PTS att utföra uppgiften som behörig myndighet enligt dataförordningen. Ytterligare en omständighet som kan underlätta för PTS är att myndigheten inom ramen för uppgiften att vara samordnare enligt EU:s förordning om digitala tjänster har utvecklat en e-tjänst där användare kan lämna in klagomål och ett ärendehandläggningssystem för handläggningen av inkomna klagomål. En liknande ordning kan med fördel gälla för hantering av ärenden enligt dataförordningen.

För att utföra uppgiften som behörig myndighet kommer det att krävas olika kompetenser hos PTS. Det kommer att krävas bl.a. tek-

[2] 3 § förordningen (2024:502) med kompletterande bestämmelser till EU:s dataförvaltningsförordning.
[3] 5 § förordningen (2022:511) om elektronisk kommunikation.
[4] 1 c § förordningen (2018:1486) med instruktion för Myndigheten för digital förvaltning.
[5] 1 d § förordningen (2018:1486) med instruktion för Myndigheten för digital förvaltning.

nisk kompetens, rättslig kompetens, ekonomisk kompetens och kompetens inom kommunikation. Insatser i form av bl.a. integration gentemot it-system som tillhandahålls av kommissionen kan också komma att krävas.

Verksamheten hos PTS bör byggas upp stegvis och vi bedömer att behoven av insatser kommer att skifta över tid. I det initiala skedet är det, utöver att myndigheten fortsätter att bygga upp verksamheten, viktigt att PTS informerar om dataförordningen. Ett rimligt antagande är att antalet klagomål och egeninitierade ärenden hos myndigheten kommer att öka över tid. Det är dock i dagsläget förenat med stor osäkerhet att bedöma hur många ärenden det kan röra sig om samt graden av komplexitet i ärendena. Antalet ärenden och komplexiteten påverkar myndighetens resursbehov. En central del av uppdraget som behörig myndighet är att säkerställa efterlevnad, dvs. utöva tillsyn. Tiden bör enligt vår uppfattning utvisa vilket behov av tillsyn som föreligger och finansieringen bör dimensioneras i första hand utifrån omfattningen på tillsynen som bedrivs.

Vi bedömer att resursbehovet initialt är cirka 6 årsarbetskrafter för 2026 och cirka 12 årsarbetskrafter för 2027, med tyngdpunkt på att bygga upp verksamheten och för att finansiera informationsinsatser. Vi föreslår inga avgifter (exempelvis tillsynsavgifter) i anslutning till den verksamhet PTS bedriver i egenskap av behörig myndighet. Resursbehovet kan inte finansieras inom befintlig ram och myndigheten beräknas därför behöva tillföras 9 miljoner kronor för 2026 och 18 miljoner kronor för 2027. Eftersom bedömningen är förenad med stor osäkerhet är vår uppfattning att resursbehovet bör utvärderas i god tid före utgången av 2027 för att säkerställa att PTS från och med 2028 och framåt tillförs rätt nivå av finansiering för att fungera som behörig myndighet enligt dataförordningen. Efter 2027 bör fokuset inom verksamheten skifta över till tillsyn och finansieringen bör då dimensioneras i första hand utifrån den tillsyn som bedrivs.

Konsekvenser för PTS med anledning av förslaget om regulatorisk testverksamhet

Vi föreslår kapitel 8 att PTS ska få ett regeringsuppdrag att inrätta regulatorisk testverksamhet avseende dataförordningen. Testverksamheten går utöver PTS uppgift att vara behörig myndighet enligt förordningen. För att driva testverksamheten krävs bl.a. rättslig och tek-

nisk kompetens. Vi föreslår att uppdraget ska vara tidsbegränsat till två år. Det kommer troligen att krävas mer omfattande insatser i inledningsskedet. Testverksamheten föreslås inte finansieras via avgifter. Resursbehovet kan inte finansieras inom befintlig ram och myndigheten beräknas behöva tillföras 4,5 miljoner kronor för det första året och 3 miljoneter för det andra året.

Konsekvenser för PTS i egenskap av certifierande myndighet

PTS föreslås vara den myndighet i Sverige som certifierar tvistlösningsorgan enligt dataförordningen (certifierande myndighet). Ett tvistlösningsorgan certifieras efter prövning av en ansökan om certifiering hos PTS. Vi bedömer att antalet ansökningar kommer att vara lågt, högst enstaka ansökningar per år och vissa år är det möjligt att det inte inkommer några ansökningar. Vi föreslår att prövning av en ansökan får finansieras via avgift utifrån principen om full kostnadstäckning. Avgiftsfinansieringen avser endast prövning av en ansökan.

PTS behöver inom ramen för uppgiften att vara certifierande myndighet inledningsvis ta fram processer och rutiner för prövning av ansökningar samt för uppföljning av verksamheten hos certifierade tvistlösningsorgan. Myndigheten behöver också ta fram föreskrifter för avgiftsfinansieringen. Därefter behöver myndigheten ha beredskap för att hantera ansökningar samt vid behov uppdatera processer och rutiner. Myndigheten behöver också kunna följa upp verksamheten hos certifierade tvistlösningsorgan.

Det ökade resursbehovet kan inte finansieras inom befintlig ram och myndigheten beräknas genom ökade anslag behöva tillföras 500 000 kronor för 2026. Därefter beräknas myndigheten behöva tillföras 300 000 kronor för 2027. Resursbehovet bör i god tid innan utgången av 2027 utvärderas för att säkerställa att Sverige från 2028 och framåt lever upp till kravet i dataförordningen att tvistlösningsorgan kan certifieras.

12.4.2 Konsekvenser för Myndigheten för samhällsskydd och beredskap

Bedömning: Förslaget att Myndigheten för samhällsskydd och beredskap ska ges ett uppdrag av regeringen att ge stöd till offentliga organ innebär nya arbetsuppgifter för myndigheten. Det medför ett ökat finansieringsbehov motsvarande 6 miljoner kronor.
Finansieringsbehovet kan inte finansieras inom befintlig ram.

Förslaget att Myndigheten för samhällsskydd (MSB)[6] och beredskap ska ges ett uppdrag att stödja offentliga organ avseende kapitel V i dataförordningen, i syfte att hantera allmänna nödläge, får konsekvenser för myndigheten.

Stödet bör bl.a. bestå i vägledning i hur offentliga organ kan underlätta för datahållare att så enkelt och säkert som möjligt tillgängliggöra data samt vägledning i hur tekniska resurser och organisatoriska förmågor kan användas för att underlätta tillämpning av kapitel V i förordningen. Vid behov kan utbildningar hållas och dialog bör föras med datahållare och representanter för datahållare.

MSB utgör den centrala samordnande myndigheten för krisberedskap och civilt försvar och har enligt sin instruktion i uppgift att stödja berörda myndigheters samordning av åtgärder vid en kris eller vid höjd beredskap. Myndigheten har redan upparbetade kanaler för att föra dialog med statliga myndigheter, kommuner och regioner samt med näringslivet. Myndigheten har den erfarenhet och kompetens som kan användas vid utförande av uppdraget. Dataförordningen är emellertid en nytt regelverket som myndigheten måste sätta sig in i och uppdraget innebär en ny arbetsuppgift för myndigheten. Uppdraget bör vara tidsbegränsat till ett år.

Resursbehovet kan inte finansieras inom befintlig ram och myndigheten beräknas behöva tillföras 6 miljoner kronor för genomförande av uppdraget.

[6] Regeringen har beslutat att MSB från och med 1 januari 2026 får det nya namnet Myndigheten för civilt försvar.

12.4.3 Konsekvenser för sektorsansvariga beredskapsmyndigheter

Bedömning: Eventuella ökade resursbehov till följd av förslaget att regeringen ska ge sektorsansvariga beredskapsmyndigheter i uppdrag att kartlägga tekniska och organisatoriska förutsättningar att begära, ta emot och använda data kan hanteras inom befintlig ram hos sektorsansvariga beredskapsmyndigheter.

Förslaget att regeringen ska ge sektorsansvariga beredskapsmyndigheter att i uppdrag att kartlägga tekniska och organisatoriska förutsättningar inom respektive beredskapssektor att begära, ta emot och använda data vid allmänt nödläge enligt kapitel V i dataförordningen, får konsekvenser för dessa myndigheter. Uppdraget ska ges till Försäkringskassan, PTS, Statens energimyndighet, Finansinspektionen, Skatteverket, Socialstyrelsen, Livsmedelsverket, Polismyndigheten, MSB, Trafikverket, Kommerskollegium och Tillväxtverket. Förslaget får konsekvenser också för övriga beredskapsmyndigheter som ingår i respektive beredskapssektor. Vi föreslår att uppdraget ska vara tidsbegränsat till ett år.

Bestämmelser om beredskapsmyndigheter och sektorsansvariga beredskapsmyndigheter finns i förordningen (2022:524) om statliga myndigheters beredskap. Syftet med förordningen är att statliga myndigheter under regeringen genom sin verksamhet ska minska sårbarheten i samhället och utveckla en god förmåga att hantera sina uppgifter vid fredstida krissituationer och höjd beredskap. I 20 § andra stycket sjunde punkten föreskrivs att beredskapsmyndigheterna särskilt ska beakta behovet av säkerhet och kompatibilitet i de tekniska system som är nödvändiga för att myndigheterna ska kunna utföra sitt arbete. Enligt 24 § ska en sektorsansvarig myndighet inom sin beredskapssektor bl.a. leda arbetet med att samordna åtgärder inför och vid fredstida krissituationer och höjd beredskap.

Att ha tillgång till nödvändiga data och att kunna använda dem är redan i dag en viktig förmåga för att utföra uppgifter vid fredstida krissituationer. Kapitel V i dataförordningen innebär ett nytt verktyg för att få tillgång till data. Arbetet inom beredskapssektorerna har enligt en rapport av Myndigheten för totalförsvarsanalys hittills fokuserat på förutsättningsskapande arbete men enskilda beredskaps-

myndigheter arbetar mycket med förmågeskapande aktiviteter.[7] Flera av sektorerna bedriver enligt myndighetens rapport utbildnings- och övningsverksamhet för sektorns operativa hantering av händelser. Möjligheten att få tillgång till data som kan användas och vid behov delas vidare bör redan vara en del av arbetet hos beredskapsmyndigheterna och inom beredskapssektorerna. Kapitel V i dataförordningen utökar möjligheterna att begära data om de behövs för att hantera ett allmänt nödläge. Det uppdrag vi föreslår för sektorsansvariga beredskapsmyndigheter bör därför kunna hanteras som ytterligare en aspekt av det arbete som redan pågår.

Uppdraget till Försäkringskassan, PTS, Statens energimyndighet, Finansinspektionen, Skatteverket, Socialstyrelsen, Livsmedelsverket, Polismyndigheten, MSB, Trafikverket, Kommerskollegium och Tillväxtverket kan eventuellt leda till en mindre ökning av resursbehovet hos vissa av myndigheterna men bör enligt vår bedömning kunna hanteras inom befintlig ram. Detsamma gäller för övriga beredskapsmyndigheter som ingår i respektive beredskapssektor som kan komma att bidra i utförandet av uppdraget.

12.4.4 Konsekvenser för domstolarna

En part som anser att skyldigheter eller rättigheter enligt dataförordningen inte respekteras av en annan part kan väcka talan i domstol. Det följer direkt av förordningen, inte av våra förslag. I vilken utsträckning parter kommer att välja att väcka talan i domstol, eller vända sig till ett tvistlösningsorgan, när de inte är överens är svårt att ha en uppfattning om i dagsläget. Vissa parter kommer att vända sig till den behöriga myndigheten, dvs. PTS och lämna in klagomål, i stället för att väcka talan i domstol eller vända sig till ett tvistlösningsorgan.

Beslut av PTS i egenskap av behörig myndighet och certifierande myndighet kan överklagas till allmän förvaltningsdomstol. När det gäller beslut avseende certifiering bedömer vi att det kan röra sig om på sin höjd enstaka ärenden per år som eventuellt kan komma att överklagas.

[7] Myndigheten för totalförsvarsanalys, Beredskapssektorernas utveckling – Huvudrapport, 2025-06-13, s. 19.

När det gäller beslut av PTS i egenskap av behörig myndighet bedömer vi att ärendetillströmningen till domstolarna kan komma att öka men att det kommer att röra sig om ett lågt antal ärenden per år. Resursbehovet bör därför kunna finansieras inom befintlig ram.

Denna bedömning är dock förenad med stor osäkerhet. I avsnitt 12.9 nedan behandlar vi utvärdering av konsekvenserna av våra förslag. Ärendetillströmningen till domstolarna bör vara en del av utvärderingen.

12.5 Konsekvenser för kommuner och regioner

Kommuner och regioner kan påverkas av dataförordningen utifrån olika roller, exempelvis i egenskap av användare av uppkopplade produkter och tillhörande tjänster, kunder av databehandlingstjänster samt i egenskap av offentliga organ.

När det kommer till våra förslag får de konsekvenser för kommuner och regioner om de agerar i egenskap av offentliga organ och begär data med stöd av kapitel V i dataförordningen. Vid överträdelse av förordningen kan de exempelvis bli föremål för sanktionsavgift. Förslaget avseende stöd till offentliga organ i tillämpningen av kapitel V får konsekvenser för kommuner och regioner eftersom förslaget avser att underlätta för offentliga organ att tillämpa kapitel V.

Våra förslag inskränker inte den kommunala självstyrelsen och förslagen i sig leder inte till ökade kostnader för kommuner och regioner.

12.6 Konsekvenser för jämställdhet

Det är svårt att dra slutsatser om, och i så fall hur, dataförordningen kan komma att påverka jämställdheten. Det är dock enligt vår uppfattning att inte möjligt att fastslå någon sådan påverkan. Frågan berörs inte i kommissionens konsekvensutredning avseende dess förordningsförslag. Av Internetstiftelsens rapport Svenskarna och internet från 2022 framgår att något fler män än kvinnor totalt sätt uppgav att de har uppkopplade prylar[8] men att det nästan enbart är i de äldsta generationerna som fler män än kvinnor har en uppkopplad

[8] Med prylar avses vardagsföremål såsom olika hushållsmaskiner, men inte dator, mobiltelefon eller surfplatta.

pryl.[9] Vidare framgår att män har fler antal uppkopplade prylar än kvinnor. Om vi gör antagandet att detta fortfarande stämmer är det trots allt svårt att dra säkra slutsatser kring hur dataförordningens bestämmelser om uppkopplade produkter och tillhörande tjänster kan komma att påverka jämställdheten. Exemplet ovan om användning av uppkopplade prylar är dessutom relevant endast för delmängd av dataförordningens bestämmelser.

I Sverige driver fler män än kvinnor företag. Den exakta fördelningen verkar bero på hur företagande definieras men Jämställdhetsmyndigheten har uppgett att 2022 var 30 procent av de som drev företag kvinnor och 70 procent män.[10] Det är troligt att fler företag som drivs av män än kvinnor kommer att omfattas av den verksamhet PTS bedriver som behörig myndighet. Om ett företag drivs av män eller kvinnor har ingen relevans för bedömningen om företaget omfattas av dataförordningen eller inte.

Vår bedömning är att våra förslag inte påverkar jämställdheten.

12.7 Konsekvenser för den personliga integriteten

När det gäller personlig integritet aktualiserar våra förslag frågor om dataskydd. Dessa behandlas i kapitel 9. Dataförordningen leder till att antalet behandlingar av personuppgifter kommer att öka. Detta faktum påverkas emellertid inte av våra förslag. Alla behandlingar av personuppgifter som sker till flöjd av dataförordningen måste ske i enlighet med de krav som ställs i dataskyddsregelverket på sådana behandlingar.

Våra förslag avser bl.a. verksamheten hos PTS i egenskap av behörig myndighet. PTS behöver behandla personuppgifter för att bedriva verksamheten. Att medlemsstaterna ska utse en eller flera behöriga myndigheter framgår av dataförordningen. Likaså föreskrivs i dataförordningen vilka arbetsuppgifter de behöriga myndigheterna ska ha. Vi bedömer därför att våra förslag avseende behöriga myndigheter i sig inte leder till ökad behandling av personuppgifter. Av kapitel 9 framgår att vi bedömer att PTS har rättslig grund enligt dataskyddsförordningen för den behandling av personuppgifter som är nödvändig i rollen som behörig myndighet. Myndigheten måste

[9] Internetstiftelsen, Svenskarna och internet 2022, s. 231.
[10] https://jamstalldhetsmyndigheten.se/jamstalldhet-i-sverige/delmal-2-ekonomisk-jamstalldhet/ (hämtad 2025-11-20).

säkerställa att den följer de krav dataskyddsförordningen ställer på behandlingen av personuppgifter.

Offentliga organ kan med stöd av kapitel V i dataförordningen begära data om de har ett exceptionellt behov av dessa data. Offentliga organ får begära personuppgifter endast om de krävs för att hantera ett allmänt nödläge. Det innebär att behandlingarna av personuppgifter kan komma att öka jämfört med situationen innan dataförordningen trädde i kraft. Detta eftersom förordningens kapitel V är ett nytt verktyg för svenska offentliga organ att begära data. Personuppgifter ska som huvudregel enligt artikel 18.4 i förordningen anonymiseras av datahållaren innan de tillgängliggörs. Om det krävs att personuppgifterna lämnas ut ska datahållaren pseudonymisera personuppgifterna. Offentliga organ måste ha en rättslig grund för att behandla personuppgifter som de begär med stöd av kapitel V i förordningen. De måste säkerställa att den eventuella behandling av personuppgifter som är nödvändig lever upp till kraven i dataskyddsförordningen. Även detta är en direkt följd av dataförordningen, inte av våra förslag.

Behandling av personuppgifter som sker mot bakgrund av dataförordningen ska vara förenlig med dataskyddsregelverket och vi bedömer att våra förslag inte får negativa konsekvenser för den personliga integriteten.

12.8 Förslagens överensstämmelse med EU-rätten

Våra förslag innebär att Sverige vidtar de åtgärder som krävs enligt dataförordningen. Förslagen är utformade på ett sådant sätt att de säkerställer att åtgärderna vidtas i enlighet med förordningen. Förslagen är förenliga med dataförordningen och EU-rätten i övrigt.

Vissa av våra förslag går utöver vad som krävs enligt förordningen. Det gäller förslagen om att regeringen ska ge uppdrag till PTS, MSB och sektorsansvariga beredskapsmyndigheter. Förslagen kan sammantaget sägas syfta till att underlätta och främja tillämpningen av förordningen. Även dessa förslag är förenliga med dataförordningen och EU-rätten i övrigt.

12.9 Utvärdering av konsekvenserna

Att i förväg bedöma konsekvenserna av dataförordningen är förenat med osäkerhet. Eftersom våra förslag kompletterar förordningen är även bedömningarna avseende konsekvenserna av våra förslag till viss del förenade med osäkerhet. En utvärdering av konsekvenserna av dataförordningen i Sverige och av våra förslag bör genomföras en tid efter att förordningen har tillämpats och våra förslag har trätt i kraft.

Denna utvärdering bör göras innan kommissionen enligt artikel 49 i förordningen ska utvärdera förordningen och lämna en rapport om de viktigaste resultaten till Europaparlamentet, rådet och Europeiska ekonomiska och sociala kommittén, vilket ska ske senast den 12 september 2028. Syftet med att göra utvärderingen innan detta datum är att Sverige då kan bidra till kommissionens utvärdering.

12.10 Ikraftträdande och informationsinsatser

Dataförordningens bestämmelser ska enligt artikel 50 i förordningen tillämpas från och med den 12 september 2025. Detta datum har redan passerat och det är därför angeläget att våra författningsförslag träder i kraft så tidigt som möjligt. Datum för ikraftträdande behandlas i kapitel 11 i betänkandet.

Vad gäller behovet av informationsinsatser framgår av kapitel 8 i betänkandet att vi anser att den behöriga myndigheten i Sverige, dvs. PTS, har en viktig roll att spela när det kommer till att sprida information om dataförordningen.

13 Författningskommentar

13.1 Förslaget till lag med kompletterande bestämmelser till EU:s dataförordning

Lagens syfte

1 § Denna lag kompletterar Europaparlamentets och rådets förordning (EU) 2023/2854 av den 13 december 2023 om harmoniserade regler för skälig åtkomst till och användning av data och om ändring av förordning (EU) 2017/2394 och direktiv (EU) 2020/1828 (dataförordningen), i denna lag benämnd EU:s dataförordning.

I paragrafen anges lagens innehåll. Övervägandena finns i avsnitt 4.2.1 och 4.2.2.

Av paragrafen framgår att syftet med lagen är att komplettera Europaparlamentets och rådets förordning (EU) 2020/1828 av den 13 december 2023 om harmoniserade regler för skälig åtkomst till och användning av data och om ändring av förordning (EU) 2017/2394 och direktiv (EU) 2020/1828 (dataförordningen) (i författningskommentaren kallad dataförordningen).

Eftersom lagen kompletterar dataförordningen ska den läsas tillsammans med denna förordning och kan inte tillämpas fristående. Hänvisningar till förordningen är i huvudsak dynamiska. Det innebär att hänvisningen avser dataförordningen i den vid varje tidpunkt gällande lydelsen. I 6 § görs dock hänvisning till dataförordningen i dess ursprungliga lydelse. Det innebär att denna bestämmelse i stället innehåller en statisk hänvisning till förordningen, dvs. att förordningens lydelse i den ursprungliga versionen gäller vid tillämpning. I paragrafen anges att förordningen i denna lag kallas EU:s dataförordning.

Ord och uttryck i lagen

2 § Ord och uttryck i lagen har samma betydelse som i EU:s dataförordning.

Paragrafen innehåller en bestämmelse om definitioner. Övervägandena finns i avsnitt 4.2.1.

Av paragrafen framgår att de ord och uttryck som används i lagen ska förstås på samma sätt som i dataförordningen, om inget annat anges. Det innebär att definitionerna i artikel 2 i dataförordningen även gäller vid tillämpningen av lagen, om inget annat anges. Även sådana ord och uttryck som används i dataförordningen utan att definieras där ska tolkas och tillämpas på samma sätt när de förekommer i lagen.

I lagen görs dock vissa anpassningar till svensk rättsordning, vilket innebär att annan terminologi kan användas. Som exempel kan nämnas att i stället för ekonomiska sanktioner med retroaktiv verkan används ordet sanktionsavgift.

Behöriga myndigheter och datasamordnare

3 § Den eller de myndigheter som regeringen bestämmer ska vara behörig myndighet enligt EU:s dataförordning, denna lag och föreskrifter som har meddelats i anslutning till lagen.

Om regeringen bestämmer att fler än en myndighet ska vara behörig myndighet enligt första stycket ska regeringen bestämma vilken myndighet som ska vara datasamordnare enligt EU:s dataförordning.

Paragrafen reglerar behöriga myndigheter och datasamordnare. Övervägandena finns i avsnitt 4.3.2.

Enligt paragrafens *första stycke* är den eller de myndigheter som regeringen bestämmer behöriga myndigheter enligt dataförordningen, den kompletterande lagen samt föreskrifter som har meddelats i anslutning till lagen. Detta innebär att de behöriga myndigheterna för svenskt vidkommande ska utöva de uppgifter som enligt dataförordningen, lagen och föreskrifter som har meddelats i anslutning till lagen tillskrivs behöriga myndigheter och vidta åtgärder för att säkerställa att dessa följs. Uttrycket ”i anslutning till lagen” används för att klargöra att hänvisningen avser att träffa såväl föreskrifter som

har meddelats med stöd av lagen som föreskrifter som har meddelats med stöd av 8 kap. 7 § regeringsformen.

Av *andra stycket* framgår att regeringen ska utse en datasamordnare enligt dataförordningen om regeringen utser fler än en behörig myndighet. Att medlemsstater som utser fler än en behörig myndighet också ska utse en datasamordnare framgår av artikel 37.2 i förordningen. En av de behöriga myndigheterna ska i så fall utses till datasamordnare. Uppgiften som datasamordnare är utöver uppgiften att vara behörig myndighet. En datasamordnare ska för svenskt vidkommande vidta alla åtgärder som enligt dataförordningen tillskrivs datasamordnare.

Begäran om upplysningar och handlingar

4 § Den som omfattas av EU:s dataförordning ska på begäran av en behörig myndighet lämna de upplysningar och handlingar som behövs för att säkerställa att EU:s dataförordning, denna lag och föreskrifter som har meddelats i anslutning till lagen följs.

Paragrafen reglerar den behöriga myndighetens rätt att begära in uppgifter och handlingar. En bestämmelse om att den behöriga myndigheten ska ha befogenhet att begära in nödvändig information finns i artikel 37.14 i dataförordningen. Överväganden finns i avsnitt 4.5.4.

Begäran om information kan riktas mot aktörer som omfattas av dataförordningen och den behöriga myndighetens behörighet. Paragrafens innebörd är att sådana aktörer är skyldiga att på begäran ge in de upplysningar eller handlingar som den myndigheten behöver inom ramen för sin uppgift att säkerställa efterlevnaden av EU:s dataförordning, denna lag och föreskrifter som har meddelats i anslutning till denna lag.

Föreläggande och vite

5 § En behörig myndighet får besluta de förelägganden som behövs för att EU:s dataförordning, denna lag eller föreskrifter som har meddelats i anslutning till lagen ska följas.

Om det finns särskilda skäl får den behöriga myndigheten besluta om förelägganden enligt första stycket för tiden till dess saken slutligt har avgjorts.

En behörig myndighet får förena ett föreläggande enligt första och andra stycket med vite.

Paragrafen innehåller bestämmelser om när den behöriga myndigheten får meddela förelägganden och att sådana förelägganden får förenas med vite. Paragrafen kompletterar artiklarna 37.5 d och 40 i dataförordningen. Övervägandena finns i avsnitt 5.4.

Den behöriga myndigheten får enligt *första stycket* meddela de förelägganden som behövs för att dataförordningen, denna lag eller föreskrifter som har meddelats i anslutning till lagen ska följas. Myndigheten kan besluta om ett föreläggande för att få en aktör att upphöra med ett förfarande som utgör en överträdelse av skyldighet enligt dataförordning eller för att få aktören att ändra sitt förfarande på ett visst sätt. Myndigheten kan också förelägga aktörer att komma in med uppgifter eller handlingar som behövs för att kontrollera efterlevnaden av dataförordningen, denna lag eller föreskrifter som meddelas i anslutning till lagen.

Av *andra stycket* följer att den behöriga myndigheten får besluta om förelägganden för tiden till dess saken slutligt har avgjorts, dvs. interimistiskt. Möjligheten är relevant för förelägganden om att upphöra med eller avhjälpa en påstådd överträdelse och t.ex. inte förelägganden om att inkomma med upplysningar eller handlingar (jfr första stycket). I skäl 109 i dataförordningen uttalas att behöriga myndigheter när det är lämpligt bör använda sig av interimistiska åtgärder för att begränsa effekterna av en påstådd överträdelse medan utredningen av överträdelsen pågår. Det bör krävas särskilda starka skäl för ett interimistiskt beslut. Normalt bör det handla om att ett agerande som tydligt står i strid med dataförordningen och som riskerar att leda till väsentliga och oåterkalleliga skador för en enskild eller det allmänna. Detta innebär att myndigheten ska fatta ett slutligt beslut som ersätter det interimistiska när utredningen är slutförd.

Enligt *tredje stycket* får den behöriga myndigheten förena förelägganden med vite. Allmänna bestämmelser om vite finns i lagen (1985:206) om viten. Vitesförelägganden enligt denna lag kan inte riktas mot statliga myndigheter.

Sanktionsavgift och anmärkning

6 § En behörig myndighet ska besluta att ta ut en sanktionsavgift från följande aktörer vid överträdelse av följande artiklar i EU:s dataförordning, i den ursprungliga lydelsen:

– tillverkare, försäljare, uthyrare, leasegivare eller leverantörer av tillhörande tjänster vid överträdelse av någon av sina skyldigheter enligt artikel 3.1, 3.2 eller 3.3,

– datahållare vid överträdelse av någon av sina skyldigheter enligt artikel 4.1, 4.2, 4.4, 4.5, 4.7, 4.8, 4.13, 4.14, 5.1, 5.4, 5.6, 5.10, 5.11, 8.1, 8.3, 8.4, 9.7 eller 18.1,

– användare vid överträdelse av någon av sina skyldigheter enligt artikel 4.7, 4.10 eller 4.11,

– tredje parter vid överträdelse av någon av sina skyldigheter enligt artikel 5.5, 6.1, 6.2, 11.2 eller 19.2,

– datamottagare vid överträdelse av någon av sina skyldigheter enligt artikel 11.2,

– grindvakter vid överträdelse av någon av sina skyldigheter enligt artikel 5.3,

– offentliga organ vid överträdelse av någon av sina skyldigheter enligt artikel 19,

– leverantörer av databehandlingstjänster vid överträdelse av någon av sina skyldigheter enligt artikel 25.1, 25.2, 25.3, 26, 28, 29.1–6, 32.1, 32.3, 32.4 eller 32.5,

– säljare av en applikation som använder smarta kontrakt eller, i avsaknad av en sådan, den person vars närings- eller yrkesverksamhet inbegriper användning av smarta kontrakt för andra inom ramen för genomförandet av ett avtal eller en del av det om att tillgängliggöra data vid överträdelse av någon av sina skyldigheter enligt artikel 36.1 eller 36.2, eller

– enheter som gör uppkopplade produkter tillgängliga eller erbjuder tillhörande tjänster som inte utser rättslig företrädare enligt artikel 37.12.

Paragrafen reglerar när den behöriga myndigheten ska besluta att ta ut en sanktionsavgift vid överträdelser av dataförordningen. Bestämmelsen kompletterar artiklarna 37.5 d och 40 i dataförordningen. Övervägandena finns i avsnitt 5.5.1 och 5.6.

I paragrafen anges de bestämmelser i dataförordningen som vid överträdelse kan läggas till grund för ett beslut om sanktionsavgift för olika typer av aktörer såsom de benämns i dataförordningen. Hänvisningen görs till dataförordningens ursprungliga lydelse, dvs. hänvisningen är statisk.

När det gäller valet av sanktion framgår av paragrafen att utgångspunkten är att en sanktionsavgift ska beslutas. I 7 § anges att den behöriga myndigheten, om det kan anses tillräckligt, i stället för sanktionsavgift får meddela en anmärkning (se författningskommentaren

till 7 §). Den behöriga myndigheten kan också avstå från att besluta om en sanktionsavgift om överträdelsen är ringa eller ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften (se författningskommentaren till 8 §). Av artikel 40.3 i dataförordningen följer att den behöriga myndigheten vid åläggande av sanktioner åtminstone ska beakta följande kriterier.

a) Överträdelsens art, allvar, omfattning och varaktighet.

b) Varje åtgärd som den överträdande parten har vidtagit för att begränsa eller avhjälpa den skada som överträdelsen har orsakat.

c) Eventuella tidigare överträdelser som begåtts av den överträdande parten.

d) De ekonomiska fördelar som den överträdande parten har erhållit eller de förluster denna har undvikit genom överträdelsen, i den mån sådana fördelar eller förluster kan fastställas på ett tillförlitligt sätt.

e) Eventuella andra försvårande eller förmildrande omständigheter som är tillämpliga på ärendet.

f) Den överträdande partens årsomsättning i unionen under det föregående räkenskapsåret.

Den behöriga myndigheten bestämmer själv om det är mest ändamålsenligt att ålägga sanktionsavgift, meddela anmärkning (7 §) eller, för pågående överträdelser, utfärda ett föreläggande som kan förenas med vite (5 §).

7 § Om det kan anses tillräckligt får en behörig myndighet vid överträdelser enligt 6 § meddela en anmärkning i stället för att ta ut en sanktionsavgift.

Paragrafen reglerar den behöriga myndighetens möjlighet att meddela en anmärkning i stället för att besluta att ta ut en sanktionsavgift enligt 6 §. Bestämmelsen kompletterar artikel 40 i dataförordningen. Övervägandena finns i avsnitt 5.5.2.

Det kan i vissa fall vara tillräckligt att besluta om anmärkning i stället för att besluta att ta ut en sanktionsavgift. Det kan vara aktuellt t.ex. vid mindre allvarliga överträdelser eller när en konstaterad överträdelse har upphört men det av olika skäl inte anses påkallat att besluta om sanktionsavgift, till exempel om en aktör frivilligt vidtagit rättelse.

Omständigheterna är likartade de som ska föreligga för att en sanktionsavgift ska kunna sättas ner enligt 8 § tredje stycket (se även författningskommentaren till 8 §). Syftet med att ge den behöriga myndigheten möjlighet att meddela anmärkning i stället för sanktionsavgift är bl.a. att minska risken för att myndigheten helt avstår från att ingripa mot en konstaterad överträdelse, på grund av att den inte vill vidta så ingripande åtgärd som en sanktionsavgift innebär.

8 § En sanktionsavgift enligt 6 § ska bestämmas till lägst 5 000 kronor och högst 20 000 000 kronor för juridiska personer och för fysiska personer som bedriver näringsverksamhet.

En sanktionsavgift enligt 6 § ska bestämmas till lägst 1 000 kronor och högst 10 000 kronor för fysiska personer som inte bedriver näringsverksamhet.

En behörig myndighet får avstå från att ta ut en sanktionsavgift helt eller delvis om överträdelsen är ringa eller ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften.

I paragrafen regleras sanktionsavgiftens storlek. Bestämmelsen kompletterar artiklarna 37.5 d och 40 i dataförordningen. Övervägandena finns i avsnitt 5.5.3.

I *första stycket* regleras det lägsta respektive det högsta belopp som en sanktionsavgift enligt 6 § ska uppgå till för juridiska personer och för fysiska personer som bedriver näringsverksamhet. Med de senare avses sådana personer, t.ex. enskilda firmor, som betraktas som företag enligt konkurrensrättens företagsbegrepp. Offentliga myndigheter och organ undantas inte i bestämmelsen. Det är upp till den behöriga myndigheten att bestämma vilket sanktionsbelopp som är proportionellt att besluta i det enskilda fallet. Se övervägandena i 5.5.1 och 5.5.3.

Av *andra stycket* regleras det lägsta respektive det högsta belopp som en sanktionsavgift enligt 6 § ska uppgå till för fysiska personer som inte bedriver näringsverksamhet. Sådana personer är konsumenter. I regel är de användare i dataförordningens mening. Möjligheten att besluta om sanktionsavgifter för konsumenter bör tillämpas restriktivt.

Enligt *tredje stycket* får den behöriga myndigheten avstå från att ta ut sanktionsavgiften helt eller delvis om överträdelsen är ringa eller ursäktlig eller om det skulle vara oskäligt att ta ut avgiften. Bestämmelsen tydliggör att 6 § om att sanktionsavgift ska tas ut inte är ovillkorlig. En omständighet som kan ha betydelse för bedömningen kan

vara att aktören har gjort allt som rimligen kan krävas för att förhindra en uppkommen skada till följd av den aktuella överträdelsen. En sanktionsavgift bör vidare kunna sättas ned helt eller delvis om exempelvis om aktören drabbas av flera sanktionsavgifter vid samma prövningstillfälle och den samlade effekten skulle bli alltför betungande. Det bör dock inte anses oskäligt att ta ut en sanktionsavgift enbart på grund av att överträdelsen exempelvis berott på att aktören inte känt till reglerna eller på grund av dålig ekonomi, tidsbrist eller bristande rutiner. Frågan om en avgift ska sättas ned får avgöras efter en helhetsbedömning utifrån omständigheterna i det enskilda fallet. Möjligheten att sätta ned avgiften är en undantagsbestämmelse och bör tillämpas restriktivt.

9 § En sanktionsavgift får inte tas ut om:

1. överträdelsen omfattas av ett föreläggande som har förenats med vite och överträdelsen ligger till grund för en ansökan om utdömande av vitet, eller
2. den som avgiften ska tas ut av inte har fått tillfälle att yttra sig inom två år från den dag då överträdelsen ägde rum.

Paragrafen reglerar när en sanktionsavgift inte får beslutas. Övervägandena finns i avsnitt 5.5.6.

Av *första stycket* framgår att en sanktionsavgift inte får beslutas om överträdelsen omfattas av ett föreläggande som har förenats med vite och överträdelsen ligger till grund för en ansökan om utdömande av vitet. Syftet är att förhindra dubbelprövning i strid mot Europakonventionen och EU:s stadga om de grundläggande rättigheterna.

Av *andra stycket* framgår att en sanktionsavgift får beslutas endast om den som avgiften ska tas ut av har fått tillfälle att yttra sig inom två år från den dag då överträdelsen ägde rum. För att någon ska anses ha fått tillfälle att yttra sig måste denne enligt 25 § förvaltningslagen (2017:900) ha underrättats om allt material av betydelse för beslutet och fått tillfälle att inom en bestämd tid yttra sig över materialet. Bevisbördan för att detta har skett ligger på den behöriga myndigheten. Tidsfristen räknas från när överträdelsen, dvs. den otillåtna eller felaktiga handlingen, ägde rum. När det gäller pågående överträdelser börjar preskriptionstiden löpa först när överträdelsen har upphört. Syftet med att ge den avgiftsskyldige tillfälle att yttra sig är att ge denne möjlighet att påtala eventuella felaktigheter och omstän-

digheter i utredningsmaterialet som kan utgöra skäl för befrielse från avgift innan beslut fattas.

10 § Ett beslut om sanktionsavgift ska delges.

I paragrafen regleras delgivning av beslut om sanktionsavgift. Övervägandena finns i avsnitt 5.5.7.

Av paragrafen framgår att beslut om sanktionsavgift ska delges. Beslutet ska delges den som i beslutet åläggs att betala sanktionsavgift. Bestämmelser om delgivning finns i delgivningslagen (2010:192).

11 § En sanktionsavgift ska betalas till den behöriga myndighet som har beslutat om avgiften, eller till den myndighet som den behöriga myndigheten anger, inom 30 dagar från det att beslutet om att ta ut avgiften fick laga kraft eller inom den längre tid som anges i beslutet.

Om sanktionsavgiften inte betalas inom den tid som anges i första stycket, ska myndigheten lämna den obetalda avgiften för indrivning. Bestämmelser om indrivning finns i lagen (1993:891) om indrivning av statliga fordringar m.m.

En sanktionsavgift tillfaller staten.

Paragrafen innehåller bestämmelser om betalningen av en sanktionsavgift. Övervägandena finns i avsnitt 5.5.7.

I *första stycket* anges att en sanktionsavgift ska betalas till den behöriga myndighet som har beslutat om avgiften eller till den myndighet som den behöriga myndigheten anger. Detta lämnar utrymme för en behörig myndighet att överlåta åt exempelvis Kammarkollegiet att ta emot betalning. Bestämmelsen ger vidare myndigheten möjlighet att fatta beslut om längre tid för betalning än 30 dagar.

Av *andra stycket* framgår att om sanktionsavgiften inte betalas inom den angivna tiden, är den myndighet som skulle ta emot avgiften skyldig att lämna den obetalda avgiften för indrivning enligt lagen (1993:891) om indrivning av statliga fordringar m.m. En sanktionsavgift som inte har betalats i tid får verkställas enligt utsökningsbalken (se 3 kap. 1 § 6 a utsökningsbalken). Det innebär att den kan drivas in utan att det krävs något domstolsavgörande.

Enligt *tredje stycket* tillfaller en sanktionsavgift staten.

Certifiering av tvistlösningsorgan

12 § Ett tvistlösningsorgan som är etablerat i Sverige får ansöka om att bli certifierat enligt EU:s dataförordning.

I paragrafen regleras möjligheten för tvistlösningsorgan att bli certifierade enligt dataförordningen. Övervägandena finns i avsnitt 6.3.1.

Av paragrafen framgår att certifiering kan ske efter ansökan av ett tvistlösningsorgan. Enligt artikel 10.5 i dataförordningen ska den medlemsstat där tvistlösningsorganet är etablerat på begäran av det organet certifiera organet. Begäran att bli certifierad sker enligt paragrafen genom ansökan.

13 § Den myndighet regeringen bestämmer ska pröva ansökningar som avses i 12 § (certifierande myndighet).

I paragrafen regleras att en certifierande myndighet ska pröva ansökningar om certifiering. Övervägandena finns i avsnitt 6.3.1.

Av paragrafen framgår att regeringen bestämmer vilken myndighet i Sverige som ska pröva ansökningar från tvistlösningsorgan, genom hänvisning till 12 §. Bestämmelsen är formulerad så att regeringen endast kan utse en myndighet som certifierande myndighet.

14 § Ett tvistlösningsorgan som uppfyller villkoren i artikel 10.5 i EU:s dataförordning ska certifieras av den certifierande myndigheten.

Certifieringen enligt första stycket ska återkallas av den certifierande myndigheten om tvistlösningsorganet inte längre uppfyller villkoren i artikel 10.5 i EU:s dataförordning.

I paragrafen regleras förutsättningarna för certifiering som tvistlösningsorgan. Övervägandena finns i avsnitt 6.3.1 och 6.3.5.

Enligt *första stycket* ska villkoren för certifiering som anges i artikel 10.5 i dataförordningen vara uppfyllda för att certifiering ska ske. Av artikel 10.5 framgår att samtliga villkor som anges ska vara uppfyllda. Ett beslut om certifiering fattas av den certifierande myndigheten.

Av *andra stycket* framgår att en certifiering ska återkallas av den certifierande myndigheten om tvistlösningsorganet inte längre uppfyller villkoren i artikel 10.5 i dataförordningen. Av skäl 52 i förordningen framgår att förordningen enbart fastställer villkoren för att bli certifierad och att det står medlemsstaterna fritt att anta särskilda

regler för certifieringsförfarandet, bl.a. för certifieringens upphörande eller återkallande.

15 § Den certifierande myndigheten får ta ut avgift för att pröva en ansökan om certifiering.

Paragrafen reglerar avgift för ansökan om certifiering. Övervägandena finns i avsnitt 6.3.4.

Paragrafen avser avgift för att pröva en ansökan om certifiering från ett tvistlösningsorgan. Andra kostnader som uppstår hos den certifierande myndigheten med anledning av certifiering av tvistlösningsorgan omfattas inte.

16 § Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om den avgift som avses i 15 §.

Paragrafen reglerar delegering av avgiftsuttag. Övervägandena finns i avsnitt 6.3.4.

I paragrafen bemyndigas regeringen eller den myndighet som regeringen bestämmer att meddela föreskrifter om avgifterna. Sådana föreskrifter ska avse prövning av ansökan om certifiering.

Underrättelse till den som har lämnat in ett klagomål

17 § I förhållande till den som har lämnat in ett klagomål till en behörig myndighet ska 33 § förvaltningslagen (2017:900) gälla.

Paragrafen reglerar att 33 § förvaltningslagen ska gälla i förhållande till den som har gett in ett klagomål enligt dataförordningen. Övervägandena finns i avsnitt 4.10.3. Bestämmelsen kompletterar artiklarna 38.2 och 39.2 i dataförordningen.

Enligt artikel 38.2 ska den som har gett in ett klagomål underrättas om de beslut som har fattats och enligt artikel 39.2 ska den ha tillgång till effektivt rättsmedel om den behöriga myndigheten underlåter att vidta åtgärder.

Enligt 33 § förvaltningslagen är myndigheter som meddelar ett beslut i ett ärende skyldiga att underrätta den som är part om beslutet och, om parten får överklaga beslutet, hur ett överklagande går till. Den som har gett in ett klagomål enligt dataförordningen har enligt 18 § denna lag rätt att överklaga ett beslut av den behörig myn-

digheten att inte vidta åtgärder med avseende på klagomålet. Syftet med bestämmelsen i 17 § denna lag är att säkerställa att den som har gett in ett klagomål har förutsättningar att tillgodogöra sig möjligheten att överklaga ett beslut om att inte vidta åtgärder.

Överklagande

18 § En behörig myndighets beslut enligt EU:s dataförordning och denna lag får överklagas till allmän förvaltningsdomstol.

En myndighet får överklaga en behörig myndighets beslut.

Den som har lämnat in ett klagomål får överklaga en behörig myndighets beslut att inte vidta åtgärder med avseende på klagomålet. Prövningstillstånd krävs vid överklagande till kammarrätten.

Paragrafen reglerar rätten att överklaga en behörig myndighets beslut enligt dataförordningen och denna lag. Bestämmelsen kompletterar artikel 39 i dataförordningen. Övervägandena finns i avsnitt 4.9.3 och 4.9.4.

Enligt *första stycket* får en behörig myndighets beslut enligt dataförordningen eller denna lag överklagas. Överklagande sker till förvaltningsrätt, vilket också gäller för andra och tredje stycket i paragrafen.

I *andra stycket* föreskrivs att en myndighet får överklaga en behörig myndighets beslut.

I *tredje stycket* anges att den som har gett in ett klagomål har rätt att överklaga en behörig myndighets beslut att inte vidta åtgärder med avseende på klagomålet. Om det saknas bestämmelser i specialförfattning om möjligheten att överklaga gäller bestämmelserna i förvaltningslagen. En förutsättning för överklagbarhet är att beslutet kan antas påverka någons situation på ett inte obetydligt sätt (41 § förvaltningslagen). Syftet med tredje stycket är dels att tydliggöra att ett beslut om att inte vidta åtgärder får överklagas, dels att rätten att överklaga tillkommer den som har gett in ett klagomål oavsett vilken rättsverkan beslutet bedöms ha.

Enligt *fjärde stycket* krävs prövningstillstånd hos kammarrätten. Kravet på prövningstillstånd gäller för mål som inleds genom överklagande till förvaltningsrätten. För övriga mål krävs prövningstillstånd vid överklagande till kammarrätten endast om det följer av bestämmelser i andra lagar, exempelvis 6 § lagen (1985:206) om viten.

19 § Beslut av den certifierande myndigheten att inte certifiera ett tvistlösningsorgan enligt 14 § första stycket eller att återkalla en certifiering enligt 14 § andra stycket får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Paragrafen reglerar rätten att överklaga ett beslut av den certifierande myndigheten. Övervägandena finns i avsnitt 6.3.6.

Enligt *första stycket* får ett beslut av den certifierande myndigheten att inte certifiera ett tvistlösningsorgan, efter prövning av en ansökan om certifiering, överklagas. Även ett beslut av den certifierande myndigheten att återkalla en certifiering av ett tvistlösningsorgan får överklagas. Överklagande sker till förvaltningsrätt.

Enligt *andra stycket* krävs prövningstillstånd vid överklagande av förvaltningsrättens beslut enligt första stycket till kammarrätten.

Ikraftträdande

Denna lag träder i kraft den 1 juli 2026.

Bestämmelsen anger när lagen träder i kraft. Övervägandena finns i kapitel 11.

13.2 Förslag till lag om ändring i lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk

5 kap. Vissa upphovsrätten närstående rättigheter

Framställare av kataloger m.m.

49 § Den som har framställt en katalog, en tabell eller ett annat dylikt arbete i vilket ett stort antal uppgifter har sammanställts eller vilket är resultatet av en väsentlig investering har uteslutande rätt att framställa exemplar av arbetet och göra det tillgängligt för allmänheten.

Rätten enligt första stycket gäller till dess femton år har förflutit efter det år då arbetet framställdes. Om arbetet har gjorts tillgängligt för allmänheten inom femton år från framställningen, gäller dock rätten till dess femton år har förflutit efter det år då arbetet först gjordes tillgängligt för allmänheten.

Bestämmelserna i 2 § andra–fjärde styckena, 6–9 §§, 11 § andra stycket, 12 § första, andra och fjärde styckena, 13–16 §§, 16 a § tredje stycket, 16 e–17 c, 17 e, 19–22, 25–26 b och 26 e §§, 26 g § femte och sjätte styckena samt i 42 a–42 k §§ ska tillämpas på arbeten som avses i denna paragraf. Är ett så-

dant arbete eller en del av det föremål för upphovsrätt, får upphovsrätten också göras gällande.

Ett avtalsvillkor som utvidgar framställarens rätt enligt första stycket till ett offentliggjort arbete är ogiltigt,

Av artikel 43 i Europaparlamentets och rådets förordning (EU) 2023/2854 av den 13 december 2023 om harmoniserade regler för skälig åtkomst till och användning av data och om ändring av förordning (EU) 2017/2394 och direktiv (EU) 2020/1828 (dataförordningen), framgår att rätten av sitt eget slag enligt artikel 7 i direktiv 96/9/EG inte ska tillämpas när data erhålls från eller genereras av en uppkopplad produkt eller en tillhörande tjänst som omfattas av förordningen, särskilt med avseende på artiklarna 4 och 5 i förordningen.

Stycket är nytt och anger upplysningsvis att rätten av sitt eget slag enligt artikel 7 i direktiv 96/9/EG inte ska tillämpas när data erhålls från eller genereras av en uppkopplad produkt eller en tillhörande tjänst som omfattas av dataförordningen, särskilt med avseende på artiklarna 4 och 5 i förordningen. Övervägandena finns i avsnitt 10.3.1.

Paragrafen är en upplysningsbestämmelse där innehållet i artikel 43 i dataförordningen återges. Av skäl 112 i dataförordningen framgår att klargörandet i artikel 43 inte påverkar den eventuella tillämpningen av rätten av sitt eget slag enligt artikel 7 i direktiv 96/9/EG på databaser som innehåller data som inte omfattas av förordningen, förutsatt att kraven om skydd enligt punkt 1 i artikel 7 i direktivet är uppfyllda.

Ikraftträdande

Denna lag träder i kraft den 1 juli 2026.

Bestämmelsen anger när lagen träder i kraft. Övervägandena finns i kapitel 11.

Kommittédirektiv 2024:97

Kompletterande bestämmelser till EU:s dataförordning

Beslut vid regeringssammanträde den 17 oktober 2024

Sammanfattning

En särskild utredare ska föreslå kompletterande bestämmelser till Europaparlamentets och rådets förordning (EU) 2023/2854 av den 13 december 2023 om harmoniserade regler för skälig åtkomst till och användning av data och om ändring av förordning (EU) 2017/2394 och direktiv (EU) 2020/1828 (dataförordningen), i fortsättningen kallad EU:s dataförordning, och lämna förslag på övriga åtgärder.

Utredaren ska dessutom bl.a.

- föreslå de författningsändringar och andra åtgärder som behövs för att berörda myndigheter ska kunna utöva sina befogenheter och vidta de åtgärder som krävs enligt EU:s dataförordning,
- analysera vilka sanktionsbestämmelser som behövs för att uppfylla kravet på sanktioner vid överträdelser av förordningen och lämna nödvändiga författningsförslag,
- analysera befintliga möjligheter till tvistlösning genom tvistlösningsorgan och lämna förslag på nödvändiga åtgärder för att uppfylla förordningens krav i fråga om denna typ av tvistlösning,
- föreslå åtgärder för att säkerställa att offentliga organ kan ta emot data under exceptionella omständigheter, och
- lämna de författningsförslag i övrigt som är nödvändiga för att uppfylla kraven i förordningen.

Uppdraget ska redovisas senast den 15 oktober 2025.

EU-förordningen

Syftet med EU:s dataförordning är att skapa ett enhetligt och rättvist regelverk inom EU för att underlätta och reglera tillgången till och användningen av data. Genom att underlätta delning och användning av data mellan företag, offentliga organ, såsom myndigheter, kommuner och regioner, och individer syftar EU:s dataförordning till att stimulera innovation, öka företagens konkurrenskraft och driva ekonomisk tillväxt inom EU. Den ska säkerställa rättvisa och transparenta villkor för dataåtkomst och dataanvändning, förhindra oskäliga avtalsvillkor och ge tydliga riktlinjer för datadelning. Genom förordningen får offentliga organ dessutom möjlighet att vid exceptionella behov begära ut data från företag och organisationer. Förordningen underlättar också byte av databehandlingstjänster och främjar interoperabilitet mellan olika datasystem. Vidare stärker förordningen skyddet av individens grundläggande rättigheter, inklusive skyddet av personuppgifter och integritet. Den förhindrar också olaglig åtkomst till data av utländska myndigheter.

Uppdraget

Befogenheter för behörig myndighet och andra berörda myndigheter

För att säkerställa efterlevnaden av förordningen ska medlemsstaterna utse en eller flera behöriga myndigheter och, om flera myndigheter utses, en datasamordnare. Regeringen avser att i närtid ge en myndighet i uppdrag att fullgöra uppgiften som behörig myndighet enligt EU:s dataförordning.

Medlemsstaterna ska vidare säkerställa att uppgifterna och befogenheterna för de behöriga myndigheterna är tydligt definierade. Enligt förordningen omfattar uppgifterna och befogenheterna bl.a. att hantera klagomål, utföra undersökningar om tillämpningen av förordningen, ålägga sanktioner samt övervaka den tekniska och kommersiella utveckling som är relevant för tillgängliggörande och användning av data.

Utredaren ska därför

- analysera behovet av nödvändiga organisatoriska och resursmässiga förstärkningar för den behöriga myndigheten,

- överväga och ta ställning till om andra myndigheter behöver tilläggsuppdrag eller instruktionsändringar, och
- föreslå de författningsändringar och andra åtgärder som behövs för att de berörda myndigheterna ska kunna utöva sina befogenheter och vidta de åtgärder som krävs enligt förordningen.

Sanktionsbestämmelser

Förordningen föreskriver en skyldighet för medlemsstaterna att fastställa regler om sanktioner för överträdelse av bestämmelserna i förordningen.

Utredaren ska därför

- analysera vilka sanktioner som behövs för att uppfylla kravet på sanktioner vid överträdelse av förordningen, och
- lämna nödvändiga författningsförslag.

Tvistlösning

Förordningen innehåller bestämmelser som ger användare, datahållare och datamottagare tillgång till ett tvistlösningsorgan för att lösa vissa tvister. Parterna kan fritt välja ett tvistlösningsorgan, oavsett om det är i eller utanför de medlemsstater där de är etablerade. Tvistlösningsorganet ska på begäran certifieras av den medlemsstat där organet är etablerat. Förordningens bestämmelser ställer dock inte krav på medlemsstaterna att inrätta nya tvistlösningsorgan.

Utredaren ska därför

- analysera befintliga möjligheter till tvistlösning genom tvistlösningsorgan och lämna förslag på nödvändiga åtgärder för att uppfylla förordningens krav i fråga om denna typ av tvistlösning.

Åtgärder för att säkerställa att offentliga organ kan ta emot data vid exceptionella behov

EU:s dataförordning innehåller en skyldighet för datahållare att under vissa förutsättningar göra data tillgängliga för offentliga organ och unionsorgan om det föreligger exceptionella behov, såsom allmänna nödlägen. Det finns ett behov av att undersöka vilka rättsliga förutsättningar som finns för svenska offentliga organ att hantera data som innehåller känsliga uppgifter, exempelvis företagshemligheter. Dessutom finns det ett behov av att utreda vilka organisatoriska, tekniska och infrastrukturella resurser som offentliga organ måste ha för att kunna ta emot, lagra och analysera stora mängder data, exempelvis dataströmmar från sensorer, på ett säkert och effektivt sätt under exceptionella omständigheter.

Vidare bör behovet av kompetenshöjande insatser för personal hos de offentliga organen analyseras. Det bör finnas kunskap och beredskap för att hantera data på ett snabbt, professionellt och rättssäkert sätt. Slutligen bör det utredas vilka metoder som kan förbättra samverkan mellan offentliga och privata aktörer, inklusive utveckling av standardiserade processer och kommunikationskanaler, för att möjliggöra smidig och säker dataöverföring i kritiska situationer.

Utredaren ska därför

- identifiera och föreslå vilka tekniska resurser, organisatoriska förmågor och digitala infrastrukturer som svenska offentliga organ behöver för att effektivt kunna ta emot, hantera, bearbeta och dela data som erhålls från företag vid exceptionella omständigheter,
- föreslå vilka åtgärder som bör vidtas för att säkerställa att det hos de offentliga organen finns nödvändig kunskap för att ta emot, hantera, bearbeta och dela data från företag vid exceptionella omständigheter,
- föreslå hur effektiva samarbets- och kommunikationskanaler kan etableras och underhållas mellan företag och offentliga organ för att säkerställa snabb och säker datadelning vid exceptionella omständigheter, och
- lämna nödvändiga författningsförslag.

Åtgärder för att underlätta för svenska företag och offentliga organ att följa förordningens bestämmelser

För att svenska företag, organisationer och offentliga organ ska kunna följa bestämmelserna i EU:s dataförordning behövs stöd och vägledning. Det kräver en analys av behovet av stödåtgärder och förslag till strategier för att tillhandahålla nödvändigt stöd. I detta ingår att analysera behov av tydliga riktlinjer och utbildningsresurser som gör det enklare att förstå regelverket samt föreslå hur sådana bör tas fram. Vid datadelning enligt förordningen kan det uppstå tekniska och organisatoriska utmaningar som behöver identifieras och lösas med fokus på att främja interoperabilitet, standardisering och utveckling av gemensamma plattformar för datadelning. Detta ska bidra till att stärka företagens konkurrenskraft och den offentliga förvaltningens effektivitet samt främja innovation och tillväxt inom den digitala sektorn.

Utredaren ska därför

- identifiera vilka administrativa och rättsliga hinder svenska företag och offentliga organ kan möta vid tillämpningen av EU:s dataförordning, och föreslå åtgärder som bör vidtas för att minimera dessa hinder,
- föreslå hur tekniska och semantiska standarder och interoperabiliteten mellan system kan förbättras för att underlätta för svenska aktörer att uppfylla kraven i förordningen, och
- analysera och föreslå utbildnings- och informationsinsatser som behövs för att öka kunskapen om förordningens krav bland svenska företag och offentliga organ.

Författningsförslag som behövs i övrigt

En analys av EU:s dataförordning kan leda till slutsatsen att befintliga svenska bestämmelser behöver ändras eller att nya bestämmelser behövs med anledning av förordningen. Fysiska och juridiska personer ska bl.a. ha rätt att lämna in klagomål vid överträdelser. Vidare kan bestämmelserna om tillsyn t.ex. aktualisera frågor om sekretess och personuppgiftsbehandling som behöver analyseras inom ramen för utredningen.

Utredaren ska därför

- analysera i vilken utsträckning det är nödvändigt eller lämpligt att ändra eller komplettera svensk rätt i andra avseenden än de som berörs i ovanstående punkter, och
- lämna nödvändiga författningsförslag.

Allmänna utgångspunkter för uppdragets genomförande

En central utgångspunkt i utredningens arbete bör vara att skapa en balans mellan effektiv tillsyn och administration och minimering av den administrativa bördan för företag och myndigheter. Utredaren ska beakta vikten av att underlätta för svenska företag, särskilt små och medelstora företag, att följa de nya reglerna utan att skapa onödiga hinder för innovation och tillväxt. Utredaren ska vid sina överväganden också inkludera perspektiv som rör jämställdhet, skyddet för den personliga integriteten samt dataskydd i enlighet med EU:s dataskyddsförordning. Utredaren bör, när det bedöms som lämpligt och främjar uppdraget, också undersöka hur andra medlemsstater planerar att genomföra förordningen, med beaktande av intresset av ett enhetligt genomförande inom EU.

Konsekvensbeskrivningar

Utredaren ska i enlighet med kommittéförordningen (1998:1474) och förordningen (2024:183) om konsekvensutredningar bedöma och beskriva förslagens ekonomiska och samhällsekonomiska konsekvenser, samt konsekvenser i övrigt för enskilda, företag och det allmänna. Utredaren ska bl.a. beskriva och beräkna eventuella offentligfinansiella konsekvenser, däribland eventuella konsekvenser för berörda myndigheter. Utredaren ska beräkna hur statens inkomster och utgifter påverkas. Om förslag som lämnas medför offentligfinansiella kostnader, ska förslag till finansiering lämnas. Utredaren ska även redovisa förslagens konsekvenser ur ett jämställdhetsperspektiv och för den personliga integriteten.

Kontakter och redovisning av uppdraget

Utredaren ska hålla sig informerad om relevant arbete inom Regeringskansliet, EU och andra utredningar. Samråd ska ske med berörda myndigheter, näringslivsrepresentanter och andra relevanta aktörer, däribland Implementeringsrådet. I den del av uppdraget som avser åtgärder för att säkerställa att offentliga organ kan ta emot data vid exceptionella behov bör utredaren samråda med Underrättelseutredningen (Fö 2023:04).

Uppdraget ska redovisas senast den 15 oktober 2025.

(Finansdepartementet)

Kommittédirektiv 2025:46

Kommittédirektiv

Tilläggsdirektiv till Utredningen om kompletterande bestämmelser till EU:s dataförordning (Fi 2024:06)

Beslut vid regeringssammanträde den 30 april 2025.

Förlängd tid för uppdraget

Regeringen beslutade den 17 oktober 2024 kommittédirektiv om kompletterande bestämmelser till EU:s dataförordning (dir. 2024:97). Uppdraget skulle enligt direktiven redovisas senast den 15 oktober 2025.

Utredningstiden förlängs. Uppdraget ska i stället redovisas senast den 22 december 2025.

(Finansdepartementet)

Europeiska unionens officiella tidning

SV
L-serien

2023/2854

22.12.2023

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2023/2854

av den 13 december 2023

om harmoniserade regler för skälig åtkomst till och användning av data och om ändring av förordning (EU) 2017/2394 och direktiv (EU) 2020/1828 (dataförordningen)

(Text av betydelse för EES)

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 114,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Europeiska centralbankens yttrande ([1]),

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande ([2]),

med beaktande av Regionkommitténs yttrande ([3]),

i enlighet med det ordinarie lagstiftningsförfarandet ([4]), och

av följande skäl:

(1) På senare år har datadriven teknik haft omdanande effekter på alla ekonomiska sektorer. Det ökade antalet produkter som är uppkopplade till internet har särskilt ökat volymen och det potentiella värdet av data för konsumenter, företag och samhälle. Högkvalitativa och interoperabla data från olika områden stärker konkurrenskraften och innovationen och säkerställer en hållbar ekonomisk tillväxt. Samma data kan användas och vidareutnyttjas för en mängd olika syften och i obegränsad omfattning, utan att dess kvalitet eller kvantitet sjunker.

(2) Hinder för datadelning står i vägen för en optimal fördelning av data som gagnar samhället. Några exempel på sådana hinder är bristande incitament för datahållare att frivilligt ingå datadelningsavtal, osäkerhet om rättigheter och skyldigheter när det gäller data, kostnader för kontrakt och genomförande när det gäller tekniska gränssnitt, en höggradigt fragmenterad information i stuprör, undermålig hantering av metadata, avsaknad av standarder för semantisk och teknisk interoperabilitet, flaskhalsar som hindrar dataåtkomst, brist på gemensam datadelningspraxis och missbruk av kontraktsmässiga obalanser när det gäller åtkomst till data och dataanvändning.

(3) Inom sektorer som kännetecknas av förekomsten av mikroföretag och små företag och medelstora företag enligt definitionen i artikel 2.1 i bilagan till kommissionens rekommendation 2003/361/EG ([5]), finns det ofta en brist på digital kapacitet och färdigheter för att samla in, analysera och använda data, och åtkomsten begränsas ofta när det är en aktör som innehar data i systemet eller när interoperabiliteten är bristfällig mellan data, mellan datatjänster eller över gränser.

(4) För att tillgodose den digitala ekonomins behov och undanröja hinder för en väl fungerande inre marknad för data är det nödvändigt att fastställa en harmoniserad ram som specificerar vem som har rätt att använda produktdata eller data från tillhörande tjänster samt villkoren och grunden för detta. Därför bör medlemsstaterna inte anta eller

([1]) EUT C 402, 19.10.2022, s. 5.
([2]) EUT C 365, 23.9.2022, s. 18.
([3]) EUT C 375, 30.9.2022, s. 112.
([4]) Europaparlamentets ståndpunkt av den 9 november 2023 (ännu inte offentliggjord i EUT) och rådets beslut av den 27 november 2023.
([5]) Kommissionens rekommendation 2003/361/EG av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag (EUT L 124, 20.5.2003, s. 36).

upprätthålla ytterligare nationella krav när det gäller frågor som omfattas av denna förordning, om det inte uttryckligen föreskrivs, eftersom detta skulle inverka på dess direkta och enhetliga tillämpning. Dessutom bör åtgärder på unionsnivå inte påverka tillämpningen av skyldigheter och åtaganden enligt internationella handelsavtal som ingås av unionen.

(5) Denna förordning säkerställer att användare av en uppkopplad produkt eller tillhörande tjänst i unionen i rätt tid kan få åtkomst till de data som genereras genom användning av denna uppkopplade produkt eller tillhörande tjänst och att dessa användare kan använda dessa data, även genom att dela dem med tredje parter efter eget val. Genom denna förordning införs en skyldighet för datahållare att göra data tillgängliga för användare och tredje parter som väljs av användaren under vissa omständigheter. Denna förordning säkerställer också att datahållare gör data tillgängliga för datamottagare i unionen på rättvisa, rimliga och icke-diskriminerande villkor och på ett transparent sätt. Privaträttsliga bestämmelser är grundläggande i den allmänna ramen för datadelning. Därför anpassar denna förordning avtalsrättsliga bestämmelser och förhindrar att kontraktsmässiga obalanser som hindrar skälig åtkomst till och användning av data utnyttjas. Denna förordning säkerställer också att datahållare, om ett exceptionellt behov uppstår, ger offentliga organ, kommissionen, Europeiska centralbanken eller unionsorgan åtkomst till de data som är nödvändiga för utförandet av en specifik uppgift av allmänt intresse. Denna förordning syftar också till att underlätta byten av databehandlingstjänster och att förbättra interoperabiliteten för data och för datadelningsmekanismer och datadelningstjänster i unionen. Denna förordning bör inte tolkas som att den erkänner eller medför någon ny rättighet för datahållare att använda de data som genereras genom användning av en uppkopplad produkt eller tillhörande tjänst.

(6) Datagenerering är resultatet av åtgärder från minst två aktörer, särskilt en uppkopplad produkts designer eller tillverkare, som i många fall också kan vara en leverantör av tillhörande tjänster, samt användaren av den uppkopplade produkten eller tillhörande tjänsten. Den ger upphov till frågor som rör rättvisa i den digitala ekonomin, eftersom de data som registreras av uppkopplade produkter eller tillhörande tjänster utgör ett viktigt underlag för eftermarknadstjänster, stödtjänster och andra tjänster. För att förverkliga de stora ekonomiska fördelarna med data, bland annat genom datadelning som bygger på frivilliga avtal och unionsföretagens utveckling av datadrivet värdeskapande, är en allmän metod för tilldelning av rättigheter avseende åtkomst till och användning av data att föredra framför tilldelning av exklusiva rättigheter avseende åtkomst och användning. I denna förordning föreskrivs horisontella regler som skulle kunna följas av unionsrätt eller nationell rätt som beaktar särskilda omständigheter inom de berörda sektorerna.

(7) Den grundläggande rättigheten till skydd av personuppgifter skyddas i synnerhet genom Europaparlamentets och rådets förordningar (EU) 2016/679 ([6]) och (EU) 2018/1725 ([7]). Dessutom skyddar Europaparlamentets och rådets direktiv 2002/58/EG ([8]) privatlivet och konfidentialiteten vid kommunikation, bland annat genom att fastställa villkor för all lagring av och åtkomst till personuppgifter och icke-personuppgifter i respektive från terminalutrustning. Dessa unionslagstiftningsakter ger grunden för en hållbar och ansvarsfull databehandling, även i de fall då datamängder innehåller en blandning av personuppgifter och icke-personuppgifter. Den här förordningen kompletterar, utan att påverka tillämpningen av, unionsrätt om skyddet av personuppgifter och integritet, i synnerhet förordningarna (EU) 2016/679 och (EU) 2018/1725 och direktiv 2002/58/EG. Ingen bestämmelse i den här förordningen bör tillämpas eller tolkas så att den minskar eller begränsar rätten till skydd av personuppgifter eller rätten till integritet eller konfidentialitet vid kommunikation. All behandling av personuppgifter enligt den här förordningen bör vara förenlig med unionens dataskyddslagstiftning, inbegripet kravet på en giltig rättslig grund för behandling enligt artikel 6 i förordning (EU) 2016/679 och, i tillämpliga fall, villkoren i artikel 9 i den förordningen

([6]) Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1).

([7]) Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (EUT L 295, 21.11.2018, s. 39).

([8]) Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation) (EGT L 201, 31.7.2002, s. 37).

och i artikel 5.3 i direktiv 2002/58/EG. Den här förordningen utgör inte någon rättslig grund för datahållarens insamling eller behandling av personuppgifter. Den här förordningen ålägger datahållare en skyldighet att göra personuppgifter tillgängliga för användare eller för tredje parter som väljs av en användare på den användarens begäran. Sådan åtkomst bör ges till personuppgifter som behandlas av datahållaren på grundval av någon av de rättsliga grunder som anges i artikel 6 i förordning (EU) 2016/679. Om användaren inte är den registrerade skapar den här förordningen inte någon rättslig grund för att tillhandahålla åtkomst till personuppgifter eller för att göra personuppgifter tillgängliga för en tredje part, och den bör inte tolkas som att den medför någon ny rättighet för datahållaren att använda personuppgifter som genereras genom användning av en uppkopplad produkt eller tillhörande tjänst. I dessa fall kan det ligga i användarens intresse att underlätta uppfyllandet av kraven i artikel 6 i förordning (EU) 2016/679. Eftersom den här förordningen inte bör påverka registrerades dataskyddsrättigheter på ett ogynnsamt sätt, kan datahållaren i dessa fall tillmötesgå en begäran bland annat genom att anonymisera personuppgifter eller, om lätt åtkomliga data innehåller personuppgifter angående flera registrerade, överföra endast personuppgifter som rör användaren.

(8) Principerna om dataminimering, inbyggt dataskydd och dataskydd som standard är viktiga när behandlingen medför betydande risker för individers grundläggande rättigheter. Med beaktande av den aktuella tekniska nivån bör alla parter som deltar i datadelning, inbegripet datadelning som omfattas av denna förordning, genomföra tekniska och organisatoriska åtgärder för att skydda dessa rättigheter. Sådana åtgärder innefattar inte bara pseudonymisering och kryptering, utan även användningen av alltmer tillgänglig teknik som tillåter att algoritmer kombineras med data och ger möjlighet till värdefull inblick utan överföring mellan parterna eller onödig kopiering av rådata eller strukturerade data.

(9) Denna förordning påverkar inte nationell avtalsrätt, inbegripet regler om avtals ingående, giltighet eller verkan, eller konsekvenserna av hävning av ett avtal, såvida inte annat föreskrivs i denna förordning. Denna förordning kompletterar, och påverkar inte tillämpningen av, unionsrätt som syftar till att främja konsumenters intressen och säkerställa en hög nivå av konsumentskydd samt att skydda deras hälsa, säkerhet och ekonomiska intressen, i synnerhet rådets direktiv 93/13/EEG ([9]) och Europaparlamentets och rådets direktiv 2005/29/EG ([10]) och 2011/83/EU ([11]).

(10) Denna förordning påverkar inte tillämpningen av unionsrättsakter och nationella rättsakter med föreskrifter om delning av, åtkomst till och användning av data i syfte att förebygga, förhindra, utreda, upptäcka eller lagföra brott eller verkställa straffrättsliga påföljder, eller för tull- och skatteändamål, oavsett på grundval av vilken rättslig grund enligt fördraget om Europeiska unionens funktionssätt (EUF-fördraget) som sådana unionsrättsakter antogs, samt internationellt samarbete på det området, i synnerhet på grundval av Europarådets konvention om it-relaterad brottslighet (ETS nr 185), utfärdad i Budapest den 23 november 2001. Sådana rättsakter omfattar Europaparlamentets och rådets förordningar (EU) 2021/784 ([12]), (EU) 2022/2065 ([13]) och (EU) 2023/1543 ([14]) och Europapar-

([9]) Rådets direktiv 93/13/EEG av den 5 april 1993 om oskäliga villkor i konsumentavtal (EGT L 95, 21.4.1993, s. 29).

([10]) Europaparlamentets och rådets direktiv 2005/29/EG av den 11 maj 2005 om otillbörliga affärsmetoder som tillämpas av näringsidkare gentemot konsumenter på den inre marknaden och om ändring av rådets direktiv 84/450/EEG och Europaparlamentets och rådets direktiv 97/7/EG, 98/27/EG och 2002/65/EG samt Europaparlamentets och rådets förordning (EG) nr 2006/2004 (direktiv om otillbörliga affärsmetoder) (EUT L 149, 11.6.2005, s. 22).

([11]) Europaparlamentets och rådets direktiv 2011/83/EU av den 25 oktober 2011 om konsumenträttigheter och om ändring av rådets direktiv 93/13/EEG och Europaparlamentets och rådets direktiv 1999/44/EG och om upphävande av rådets direktiv 85/577/EEG och Europaparlamentets och rådets direktiv 97/7/EG (EUT L 304, 22.11.2011, s. 64).

([12]) Europaparlamentets och rådets förordning (EU) 2021/784 av den 29 april 2021 om åtgärder mot spridning av terrorisminnehåll online (EUT L 172, 17.5.2021, s. 79).

([13]) Europaparlamentets och rådets förordning (EU) 2022/2065 av den 19 oktober 2022 om en inre marknad för digitala tjänster och om ändring av direktiv 2000/31/EG (förordningen om digitala tjänster) (EUT L 277, 27.10.2022, s. 1).

([14]) Europaparlamentets och rådets förordning (EU) 2023/1543 av den 12 juli 2023 om europeiska utlämnandeorder och europeiska bevarandeorder för elektroniska bevis i straffrättsliga förfaranden och för verkställighet av fängelsestraff eller annan frihetsberövande åtgärd till följd av straffrättsliga förfaranden (EUT L 191, 28.7.2023, s. 118).

lamentets och rådets direktiv (EU) 2023/1544 ([15]). Den här förordningen är inte tillämplig på insamling eller utbyte av, åtkomst till eller användning av data enligt Europaparlamentets och rådets förordning (EU) 2015/847 ([16]) och Europaparlamentets och rådets direktiv (EU) 2015/849 ([17]). Den här förordningen är inte tillämplig på områden som inte omfattas av unionsrätten och påverkar under inga omständigheter medlemsstaternas befogenheter i fråga om allmän säkerhet, försvar eller nationell säkerhet, tull- och skatteförvaltning eller medborgares hälsa och säkerhet, oavsett vilken typ av enhet som medlemsstaterna har bemyndigat att utföra uppgifter inom ramen för dessa befogenheter.

(11) Unionsrätt som fastställer den fysiska utformningen av och datakraven för produkter som ska släppas ut på unionsmarknaden bör inte påverkas, såvida det inte uttryckligen föreskrivs i denna förordning.

(12) Denna förordning kompletterar, och påverkar inte tillämpningen av, unionsrätt som syftar till fastställande av tillgänglighetskrav för vissa produkter och tjänster, i synnerhet Europaparlamentets och rådets direktiv (EU) 2019/882 ([18]).

(13) Denna förordning påverkar inte tillämpningen av unionsrättsakter och nationella rättsakter som skyddar immateriella rättigheter, inbegripet Europaparlamentets och rådets direktiv 2001/29/EG ([19]), 2004/48/EG ([20]) och (EU) 2019/790 ([21]).

(14) Uppkopplade produkter som genom sina komponenter eller operativsystem erhåller, genererar eller samlar in data om sin prestanda, användning eller miljö och som kan kommunicera dessa data via en elektronisk kommunikationstjänst, via fysisk åtkomst eller via åtkomst i enheten, ofta benämnt sakernas internet, bör omfattas av denna förordning, med undantag av prototyper. Exempel på sådana elektroniska kommunikationstjänster är framför allt markbaserade telefonnät, kabel-tv-nät, satellitbaserade nät och NFC-nät (*near-field communication networks*). Uppkopplade produkter återfinns i alla aspekter av ekonomin och samhället, inbegripet i privat, civil eller kommersiell infrastruktur, fordon, hälso- och livsstilsprodukter, fartyg, flygplan, hushållsprodukter och konsumentvaror, medicinsk och hälsorelaterad utrustning och maskiner för jordbruk och industri. Tillverkarnas val av utformning och, i förekommande fall, unionsrätt eller nationell rätt som tillgodoser sektorsspecifika behov samt mål eller relevanta beslut från behöriga myndigheter bör avgöra vilka data en uppkopplad produkt kan göra tillgängliga.

(15) Data representerar digitaliseringen av användaråtgärder och användarhändelser och bör därmed vara tillgängliga för användaren. Reglerna för åtkomst till och användning av data från uppkopplade produkter och tillhörande tjänster enligt denna förordning gäller både produktdata och data från en tillhörande tjänst. Med produktdata avses data som genereras genom användning av en uppkopplad produkt och som av tillverkaren har utformats för att kunna hämtas via den uppkopplade produkten av en användare, datahållare eller en tredje part, inbegripet, när så är lämpligt, tillverkaren. Med data från en tillhörande tjänst avses data som också representerar digitaliseringen av användaråtgärder eller användarhändelser som kan härledas från den uppkopplade produkten och som genereras

([15]) Europaparlamentets och rådets direktiv (EU) 2023/1544 av den 12 juli 2023 om fastställande av harmoniserade regler för att utse utsedda verksamhetsställen och rättsliga ombud för insamling av elektroniska bevis i straffrättsliga förfaranden (EUT L 191, 28.7.2023, s. 181).

([16]) Europaparlamentets och rådets förordning (EU) 2015/847 av den 20 maj 2015 om uppgifter som ska åtföljа överföringar av medel och om upphävande av förordning (EG) nr 1781/2006 (EUT L 141, 5.6.2015, s. 1).

([17]) Europaparlamentets och rådets direktiv (EU) 2015/849 av den 20 maj 2015 om åtgärder för att förhindra att det finansiella systemet används för penningtvätt eller finansiering av terrorism, om ändring av Europaparlamentets och rådets förordning (EU) nr 648/2012 och om upphävande av Europaparlamentets och rådets direktiv 2005/60/EG och kommissionens direktiv 2006/70/EG (EUT L 141, 5.6.2015, s. 73).

([18]) Europaparlamentets och rådets direktiv (EU) 2019/882 av den 17 april 2019 om tillgänglighetskrav för produkter och tjänster (EUT L 151, 7.6.2019, s. 70).

([19]) Europaparlamentets och rådets direktiv 2001/29/EG av den 22 maj 2001 om harmonisering av vissa aspekter av upphovsrätt och närstående rättigheter i informationssamhället (EGT L 167, 22.6.2001, s. 10).

([20]) Europaparlamentets och rådets direktiv 2004/48/EG av den 29 april 2004 om säkerställande av skyddet för immateriella rättigheter (EUT L 157, 30.4.2004, s. 45).

([21]) Europaparlamentets och rådets direktiv (EU) 2019/790 av den 17 april 2019 om upphovsrätt och närstående rättigheter på den digitala inre marknaden och om ändring av direktiven 96/9/EG och 2001/29/EG (EUT L 130, 17.5.2019, s. 92).

när leverantören tillhandahåller en tillhörande tjänst. Data som genereras genom användning av en uppkopplad produkt eller tillhörande tjänst bör anses innefatta data som avsiktligt registrerats eller data som indirekt följder av användarens åtgärder, såsom data om den uppkopplade produktens miljö eller interaktion. Detta bör innefatta data om användningen av en uppkopplad produkt som genereras av ett användargränssnitt eller genom en tillhörande tjänst, och bör inte vara begränsat till information om att en sådan användning har ägt rum, utan innefatta alla data som genereras av den uppkopplade produkten till följd av sådan användning, till exempel data som genereras automatiskt av sensorer och data som registreras av inbäddade tillämpningar, inbegripet applikationer som visar maskinvarustatus och funktionsfel. Detta bör även innefatta data som genereras av den uppkopplade produkten eller en tillhörande tjänst när användaren är inaktiv, till exempel när användaren väljer att inte använda den uppkopplade produkten under en viss tid och i stället låter den vara i viloläge eller till och med avstängd, eftersom statusen för en uppkopplad produkt eller dess komponenter, till exempel dess batterier, kan variera när den uppkopplade produkten är i viloläge eller avstängd. Data som inte ändras väsentligt, dvs. data i obearbetad form, även kallade rådata eller primärdata som avser datapunkter som genereras automatiskt utan någon ytterligare form av behandling samt data som har förbehandlats i syfte att göra dem begripliga och användbara för senare behandling och analys, omfattas av denna förordning. Sådana data innefattar data som samlas in från en enda sensor eller en uppkopplad grupp av sensorer i syfte att göra insamlade data begripliga för bredare användningsfall genom att fastställa en fysisk kvantitet eller kvalitet eller en förändring av en fysisk kvantitet, såsom temperatur, tryck, flödeshastighet, ljud, pH-värde, vätskenivå, position, acceleration eller hastighet. Begreppet *förbehandlade data* bör inte tolkas på ett sådant sätt att det införs en skyldighet för datahållaren att göra betydande investeringar i rensning och anpassning av data. De data som ska göras tillgängliga bör innefatta relevanta metadata, bland annat grundläggande information om sammanhang och tidsstämpel, för att göra datan användbar när den kombineras med andra data, såsom data sorterade och klassificerade med andra relaterade datapunkter, eller omformateras till ett allmänt använt format. Sådana data är potentiellt värdefulla för användaren och stöder innovation och utveckling av digitala och andra tjänster för att skydda miljön, människors hälsa och den cirkulära ekonomin, bland annat genom att underlätta underhåll och reparation av de uppkopplade produkterna i fråga. Information som avleds eller härleds från sådana data, som är resultatet av ytterligare investeringar i tilldelning av värden eller insikter från dessa data, särskilt med hjälp av komplexa proprietära algoritmer, inbegripet sådana som utgör en del av proprietär programvara, bör däremot inte anses omfattas av denna förordning och bör följaktligen inte omfattas av skyldigheten för en datahållare att göra dem tillgängliga för en användare eller datamottagare, såvida inte användaren och datahållaren kommit överens om något annat. Sådana data kan i synnerhet innefatta information som härleds från sensorfusion, där data infereras eller härleds från flera sensorer och samlas in i den uppkopplade produkten med hjälp av komplexa proprietära algoritmer och kan vara föremål för immateriella rättigheter.

(16) Denna förordning gör det möjligt för användare av uppkopplade produkter att dra nytta av eftermarknadstjänster, stödtjänster och andra tjänster baserade på data som samlas in av sensorer som är inbyggda i sådana produkter, och insamlingen av dessa data är av potentiellt värde när det gäller att förbättra de uppkopplade produkternas prestanda. Det är viktigt att skilja mellan marknader för tillhandahållande av sådana sensorutrustade uppkopplade produkter och tillhörande tjänster, å ena sidan, och marknader för icke-tillhörande programvara och innehåll såsom text- och ljudinnehåll och audiovisuellt innehåll som ofta omfattas av immateriella rättigheter, å andra sidan. Därför bör denna förordning inte omfatta data som sådana sensorutrustade uppkopplade produkter genererar när användaren spelar in, överför, visar eller spelar innehåll, liksom själva innehållet, som ofta omfattas av immateriella rättigheter, bland annat för användning av en onlinetjänst. Denna förordning bör inte heller omfatta data som erhållits, genererats eller blivit åtkomliga från den uppkopplade produkten eller som överförts till den för lagring eller annan behandling till förmån för andra parter, som inte är användaren, vilket kan vara fallet med servrar eller molninfrastruktur som drivs av sina ägare uteslutande för tredje parts räkning, bland annat för användning av en onlinetjänst.

(17) Det är nödvändigt att fastställa regler för produkter som vid tidpunkten för köp, hyra eller leasing är uppkopplade till en tillhörande tjänst på ett sådant sätt att den uppkopplade produkten inte skulle kunna utföra en eller flera av sina funktioner utan den, eller som tillverkaren eller en tredje part senare kopplar upp till produkten för att utöka eller anpassa den uppkopplade produktens funktionalitet. Sådana tillhörande tjänster inbegriper utbyte av data mellan den uppkopplade produkten och tjänsteleverantören och bör tolkas som att de uttryckligen är kopplade till driften av den uppkopplade produktens funktioner, till exempel tjänster som i tillämpliga fall överför kommandon till den uppkopplade produkten som kan påverka dess åtgärder eller beteende. Tjänster som inte påverkar driften av den uppkopplade produkten och som inte innebär att tjänsteleverantören överför data eller kommandon till den uppkopplade produkten bör inte betraktas som tillhörande tjänster. Sådana tjänster kan till exempel omfatta

stödjande rådgivning, analyser eller finansiella tjänster samt reparation och underhåll som utförs regelbundet. Tillhörande tjänster kan erbjudas som en del av försäljnings-, hyres- eller leasingavtalet. Sådana tillhörande tjänster kan också tillhandahållas för produkter av samma typ, och användarna kan rimligtvis förvänta sig att de ska tillhandahållas med beaktande av den uppkopplade produktens art och eventuella offentliga uttalanden som gjorts av försäljaren, uthyraren eller leasegivaren eller för deras räkning, eller av andra personer i tidigare länkar i transaktionskedjan, inbegripet tillverkaren. Tillhörande tjänster kan i sig generera data av värde för användaren oberoende av datainsamlingskapaciteten i den uppkopplade produkt som de är sammankopplade med. Denna förordning bör också tillämpas på tillhörande tjänster som inte tillhandahålls av försäljaren, uthyraren eller leasegivaren själv, utan som tillhandahålls av tredje part. Om det är osäkert om tjänsten tillhandahålls som en del av försäljnings-, hyres- eller leasingavtalet bör denna förordning tillämpas. Varken strömförsörjning eller tillhandahållande av konnektivitet får tolkas som tillhörande tjänster enligt denna förordning.

(18) Användaren av en uppkopplad produkt bör förstås som en fysisk eller juridisk person, såsom ett företag, en konsument eller ett offentligt organ, som äger en uppkopplad produkt, har fått vissa tillfälliga rättigheter, till exempel genom ett hyres- eller leasingavtal, att få åtkomst till eller använda data som erhålls från den uppkopplade produkten, eller tar emot tillhörande tjänster för den uppkopplade produkten. Dessa åtkomsträttigheter bör, när det gäller personuppgifter som genereras av en uppkopplad produkt eller vid tillhandahållande av en tillhörande tjänst, inte på något sätt ändra eller inkräkta på rättigheterna för registrerade som kan interagera med den uppkopplade produkten eller tillhörande tjänsten. Användaren bär riskerna för och åtnjuter fördelarna av användningen av den uppkopplade produkten och bör även ha åtkomst till de data som produkten genererar. Användaren bör därför ha rätt att utnyttja fördelarna av data som genereras av den berörda uppkopplade produkten och eventuella tillhörande tjänster. En ägare, hyrestagare eller leasetagare bör också betraktas som användare, även när flera enheter kan betraktas som användare. När det rör sig om flera användare kan varje användare bidra på olika sätt till datagenereringen och ha ett intresse av flera olika former av användning, såsom förvaltning av fordonsparker för ett leasingföretag eller mobilitetslösningar för enskilda personer som använder en bildelningstjänst.

(19) Med datakompetens avses färdigheter, kunskap och förståelse som gör det möjligt för användare, konsumenter och företag, särskilt mikroföretag och små och medelstora företag som omfattas av denna förordning, att dels bli medvetna om det potentiella värdet av de data de genererar, producerar och delar, dels bli motiverade att erbjuda och ge åtkomst till sina data i enlighet med relevanta rättsliga regler. Datakompetens bör omfatta mer än kunskaper om verktyg och teknik och syfta till att ge medborgare och företag förmåga och egenmakt att dra nytta av en inkluderande och rättvis datamarknad. En utbredning av åtgärder för datakompetens och införande av lämpliga uppföljningsåtgärder skulle kunna bidra till att förbättra arbetsvillkoren och i slutändan stödja dataekonomins konsolidering och innovationsbana i unionen. De behöriga myndigheterna bör främja verktyg och anta åtgärder för att förbättra datakompetensen bland de användare och enheter som omfattas av denna förordning samt öka medvetenheten om deras rättigheter och skyldigheter enligt denna förordning.

(20) I praktiken är inte alla data som genereras av uppkopplade produkter eller tillhörande tjänster lättillgängliga för sina användare, och ofta finns endast begränsade möjligheter när det gäller portabilitet för data som genereras av produkter som är uppkopplade till internet. Användarna kan inte få fram de data som krävs för att utnyttja leverantörer av reparationstjänster eller andra tjänster, och företagen kan inte sjösätta innovativa tjänster som är mer lättanvända och effektiva. Inom många sektorer kan tillverkarna, genom sin kontroll av de uppkopplade produkternas eller de tillhörande tjänsternas tekniska design, bestämma vilka data som genereras och hur åtkomsten till dem ska ske, trots att de inte har någon laglig rätt till dessa data. Det är därför nödvändigt att säkerställa att uppkopplade produkter utformas och tillverkas, och att tillhörande tjänster tillhandahålls, på ett sådant sätt att en användare utan kostnad alltid kan få enkel och säker åtkomst till produktdata och data från den tillhörande tjänsten, inklusive tillhörande metadata som är nödvändiga för att tolka och använda dessa data, i ett heltäckande, strukturerat, allmänt använt och maskinläsbart format, även för hämtning, användning eller delning av data. Med *lätt åtkomliga data* avses produktdata och data från en tillhörande tjänst som en datahållare, utan oproportionell ansträngning, lagligen erhåller eller lagligen kan erhålla från den uppkopplade produkten eller tillhörande tjänsten, till exempel genom den uppkopplade produktens utformning, datahållarens avtal med användaren om tillhandahållande av tillhörande tjänster och dess tekniska medel för åtkomst till data. Lätt åtkomliga data omfattar inte data som genereras genom användning av en uppkopplad produkt om den uppkopplade produkten inte har utformats för att lagra eller överföra sådana data utanför den komponent i vilken de genereras eller den uppkopplade produkten som helhet. Denna förordning bör därför inte tolkas som att den

inför en skyldighet att lagra data på en uppkopplad produkts centrala datorenhet. Avsaknaden av en sådan skyldighet bör inte hindra tillverkaren eller datahållaren att frivilligt komma överens med användaren om att göra sådana anpassningar. Designskyldigheterna i denna förordning påverkar inte heller tillämpningen av principen om uppgiftsminimering i artikel 5.1 c i förordning (EU) 2016/679, och de bör inte tolkas som att de medför en skyldighet att utforma uppkopplade produkter och tillhörande tjänster på ett sådant sätt att de lagrar eller på annat sätt behandlar andra personuppgifter än personuppgifter som är nödvändiga för de ändamål för vilka de behandlas. Unionsrätt eller nationell rätt skulle kunna införas för att ange ytterligare detaljer, till exempel de produktdata som bör vara åtkomliga från uppkopplade produkter eller tillhörande tjänster, eftersom sådana data kan vara nödvändiga för effektiv drift eller reparation eller effektivt underhåll av dessa uppkopplade produkter eller tillhörande tjänster. Om senare uppdateringar eller ändringar av en uppkopplad produkt eller en tillhörande tjänst från tillverkarens eller någon annan parts sida leder till ytterligare tillgängliga data eller till en begränsning av data som ursprungligen var tillgängliga, bör sådana ändringar meddelas användaren i samband med uppdateringen eller ändringen.

(21) Om flera personer eller enheter betraktas som användare, till exempel i fall av gemensamt ägande eller om en ägare, hyrestagare eller leasetagare delar rättigheter till åtkomst till eller användning av data, bör utformningen av den uppkopplade produkten, den tillhörande tjänsten eller det berörda gränssnittet göra det möjligt för varje användare att få åtkomst till de data som de genererar. Användning av uppkopplade produkter som genererar data kräver vanligtvis att användaren skapar ett användarkonto. Genom ett sådant konto kan användaren identifieras av datahållaren, som kan vara tillverkaren. Det kan också användas som ett kommunikationsmedel och för att lämna in och behandla begäranden om åtkomst till data. Om flera tillverkare eller leverantörer av tillhörande tjänster har sålt, hyrt ut eller leasat uppkopplade produkter eller tillhandahållit tillhörande tjänster, tillsammans och till samma användare, bör användaren vända sig till var och en av de parter som den har ett avtal med. Tillverkare eller designer av en uppkopplad produkt som vanligtvis används av flera personer bör införa nödvändiga mekanismer som möjliggör separata användarkonton för enskilda personer, vid behov, eller gör det möjligt för flera personer att använda samma användarkonto. Kontolösningarna bör göra det möjligt för användarna att radera sina konton och radera tillhörande data och kan göra det möjligt för användarna att avsluta åtkomsten till eller användningen eller delningen av data, eller att lämna in begäranden om detta, särskilt med beaktande av situationer där äganderätten till eller användningen av den uppkopplade produkten förändras. Användaren bör beviljas åtkomst genom ett automatiskt beviljande som verkställs på grundval av en enkel begärandemekanism, utan att det krävs någon granskning eller något godkännande från tillverkaren eller datahållaren. Detta innebär att data endast bör göras tillgängliga när användaren faktiskt önskar åtkomst. I de fall då ett automatiserat beviljande av begäran om dataåtkomst inte är möjligt, exempelvis via ett användarkonto eller en mobilapplikation som tillhandahålls tillsammans med den uppkopplade produkten eller tillhörande tjänsten, bör tillverkaren underrätta användaren om hur åtkomst kan fås till data.

(22) Uppkopplade produkter får vara utformade så att vissa data görs direkt tillgängliga genom datalagring i enheten eller från en fjärrserver till vilken data kommuniceras. Åtkomst till datalagringen i enheten kan möjliggöras genom kabelbaserade eller trådlösa lokala nät som är anslutna till en allmänt tillgänglig elektronisk kommunikationstjänst eller ett mobilnät. Servern kan vara tillverkarens egen lokala serverkapacitet eller den lokala serverkapaciteten hos en tredje part eller en leverantör av molntjänster. Personuppgiftsbiträden enligt definitionen i artikel 4.8 i förordning (EU) 2016/679 anses inte agera som datahållare. De kan dock särskilt ges i uppdrag att göra data tillgängliga av den personuppgiftsansvarige enligt definitionen i artikel 4.7 i förordning (EU) 2016/679. Uppkopplade produkter får vara utformade så att de tillåter användaren eller en tredje part att behandla dessa data i den uppkopplade produkten, i en databehandlingsinstans hos tillverkaren eller i en miljö för informations- och kommunikationsteknik (IKT) som användaren eller den tredje parten väljer.

(23) Virtuella assistenter spelar en allt viktigare roll i digitaliseringen av konsument- och yrkesmiljöer och fungerar som ett användarvänligt gränssnitt för att spela upp innehåll, erhålla information eller aktivera produkter som är uppkopplade till internet. Virtuella assistenter kan fungera som en gemensam portal för exempelvis en smart hushållsmiljö och registrera betydande mängder relevanta data om hur användarna interagerar med produkter som är uppkopplade till internet, även produkter som är tillverkade av andra parter, och kan ersätta användningen av tillverkartillhandahållna gränssnitt såsom pekskärmar eller mobilappar. Användaren kan önska göra sådana data tillgängliga för tredjepartstillverkare och möjliggöra nya smarta tjänster. Virtuella assistenter bör omfattas av den rätt till dataåtkomst som föreskrivs i denna förordning. Data som genereras när användaren interagerar med en

uppkopplad produkt via en virtuell assistent som tillhandahålls av någon annan än tillverkararen av den uppkopplade produkten bör också omfattas av den rätt till dataåtkomst som föreskrivs i denna förordning. Det är dock endast data som härrör från interaktionen mellan användaren och en uppkopplad produkt eller tillhörande tjänst via den virtuella assistenten som bör omfattas av denna förordning. Data som produceras av den virtuella assistenten men som inte är förbundna med användningen av en uppkopplad produkt eller tillhörande tjänst omfattas inte av denna förordning.

(24) Innan ett avtal ingås om köp, hyra eller leasing av en uppkopplad produkt bör försäljaren, uthyraren eller leasegivaren, som kan vara tillverkaren, förse användaren med information om de produktdata som den uppkopplade produkten har möjlighet att generera, inbegripet typ, format och uppskattad volym av sådana data, på ett tydligt och begripligt sätt. Detta kan inbegripa information om datastrukturer, dataformat, vokabulärer, klassificeringssystem, taxonomier och kodförteckningar, om sådana finns tillgängliga, samt tydlig och tillräcklig information som är relevant för användarens utövande av sina rättigheter om hur data kan lagras eller hämtas eller hur åtkomst kan fås till data, inbegripet information om användningsvillkor och tjänstekvalitet för programmeringsgränssnitt eller i tillämpliga fall tillhandahållande av programvaruutvecklingsverktyg. Den skyldigheten säkrar transparens när det gäller genererade produktdata och förenklar åtkomsten för användaren. Informationsskyldigheten skulle kunna fullgöras till exempel genom en stabil webbadress (URL) som kan distribueras som en webblänk eller QR-kod och hänvisa till relevant information som försäljaren, uthyraren eller leasegivaren, som kan vara tillverkaren, kan tillhandahålla användaren innan avtalet om köp, hyra eller leasing av en uppkopplad produkt ingås. Det är under alla omständigheter nödvändigt att användaren kan lagra informationen på ett sätt som medger åtkomst för användning i framtiden och som tillåter oförändrad återgivning av den lagrade informationen. Datahållaren kan inte förväntas lagra data på obestämd tid med tanke på behoven hos användaren av den uppkopplade produkten men bör tillämpa en rimlig policy för lagring av data, i förekommande fall i enlighet med principen om lagringsminimering enligt artikel 5.1 e i förordning (EU) 2016/679, som möjliggör en effektiv tillämpning av rätten till dataåtkomst enligt den här förordningen. Skyldigheten att lämna information påverkar inte den personuppgiftsansvariges skyldighet att lämna information till den registrerade enligt artiklarna 12, 13 och 14 i förordning (EU) 2016/679. Den presumtiva datahållaren bör ha skyldighet att lämna information innan ett avtal om tillhandahållande av en tillhörande tjänst ingås, oavsett om datahållaren ingår ett avtal om köp, hyra eller leasing av en uppkopplad produkt. Om informationen ändras under den uppkopplade produktens livslängd eller under avtalsperioden för den tillhörande tjänsten, liksom när det ändamål för vilket dessa data ska användas ändras i förhållande till det ursprungligen angivna ändamålet, bör denna information också lämnas till användaren.

(25) Denna förordning bör inte tolkas som att den medför någon ny rättighet för datahållare att använda produktdata eller data från en tillhörande tjänst. Om tillverkaren av en uppkopplad produkt är en datahållare, bör tillverkarens användning av icke-personuppgifter grundas på ett avtal mellan tillverkaren och användaren. Ett sådant avtal kan ingå i ett avtal om tillhandahållande av den tillhörande tjänsten, som kan ingås tillsammans med försäljnings-, hyres- eller leasingavtalet för den uppkopplade produkten. Varje avtalsvillkor som föreskriver att datahållaren får använda produktdata eller data från en tillhörande tjänst bör vara transparent för användaren, även vad gäller de ändamål för vilka datahållaren avser att använda berörda data. Sådana ändamål skulle bland annat kunna vara att förbättra funktionen hos den uppkopplade produkten eller de tillhörande tjänsterna, att utveckla nya produkter eller tjänster eller att aggregera data i syfte att göra de resulterande härledda data tillgängliga för tredje parter, förutsatt att sådana härledda data inte gör det möjligt att identifiera de specifika data som överförs till datahållaren från den uppkopplade produkten eller gör det möjligt för en tredje part att härleda dessa data från datamängden. Varje ändring av avtalet bör vara beroende av användarens informerade samtycke. Denna förordning hindrar inte parter från att komma överens om avtalsvillkor vars effekt är att utesluta eller begränsa en datahållares användning av icke-personuppgifter, eller vissa kategorier av icke-personuppgifter. Den hindrar inte heller parter från att komma

överens om att göra produktdata eller data från en tillhörande tjänst tillgängliga för tredje parter, direkt eller indirekt, inbegripet, i tillämpliga fall, via en annan datahållare. Denna förordning hindrar inte heller sektorsspecifika regleringskrav enligt unionsrätten, eller nationell rätt som är förenlig med unionsrätten, som skulle utesluta eller begränsa datahållarens användning av vissa sådana data av tydligt definierade skäl grundade på offentlig policy. Denna förordning hindrar inte att användare vid förbindelser mellan företag gör data tillgängliga för tredje parter eller datahållare enligt något lagligt avtalsvillkor, bland annat genom att samtycka till att begränsa eller inskränka vidare delning av sådana data, eller att de får proportionell ersättning, till exempel i utbyte mot att de avstår från sin rätt att använda eller dela sådana data. Trots att begreppet *datahållare* i allmänhet inte omfattar offentliga organ kan det dock omfatta offentliga företag.

(26) För att främja uppkomsten av likvida, rättvisa och effektiva marknader för icke-personuppgifter bör användare av uppkopplade produkter kunna dela data med andra, även för kommersiella ändamål, med minimala rättsliga och tekniska insatser. Det är för närvarande ofta svårt för företag att motivera de personal- eller databehandlingskostnader som är nödvändiga för att förbereda datamängder som inte består av personuppgifter eller dataprodukter och erbjuda dem till potentiella motparter via dataförmedlingstjänster, inbegripet datamarknader. Ett betydande hinder för företagens delning av icke-personuppgifter är därför en följd av bristen på förutsägbarhet när det gäller ekonomisk avkastning från investeringar i kurering och tillgängliggörande av datamängder eller dataprodukter. För att möjliggöra uppkomsten av likvida, rättvisa och effektiva marknader för icke-personuppgifter i unionen måste det klargöras vilken part som har rätt att erbjuda sådana data på en marknad. Användare bör därför ha rätt att dela icke-personuppgifter med datamottagare för kommersiella och icke-kommersiella ändamål. Sådan datadelning kan utföras direkt av användaren, på begäran av användaren via en datahållare, eller genom dataförmedlingstjänster. Dataförmedlingstjänster, som regleras i Europaparlamentets och rådets förordning (EU) 2022/868 ([22]), skulle kunna underlätta en dataekonomi genom att upprätta affärsförbindelser mellan användare, datamottagare och tredje parter och kan hjälpa användare att utöva sin rätt att använda data, till exempel genom att säkerställa anonymisering av personuppgifter eller aggregering av åtkomst till data från flera enskilda användare. Om data undantas från en datahållares skyldighet att göra dem tillgängliga för användare eller tredje parter kan omfattningen av sådana data specificeras i avtalet mellan användaren och datahållaren om tillhandahållande av en tillhörande tjänst så att användarna enkelt kan fastställa vilka data som är tillgängliga för dem för delning med datamottagare eller tredje parter. Datahållare bör inte göra produktdata som inte består av personuppgifter tillgängliga för tredje parter för kommersiella eller icke-kommersiella ändamål annat än för att fullgöra avtalet med användaren, utan att det påverkar rättsliga krav enligt unionsrätten eller nationell rätt och som innebär att en datahållare ska göra data tillgängliga. Vid behov bör datahållare genom avtal förbinda tredje parter att inte dela vidare data som de har mottagit från dem.

(27) Inom sektorer som kännetecknas av koncentration av ett litet antal tillverkare som levererar uppkopplade produkter till slutanvändarna kan det förekomma att det endast finns ett begränsat antal alternativ för användarna vad gäller åtkomst till och användning och delning av data. Under sådana omständigheter kan avtal vara otillräckliga för att uppnå målet att stärka användarnas egenmakt, vilket gör det svårt för användarna att få ut ett värde från de data som genereras av de uppkopplade produkter som de köper, hyr eller leasar. Därmed finns det bara begränsade möjligheter för innovativa mindre företag att erbjuda databaserade lösningar på ett konkurrenskraftigt sätt och för en diversifierad dataekonomi i unionen. Denna förordning bör därför bygga vidare på senare tids utveckling inom enskilda sektorer, såsom uppförandekoden för delning av jordbruksdata genom avtal. Unionsrätt eller nationell rätt kan antas för att hantera sektorsspecifika behov och mål. Datahållare bör inte heller använda lätt åtkomliga data som är icke-personuppgifter för att få inblick i användarens ekonomiska situation, tillgångar eller produktionsmetoder eller i sådan användning från användarens sida som på något annat sätt skulle kunna undergräva användarens affärsmässiga ställning på de marknader där denne är verksam. Detta skulle kunna innefatta att använda kunskap om ett företags eller ett jordbruks allmänna resultat i avtalsförhandlingar med

([22]) Europaparlamentets och rådets förordning (EU) 2022/868 av den 30 maj 2022 om europeisk dataförvaltning och om ändring av förordning (EU) 2018/1724 (dataförvaltningsakten) (EUT L 152, 3.6.2022, s. 1).

användaren om potentiella förvärv av användarens produkter eller jordbruksprodukter till skada för användaren, eller att använda sådan information i aggregerad form för inmatning i större databaser om vissa marknader, till exempel databaser om skördeavkastningen för den kommande skördesäsongen, eftersom en sådan användning indirekt skulle kunna påverka användaren negativt. Användaren bör förses med det tekniska gränssnitt som behövs för hantering av tillstånd, företrädesvis med detaljerade tillståndsalternativ, såsom ”tillåt en gång” eller ”tillåt när denna app eller tjänst används”, inklusive alternativet att återkalla sådana tillstånd.

(28) I avtal mellan en datahållare och en konsument som är användare av en uppkopplad produkt eller tillhörande tjänst som genererar data är unionens konsumentlagstiftning, särskilt direktiven 93/13/EEG och 2005/29/EG, tillämplig för att säkerställa att en konsument inte omfattas av oskäliga avtalsvillkor. Vid tillämpningen av denna förordning bör oskäliga avtalsvillkor som ensidigt åläggs ett företag inte vara bindande för företaget.

(29) Datahållare kan kräva lämplig användaridentifiering för att kontrollera en användares rätt till dataåtkomst. När det gäller personuppgifter som behandlas av ett personuppgiftsbiträde på uppdrag av den personuppgiftsansvarige bör datahållare säkerställa att begäran om åtkomst tas emot och hanteras av personuppgiftsbiträdet.

(30) Användaren bör vara fri att använda dessa data för alla lagliga ändamål. Detta innefattar att tillhandahålla de data som användaren har erhållit vid utövandet av sina rättigheter enligt denna förordning åt en tredje part som erbjuder en eftermarknadstjänst som kan konkurrera med en tjänst som tillhandahålls av en datahållare, eller instruera datahållaren att göra detta. Begäran bör lämnas in av användaren eller en tredje part som har rätt att agera för användarens räkning, inbegripet en leverantör av en dataförmedlingstjänst. Datahållare bör säkerställa att de data som görs tillgängliga för den tredje parten är lika korrekta, fullständiga, tillförlitliga, relevanta och aktuella som de data som datahållaren själv kan ha eller har rätt att få åtkomst till från användningen av den uppkopplade produkten eller den tillhörande tjänsten. Eventuella immateriella rättigheter bör respekteras vid hanteringen av data. Det är viktigt att bevara incitamenten för investering i produkter med funktioner som baseras på användningen av data från sensorer som är inbyggda i dessa produkter.

(31) I Europaparlamentets och rådets direktiv (EU) 2016/943 ([23]) föreskrivs att anskaffande, utnyttjande eller röjande av en företagshemlighet ska anses som lagligt, bland annat om sådant anskaffande, utnyttjande eller röjande krävs eller medges enligt unionsrätten eller nationell rätt. Enligt denna förordning krävs att datahållare röjer vissa data för användarna, eller för de tredje parter som väljs av en användare, även när dessa data uppfyller kraven för skydd i egenskap av företagshemligheter; den bör dock tolkas på ett sådant sätt att skyddet för företagshemligheter enligt direktiv (EU) 2016/943 bevaras. I detta sammanhang bör datahållare kunna kräva att användarna, eller de tredje parter som väljs av en användare, bevarar konfidentialiteten hos data som betraktas som företagshemligheter. Datahållare bör därför identifiera företagshemligheter innan data röjs och ha möjlighet att komma överens med användarna, eller de tredje parter som väljs av en användare, om nödvändiga åtgärder för att bevara deras konfidentialitet, bland annat användning av standardavtalsvillkor, avtal om konfidentialitet, strikta åtkomstprotokoll, tekniska standarder och tillämpning av uppförandekoder. Utöver användning av standardavtalsvillkor som ska utarbetas och rekommenderas av kommissionen skulle ett fastställande av uppförandekoder och tekniska standarder för skydd av företagshemligheter vid hantering av data kunna bidra till att syftet med denna förordning uppnås, och det bör därför uppmuntras. Om det inte finns något avtal om de nödvändiga åtgärderna eller om en användare, eller de tredje parter som väljs av en användare, underlåter att genomföra överenskomna åtgärder eller äventyrar konfidentialiteten för företagshemligheter bör datahållaren kunna hindra eller avbryta delningen av data som identifierats som företagshemligheter. I sådana fall bör datahållaren meddela användaren eller den tredje parten beslutet skriftligen utan oskäligt dröjsmål och underrätta den behöriga myndigheten i den medlemsstat där datahållaren är etablerad om att den har hindrat eller avbrutit datadelningen och identifiera vilka åtgärder som inte har överenskommits eller genomförts och, i förekommande fall, vilka företagshemligheter som har äventyrats. Datahållare kan i princip inte avslå en begäran om åtkomst till data enligt denna förordning enbart

([23]) Europaparlamentets och rådets direktiv (EU) 2016/943 av den 8 juni 2016 om skydd mot att icke röjd know-how och företagsinformation (företagshemligheter) olagligen anskaffas, utnyttjas och röjs (EUT L 157, 15.6.2016, s. 1).

på grundval av att vissa data anses vara en företagshemlighet, eftersom detta skulle undergräva de avsedda verkningarna av denna förordning. Under särskilda omständigheter bör dock en datahållare som är innehavare av en företagshemlighet från fall till fall kunna avslå en begäran om åtkomst till de specifika data i fråga om den kan visa för användaren eller den tredje parten att röjandet av den företagshemligheten, trots tekniska och organisatoriska åtgärder som vidtas av användaren eller av den tredje parten, med stor sannolikhet kommer att orsaka allvarlig ekonomisk skada. Allvarlig ekonomisk skada innebär allvarliga och irreparabla ekonomiska förluster. Datahållaren bör utan oskäligt dröjsmål vederbörligen motivera sitt avslag skriftligen för användaren eller den tredje parten och underrätta den behöriga myndigheten. Denna motivering bör bygga på objektiva faktorer som visar den konkreta risken för allvarlig ekonomisk skada som väntas uppstå till följd av ett visst röjande av data och skälen till att de åtgärder som vidtagits för att skydda de data som begärts inte anses vara tillräckliga. Eventuell negativ inverkan på cybersäkerheten kan beaktas i detta sammanhang. Om användaren eller en tredje part vill bestrida datahållarens beslut att vägra eller att hindra eller avbryta delningen av data kan användaren eller den tredje parten, utan att det påverkar rätten att få sin sak prövad i en domstol, lämna in ett klagomål till den behöriga myndigheten, som utan oskäligt dröjsmål bör besluta huruvida och på vilka villkor datadelning bör inledas eller återupptas eller kan komma överens med datahållaren om att hänskjuta frågan till ett tvistlösningsorgan. Undantagen från rätten till dataåtkomst enligt denna förordning bör under inga omständigheter begränsa de registrerades rätt till tillgång och rätt till dataportabilitet enligt förordning (EU) 2016/679.

(32) Syftet med denna förordning är inte enbart att främja utvecklingen av nya innovativa uppkopplade produkter eller tillhörande tjänster och stimulera innovation på eftermarknaderna, utan även att stimulera utvecklingen av helt nya tjänster som utnyttjar berörda data, även baserat på data från en rad olika uppkopplade produkter eller tillhörande tjänster. Samtidigt syftar denna förordning till att undvika att undergräva investeringsincitamenten för den typ av uppkopplad produkt som data erhålls från, exempelvis genom användning av data för utveckling av en konkurrerande uppkopplad produkt som av användarna betraktas som likvärdig eller utbytbar, särskilt på grund av den uppkopplade produktens egenskaper, pris och avsedda användning. I denna förordning föreskrivs inget förbud mot utveckling av en tillhörande tjänst med hjälp av data som erhålls enligt denna förordning, eftersom detta skulle ha en oönskad avskräckande effekt på innovation. Att förbjuda användning av data som görs tillgängliga enligt denna förordning för att utveckla konkurrerande uppkopplade produkter skyddar datahållares innovationsinsatser. Huruvida en uppkopplad produkt konkurrerar med den uppkopplade produkt som data härrör från beror på om de båda uppkopplade produkterna konkurrerar på samma produktmarknad. Detta bör fastställas på grundval av de principer i unionens konkurrenslagstiftning som fastslagits för att definiera den relevanta produktmarknaden. Lagliga ändamål för användningen av data kan dock omfatta bakåtkompilering, under förutsättning den uppfyller kraven i denna förordning och i unionsrätten eller nationell rätt. Detta kan vara fallet när det gäller reparation eller förlängning av en uppkopplad produkts livslängd eller tillhandahållande av eftermarknadstjänster för uppkopplade produkter.

(33) En tredje part som ges tillgång till data kan vara en fysisk eller juridisk person, till exempel en konsument, ett företag, en forskningsorganisation, en organisation utan vinstsyfte eller en enhet som agerar i egenskap av näringsidkare. När en datahållare gör data tillgängliga för den tredje parten bör datahållaren inte missbruka sin ställning för att uppnå en konkurrensfördel på marknader där datahållaren och den tredje parten kan stå i direkt konkurrens med varandra. Datahållaren bör därför inte använda några lätt åtkomliga data för att få inblick i den tredje partens ekonomiska situation, tillgångar eller produktionsmetoder eller i användningen på något annat sätt som skulle kunna undergräva den tredje partens affärsmässiga ställning på de marknader där den tredje parten är verksam. Användaren bör kunna dela icke-personuppgifter med tredje parter för kommersiella ändamål. Efter överenskommelse med användaren, och om inte annat följer av bestämmelserna i denna förordning, bör tredje parter kunna överföra de rättigheter till dataåtkomst som användaren beviljat andra tredje parter, även i utbyte mot ersättning. Dataförmedlare mellan företag och system för hantering av personuppgifter (PIMS), kallade dataförmedlingstjänster i förordning (EU) 2022/868, kan stödja användarna eller de tredje parterna vid upprättandet av affärsförbindelser med ett obestämt antal potentiella motparter för alla lagliga ändamål som omfattas av den här förordningen. De skulle kunna spela en avgörande roll när det gäller att aggregera åtkomst till data så att stordataanalyser eller maskininlärning kan underlättas, förutsatt att användare har full kontroll över huruvida deras data ska tillhandahållas för sådan aggregering och de kommersiella villkor enligt vilka deras data kommer att användas.

(34) Användningen av en uppkopplad produkt eller tillhörande tjänst kan, i synnerhet när användaren är en fysisk person, generera data som rör den registrerade. Behandlingen av sådana data omfattas av de regler som fastställs inom ramen för förordning (EU) 2016/679, även när personuppgifter och icke-personuppgifter i en datamängd hänger oupplösligt samman. Den registrerade kan vara användaren eller en annan fysisk person. Det är endast den personuppgiftsansvarige eller den registrerade som får begära personuppgifter. En användare som är den registrerade har under vissa omständigheter enligt förordning (EU) 2016/679 rätt att få åtkomst till sina personuppgifter, och dessa rättigheter påverkas inte av den här förordningen. Enligt den här förordningen har en användare som är en fysisk person dessutom rätt att få åtkomst till alla data som genereras genom användning av en uppkopplad produkt, oavsett om det handlar om personuppgifter eller icke-personuppgifter. Om användaren inte är den registrerade utan ett företag, inbegripet ett enmansföretag, och det inte är ett gemensamt hushåll som använder den uppkopplade produkten, ska användaren anses vara en personuppgiftsansvarig. Följaktligen måste en sådan användare som i egenskap av personuppgiftsansvarig avser att begära personuppgifter som genererats genom användning av en uppkopplad produkt eller tillhörande tjänst ha en rättslig grund för behandling av data i enlighet med artikel 6.1 i förordning (EU) 2016/679, såsom samtycke av den registrerade eller fullgörande av ett avtal som den registrerade är part i. En sådan användare bör säkerställa att den registrerade på lämpligt sätt informeras om de särskilda, uttryckligt angivna och berättigade ändamålen för behandlingen av berörda data, och om hur den registrerade kan utöva sina rättigheter på ett effektivt sätt. Om datahållaren och användaren är gemensamt personuppgiftsansvariga i den mening som avses i artikel 26 i förordning (EU) 2016/679 måste de, på ett transparent sätt genom ett arrangemang sinsemellan, fastställa sitt respektive ansvar för att fullgöra skyldigheterna enligt den förordningen. Det bör anses att en sådan användare, när berörda data har gjorts tillgängliga, i sin tur kan bli datahållare, om användaren uppfyller kriterierna enligt den här förordningen och därmed omfattas av skyldigheten att göra data tillgängliga enligt den här förordningen.

(35) Produktdata eller data från en tillhörande tjänst bör endast göras tillgängliga för en tredje part på användarens begäran. Denna förordning kompletterar därmed den rättighet som föreskrivs i artikel 20 i förordning (EU) 2016/679, nämligen att den registrerade har rätt att få ut sina personuppgifter i ett strukturerat, allmänt använt och maskinläsbart format och rätt att överföra dessa uppgifter till en annan personuppgiftsansvarig, när dessa uppgifter behandlas automatiserat på grundval av artikel 6.1 a eller 9.2 a eller på grundval av ett avtal enligt artikel 6.1 b i den förordningen. Den registrerade har också rätt att få dessa personuppgifter överförda direkt från en personuppgiftsansvarig till en annan, men endast när detta är tekniskt möjligt. I artikel 20 i förordning (EU) 2016/679 specificeras att detta avser data som tillhandahålls av den registrerade, men det anges inte om det förutsätter en aktiv handling från den registrerades sida eller om det också gäller för situationer där en uppkopplad produkt eller tillhörande tjänst genom sin konstruktion på ett passivt sätt iakttar en registrerads beteende eller annan information som rör en registrerad. Rättigheterna enligt den här förordningen kompletterar rätten att få ut och portera personuppgifter enligt artikel 20 i förordning (EU) 2016/679 på att antal sätt. Den här förordningen ger användaren rätt att få åtkomst och ge tredje part tillgång till alla produktdata eller data från en tillhörande tjänst, oavsett om det rör sig om personuppgifter, utan någon skillnad mellan data som aktivt görs tillgängliga och data som passivt iakttas, och oavsett den rättsliga grunden för behandlingen. Till skillnad från artikel 20 i förordning (EU) 2016/679 kräver och säkerställer den här förordningen den tekniska genomförbarheten för tredjepartsåtkomst till alla typer av data som omfattas av den här förordningens tillämpningsområde, oavsett om det handlar om personuppgifter eller icke-personuppgifter, och därigenom säkerställs att tekniska hinder inte längre står i vägen för eller förhindrar åtkomsten till sådana data. Den ger också datahållare rätt att fastställa rimlig ersättning som ska betalas av tredje parter, men inte av användaren, för kostnader som uppstår när direkt åtkomst ges till de data som genereras av användarens uppkopplade produkt. Om en datahållare och en tredje part inte kan enas om villkoren för sådan direkt åtkomst bör den registrerade inte på något sätt hindras från att utöva de rättigheter som fastställs i förordning (EU) 2016/679, inbegripet rätten till dataportabilitet, genom att utnyttja rättsmedel i enlighet med den förordningen. Det bör i detta sammanhang förstås att enligt förordning (EU) 2016/679 tillåter ett avtal inte behandling av särskilda kategorier av personuppgifter från datahållarens eller den tredje partens sida.

(36) Åtkomst till data som lagras och nås från terminalutrustning omfattas av direktiv 2002/58/EG och förutsätter ett samtycke från abonnenten eller användaren i den mening som avses i det direktivet, om det inte är strikt nödvändigt för tillhandhållandet av en informationssamhällestjänst som uttryckligen begärs av användaren eller abonnenten eller endast i syfte att överföra ett meddelande. Direktiv 2002/58/EG skyddar integriteten för en användares terminalutrustning i fråga om användningen av behandlings- och lagringskapacitet och insamling av information. Utrustning för sakernas internet betraktas som terminalutrustning om den är direkt eller indirekt ansluten till ett allmänt kommunikationsnät.

(37) För att förhindra att användare utnyttjas bör tredje parter som fått tillgång till data på användarens begäran endast behandla dessa data för de ändamål som överenskommits med användaren och endast dela dem med annan tredje part med användarens samtycke till en sådan datadelning.

(38) I enlighet med principen om uppgiftsminimering bör tredje parter endast få tillgång till information som är nödvändig för tillhandahållandet av den tjänst som begärts av användaren. När den tredje parten fått tillgång till data bör den behandla dessa data för de ändamål som överenskommits med användaren, utan inblandning från datahållaren. Det bör vara enkelt för användaren att vägra eller avbryta tredje parts tillgång till data eftersom det är användarens sak att godkänna åtkomsten. Varken tredje parter eller datahållare bör på något sätt göra det orimligt svårt för användaren att göra sina val eller utöva sina rättigheter, inbegripet genom att erbjuda användaren val på ett icke-neutralt sätt, eller genom att utöva tvång mot, vilseleda eller manipulera användaren eller undergräva eller inskränka användarens handlingsfrihet, beslutsfattande eller val, inbegripet genom ett digitalt användargränssnitt eller en del därav. I detta sammanhang bör tredje parter eller datahållare inte förlita sig på så kallade mörka mönster i designen av sina digitala gränssnitt. Mörka mönster är designtekniker som driver eller vilseleder konsumenter till beslut som har negativa konsekvenser för dem. Dessa manipulationstekniker kan användas för att övertyga användarna, i synnerhet utsatta konsumenter, att ägna sig åt oönskat beteende, för att vilseleda dem genom att "puffa" dem så att de fattar beslut om att lämna ut data eller för att otillbörligt påverka de beslut som fattas av tjänstens användare på ett sådant sätt att det undergräver eller inskränker deras handlingsfrihet, beslutsfattande och valfrihet. Gemensamma och legitima affärsmetoder som är förenliga med unionsrätten bör inte i sig anses utgöra mörka mönster. Tredje parter och datahållare bör fullgöra sina skyldigheter enligt relevant unionsrätt, i synnerhet kraven i Europaparlamentets och rådets direktiv 98/6/EG ([24]) och 2000/31/EG ([25]) samt i direktiven 2005/29/EG och 2011/83/EU.

(39) Tredje parter bör också avstå från att använda data som omfattas av denna förordning för profilering av individer om inte sådan behandling är strikt nödvändig för tillhandahållandet av den tjänst som begärs av användaren, bland annat i samband med automatiserat beslutsfattande. Kravet att radera data när de inte längre krävs för det ändamål som överenskommits med användaren, om inte annat överenskommits när det gäller icke-personuppgifter, kompletterar den registrerades rätt till radering enligt artikel 17 i förordning (EU) 2016/679. När en tredje part är en leverantör av en dataförmedlingstjänst tillämpas de skyddsåtgärder för den registrerade som föreskrivs i förordning (EU) 2022/868. Den tredje parten får använda data för att utveckla en ny och innovativ uppkopplad produkt eller tillhörande tjänst men inte för att utveckla en konkurrerande uppkopplad produkt.

(40) Uppstartsföretag, små företag, företag som betraktas som medelstora företag enligt artikel 2 i bilagan till rekommendation 2003/361/EG samt företag från traditionella sektorer med mindre utvecklad digital kapacitet har svårt att få åtkomst till relevanta data. Denna förordning syftar till att underlätta åtkomsten till data för dessa enheter och samtidigt säkerställa att de motsvarande skyldigheterna är så proportionella som möjligt så att de inte blir alltför betungande. Samtidigt har ett litet antal mycket stora företag med betydande ekonomisk styrka vuxit fram i den digitala ekonomin genom ackumulering och aggregering av enorma datavolymer och den tekniska infrastrukturen för monetarisering av dem. Dessa mycket stora företag inkluderar företag som tillhandahåller centrala plattformstjänster och kontrollerar hela plattformsekosystem i den digitala ekonomin och som befintliga eller nya marknadsaktörer inte kan utmana eller konkurrera med. Europaparlamentets och rådets förordning (EU) 2022/1925 ([26]) syftar till att avhjälpa dessa ineffektiva aspekter och obalanser genom att tillåta att kommissionen utser ett företag till *grindvakt*, och inför ett antal skyldigheter för sådana grindvakter, inbegripet ett förbud mot att kombinera vissa data utan samtycke, och en skyldighet att säkerställa en rätt till effektiv dataportabilitet i enlighet med artikel 20 i förordning (EU) 2016/679. I enlighet med förordning (EU) 2022/1925) och mot bakgrund av dessa företags unika möjlighet att förvärva data, är det inte nödvändigt för uppnåendet av den här förordningens mål, och därför oproportionellt för datahållare som omfattas av sådana skyldigheter, att låta

([24]) Europaparlamentets och rådets direktiv 98/6/EG av den 16 februari 1998 om konsumentskydd i samband med prismärkning av varor som erbjuds konsumenter (EGT L 80, 18.3.1998, s. 27).

([25]) Europaparlamentets och rådets direktiv 2000/31/EG av den 8 juni 2000 om vissa rättsliga aspekter på informationssamhällets tjänster, särskilt elektronisk handel, på den inre marknaden ("Direktiv om elektronisk handel") (EGT L 178, 17.7.2000, s. 1).

([26]) Europaparlamentets och rådets förordning (EU) 2022/1925 av den 14 september 2022 om öppna och rättvisa marknader inom den digitala sektorn och om ändring av direktiv (EU) 2019/1937 och (EU) 2020/1828 (förordningen om digitala marknader) (EUT L 265, 12.10.2022, s. 1).

grindvakter omfattas av rätten till dataåtkomst. Om sådana företag omfattades skulle sannolikt även fördelarna med den här förordningen begränsas för mikroföretag och små och medelstora företag med avseende på en rättvis fördelning av datavärdet mellan marknadsaktörerna. Detta betyder att ett företag som tillhandahåller centrala plattformstjänster som har utsetts till grindvakt inte kan begära eller beviljas åtkomst till användares data som genereras genom användning av en uppkopplad produkt eller tillhörande tjänst eller av en virtuell assistent enligt den här förordningen. Dessutom får tredje parter som får tillgång till data på begäran av användaren inte göra dessa data tillgängliga för en grindvakt. Den tredje parten får exempelvis inte lägga ut tjänstetillhandahållandet på entreprenad hos en grindvakt. Detta hindrar dock inte tredje parter från att använda databehandlingstjänster som erbjuds av en grindvakt. Det hindrar inte heller dessa företag från att erhålla och använda samma data på annat lagligt sätt. Åtkomsträttigheterna enligt den här förordningen bidrar till ett större urval av tjänster för konsumenter. Eftersom frivilliga avtal mellan grindvakter och datahållare inte påverkas, skulle begränsningen när det gäller beviljande av åtkomst för grindvakter inte utestänga dem från marknaden eller hindra dem från att erbjuda sina tjänster.

(41) Med tanke på det nuvarande tekniska läget vore det alltför betungande för mikroföretag och små företag att införa ytterligare designskyldigheter avseende uppkopplade produkter som tillverkas eller designas av mikroföretag och små företag eller tillhörande tjänster som tillhandahålls av dem. Detta gäller dock inte om ett mikroföretag eller ett litet företag har ett partnerföretag eller ett anknutet företag i den mening som avses i punkt 3 i bilagan till rekommendation 2003/361/EG som inte betraktas som ett mikroföretag eller ett litet företag och när det tillverkar eller utformar en uppkopplad produkt eller tillhandahåller en tillhörande tjänst på entreprenad. I sådana situationer kan det företag som har lagt ut tillverkningen eller designen på entreprenad på ett mikroföretag eller ett litet företag ersätta detta på lämpligt sätt. Ett mikroföretag eller ett litet företag kan dock ändå omfattas av krav enligt denna förordning såsom datahållare, om det inte är den uppkopplade produktens tillverkare eller leverantör av tillhörande tjänster. En övergångsperiod bör vara tillämplig för ett företag som har betraktats som ett medelstort företag i mindre än ett år och för uppkopplade produkter under ett år från den dag då de släpptes ut på marknaden av ett medelstort företag. En sådan övergångsperiod på ett år ger det medelstora företaget möjlighet att anpassa och förbereda sig innan det utsätts för konkurrens på tjänstemarknaden för de uppkopplade produkter som det tillverkar, på grundval av de åtkomsträttigheter som föreskrivs i denna förordning. En sådan övergångsperiod är inte tillämplig när ett sådant medelstort företag har ett partnerföretag eller ett anknutet företag som inte betraktas som ett mikroföretag eller ett litet företag eller när ett sådant medelstort företag tillverkade eller utformade den uppkopplade produkten eller tillhandahöll den tillhörande tjänsten på entreprenad.

(42) Med beaktande av mångfalden av uppkopplade produkter, vilka producerar data av olika art, volym och frekvens, uppvisar olika nivåer av datarelaterade risker och cybersäkerhetsrisker och ger ekonomiska möjligheter av olika värde, och för att säkerställa enhetlig datadelningspraxis på den inre marknaden, även mellan sektorer, samt uppmuntra och främja rättvis datadelningspraxis även på områden där ingen sådan rätt till dataåtkomst föreskrivs, fastställs i denna förordning övergripande regler om villkoren för åtkomst till data närhelst en datahållare enligt unionsrätten eller nationell lagstiftning som antagits i enlighet med unionsrätten är skyldig att göra data tillgängliga för en datamottagare. Sådan åtkomst bör baseras på rättvisa, rimliga, icke-diskriminerande och transparenta villkor. Dessa allmänna åtkomstregler är inte tillämpliga på skyldigheter att göra data tillgängliga enligt förordning (EU) 2016/679. Frivillig datadelning påverkas inte av dessa regler. De icke-bindande standardavtalsvillkor för datadelning mellan företag som ska utarbetas och rekommenderas av kommissionen kan hjälpa parterna att ingå avtal som innehåller rättvisa, rimliga och icke-diskriminerande villkor och som genomförs på ett transparent sätt. Ingående av ett sådant avtal, som kan inkludera de icke-bindande standardavtalsvillkoren, bör inte innebära att rätten att dela data med tredje parter på något sätt är avhängig av att det finns ett sådant avtal. Om parterna inte kan ingå ett avtal om datadelning, inbegripet med stöd av tvistlösningsorgan, kan rätten att dela data med tredje parter inte åberopas i nationella domstolar.

(43) På grundval av principen om avtalsfrihet bör parterna fortsatt vara fria att förhandla fram de exakta villkoren för att göra data tillgängliga i sina avtal, inom ramen för de allmänna åtkomstreglerna för tillgängliggörandet av data. Villkoren i sådana avtal kan omfatta tekniska och organisatoriska åtgärder, bland annat i samband med datasäkerhet.

(44) För att säkerställa att villkoren för obligatorisk dataåtkomst är rättvisa för båda parter i ett avtal bör de allmänna reglerna för rätten till dataåtkomst hänvisa till regeln om undvikande av oskäliga avtalsvillkor.

(45) Avtal mellan företag om att göra data tillgängliga bör vara icke-diskriminerande mellan jämförbara kategorier av datamottagare, oberoende av om parterna är stora företag, mikroföretag eller små och medelstora företag. För att kompensera bristen på information om villkoren i olika avtal, som gör det svårt för datamottagaren att bedöma om villkoren för att göra data tillgängliga är icke-diskriminerande, bör det vara datahållarnas ansvar att visa att ett avtalsvillkor inte är diskriminerande. Det rör sig inte om olaglig diskriminering om en datahållare använder olika avtalsvillkor för att göra data tillgängliga om dessa skillnader är motiverade av objektiva skäl. Dessa skyldigheter påverkar inte tillämpningen av förordning (EU) 2016/679.

(46) För att uppmuntra fortsatta investeringar i generering och tillgängliggörande av värdefulla data, inbegripet investeringar i relevanta tekniska verktyg, och samtidigt undvika alltför stora bördor för åtkomst till och användning av data som gör att datadelningen inte längre blir affärsmässigt lönsam, omfattar denna förordning principen att datahållare vid förbindelser mellan företag får begära rimlig ersättning i de fall då dessa enligt unionsrätten eller nationell lagstiftning som antagits i enlighet med unionsrätten är skyldiga att göra data tillgängliga för en datamottagare. Sådan ersättning bör inte anses utgöra betalning för dessa data som sådana. Kommissionen bör anta riktlinjer för beräkningen av rimlig ersättning i dataekonomin.

(47) För det första kan rimlig ersättning för att fullgöra skyldigheten enligt unionsrätten eller nationell lagstiftning som antagits i enlighet med unionsrätten att tillmötesgå en begäran om att göra data tillgängliga inbegripa ersättning för de kostnader som uppstår till följd av att data görs tillgängliga. Dessa kostnader kan vara tekniska kostnader, såsom kostnader som är nödvändiga för återgivning av data, spridning på elektronisk väg och lagring av data, men inte för datainsamling eller dataproduktion. Sådana tekniska kostnader kan även omfatta de behandlingskostnader som är nödvändiga för att göra data tillgängliga, inbegripet kostnader i samband med formatering av data. Kostnaderna för att göra data tillgängliga kan också omfatta kostnaderna för att i praktiken underlätta begäranden om datadelning. De kan också variera beroende på datavolymen och de åtgärder som vidtas för att göra data tillgängliga. Långsiktiga arrangemang mellan datahållare och datamottagare, exempelvis genom en abonnemangsmodell eller användning av smarta kontrakt, kan minska kostnaderna i regelbundna eller upprepade transaktioner i ett affärsförhållande. Kostnaderna för att göra data tillgängliga är antingen specifika för en viss begäran eller delade med andra begäranden. I det senare fallet bör en enda datamottagare inte betala hela kostnaden för att göra data tillgängliga. För det andra kan rimlig ersättning också omfatta en marginal, utom i fråga om mikroföretag och små och medelstora företag samt forskningsorganisationer utan vinstsyfte. En marginal kan variera beroende på faktorer som rör dessa data som sådana, såsom deras volym, format eller art. Den kan beakta kostnaderna för att samla in data. En marginal kan därför minska om datahållaren har samlat in data för sin egen verksamhet utan betydande investeringar eller öka om investeringarna i datainsamlingen för datahållarens verksamhet är stora. Den kan begränsas eller till och med uteslutas i situationer där datamottagarens användning av data inte påverkar datahållarens egen verksamhet. Det faktum att data samgenereras av en uppkopplad produkt som ägs, hyrs eller leasas av användaren skulle också kunna sänka ersättningsbeloppet jämfört med andra situationer där data genereras av datahållaren, till exempel under tillhandahållandet av en tillhörande tjänst.

(48) Det är inte nödvändigt att ingripa vid datadelning mellan stora företag eller när datahållaren är ett litet företag eller ett medelstort företag och datamottagaren är ett stort företag. I sådana fall anses företagen själva kunna förhandla fram ersättningen inom gränserna för vad som är rimligt och icke-diskriminerande.

(49) För att skydda mikroföretag och små och medelstora företag från alltför betungande ekonomiska bördor som affärsmässigt sett skulle göra det alltför svårt för dem att utveckla och driva innovativa affärsmodeller, bör den rimliga ersättning för tillhandahållande av data som de betalar inte överstiga de kostnader som är direkt förknippade med att göra dessa data tillgängliga. Direkt förknippade kostnader är sådana kostnader som kan hänföras till enskilda begäranden, med beaktande av de nödvändiga tekniska gränssnitten eller tillhörande programvara och konnektivitet som ska inrättas permanent av datahållaren. Samma ordning bör gälla för forskningsorganisationer utan vinstsyfte.

(50) I vederbörligen motiverade fall, exempelvis om det finns ett behov av att skydda konsumenters deltagande och konkurrensen eller främja innovation på vissa marknader, kan unionsrätten eller den nationella lagstiftning som antas i enlighet med unionsrätten omfatta reglerad ersättning för tillgängliggörandet av specifika typer av data.

(51) Transparens är en viktig princip för att säkerställa att den ersättning som begärs av en datahållare är rimlig eller, om datamottagaren är ett mikroföretag, litet företag eller medelstort företag eller en forskningsorganisation utan vinstsyfte, att ersättningen inte överstiger de kostnader som är direkt förknippade med att göra berörda data tillgängliga för datamottagaren och kan hänföras till den enskilda begäran. För att ge datamottagare möjlighet att bedöma om och kontrollera att ersättningen uppfyller kraven i denna förordning bör datahållaren förse datamottagaren med tillräckligt detaljerad information om hur ersättningen beräknats.

(52) Att tillgång säkerställs till alternativa sätt att lösa inhemska och gränsöverskridande tvister som uppstår i samband med tillhandahållandet av data bör gagna datahållare och datamottagare och därmed stärka förtroendet för datadelning. Om parterna inte kan enas om rättvisa, rimliga och icke-diskriminerande villkor för tillgängliggörandet av data bör tvistlösningsorgan erbjuda parterna en enkel och snabb lågkostnadslösning. I denna förordning fastställs enbart de villkor som tvistlösningsorgan måste uppfylla för att bli certifierade, men det står medlemsstaterna fritt att anta särskilda regler för certifieringsförfarandet, bland annat för certifieringens upphörande eller återkallande. Bestämmelserna om tvistlösning i denna förordning bör inte kräva att medlemsstaterna inrättar tvistlösningsorgan.

(53) Tvistlösningsförfarandet enligt denna förordning är ett frivilligt förfarande som gör det möjligt för användare, datahållare och datamottagare att komma överens om att hänskjuta sina tvister till tvistlösningsorgan. Parterna bör därför fritt kunna vända sig till ett tvistlösningsorgan efter eget val i eller utanför de medlemsstater där dessa parter är etablerade.

(54) För att undvika fall där två eller fler tvistlösningsorgan används för samma tvist, i synnerhet i gränsöverskridande situationer, bör ett tvistlösningsorgan kunna avvisa en begäran om att lösa en tvist som redan har hänskjutits till ett annat tvistlösningsorgan eller en domstol i en medlemsstat.

(55) För att säkerställa en enhetlig tillämpning av denna förordning bör tvistlösningsorganen beakta de icke-bindande standardavtalsvillkor som ska utarbetas och rekommenderas av kommissionen samt unionsrätt eller nationell rätt som anger skyldigheter vad gäller datadelning eller riktlinjer som utfärdas av sektorsmyndigheter för tillämpningen av sådan rätt.

(56) Parter i tvistlösningsförfaranden bör inte hindras från att utöva sin grundläggande rätt till ett effektivt rättsmedel och en opartisk domstol. Därför bör beslutet att hänskjuta en tvist till ett tvistlösningsorgan inte innebära att dessa parter berövas sin rätt att få sin sak prövad i en domstol i en medlemsstat. Tvistlösningsorganen bör offentliggöra årliga verksamhetsrapporter.

(57) Datahållare kan vidta lämpliga tekniska skyddsåtgärder för att förhindra olagligt utlämnande av eller olaglig åtkomst till data. Dessa åtgärder får emellertid varken diskriminera mellan datamottagare eller hindra användarnas eller datamottagarnas åtkomst till eller användning av data. Om en datamottagare använder otillbörliga metoder, såsom vilseledande av datahållaren genom att tillhandahålla falsk information med uppsåt att använda data för olagliga ändamål, inbegripet utveckling av en konkurrerande uppkopplad produkt på grundval av dessa data, kan datahållaren och, i tillämpliga fall och om det inte rör sig om samma person, innehavaren av en företagshemlighet eller dataanvändaren begära att den tredje parten eller datamottagaren utan oskäligt dröjsmål ska vidta korrigerande eller avhjälpande åtgärder. Alla sådana begäranden, särskilt begäranden om att avsluta produktion, erbjudande eller utsläppande på marknaden av varor, härledda data eller tjänster samt begäranden om att avsluta import, export eller lagring av varor som innebär intrång eller om att förstöra dem, bör bedömas mot bakgrund av deras proportionalitet i förhållande till intressena hos datahållaren, innehavaren av en företagshemlighet eller användaren.

(58) Om en part har en starkare förhandlingsposition finns det en risk för att den kan utnyttja denna till nackdel för den andra avtalsslutande parten vid förhandlingarna om åtkomst till data så att åtkomsten till dessa data blir mindre affärsmässigt lönsam eller till och med ekonomiskt oöverkomlig. Sådana avtalsmässiga obalanser skadar alla företag som saknar en meningsfull förmåga att förhandla om villkoren för åtkomst till data och som kanske inte har något annat val än att godta de avtalsvillkor som de erbjuds. Därför bör oskäliga avtalsvillkor för åtkomst till och användning av data eller avtalsrättsligt ansvar och rättsmedel vid överträdelse eller uppsägning av datarelaterade skyldigheter inte vara bindande för företag när dessa villkor åläggs dessa företag ensidigt.

(59) Regler om avtalsvillkor bör ta hänsyn till principen om avtalsfrihet som ett grundläggande begrepp i förbindelserna mellan företag. Därför bör inte alla avtalsvillkor omfattas av en skälighetsprövning utan endast de villkor som ensidigt åläggs. Detta omfattar situationer där en part tillhandahåller ett visst avtalsvillkor och det andra företaget inte kan påverka innehållet i detta villkor trots ett förhandlingsförsök. Ett avtalsvillkor som helt enkelt föreskrivs av en part och godtas av det andra företaget eller ett villkor som förhandlats fram och sedan i ändrad lydelse godkänns av de avtalsslutande parterna bör inte anses som ensidigt ålagt.

(60) Dessutom bör reglerna om oskäliga avtalsvillkor tillämpas endast på de delar av ett avtal som rör tillgängliggörandet av data, alltså avtalsvillkor som rör åtkomst till och användning av data samt avtalsrättsligt ansvar och rättsmedel vid överträdelse eller uppsägning av datarelaterade skyldigheter. Andra delar av samma avtal, som inte rör tillgängliggörandet av data, bör inte vara föremål för skälighetsprövningen enligt denna förordning.

(61) Kriterier för identifiering av oskäliga avtalsvillkor bör endast tillämpas på orimliga avtalsvillkor, i de fall då en starkare förhandlingsposition har missbrukats. De allra flesta avtalsvillkor som affärsmässigt gynnar en part mer än en annan, inbegripet sådana som är normala i avtal mellan företag, är ett normalt uttryck för principen om avtalsfrihet och fortsätter att gälla. Att i hög grad avvika från god affärssed omfattar i denna förordning bland annat att objektivt försämra möjligheten för den part som ensidigt har ålagts villkoret att skydda sitt berättigade kommersiella intresse av de data som berörs.

(62) För att säkerställa rättssäkerheten fastställs i denna förordning en förteckning över villkor som alltid anses vara oskäliga och en förteckning över villkor som antas vara oskäliga. I det senare fallet bör det företag som inför avtalsvillkoret kunna motbevisa presumtionen om oskälighet genom att visa att det avtalsvillkor som anges i förteckningen i denna förordning inte är oskäligt i det konkreta fallet. Om ett avtalsvillkor inte finns med i förteckningen över villkor som alltid anses vara oskäliga eller som antas vara oskäliga bör den allmänna oskälighetsbestämmelsen gälla. I detta hänseende bör de villkor som förtecknas som oskäliga avtalsvillkor i denna förordning fungera som måttstock för tolkningen av den allmänna oskälighetsbestämmelsen. Slutligen kan också icke-bindande standardavtalsvillkor för datadelningsavtal mellan företag som utarbetas och rekommenderas av kommissionen vara till hjälp för affärspartner som förhandlar fram avtal. Om ett avtalsvillkor förklaras vara oskäligt bör det berörda avtalet fortsätta att gälla utan detta villkor, såvida inte det oskäliga avtalsvillkoret inte kan avskiljas från övriga avtalsvillkor.

(63) Vid situationer då det finns exceptionella behov kan det vara nödvändigt för offentliga organ, kommissionen, Europeiska centralbanken eller unionsorgan att vid fullgörandet av sina lagstadgade skyldigheter av allmänt intresse använda befintliga data, i förekommande fall inbegripet åtföljande metadata, för att hantera ett allmänt nödläge eller andra exceptionella situationer. Exceptionella behov är omständigheter som är oförutsebara och tidsbegränsade, till skillnad från andra omständigheter som kan vara planerade, schemalagda, periodiska eller ofta förekommande. Begreppet datahållare omfattar i allmänhet inte offentliga organ, men det kan omfatta offentliga företag. Organisationer som bedriver forskning och organisationer som finansierar forskning kan också organiseras som offentliga organ eller offentligrättsliga organ. För att minska bördan för företag bör mikroföretag och små företag endast omfattas av skyldigheten att förse offentliga organ, kommissionen, Europeiska centralbanken eller unionsorgan med data i situationer då det finns exceptionella behov om sådana data krävs för att hantera ett allmänt nödläge och det offentliga organet, kommissionen, Europeiska centralbanken eller unionsorganet inte i tid, på ett ändamålsenligt sätt och på likvärdiga villkor kan erhålla sådana data på alternativa sätt.

(64) Vid allmänna nödlägen, såsom hot mot folkhälsan, nödsituationer till följd av naturkatastrofer, inbegripet sådana som förvärras av klimatförändringar och miljöförstöring, samt vid större katastrofer orsakade av människor, såsom större cybersäkerhetsincidenter, bör allmänintresset av dataanvändningen väga tyngre än datahållarnas intresse av att fritt förfoga över de data de innehar. I sådana fall bör datahållare åläggas att göra dessa data tillgängliga för offentliga organ, kommissionen, Europeiska centralbanken eller unionsorgan på deras begäran. Förekomsten av ett allmänt nödläge bör fastställas eller förklaras i enlighet med unionsrätten eller nationell rätt och på grundval av relevanta förfaranden, inbegripet berörda internationella organisationers förfaranden. I sådana fall bör det offentliga organet visa att de data som omfattas av begäran annars inte skulle kunna erhållas i tid, på ett ändamålsenligt sätt och på likvärdiga villkor, till exempel genom ett annat företags frivilliga tillhandahållande av data eller genom sökning i en offentlig databas.

(65) Ett exceptionellt behov kan också bero på andra situationer än nödlägen. I sådana fall bör ett offentligt organ, kommissionen, Europeiska centralbanken eller ett unionsorgan ha rätt att begära endast icke-personuppgifter. Det offentliga organet bör visa att dessa data är nödvändiga för att utföra en specifik uppgift av allmänt intresse som uttryckligen föreskrivs i lag, såsom framställningen av officiell statistik eller begränsning av eller återhämtning från ett allmänt nödläge. En sådan begäran kan dessutom göras endast när det offentliga organet, kommissionen, Europeiska centralbanken eller ett unionsorgan har identifierat specifika data som annars inte skulle kunna erhållas i tid, på ett ändamålsenligt sätt eller på likvärdiga villkor och har uttömt alla andra till buds stående medel för att erhålla sådana data, till exempel att erhålla data genom frivilliga avtal, inbegripet att köpa in icke-personuppgifter på marknaden genom att erbjuda marknadspris, eller att förlita sig på befintliga skyldigheter att göra data tillgängliga eller att anta nya lagstiftningsåtgärder som skulle kunna säkerställa att data finns tillgängliga i tid. Sådana villkor och principer för begäranden som rör ändamålsbegränsning, proportionalitet, transparens och tidsbegränsning bör också tillämpas. När det gäller begäranden om data som är nödvändiga för framställning av officiell statistik bör det begärande offentliga organet också visa huruvida det enligt nationell rätt har rätt att köpa in icke-personuppgifter på marknaden.

(66) Denna förordning bör inte tillämpas på eller föregripa frivilliga arrangemang för utbyte av data mellan privata och offentliga enheter, inbegripet mikroföretags och små och medelstora företags tillhandahållande av data, och påverkar inte tillämpningen av unionsrättsakter som föreskriver att offentliga enheter ska begära information från privata enheter. Skyldigheter för datahållare att tillhandahålla data som motiveras av behov av icke-exceptionell art, i synnerhet när datauppsättningen och datahållarna är kända eller dataanvändningen kan ske regelbundet, såsom är fallet med rapporteringsskyldigheter och skyldigheter kopplade till den inre marknaden, bör inte påverkas av denna förordning. Kraven på åtkomst till data för kontroll av efterlevnaden av tillämpliga regler, även då offentliga organ anförtror efterlevnadskontrollen åt andra enheter än offentliga organ, bör inte heller påverkas av denna förordning.

(67) Denna förordning kompletterar, och påverkar inte tillämpningen av, unionsrätt och nationell rätt om åtkomst till och användning av data för statistiska ändamål, särskilt Europaparlamentets och rådets förordning (EG) nr 223/2009 ([27]) samt nationella rättsakter som rör officiell statistik.

(68) Offentliga organ, kommissionen, Europeiska centralbanken eller unionsorgan bör förlita sig på sina befogenheter enligt unionsrätten eller nationell rätt för utövandet av sina uppgifter när det gäller förebyggande, förhindrande, utredning, upptäckt eller lagföring av brott eller administrativa förseelser eller verkställandet av straffrättsliga och administrativa påföljder samt insamlingen av data för skatte- eller tulländamål. Denna förordning påverkar därmed inte lagstiftningsakter om delning eller användning av data eller åtkomst till data inom dessa områden.

(69) I enlighet med artikel 6.1 och 6.3 i förordning (EU) 2016/679 är en proportionell, begränsad och förutsebar ram på unionsnivå nödvändig när den rättsliga grunden föreskrivs för datahållares tillhandahållande av data, vid exceptionella behov, till offentliga organ, kommissionen, Europeiska centralbanken eller unionsorgan, både för att säkerställa rättssäkerhet och för att minimera de administrativa bördorna för företagen. Därför bör begäranden avseende dataåtkomst från offentliga organ, kommissionen, Europeiska centralbanken eller unionsorgan till datahållare vara specifika, transparenta och proportionella i fråga om innehållets omfång och detaljrikedom. Begärans syfte och den avsedda användningen av begärda data bör specificeras och förklaras tydligt, med tillräckligt utrymme för den begärande enheten att utföra sina specifika uppgifter i allmänhetens intresse på ett flexibelt sätt. Begäran bör också respektera legitima intressen hos den datahållare som mottar begäran. Datahållarnas börda bör minimeras genom att begärande enheter åläggs att iaktta engångsprincipen, som förhindrar att samma data begärs mer än en gång av mer än ett offentligt organ, kommissionen, Europeiska centralbanken eller unionsorgan. För att säkerställa transparens bör begäranden om data som görs av kommissionen, Europeiska centralbanken eller unionsorgan offentliggöras utan oskäligt dröjsmål av den enhet som begär dessa data. Europeiska centralbanken och unionsorgan bör underrätta kommissionen om sina begäranden. Om begäran om data har gjorts av ett offentligt organ bör det organet även underrätta datasamordnaren i den medlemsstat där det offentliga organet är etablerat. Det bör säkerställas att alla begäranden finns tillgängliga online. Efter mottagandet av en underrättelse om en begäran om data kan den behöriga myndigheten besluta att bedöma om begäran är lagenlig och utöva sina uppgifter i samband med verkställandet och tillämpningen av den här förordningen. Datasamordnaren bör säkerställa att alla begäranden som gjorts av offentliga organ är tillgängliga online.

(70) Syftet med skyldigheten att tillhandahålla data är att säkerställa att offentliga organ, kommissionen, Europeiska centralbanken eller unionsorgan har den kunskap som krävs för att hantera, förhindra eller bidra till återhämtningen från allmänna nödlägen eller att bidra till fullgörandet av de specifika uppgifter som uttryckligen föreskrivs i lag. De data som erhålls av dessa enheter kan vara affärsmässigt känsliga. Därför bör varken förordning (EU) 2022/868 eller Europaparlamentets och rådets direktiv (EU) 2019/1024 ([28]) tillämpas på data som tillhandahålls enligt den här förordningen och bör inte anses som öppna data som är tillgängliga för vidareutnyttjande av tredje parter. Detta bör dock inte påverka tillämpligheten för direktiv (EU) 2019/1024 på vidareutnyttjandet av officiell statistik där data som erhållits enligt den här förordningen har använts för framtagandet, förutsatt att vidareutnyttjandet inte inkluderar de data som finns i underlaget. Förutsatt att villkoren i den här förordningen uppfylls bör möjligheten till utbyte av data för forskningsändamål eller för utveckling, framställning och spridning av officiell statistik inte påverkas. Offentliga organ bör också ha rätt att utbyta data som erhållits enligt den här förordningen med andra offentliga organ, kommissionen, Europeiska centralbanken eller unionsorgan för att hantera de exceptionella behov som begäran om data avser.

([27]) Europaparlamentets och rådets förordning (EG) nr 223/2009 av den 11 mars 2009 om europeisk statistik och om upphävande av Europaparlamentets och rådets förordning (EG, Euratom) nr 1101/2008 om utlämnande av insynsskyddade statistiska uppgifter till Europeiska gemenskapernas statistikkontor, rådets förordning (EG) nr 322/97 om gemenskapsstatistik och rådets beslut 89/382/EEG, Euratom om inrättande av en kommitté för Europeiska gemenskapernas statistiska program (EUT L 87, 31.3.2009, s. 164).

([28]) Europaparlamentets och rådets direktiv (EU) 2019/1024 av den 20 juni 2019 om öppna data och vidareutnyttjande av information från den offentliga sektorn (EUT L 172, 26.6.2019, s. 56).

(71) Datahållare bör ha möjlighet att antingen avslå en begäran som gjorts av ett offentligt organ, kommissionen, Europeiska centralbanken eller ett unionsorgan eller begära en ändring av den utan onödigt dröjsmål och under alla omständigheter senast inom fem eller 30 arbetsdagar, beroende på vilken typ av exceptionellt behov som åberopas i begäran. I förekommande fall bör datahållaren ha denna möjlighet om den inte har kontroll över de data som begärts, det vill säga om den inte har omedelbar tillgång till datan och inte kan avgöra dess tillgänglighet. Ett giltigt skäl till att inte göra data tillgängliga bör föreligga om det kan visas att begäran liknar en tidigare begäran för samma ändamål som gjorts av ett annat offentligt organ eller, kommissionen, Europeiska centralbanken eller ett unionsorgan och datahållaren har underrättats om radering av data enligt denna förordning. En datahållare som avvisar begäran eller begär en ändring av den bör meddela den motivering som ligger till grund för detta till det offentliga organ, kommissionen, Europeiska centralbanken eller ett unionsorgan som begär data. I de fall då rätten av sitt eget slag avseende databaser enligt Europaparlamentets och rådets direktiv 96/9/EG ([29]) gäller för de datamängder som begärts, bör datahållare utöva sina rättigheter på ett sådant sätt att det inte hindrar ett offentligt organ, kommissionen, Europeiska centralbanken eller ett unionsorgan från att erhålla dessa data eller från att dela dessa data, i enlighet med denna förordning.

(72) I händelse av ett exceptionellt behov i samband med hantering av ett allmänt nödläge bör offentliga organ om möjligt använda icke-personuppgifter. Vid begäranden som grundar sig på ett exceptionellt behov som inte rör ett allmänt nödläge får personuppgifter inte begäras. När personuppgifter omfattas av begäran bör datahållaren anonymisera datan. När det är strikt nödvändigt att inkludera personuppgifter i de data som görs tillgängliga för ett offentligt organ, kommissionen, Europeiska centralbanken eller ett unionsorgan, eller när anonymisering visar sig vara omöjlig, bör den enhet som begär uppgifterna visa att det är strikt nödvändigt och att behandlingen sker för specifika och begränsade ändamål. De tillämpliga reglerna om skydd av personuppgifter bör följas. Vid tillhandahållandet och den senare användningen av dessa data bör det finnas skyddsåtgärder avseende rättigheterna och intressena för de individer som berörs av uppgifterna.

(73) Data som görs tillgängliga för offentliga organ, kommissionen, Europeiska centralbanken eller unionsorgan baserat på ett exceptionellt behov bör endast användas för de ändamål som de begärdes för, om inte den datahållare som gjorde uppgifterna tillgängliga uttryckligen godkänt att de används för andra ändamål. Dessa data bör raderas när de inte längre behövs för de ändamål som anges i begäran, om inte annat överenskommits, och datahållaren bör underrättas om detta. Denna förordning bygger på de befintliga bestämmelserna om tillgång i unionen och medlemsstaterna och ändrar inte nationell rätt om allmänhetens tillgång till handlingar inom ramen för insynsskyldigheter. Data bör raderas när de inte längre behövs för att uppfylla sådana insynsskyldigheter.

(74) Vid vidareutnyttjande av data som tillhandahållits av datahållare bör offentliga organ, kommissionen, Europeiska centralbanken eller unionsorgan iaktta både befintlig tillämplig unionsrätt eller nationell rätt och avtalsskyldigheter som datahållaren omfattas av. De bör avstå från att utveckla eller förbättra en uppkopplad produkt eller tillhörande tjänst som konkurrerar med datahållarens uppkopplade produkt eller tillhörande tjänst samt från att dela data med en tredje part för dessa ändamål. De bör även ge datahållarna offentligt erkännande på deras begäran och bör ansvara för att mottagna datas säkerhet upprätthålls. När röjandet av datahållarens företagshemligheter för offentliga organ, kommissionen, Europeiska centralbanken eller unionsorgan är strikt nödvändig för uppfyllandet av det ändamål för vilka data har begärts, bör konfidentialiteten för sådant röjande garanteras innan uppgifterna röjs.

(75) När skydd av en betydande kollektiv nyttighet berörs, som vid hantering av ett allmänt nödläge, bör det offentliga organ, kommissionen, Europeiska centralbanken eller det unionsorgan som berörs inte förväntas ersätta företagen för de data som erhålls. Allmänna nödlägen är ovanliga händelser och det är inte alla sådana nödlägen som kräver användning av data som innehas av företag. Samtidigt kan skyldigheten att tillhandahålla data utgöra en betydande börda för mikroföretag och små företag. De bör därför ha rätt att kräva ersättning även i samband med hantering av ett allmänt nödläge. Datahållarnas affärsverksamhet kommer därför sannolikt inte påverkas negativt av att offentliga

([29]) Europaparlamentets och rådets direktiv 96/9/EG av den 11 mars 1996 om rättsligt skydd för databaser (EGT L 77, 27.3.1996, s. 20).

organ, kommissionen, Europeiska centralbanken eller unionsorgan använder sig av denna förordning. Fall som rör andra exceptionella behov än hantering av allmänna nödlägen är förmodligen vanligare, och därför bör datahållare i sådana fall ha rätt till rimlig ersättning som inte bör överstiga de tekniska och organisatoriska kostnaderna för att tillgodose begäran och den rimliga marginal som krävs för att göra data tillgängliga för det offentliga organet, kommissionen, Europeiska centralbanken eller unionsorganet. Ersättningen bör inte anses utgöra betalning för själva uppgifterna eller anses obligatorisk. Datahållare bör inte kunna kräva ersättning om nationell rätt hindrar nationella statistikbyråer eller andra nationella myndigheter med ansvar för statistikframställning från att kompensera datahållare för att de gör data tillgängliga. Det offentliga organet, kommissionen, Europeiska centralbanken eller det berörda unionsorganet bör kunna ifrågasätta den ersättningsnivå som datahållaren begär genom att hänskjuta ärendet till den behöriga myndigheten i den medlemsstat där datahållaren är etablerad.

(76) Ett offentligt organ, kommissionen, Europeiska centralbanken eller ett unionsorgan bör ha rätt att dela de data som erhållits till följd av en begäran med andra enheter eller personer när det är nödvändigt för genomförandet av forskningsverksamhet eller analysverksamhet som de själva inte kan utföra, under förutsättning att sådan verksamhet är förenlig med det ändamål för vilket data begärdes. De bör i god tid informera datahållaren om sådan delning. Sådana data får också under samma omständigheter delas med de nationella statistikbyråerna och Eurostat för utveckling, framställning och spridning av officiell statistik. Denna forskningsverksamhet bör dock vara förenlig med det ändamål som uppgifterna begärdes för och datahållaren bör underrättas om vidare delning av de data som tillhandahållits. De individer som bedriver forskning eller de forskningsorganisationer med vilka dessa data får delas bör agera antingen på icke vinstdrivande grund eller inom ramen för ett uppdrag i det allmännas intresse som erkänns av staten. Organisationer över vilka kommersiella företag har ett avsevärt inflytande, som innebär att de kan utöva kontroll på grund av strukturella situationer, vilket skulle kunna medföra förmånstillträde till forskningsresultat, bör inte anses som forskningsorganisationer vid tillämpningen av denna förordning.

(77) När ett gränsöverskridande allmänt nödläge eller ett annat exceptionellt behov ska hanteras får begäranden om data riktas till datahållare i andra medlemsstater än den där det begärande offentliga organet är beläget. I ett sådant fall bör det begärande offentliga organet underrätta den behöriga myndigheten i den medlemsstat där datahållaren är etablerad, så att den kan pröva begäran mot de kriterier som fastställs i denna förordning. Detsamma bör gälla ansökningar från kommissionen, Europeiska centralbanken eller ett unionsorgan. Om personuppgifter begärs bör det offentliga organet underrätta den tillsynsmyndighet som ansvarar för att övervaka tillämpningen av förordning (EU) 2016/679 i den medlemsstat där det offentliga organet är etablerat. Den berörda behöriga myndigheten bör ha rätt att råda det offentliga organet, kommissionen, Europeiska centralbanken eller unionsorganet att samarbeta med de offentliga organen i den medlemsstat där datahållaren är etablerad om behovet av att säkerställa en minimal administrativ börda för datahållaren. När den behöriga myndigheten har motiverade invändningar vad gäller begärans förenlighet med den här förordningen bör den avslå begäran från det offentliga organet, kommissionen, Europeiska centralbanken eller unionsorganet, som bör beakta dessa invändningar innan ytterligare åtgärder vidtas, inbegripet en inlämning på nytt av begäran.

(78) Möjligheten för kunder av databehandlingstjänster, inbegripet molntjänster och edgetjänster, att byta från en databehandlingstjänst till en annan och samtidigt behålla en miniminivå av tjänstefunktioner utan att tjänsterna drabbas av driftstopp, eller att använda flera leverantörers tjänster samtidigt utan onödiga hinder och kostnader för dataöverföring, är ett centralt villkor för en mer konkurrenspräglad marknad med lägre inträdeshinder för nya leverantörer av databehandlingstjänster och för en säkerställd ytterligare motståndskraft hos användarna av dessa tjänster. Kunder som omfattas av kostnadsfria erbjudanden bör också omfattas av de bestämmelser om byte som fastställs i denna förordning, så att dessa erbjudanden inte leder till en inlåsningssituation för kunderna.

(79) Europaparlamentets och rådets förordning (EU) 2018/1807 ([30]) uppmuntrar leverantörer av databehandlingstjänster att utveckla och effektivt genomföra självreglerande uppförandekoder som omfattar bästa praxis när det gäller bland annat att underlätta byten av leverantör av databehandlingstjänster och dataportering. Mot bakgrund av att de självregleringsramar som utvecklades till följd av detta har fått begränsad användning, och den allmänna avsaknaden av öppna standarder och gränssnitt, är det nödvändigt att anta ett antal minimiregleringsskyldigheter för leverantörer av databehandlingstjänster för att undanröja förkommersiella, kommersiella, tekniska, avtalsmässiga, ekonomiska och organisatoriska hinder, vilka inte är begränsade till begränsad dataöverföringshastighet vid kundens utträde, som hindrar effektiva byten av databehandlingstjänster.

(80) Databehandlingstjänster bör omfatta tjänster som möjliggör allmän nätverkstillgång på begäran till en konfigurerbar, skalbar och elastisk gemensam pool av distribuerade dataresurser. Dessa dataresurser innefattar sådana resurser som nät, servrar eller annan virtuell eller fysisk infrastruktur, programvara, inbegripet verktyg för programvaruutveckling, samt lagring, applikationer och tjänster. Databehandlingstjänstens kunds förmåga att ensidigt självständigt tillhandahålla datorkapacitet, såsom servertid eller nätlagring, utan någon mänsklig medverkan från leverantören av databehandlingstjänster, kan beskrivas som att den kräver minsta möjliga administration och som att den innehåller minsta möjliga interaktion mellan leverantör och kund. Termen *allmän* används för att beskriva den datorkapacitet som tillhandahålls över nätet och som nås genom mekanismer som främjar användning av heterogena tunna eller tjocka klientplattformar (däribland webbläsare, mobilenheter och arbetsstationer). Termen *skalbar* avser datorresurser som leverantören av databehandlingstjänster fördelar på ett flexibelt sätt, oberoende av resursernas geografiska läge, för att hantera fluktuationer i efterfrågan. Termen *elastisk* används för att beskriva datorresurser som avsätts och utnyttjas beroende på efterfrågan för att tillgängliga resurser snabbt ska kunna utökas eller minskas i takt med arbetsbördan. Termen *gemensam pool* används för att beskriva datorresurser som tillhandahålls flera användare som delar en gemensam åtkomst till tjänsten, men där behandlingen genomförs separat för varje användare, även om tjänsten tillhandahålls från samma elektroniska utrustning. Termen *distribuerad* används för att beskriva de datorresurser som finns på olika nätverksanslutna datorer eller enheter och som kommunicerar och samordnar sig sinsemellan genom meddelandepassning. Termen *mycket distribuerad* används för att beskriva databehandlingstjänster som involverar databehandling som sker närmare den plats där data genereras eller samlas in, exempelvis i en uppkopplad databehandlingsenhet. *Edge computing*, som är en form av sådan mycket distribuerad databehandling, förväntas generera nya affärsmodeller och modeller för leverans av molntjänster, som bör vara öppna och interoperabla från början.

(81) Det allmänna begreppet *databehandlingstjänster* omfattar ett stort antal tjänster med ett mycket brett spektrum av olika ändamål, funktioner och tekniska upplägg. Såsom det allmänt förstås av leverantörer och användare och i linje med vedertagna standarder, gäller databehandlingstjänster en eller flera av följande tre modeller för leverans av databehandlingstjänster, nämligen infrastruktur som en tjänst (Iaas), plattform som en tjänst (Paas) och programvara som en tjänst (SaaS). Dessa tjänsteleveransmodeller utgör en specifik, färdigförpackad kombination av IKT-resurser som erbjuds av en leverantör av databehandlingstjänster. Dessa tre grundläggande modeller för leverans av databehandling kompletteras ytterligare med nya varianter, som var och en består av en särskild kombination av IKT-resurser, såsom lagring som en tjänst och databas som en tjänst. Databehandlingstjänster kan kategoriseras på grundval av ytterligare detaljrikedom och delas in i en icke uttömmande förteckning över uppsättningar av databehandlingstjänster som har samma primära syfte och huvudsakliga funktioner samt samma typ av databehandlingsmodeller, vilka inte är kopplade till tjänstens operativa egenskaper (samma tjänstetyp). Tjänster som är av samma tjänstetyp kan ha samma modell för databehandlingstjänster, men två databaser kan förefalla ha samma primära syfte, men med beaktande av deras databehandlingsmodell, distributionsmodell och de användningsfall som de riktar sig till skulle sådana databaser kunna ingå i en mer detaljerad underkategori av liknande tjänster. Tjänster av samma tjänstetyp kan ha olika och konkurrerande egenskaper såsom prestanda, säkerhet, motståndskraft och tjänstekvalitet.

([30]) Europaparlamentets och rådets förordning (EU) 2018/1807 av den 14 november 2018 om en ram för det fria flödet av andra data än personuppgifter i Europeiska unionen (EUT L 303, 28.11.2018, s. 59).

(82) Att undergräva utvinningen av de exporterbara data som tillhör kunden från den ursprungliga leverantören av databehandlingstjänster kan hindra återställandet av tjänstefunktionerna i infrastrukturen hos destinationsleverantören av databehandlingstjänster. För att underlätta kundens utträdesstrategi, undvika onödiga och betungande uppgifter och säkerställa att kunden inte förlorar några av sina data till följd av bytesprocessen bör den ursprungliga leverantören av databehandlingstjänster i förväg informera kunden om omfattningen av de data som kan exporteras när den kunden väl beslutar sig för att byta till en annan tjänst som tillhandahålls av en annan leverantör av databehandlingstjänster eller gå över till lokal IKT-infrastruktur. Exporterbara data bör åtminstone omfatta in- och utdata, inklusive metadata, som direkt eller indirekt genereras eller samgenereras genom kundens användning av databehandlingstjänsten, med undantag för tillgångar eller data som tillhör leverantören av databehandlingstjänster eller en tredje part. Exporterbara data bör inte omfatta sådana tillgångar eller data som tillhör leverantören av databehandlingstjänster eller tredje parter och som omfattas av immateriella rättigheter eller utgör företagshemligheter för den leverantören eller den tredje parten, eller data med anknytning till tjänstens integritet och säkerhet, vars export kommer att utsätta leverantörerna av databehandlingstjänster för cybersäkerhetssårbarheter. Dessa undantag bör inte hindra eller försena bytesprocessen.

(83) Digitala tillgångar avser element i digitalt format för vilka kunden har nyttjanderätten, inbegripet applikationer och metadata som rör konfigurering av inställningar, säkerhet och förvaltning av åtkomst- och kontrollrättigheter, och andra element såsom uttryck för virtualiseringsteknik, inbegripet virtuella maskiner och behållare. Digitala tillgångar kan överföras om kunden har nyttjanderätt oberoende av avtalsförhållandet med den databehandlingstjänst som kunden avser att byta från. Dessa andra element är avgörande för en effektiv användning av kundens data och applikationer i miljön hos destinationsleverantören av databehandlingstjänster.

(84) Denna förordning syftar till att underlätta byten av databehandlingstjänster, på ett sätt som omfattar villkor och åtgärder som är nödvändiga för att en kund ska kunna avsluta ett avtal om en databehandlingstjänst, ingå ett eller flera nya avtal med olika leverantörer av databehandlingstjänster, portera sina exporterbara data och digitala tillgångar, och när så är tillämpligt, dra nytta av funktionell likvärdighet.

(85) Byte är en kundstyrd process som består av flera steg, inbegripet datautvinning, vilket avser nedladdning av data från ekosystemet hos en ursprunglig leverantör av databehandlingstjänster, anpassning, om data är strukturerade på ett sätt som inte överensstämmer med målplatsens schema, och uppladdning av data till en ny destination. I en specifik situation som beskrivs i denna förordning bör separation av en viss tjänst från avtalet och överföring av den till en annan leverantör också betraktas som byte. Bytesprocessen hanteras ibland för kundens räkning av en tredjepartsenhet. Därför bör kundens alla rättigheter och skyldigheter som fastställs i denna förordning, inbegripet skyldigheten att samarbeta i god tro, anses vara tillämpliga på en sådan tredjepartsenhet under dessa omständigheter. Leverantörer av databehandlingstjänster och kunder har olika ansvarsnivåer, beroende på de olika stegen i den process som avses. Exempelvis ansvarar den ursprungliga leverantören av databehandlingstjänster för utvinning av data i ett maskinläsbart format, men det åligger kunden och destinationsleverantören av databehandlingstjänster att ladda upp data till den nya miljön, såvida inte en särskild, professionell övergångstjänst har erhållits. En kund som avser att utöva rättigheter rörande ett byte, vilka föreskrivs i denna förordning, bör informera den ursprungliga leverantören av databehandlingstjänster om beslutet att antingen byta till en annan leverantör av databehandlingstjänster, byta till lokal IKT-infrastruktur eller radera kundens tillgångar och radera dennes exporterbara data.

(86) Funktionell likvärdighet innebär att man på grundval av kundens exporterbara data och digitala tillgångar återställer en miniminivå av funktionalitet i miljön för en ny databehandlingstjänst av samma tjänstetyp efter ett byte, där destinationstjänsten för databehandling levererar ett väsentligen jämförbart resultat som svar på samma input för delade funktioner som tillhandahålls kunden enligt avtalet. Leverantörer av databehandlingstjänster kan endast förväntas underlätta funktionell likvärdighet för de funktioner som både de ursprungliga tjänsterna och destinationstjänsterna för databehandling erbjuder oberoende av varandra. Denna förordning medför inte en skyldighet att underlätta funktionell likvärdighet för andra leverantörer av databehandlingstjänster än de som erbjuder tjänster enligt IaaS-leveransmodellen.

(87) Databehandlingstjänster används inom olika sektorer och varierar i fråga om komplexitet och tjänstetyp. Detta är en viktig aspekt när det gäller porteringsprocessen och tidsramarna. En förlängning av övergångsperioden på grund av att det är tekniskt omöjligt att slutföra bytesprocessen inom den givna tidsramen bör dock endast åberopas i vederbörligen motiverade fall. Bevisbördan i detta avseende bör helt och hållet ligga på leverantören av den berörda databehandlingstjänsten. Detta påverkar inte kundens ensamrätt att förlänga övergångsperioden en gång med en tidsperiod som kunden anser lämpligare för sina egna behov. Kunden får åberopa denna rätt till förlängning före eller under övergångsperioden, med beaktande av att avtalet fortfarande är tillämpligt under övergångsperioden.

(88) Bytesavgifter är sådana avgifter som leverantörer av databehandlingstjänster debiterar sina kunder för bytesprocessen. Syftet med dessa avgifter är vanligen att föra vidare de kostnader som den ursprungliga leverantören av databehandlingstjänster kan komma att ådra sig på grund av bytesprocessen till den kund som vill byta leverantör. Vanliga exempel på bytesavgifter är kostnader som rör överföringen av data från en leverantör till en annan leverantör av databehandlingstjänster eller till lokal IKT-infrastruktur (uttagsavgifter för data) eller kostnader för särskilda stödåtgärder under bytesprocessen. Onödigt höga uttagsavgifter för data och andra omotiverade avgifter utan anknytning till faktiska byteskostnader hindrar kunderna från att byta, begränsar det fria flödet av data, riskerar att begränsa konkurrensen samt skapar inlåsningseffekter för kunderna genom att de minskar incitamenten att välja en annan eller ytterligare en tjänsteleverantör. Bytesavgifter bör därför avskaffas tre år från dagen för denna förordnings ikraftträdande. Leverantörer av databehandlingstjänster bör kunna ta ut nedsatta bytesavgifter till och med den dagen.

(89) En ursprunglig leverantör av databehandlingstjänster bör kunna utkontraktera vissa uppgifter och ersätta tredjepartsenheter för att fullgöra de skyldigheter som föreskrivs i denna förordning. En kund bör inte bära de kostnader som uppstår till följd av utkontraktering av tjänster som ingåtts av den ursprungliga leverantören av databehandlingstjänster under bytesprocessen, och sådana kostnader bör betraktas som omotiverade såvida de inte täcker arbete som utförs av leverantören av databehandlingstjänster på kundens begäran för ytterligare stöd i bytesprocessen som går utöver leverantörens bytesskyldigheter enligt vad som uttryckligen föreskrivs i denna förordning. Ingenting i denna förordning hindrar en kund från att ersätta tredjepartsenheter för stöd i migreringsprocessen eller parter från att komma överens om avtal om databehandlingstjänster med en fast löptid, inbegripet proportionella straffavgifter för förtida uppsägning för att täcka förtida uppsägning av dessa avtal, i enlighet med unionsrätten eller nationell rätt. För att främja konkurrens bör det gradvisa avskaffandet av de avgifter som hör ihop med bytet mellan olika leverantörer av databehandlingstjänster specifikt omfatta avskaffandet av de uttagsavgifter för data som en leverantör av databehandlingstjänst debiterar en kund. Standardavgifter för tillhandahållandet av själva databehandlingstjänsterna är inte bytesavgifter. Dessa standardavgifter är inte föremål för avskaffande och gäller fram till dess att avtalet om tillhandahållande av relevant tjänst upphör att gälla. Denna förordning gör det möjligt för kunden att begära tillhandahållande av ytterligare tjänster som går utöver leverantörens bytesskyldigheter enligt denna förordning. Dessa ytterligare tjänster kan utföras och debiteras av leverantören när de utförs på kundens begäran och kunden samtycker till priset för dessa tjänster i förväg.

(90) Det krävs en ambitiös och innovationsfrämjande regleringsstrategi för interoperabilitet för att råda bot på inlåsning till en säljare, som undergräver både konkurrensen och utvecklingen av nya tjänster. Interoperabilitet mellan databehandlingstjänster involverar flera olika gränssnitt och lager av infrastruktur och programvara och kan sällan reduceras till ett binärt test av om interoperabilitet är möjlig eller inte. I stället blir uppbyggnaden av sådan interoperabilitet föremål för en kostnads-nyttoanalys som är nödvändig för att fastställa om det är värt att eftersträva de resultat som rimligen kan förutses. ISO/IEC 19941:2017 utgör en viktig internationell standard som utgör en referens för uppnåendet av målen i denna förordning, eftersom den omfattar tekniska överväganden som klargör komplexiteten i en sådan process.

(91) I de fall då leverantörer av databehandlingstjänster i sin tur är kunder till databehandlingstjänster som tillhandahålls av en tredjepartsleverantör, kommer de själva att omfattas av effektivare byten, samtidigt som de fortfarande är bundna av denna förordnings skyldigheter när det gäller det egna tjänsteutbudet.

(92) Leverantörer av databehandlingstjänster bör åläggas att erbjuda allt bistånd och stöd som de har kapacitet till, i proportion till deras respektive skyldigheter, som krävs för att göra bytesprocessen till en tjänst hos en annan leverantör av databehandlingstjänster framgångsrik, effektiv och säker. Denna förordning kräver inte att leverantörer av databehandlingstjänster utvecklar nya kategorier av databehandlingstjänster, inbegripet inom eller på grundval av IKT-infrastrukturen hos andra leverantörer av databehandlingstjänster för att garantera funktionell likvärdighet i en annan miljö än de egna systemen. En ursprunglig leverantör av databehandlingstjänster har inte tillgång till eller inblick i miljön hos destinationsleverantören av databehandlingstjänster. Funktionell likvärdighet bör inte tolkas som en skyldighet för den ursprungliga leverantören av databehandlingstjänster att återuppbygga tjänsten i fråga inom infrastrukturen hos destinationsleverantören av databehandlingstjänster. Den ursprungliga leverantören av databehandlingstjänster bör i stället vidta alla rimliga åtgärder inom ramen för sina befogenheter i syfte att underlätta processen med att uppnå funktionell likvärdighet genom tillhandahållande av kapacitet, adekvat information, dokumentation, tekniskt stöd och, vid behov, de nödvändiga verktygen.

(93) Leverantörer av databehandlingstjänster bör också vara skyldiga att undanröja befintliga hinder och inte införa nya, även för kunder som vill byta till lokal IKT-infrastruktur. Hindren kan bland annat vara förkommersiella, kommersiella, tekniska, avtalsmässiga eller organisatoriska. Leverantörer av databehandlingstjänster bör också vara skyldiga att undanröja hinder för separation av en viss enskild tjänst från andra databehandlingstjänster som tillhandahålls enligt ett avtal och göra den relevanta tjänsten tillgänglig för byte, om det inte finns några större och påvisade tekniska hinder för sådan separation.

(94) Under hela bytesprocessen bör en hög säkerhetsnivå upprätthållas. Detta innebär att den ursprungliga leverantören av databehandlingstjänster bör utöka den säkerhetsnivå som den åtagit sig för tjänsten till att omfatta alla tekniska villkor som leverantören ansvarar för under bytesprocessen, såsom nätanslutningar eller fysiska enheter. Befintliga rättigheter avseende uppsägning av avtal, inbegripet de som infördes genom förordning (EU) 2016/679 och Europaparlamentets och rådets direktiv (EU) 2019/770 ([31]), bör inte påverkas. Den här förordningen bör inte tolkas som att den hindrar en leverantör av databehandlingstjänster från att tillhandahålla sina kunder nya och förbättrade tjänster, egenskaper och funktioner eller från att konkurrera med andra leverantörer av databehandlingstjänster på denna grund.

(95) Den information som leverantörer av databehandlingstjänster ska tillhandahålla kunden skulle kunna stödja kundens utträdesstrategi. Informationen bör omfatta förfaranden för att påbörja ett byte från databehandlingstjänsten, de maskinläsbara dataformat till vilka användarens data kan exporteras, verktygen för export av data, inklusive ett öppet gränssnitt och information om kompabilitet med harmoniserade standarder eller gemensamma specifikationer baserade på öppna interoperabilitetsspecifikationer, information om kända tekniska restriktioner och begränsningar som kan påverka bytesprocessen och den beräknade tid som krävs för att slutföra bytesprocessen.

(96) För att främja interoperabilitet och byten av databehandlingstjänster bör användare och leverantörer av databehandlingstjänster överväga att använda genomförandeverktyg och verktyg för kontroll av efterlevnaden, i synnerhet de som kommissionen offentliggör i form av en *EU Cloud Rulebook* och en vägledning om offentlig upphandling av databehandlingstjänster. Standardavtalsklausuler är särskilt fördelaktiga eftersom de ökar förtroendet för

([31]) Europaparlamentets och rådets direktiv (EU) 2019/770 av den 20 maj 2019 om vissa aspekter på avtal om tillhandahållande av digitalt innehåll och digitala tjänster (EUT L 136, 22.5.2019, s. 1).

databehandlingstjänster, upprättar ett mer balanserat förhållande mellan användare och leverantörer av databehandlingstjänster och förbättrar rättssäkerheten vad gäller de villkor som är tillämpliga på byten till andra databehandlingstjänster. I det sammanhanget bör användare och leverantörer av databehandlingstjänster överväga att använda standardavtalsklausuler eller andra självreglerande verktyg för regelefterlevnad förutsatt att de till fullo uppfyller kraven i denna förordning, som utarbetats av relevanta organ eller expertgrupper som inrättats inom ramen för unionsrätten.

(97) För att underlätta byte av databehandlingstjänster bör alla berörda parter, inbegripet såväl ursprungliga leverantörer som destinationsleverantörer av databehandlingstjänster, samarbeta i god tro för att möjliggöra en effektiv bytesprocess och säker och snabb överföring av nödvändiga data i ett allmänt använt, maskinläsbart format och genom öppna gränssnitt samtidigt som störningar i tjänsten undviks och dess kontinuitet bibehålls.

(98) Databehandlingstjänster som rör tjänster där de flesta av huvudfunktionerna har skräddarsytts för att tillgodose en enskild kunds specifika behov eller där alla komponenter har utvecklats för en enskild kunds ändamål bör undantas från vissa av de skyldigheter som gäller för byte av databehandlingstjänster. Detta bör inte omfatta tjänster som leverantören av databehandlingstjänster erbjuder i stor kommersiell skala via sin tjänstekatalog. Det hör till skyldigheterna för leverantören av databehandlingstjänster att innan ett avtal ingås vederbörligen informera potentiella kunder för sådana tjänster om vilka skyldigheter enligt denna förordning som inte är tillämpliga på de berörda tjänsterna. Ingenting hindrar leverantören av databehandlingstjänster från att så småningom börja erbjuda sådana tjänster i stor skala, i vilket fall den leverantören måste uppfylla alla de skyldigheter avseende byte som anges i denna förordning.

(99) I linje med minimikravet på att tillåta byte mellan leverantörer av databehandlingstjänster syftar denna förordning också till att förbättra interoperabiliteten för parallell användning av flera databehandlingstjänster med kompletterande funktioner. Detta gäller situationer där kunder inte säger upp ett avtal för att byta till en annan leverantör av databehandlingstjänster, utan där flera tjänster från olika leverantörer används parallellt, på ett interoperabelt sätt, för att dra nytta av de kompletterande funktionerna hos de olika tjänsterna i kundens systemstruktur. Det erkänns dock att uttaget av data från en leverantör av databehandlingstjänster till en annan för att underlätta parallell användning av tjänster kan vara en pågående verksamhet, till skillnad från det engångsuttag som behövs som en del av bytesprocessen. Leverantörer av databehandlingstjänster bör därför kunna fortsätta att påföra uttagsavgifter för data, som inte överstiger de uppkomna kostnaderna, för parallell användning efter tre år från dagen för denna förordnings ikraftträdande. Detta är viktigt bland annat för en lyckad spridning av multimolnstrategier, som ger kunderna möjlighet att genomföra framtidssäkrade IKT-strategier och som kan minska beroendet av individuella leverantörer av databehandlingstjänster. Att främja en multimolnstrategi för kunder som använder sig av databehandlingstjänster kan också bidra till att öka deras digitala operativa motståndskraft, vilket erkänts med avseende på institutioner som tillhandahåller finansiella tjänster i Europaparlamentets och rådets förordning (EU) 2022/2554 ([12]).

(100) Öppna interoperabilitetsspecifikationer och standarder som utvecklats i enlighet med bilaga II till Europaparlamentets och rådets förordning (EU) nr 1025/2012 ([13]) på området interoperabilitet och portabilitet förväntas möjliggöra den molnmiljö med flera säljare som är en förutsättning för öppen innovation i den europeiska dataekonomin. Eftersom marknadsgenomslaget för identifierade standarder inom ramen för det initiativ för samordning av molnbaserad standardisering som avslutades 2016 har varit begränsat, är det också nödvändigt att kommissionen förlitar sig på att parterna på marknaden utvecklar relevanta öppna interoperabilitetsspecifikationer för att hålla jämna steg med den snabba tekniska utvecklingen inom denna industri. Sådana öppna interoperabilitets-

([12]) Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 (EUT L 333, 27.12.2022, s. 1).

([13]) Europaparlamentets och rådets förordning (EU) nr 1025/2012 av den 25 oktober 2012 om europeisk standardisering och om ändring av rådets direktiv 89/686/EEG och 93/15/EEG samt av Europaparlamentets och rådets direktiv 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG och 2009/105/EG samt om upphävande av rådets beslut 87/95/EEG och Europaparlamentets och rådets beslut 1673/2006/EG (EUT L 316, 14.11.2012, s. 12).

specifikationer kan sedan antas av kommissionen i form av gemensamma specifikationer. I de fall där marknadsdrivna processer inte har visat sig fungera för fastställandet av gemensamma specifikationer eller standarder för att främja molninteroperabilitet i praktiken på nivåerna PaaS och SaaS bör kommissionen dessutom, på grundval av den här förordningen och i enlighet med förordning (EU) nr 1025/2012, kunna begära att europeiska standardiseringsorgan utarbetar sådana standarder för specifika tjänstetyper som fortfarande saknar sådana. Kommissionen kommer också att uppmana marknadsaktörerna att utveckla relevanta öppna interoperabilitetsspecifikationer. Efter samråd med berörda aktörer bör kommissionen, genom genomförandeakter, kunna föreskriva användningen av harmoniserade standarder för interoperabilitet eller gemensamma specifikationer för specifika typer av tjänster genom en referens i ett centralt unionsregister över standarder för interoperabla databehandlingstjänster. Leverantörer av databehandlingstjänster bör säkerställa kompatibilitet med dessa harmoniserade standarder och gemensamma specifikationer baserade på öppna interoperabilitetsspecifikationer, vilket inte bör inverka negativt på säkerheten eller integriteten för data. Det kommer endast att refereras till harmoniserade standarder för interoperabla databehandlingstjänster och gemensamma specifikationer baserade på öppna interoperabilitetsspecifikationer om de uppfyller de kriterier som anges i den här förordningen, som har samma innebörd som kraven i bilaga II till förordning (EU) nr 1025/2012 och de interoperabilitetsaspekter som definieras i den internationella standarden ISO/IEC 19941:2017. Dessutom bör standardiseringen ta hänsyn till mikroföretags och små och medelstora företags behov.

(101) Tredjeländer kan anta lagar och andra författningar som syftar till att direkt överföra eller ge statlig åtkomst till icke-personuppgifter som finns utanför det egna landets gränser, inbegripet inom unionen. Rättsliga avgöranden eller beslut av rättsliga eller administrativa myndigheter, däribland brottsbekämpande myndigheter, i tredjeländer som innehåller krav på sådan överföring eller åtkomst till icke-personuppgifter ska vara verkställbara, om de grundar sig på ett gällande internationellt avtal, såsom ett fördrag om ömsesidig rättshjälp, mellan det begärande tredjelandet och unionen eller en medlemsstat. I andra fall kan det uppstå situationer där en begäran om överföring av eller åtkomst till icke-personuppgifter inom ramen för tredje lands lagstiftning står i strid med en skyldighet att skydda sådana data enligt unionsrätten eller enligt den berörda medlemsstatens nationella rätt, i synnerhet när det gäller skyddet av individers grundläggande rättigheter, såsom rätten till säkerhet och rätten till ett effektivt rättsmedel, eller en medlemsstats grundläggande intressen med avseende på nationell säkerhet eller försvar samt skyddet av kommersiellt känsliga uppgifter och skyddet av immateriella rättigheter, inbegripet dess avtalsskyldigheter i fråga om konfidentialitet i enlighet med sådan rätt. I avsaknad av internationella avtal som reglerar sådana frågor bör överföring av eller åtkomst till icke-personuppgifter endast tillåtas om det har kontrollerats att tredjelandets rättssystem omfattar krav på att beslutets skäl och proportionalitet anges, att domstolsavgörandet eller beslutet är specifikt till sin karaktär och att den motiverade invändningen från mottagaren är föremål för prövning av en behörig tredjelandsdomstol som har befogenhet att vederbörligen beakta de relevanta rättsliga intressena för leverantören av sådana data. När det är möjligt enligt villkoren för tredjelandsmyndighetens begäran om dataåtkomst bör leverantören av databehandlingstjänster kunna informera den kund vars data omfattas av begäran innan åtkomst beviljas för sådana data för att kontrollera om denna åtkomst potentiellt kan strida mot unionsrätten eller nationell rätt, såsom reglerna om skydd av kommersiellt känsliga uppgifter, inbegripet skyddet av företagshemligheter och immateriella rättigheter samt avtalsåtaganden avseende konfidentialitet.

(102) För att främja förtroendet för data är det viktigt att det i möjligaste mån genomförs skyddsåtgärder för unionens medborgare, offentliga organ och företag för att säkra deras kontroll över sina data. Dessutom bör unionsrätten och unionens värden och standarder med avseende på bland annat säkerhet, dataskydd och integritet samt konsumentskydd upprätthållas. För att förhindra olaglig statlig åtkomst till icke-personuppgifter av myndigheter i tredjeländer bör leverantörer av databehandlingstjänster som omfattas av denna förordning, däribland molntjänster och edgetjänster, vidta alla rimliga åtgärder för att förhindra åtkomst till system där icke-personuppgifter lagras, inbegripet, när så är lämpligt, genom kryptering av data, frekventa revisioner, verifierad anslutning till relevanta certifieringssystem för säkerhetsförsäkran och ändring av företagspolicyer.

(103) Standardisering och semantisk interoperabilitet bör ha en nyckelroll för tekniska lösningar som säkerställer interoperabilitet inom och mellan gemensamma europeiska dataområden, som är ändamåls- eller sektorsspecifika eller sektorsöverskridande interoperabla ramar för gemensamma standarder och praxisformer för delning eller gemensam behandling av data för bland annat utveckling av nya produkter och tjänster, vetenskaplig forskning eller civilsamhällesinitiativ. Genom denna förordning fastställs vissa väsentliga krav för interoperabilitet. Deltagare i dataområden som erbjuder data eller datatjänster till andra deltagare, som är enheter som underlättar eller deltar i datadelning inom gemensamma europeiska dataområden, inbegripet datahållare, bör uppfylla dessa krav när det gäller element som står under deras kontroll. Efterlevnaden av de reglerna kan säkerställas genom uppfyllelse av de väsentliga krav som fastställs i denna förordning eller förmodas genom efterlevnad av harmoniserade standarder eller gemensamma specifikationer via presumtion om överensstämmelse. För att främja överensstämmelse med interoperabilitetskraven är det nödvändigt att föreskriva presumtion om överensstämmelse för interoperabilitetslösningar som motsvarar harmoniserade standarder – eller delar av sådana – i enlighet med förordning (EU) nr 1025/2012, vilken utgör det grundläggande regelverket för utarbetande av standarder som möjliggör sådana presumtioner. Kommissionen bör bedöma hindren för interoperabilitet och prioritera standardiseringsbehov, på grundval av vilka den kan begära att en eller flera europeiska standardiseringsorganisationer, enligt förordning (EU) nr 1025/2012, ska utarbeta utkast till harmoniserade standarder som tillgodoser de väsentliga krav som fastställs i den här förordningen. Om en sådan begäran inte leder till harmoniserade standarder eller om sådana harmoniserade standarder är otillräckliga för att säkerställa överensstämmelse med de väsentliga kraven i den här förordningen, bör kommissionen kunna anta gemensamma specifikationer för dessa områden, förutsatt att den därvid vederbörligen respekterar standardiseringsorganisationernas roll och funktioner. Gemensamma specifikationer bör endast antas som en exceptionell nödlösning för att underlätta efterlevnad av de väsentliga kraven i den här förordningen, när standardiseringsprocessen är blockerad eller när fastställandet av lämpliga harmoniserade standarder försenas. Om en sådan försening beror på den tekniska komplexiteten hos standarden i fråga bör kommissionen beakta detta innan den överväger att fastställa gemensamma specifikationer. Gemensamma specifikationer bör utarbetas på ett öppet och inkluderande sätt och i förekommande fall beakta råd från Europeiska datainnovationsstyrelsen, som inrättats genom förordning (EU) 2022/868. Gemensamma specifikationer inom olika sektorer skulle också kunna antas, i enlighet med unionsrätten eller nationell rätt, på grund av specifika behov inom dessa sektorer. Kommissionen bör också ges möjlighet att föreskriva utarbetandet av harmoniserade standarder för interoperabla databehandlingstjänster.

(104) För att främja interoperabiliteten för verktyg för automatiserat genomförande av datadelningsavtal är det nödvändigt att fastställa väsentliga krav för smarta kontrakt som yrkespersoner skapar för andra eller integrerar i applikationer som stöder genomförandet av avtal om datadelning. För att främja sådana smarta kontrakts överensstämmelse med dessa väsentliga krav är det nödvändigt att föreskriva presumtion om överensstämmelse för smarta kontrakt som uppfyller harmoniserade standarder – eller delar av sådana – i enlighet med förordning (EU) nr 1025/2012. Begreppet *smart kontrakt* i den här förordningen är teknikneutralt. Smarta kontrakt kan till exempel kopplas till en elektronisk liggare. De väsentliga kraven bör endast gälla säljare av smarta kontrakt, men inte när de internt utvecklar smarta kontrakt uteslutande för eget bruk. Det väsentliga kravet på att säkerställa att smarta kontrakt kan avbrytas och sägas upp förutsätter ömsesidigt samtycke från parterna i datadelningsavtalet. Tillämpligheten av de relevanta bestämmelserna i civilrätt, avtalsrätt och konsumentskyddslagstiftning på datadelningsavtal förblir eller bör förbli opåverkad av användningen av smarta kontrakt för automatiserat genomförande av sådana avtal.

(105) För att visa att de väsentliga kraven i denna förordning är uppfyllda bör försäljaren av ett smart kontrakt eller, i avsaknad av en sådan, den person vars närings- eller yrkesverksamhet inbegriper användning av smarta kontrakt för andra i samband med genomförandet av ett avtal eller en del av det om att göra data tillgängliga inom ramen för denna förordning utföra en bedömning av överensstämmelse och utfärda en EU-försäkran om överensstämmelse. En sådan bedömning av överensstämmelse bör omfattas av de allmänna principerna i Europaparlamentets och rådets förordning (EG) nr 765/2008 ([34]) och Europaparlamentets och rådets beslut (EG) nr 768/2008 ([35]).

([34]) Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och upphävande av förordning (EEG) nr 339/93 (EUT L 218, 13.8.2008, s. 30).

([35]) Europaparlamentets och rådets beslut nr 768/2008/EG av den 9 juli 2008 om en gemensam ram för saluföring av produkter och upphävande av rådets beslut 93/465/EEG (EUT L 218, 13.8.2008, s. 82).

(106) Utöver skyldigheten för professionella utvecklare av smarta kontrakt att uppfylla väsentliga krav är det också viktigt att uppmuntra de deltagare inom dataområden som erbjuder data eller databaserade tjänster till andra deltagare inom och mellan gemensamma europeiska dataområden att stödja interoperabilitet mellan verktyg för datadelning, inbegripet smarta kontrakt.

(107) För att säkerställa tillämpning och efterlevnad av denna förordning bör medlemsstaterna utse en eller flera behöriga myndigheter. Om en medlemsstat utser mer än en behörig myndighet bör den också bland dem utse en datasamordnare. De behöriga myndigheterna bör samarbeta med varandra. Genom att utöva sina utredningsbefogenheter i enlighet med tillämpliga nationella förfaranden bör de behöriga myndigheterna kunna söka efter och erhålla information, särskilt om en enhets verksamhet som omfattas av deras behörighet och, inbegripet i samband med gemensamma utredningar, med vederbörlig hänsyn till det faktum att åtgärder för tillsyn och efterlevnadskontroll avseende en enhet som omfattas av en annan medlemsstats behörighet bör antas av den behöriga myndigheten i den andra medlemsstaten, i förekommande fall, i enlighet med förfarandena för gränsöverskridande samarbete. De behöriga myndigheterna bör bistå varandra i god tid, särskilt när en behörig myndighet i en medlemsstat har relevant information för en utredning som utförs av de behöriga myndigheterna i andra medlemsstater, eller kan samla in sådan information som de behöriga myndigheterna i den medlemsstat där enheten är etablerad inte har tillgång till. De behöriga myndigheterna och datasamordnarna bör anges i ett offentligt register som upprätthålls av kommissionen. Datasamordnaren skulle kunna bidra till att underlätta samarbete i gränsöverskridande situationer, som när en behörig myndighet i en viss medlemsstat inte vet vilken myndighet den bör vända sig till i datasamordnarens medlemsstat, till exempel om ärendet rör mer än en behörig myndighet eller sektor. Datasamordnaren bör bland annat fungera som gemensam kontaktpunkt för alla frågor som rör tillämpningen av denna förordning. Om ingen datasamordnare har utsetts bör den behöriga myndigheten åta sig de uppgifter som tilldelas datasamordnaren enligt denna förordning. De myndigheter som ansvarar för tillsynen över uppfyllandet av rätten på området dataskydd och de behöriga myndigheter som utses inom ramen för unionsrätten eller nationell rätt bör ansvara för denna förordnings tillämpning inom sina behörighetsområden. För att undvika intressekonflikter bör de behöriga myndigheter som ansvarar för tillämpningen och efterlevnaden av denna förordning på området för tillhandahållande av data efter en begäran på grundval av ett exceptionellt behov inte ha rätt att lämna in en sådan begäran.

(108) Fysiska och juridiska personer bör, för att hävda sina rättigheter enligt denna förordning vid överträdelse av deras rättigheter enligt denna förordning, ha rätt att söka omprövning genom att inkomma med ett klagomål. Datasamordnaren bör, på begäran, förse fysiska och juridiska personer med all nödvändig information för att de ska kunna lämna in sina klagomål till den relevanta behöriga myndigheten. Dessa myndigheter bör vara skyldiga att samarbeta för att säkerställa att ett klagomål hanteras på rätt sätt och löses effektivt och i god tid. För att utnyttja mekanismen för nätverket för konsumentskyddssamarbete och möjliggöra representativa åtgärder omfattar denna förordning en ändring av bilagorna till Europaparlamentets och rådets förordning (EU) 2017/2394 ([36]) och Europaparlamentets och rådets direktiv (EU) 2020/1828 ([37]).

(109) De behöriga myndigheterna bör säkerställa att överträdelser av de skyldigheter som fastställs i denna förordning blir föremål för sanktioner. Sådana sanktioner kan bland annat inkludera ekonomiska sanktioner, varningar, reprimander eller föreläggande om att affärsmetoder ska uppfylla de skyldigheter som föreskrivs i denna förordning. Sanktioner som fastställs av medlemsstaterna bör vara ändamålsenliga, proportionella och avskräckande och bör ta hänsyn till rekommendationerna från Europeiska datainnovationsstyrelsen och på så sätt bidra till att största möjliga enhetlighet uppnås vid fastställandet och tillämpningen av sanktioner. När så är lämpligt bör de behöriga myndigheterna använda sig av interimistiska åtgärder för att begränsa effekterna av en påstådd överträdelse medan utredningen av överträdelsen pågår. När de gör detta bör de ta hänsyn till bland annat

([36]) Europaparlamentets och rådets förordning (EU) 2017/2394 av den 12 december 2017 om samarbete mellan de nationella myndigheter som har tillsynsansvar för konsumentskyddslagstiftningen och om upphävande av förordning (EG) nr 2006/2004 (EUT L 345, 27.12.2017, s. 1).

([37]) Europaparlamentets och rådets direktiv (EU) 2020/1828 av den 25 november 2020 om grupptalan för att skydda konsumenters kollektiva intressen och om upphävande av direktiv 2009/22/EG (EUT L 409, 4.12.2020, s. 1).

överträdelsens art, allvar, omfattning och varaktighet med tanke på det allmänintresse som står på spel, omfattningen och typen av verksamhet som bedrivs samt överträdarens ekonomiska kapacitet. De bör även ta hänsyn till om den överträdande parten till överträdelsen systematiskt eller återkommande underlåter att uppfylla sina skyldigheter enligt den här förordningen. För att säkerställa efterlevnaden av principen *ne bis in idem*, och i synnerhet för att undvika att samma överträdelse av skyldigheterna enligt den här förordningen bestraffas mer än en gång, bör en medlemsstat som avser att utöva sin behörighet gentemot en överträdare som inte är etablerad och inte har utsett en rättslig företrädare i unionen utan oskäligt dröjsmål informera alla datasamordnare och kommissionen.

(110) Europeiska datainnovationsstyrelsen bör ge råd till och bistå kommissionen i samordningen av nationell praxis och politik på de områden som omfattas av denna förordning samt i uppnåendet av dess mål när det gäller teknisk standardisering för att förbättra interoperabiliteten. Den bör också spela en nyckelroll när det gäller att underlätta omfattande diskussioner mellan behöriga myndigheter om tillämpningen och efterlevnaden av denna förordning. Detta informationsutbyte är utformat för att öka den faktiska tillgången till rättslig prövning samt kontrollen av efterlevnad och rättsligt samarbete i hela unionen. De behöriga myndigheterna bör bland annat använda Europeiska datainnovationsstyrelsen som en plattform för att utvärdera, samordna och anta rekommendationer om fastställande av sanktioner för överträdelser av denna förordning. Den bör göra det möjligt för behöriga myndigheter att, med bistånd av kommissionen, samordna det optimala tillvägagångssättet för att fastställa och ålägga sådana sanktioner. Detta tillvägagångssätt förhindrar fragmentering samtidigt som medlemsstaterna ges flexibilitet, och bör leda till effektiva rekommendationer som stöder en konsekvent tillämpning av denna förordning. Europeiska datainnovationsstyrelsen bör också ha en rådgivande roll i standardiseringsprocesserna och antagandet av gemensamma specifikationer genom genomförandeakter, i antagandet av delegerade akter för att inrätta en övervakningsmekanism för uttags- och bytesavgifter som åläggs av leverantörer av databehandlingstjänster och för att ytterligare specificera de väsentliga kraven för interoperabilitet mellan data, för mekanismer och tjänster för datadelning samt för de gemensamma europeiska dataområdena. Den bör också ge råd till och bistå kommissionen vid antagandet av riktlinjerna med interoperabilitetsspecifikationer för de gemensamma europeiska dataområdenas funktion.

(111) För att hjälpa företagen att utarbeta och förhandla fram avtal bör kommissionen utveckla och rekommendera icke-bindande standardavtalsvillkor för avtal om datadelning mellan företag, vid behov med beaktande av förhållandena inom enskilda sektorer och befintlig praxis för frivilliga datadelningsmekanismer. Dessa standardavtalsvillkor bör i första hand fungera som ett praktiskt verktyg som hjälper i synnerhet mikroföretag och små och medelstora företag att ingå avtal. När sådana standardavtalsvillkor används brett och på ett integrerat sätt bör de också ha den positiva effekten att de påverkar utformningen av avtal avseende åtkomst till och användning av data och därmed mer generellt leder till rättvisare avtalsförhållanden för åtkomst till och delning av data.

(112) För att undanröja risken för att innehavare av data i databaser som erhålls eller genereras med hjälp av fysiska komponenter, såsom sensorer, i en uppkopplad produkt och en tillhörande tjänst eller andra maskingenererade data, åberopar rätten av sitt eget slag enligt artikel 7 i direktiv 96/9/EG och därigenom i synnerhet hindrar ett effektivt utövande av användarnas rätt till åtkomst till och användning av data och deras rätt att dela data med tredje parter enligt denna förordning, bör det klargöras att rätten av sitt eget slag inte gäller för sådana databaser. Detta påverkar inte den eventuella tillämpningen av rätten av sitt eget slag enligt artikel 7 i direktiv 96/9/EG på databaser som innehåller data som inte omfattas av denna förordning, förutsatt att kraven om skydd enligt punkt 1 i den artikeln är uppfyllda.

(113) För att ta hänsyn till tekniska aspekter av databehandlingstjänster bör befogenheten att anta akter i enlighet med artikel 290 i EUF-fördraget delegeras till kommissionen med avseende på komplettering av denna förordning för att införa en mekanism för övervakning av de avgifter som leverantörer av databehandlingstjänster på marknaden tar ut vid leverantörsbyten och för att ytterligare specificera de väsentliga kraven avseende interoperabilitet för deltagare i dataområden som erbjuder andra deltagare data eller datatjänster. Det är särskilt viktigt att kommissionen genomför

lämpliga samråd under sitt förberedande arbete, inklusive på expertnivå, och att dessa samråd genomförs i enlighet med principerna i det interinstitutionella avtalet av den 13 april 2016 om bättre lagstiftning ([38]). För att säkerställa lika stor delaktighet i förberedelsen av delegerade akter erhåller Europaparlamentet och rådet alla handlingar samtidigt som medlemsstaternas experter, och deras experter ges systematiskt tillträde till möten i kommissionens expertgrupper som arbetar med förberedelse av delegerade akter.

(114) För att säkerställa enhetliga villkor för genomförandet av denna förordning bör kommissionen tilldelas genomförandebefogenheter med avseende på antagandet av gemensamma specifikationer för att säkerställa interoperabiliteten för data, för datadelningsmekanismer och tjänster, samt för gemensamma europeiska dataområden, gemensamma specifikationer för interoperabla databehandlingstjänster, och gemensamma specifikationer för smarta kontrakt. Genomförandebefogenheter bör även tilldelas kommissionen med avseende på att offentliggöra hänvisningar till harmoniserade standarder och gemensamma specifikationer för interoperabla databehandlingstjänster i ett centralt unionsregister över standarder för interoperabla databehandlingstjänster. Dessa befogenheter bör utövas i enlighet med Europaparlamentets och rådets förordning (EU) nr 182/2011 ([39]).

(115) Denna förordning bör inte påverka tillämpningen av regler som avser behov som är specifika för enskilda sektorer eller områden av allmänt intresse. Sådana regler kan innefatta ytterligare krav som avser de tekniska aspekterna av åtkomsten till data, såsom gränssnitt för dataåtkomst, eller hur dataåtkomsten kan tillhandahållas, exempelvis direkt från en produkt eller via dataförmedlingstjänster. Sådana regler kan också omfatta begränsningar av datahållares rätt till åtkomst till eller användning av användardata, eller andra aspekter utöver dataåtkomst och dataanvändning, såsom styrningsaspekter eller säkerhetskrav, inbegripet cybersäkerhetskrav. Denna förordning bör inte heller påverka tillämpningen av mer specifika regler i samband med utvecklingen av gemensamma europeiska dataområden eller, med förbehåll för de undantag som anges i denna förordning, unionsrätt och nationell rätt som föreskriver åtkomst till och godkännande av användning av data för vetenskapliga forskningsändamål.

(116) Denna förordning bör inte påverka tillämpningen av konkurrensreglerna, särskilt artiklarna 101 och 102 i EUF-fördraget. De åtgärder som föreskrivs i denna förordning bör inte användas för att begränsa konkurrensen på ett sätt som strider mot EUF-fördraget.

(117) För att ge de aktörer som omfattas av denna förordning möjlighet att anpassa sig till de nya reglerna i denna förordning och inrätta de nödvändiga tekniska arrangemangen bör dessa regler börja gälla från och med den 12 september 2025.

(118) Europeiska datatillsynsmannen och Europeiska dataskyddsstyrelsen har hörts i enlighet med artikel 42.1 och 42.2 i förordning (EU) 2018/1725 och avgav sina yttranden den 4 maj 2022.

(119) Eftersom målen för denna förordning, nämligen att säkerställa en rättvis fördelning av värdet från data bland aktörer i dataekonomin och främja en rättvis åtkomst till och användning av data för att bidra till genomförandet av en verklig inre marknad för data, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna utan snarare, på grund av åtgärdens omfattning eller verkningar och den gränsöverskridande användningen av data, kan uppnås bättre på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen. I enlighet med proportionalitetsprincipen i samma artikel går denna förordning inte utöver vad som är nödvändigt för att uppnå dessa mål.

([38]) EUT L 123, 12.5.2016, s. 1.

([39]) Europaparlamentets och rådets förordning (EU) nr 182/2011 av den 16 februari 2011 om fastställande av allmänna regler och principer för medlemsstaternas kontroll av kommissionens utövande av sina genomförandebefogenheter (EUT L 55, 28.2.2011, s. 13).

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I

ALLMÄNNA BESTÄMMELSER

Artikel 1

Innehåll och tillämpningsområde

1. I denna förordning fastställs harmoniserade regler om bland annat

a) att göra produktdata och data från en tillhörande tjänst tillgängliga för användaren av den uppkopplade produkten eller den tillhörande tjänsten,

b) datahållares tillhandahållande av data till datamottagare,

c) datahållares tillhandahållande av data till offentliga organ, kommissionen, Europeiska centralbanken och unionsorgan, när det finns ett exceptionellt behov av dessa data för utförandet av en specifik uppgift av allmänt intresse,

d) att underlätta byten av databehandlingstjänster,

e) att införa skyddsåtgärder mot olaglig åtkomst för tredje part till icke-personuppgifter, och

f) utveckling av interoperabilitetsstandarder för åtkomst till, överföring och användning av data.

2. Denna förordning omfattar personuppgifter och icke-personuppgifter, inbegripet följande typer av data i följande sammanhang:

a) Kapitel II är tillämpligt på data, med undantag för innehåll, avseende uppkopplade produkters och tillhörande tjänsters prestanda, användning och miljö.

b) Kapitel III är tillämpligt på data från den privata sektorn som omfattas av lagstadgade skyldigheter i fråga om datadelning.

c) Kapitel IV är tillämpligt på data från den privata sektorn som är åtkomliga och används på grundval av avtal mellan företag.

d) Kapitel V är tillämpligt på data från den privata sektorn med fokus på icke-personuppgifter.

e) Kapitel VI är tillämpligt på data och tjänster som behandlas av leverantörer av databehandlingstjänster.

f) Kapitel VII är tillämpligt på icke-personuppgifter som innehas i unionen av leverantörer av databehandlingstjänster.

3. Denna förordning är tillämplig på följande:

a) Tillverkare av uppkopplade produkter som släpps ut på marknaden i unionen och leverantörer av tillhörande tjänster, oberoende av dessa tillverkares och leverantörers etableringsort.

b) Användare i unionen av uppkopplade produkter eller tillhörande tjänster som avses i led a.

c) Datahållare, oberoende av etableringsort, som gör data tillgängliga för datamottagare i unionen.

d) Datamottagare i unionen som ges tillgång till data.

e) Offentliga organ, kommissionen, Europeiska centralbanken och unionsorgan som begär att datahållare gör data tillgängliga när det finns ett exceptionellt behov av dessa data för utförandet av en specifik uppgift av allmänt intresse samt de datahållare som tillhandahåller data till följd av en sådan begäran.

f) Leverantörer av databehandlingstjänster, oberoende av deras etableringsort, som tillhandahåller sådana tjänster till kunder i unionen.

g) Deltagare i dataområden och leverantörer av applikationer som använder smarta kontrakt och personer vars närings- eller yrkesverksamhet inbegriper användning av smarta kontrakt för andra i samband med genomförandet av ett avtal.

4. När det i denna förordning hänvisas till uppkopplade produkter eller tillhörande tjänster anses sådana hänvisningar även omfatta virtuella assistenter, i den mån de interagerar med en uppkopplad produkt eller tillhörande tjänst.

5. Denna förordning påverkar inte tillämpningen av unionsrätt och nationell rätt om skydd av personuppgifter, integritet och konfidentialitet vid kommunikation samt terminalutrustningens integritet, som ska tillämpas på personuppgifter som behandlas i samband med de rättigheter och skyldigheter som fastställs i denna förordning, i synnerhet förordningarna (EU) 2016/679 och (EU) 2018/1725 och direktiv 2002/58/EG, inbegripet tillsynsmyndigheternas befogenheter och behörighet och registrerades rättigheter. I den mån användare är registrerade ska de rättigheter som fastställs i kapitel II i den här förordningen komplettera registrerades rättigheter till tillgång och rättigheter till dataportabilitet enligt artiklarna 15 och 20 i förordning (EU) 2016/679. Om den här förordningen står i strid med unionsrätt om skydd av personuppgifter eller integritet eller med nationell lagstiftning som antagits i enlighet med sådan unionsrätt, ska relevant unionsrätt eller nationell rätt om skydd av personuppgifter eller integritet äga företräde.

6. Denna förordning ska inte tillämpas på eller föregripa frivilliga arrangemang för utbyte av data mellan privata och offentliga enheter, i synnerhet frivilliga arrangemang för datadelning.

Denna förordning påverkar inte unionsrättsakter eller nationella rättsakter som föreskriver delning, åtkomst till och användning av data för att förebygga, förhindra, utreda, upptäcka eller lagföra brott eller verkställa straffrättsliga påföljder, eller för tull- och skatteändamål, i synnerhet förordningarna (EU) 2021/784, (EU) 2022/2065 och (EU) 2023/1543 samt direktiv (EU) 2023/1544, eller internationellt samarbete på det området. Den här förordningen är inte tillämplig på insamling, delning eller användning av eller åtkomst till data enligt förordning (EU) 2015/847 och direktiv (EU) 2015/849. Den här förordningen är inte tillämplig på områden som inte omfattas av unionsrätten och påverkar under inga omständigheter medlemsstaternas befogenheter i fråga om allmän säkerhet, försvar eller nationell säkerhet, oavsett vilken typ av enhet som medlemsstaterna har anförtrott att utföra uppgifter inom ramen för dessa befogenheter eller deras befogenhet att skydda andra väsentliga statliga funktioner, inbegripet att säkerställa statens territoriella integritet och upprätthålla lag och ordning. Den här förordningen påverkar inte medlemsstaternas befogenheter i fråga om tull- och skatteförvaltning eller medborgares hälsa och säkerhet.

7. Denna förordning kompletterar metoden för självreglering i förordning (EU) 2018/1807 genom att lägga till allmänt tillämpliga skyldigheter för byte av molntjänster.

8. Denna förordning påverkar inte tillämpningen av unionsrättsakter och nationella rättsakter som skyddar immateriella rättigheter, i synnerhet direktiv 2001/29/EG, 2004/48/EG och (EU) 2019/790.

9. Denna förordning kompletterar, och påverkar inte tillämpningen av, unionsrätt som syftar till att främja konsumenters intressen och säkerställa en hög nivå av konsumentskydd samt att skydda deras hälsa, säkerhet och ekonomiska intressen, i synnerhet direktiv 93/13/EEG, 2005/29/EG och 2011/83/EU.

10. Denna förordning hindrar inte ingåendet av frivilliga avtal om laglig datadelning, inbegripet avtal som ingås på ömsesidig grund, som uppfyller kraven i denna förordning.

Artikel 2

Definitioner

I denna förordning gäller följande definitioner:

1. *data*: varje digital återgivning av handlingar, fakta eller information och varje sammanställning av sådana handlingar, fakta eller information, även i form av ljudupptagningar, bildupptagningar eller audiovisuella upptagningar.

2. *metadata*: en strukturerad beskrivning av innehållet i eller användningen av data som underlättar sökningen i eller användningen av dessa data.

3. *personuppgifter*: personuppgifter enligt definitionen i artikel 4.1 i förordning (EU) 2016/679.

4. *icke-personuppgifter*: andra data än personuppgifter.

5. *uppkopplad produkt*: en vara som erhåller, genererar eller samlar in data om sin användning eller om sin miljö, och som kan kommunicera produktdata via en elektronisk kommunikationstjänst, fysisk åtkomst, åtkomst genom uppkoppling eller åtkomst i enheten, och vars huvudfunktion inte är att lagra, behandla eller överföra data för någon annan part än användaren.

6. *tillhörande tjänst*: en digital tjänst, annan än en elektronisk kommunikationstjänst, inbegripet programvara, som är ansluten till produkten vid tidpunkten för köp, hyra eller leasing på ett sådant sätt att den uppkopplade produkten inte skulle kunna utföra en eller flera av sina funktioner utan den, eller som senare ansluts till produkten av tillverkaren eller en tredje part för att lägga till, uppdatera eller anpassa funktioner hos den uppkopplade produkten.

7. *behandling*: en åtgärd eller kombination av åtgärder som utförs på data eller datamängder, oberoende av om de utförs automatiserat eller inte, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämnande genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

8. *databehandlingstjänst*: en digital tjänst som tillhandahålls en kund och som möjliggör allmän nätverkstillgång på begäran till en gemensam pool av konfigurerbara, skalbara och elastiska databehandlingsresurser av centraliserad, distribuerad eller mycket distribuerad art och som snabbt kan tillhandahållas och levereras med minsta möjliga administration eller interaktion med tjänsteleverantören.

9. *samma tjänstetyp*: en uppsättning databehandlingstjänster som delar samma primära mål, databehandlingstjänstemodell och huvudsakliga funktioner.

10. *dataförmedlingstjänst*: dataförmedlingstjänst enligt definitionen i artikel 2.11 i förordning (EU) 2022/868.

11. *registrerad*: registrerad som avses i artikel 4.1 i förordning (EU) 2016/679.

12. *användare*: en fysisk eller juridisk person som äger en uppkopplad produkt eller till vilken tillfälliga rättigheter att använda den uppkopplade produkten har överlåtits genom avtal, eller som erhåller tillhörande tjänster.

13. *datahållare*: en fysisk eller juridisk person som har en rätt eller skyldighet, i enlighet med denna förordning, tillämplig unionsrätt eller nationell lagstiftning som antagits i enlighet med unionsrätten, att använda och tillgängliggöra data, inbegripet produktdata eller data från tillhörande tjänster som denne har hämtat eller genererat under tillhandahållandet av en tillhörande tjänst, om detta avtalats.

14. *datamottagare*: en fysisk eller juridisk person som agerar för syften kopplade till personens näringsverksamhet, affärsverksamhet, hantverk eller yrke och som är en annan än användaren av en uppkopplad produkt eller tillhörande tjänst, för vilken datahållaren gör data tillgängliga, inbegripet en tredje part på begäran från användaren till datahållaren eller i enlighet med en rättslig skyldighet enligt unionsrätten eller nationell lagstiftning som antagits i enlighet med unionsrätten.

15. *produktdata*: data som genereras genom användning av en uppkopplad produkt och som tillverkaren har utformat för att kunna hämtas via en elektronisk kommunikationstjänst, via fysisk åtkomst eller åtkomst i enheten av en användare, datahållare eller en tredje part, inbegripet tillverkaren i tillämpliga fall.

16. *data från en tillhörande tjänst*: data som representerar digitaliseringen av användaråtgärder eller användarhändelser som kan härledas från den uppkopplade produkten och som registreras avsiktligt av användaren eller genereras som en biprodukt av användarens åtgärder under leverantörens tillhandahållande av en tillhörande tjänst.

17. *lätt åtkomliga data*: produktdata och data från en tillhörande tjänst som en datahållare lagligen erhåller eller lagligen kan erhålla från den uppkopplade produkten eller tillhörande tjänsten, utan oproportionella ansträngningar som går utöver en enkel åtgärd.

18. *företagshemlighet*: företagshemlighet enligt definitionen i artikel 2.1 i direktiv (EU) 2016/943.

19. *innehavare av en företagshemlighet*: en innehavare av en företagshemlighet enligt definitionen i artikel 2.2 i direktiv (EU) 2016/943.

20. *profilering*: profilering enligt definitionen i artikel 4.4 i förordning (EU) 2016/679.

21. *tillhandahållande på marknaden*: leverans av en uppkopplad produkt för distribution, förbrukning eller användning på unionsmarknaden i samband med kommersiell verksamhet, mot betalning eller gratis.

22. *utsläppande på marknaden*: det första tillhandahållandet av en uppkopplad produkt på unionens marknad.

23. *konsument*: en fysisk person som agerar för ändamål som faller utanför den personens näringsverksamhet, affärsverksamhet, hantverk eller yrke.

24. *företag*: en fysisk eller juridisk person som när det gäller avtal eller praxis som omfattas av denna förordning agerar för syften som är kopplade till personens näringsverksamhet, affärsverksamhet, hantverk eller yrke.

25. *små företag*: små företag enligt definitionen i artikel 2.2 i bilagan till rekommendation 2003/361/EG.

26. *mikroföretag*: ett mikroföretag enligt definitionen i artikel 2.3 i bilagan till rekommendation 2003/361/EG.

27. *unionsorgan*: de unionsorgan och unionsbyråer som inrättats genom eller enligt akter som antagits på grundval av fördraget om Europeiska unionen, EUF-fördraget eller fördraget om upprättandet av Europeiska atomenergigemenskapen.

28. *offentliga organ*: medlemsstaternas nationella, regionala eller lokala myndigheter och medlemsstaternas offentligrättsliga organ, eller sammanslutningar som bildats av en eller flera sådana myndigheter eller ett eller flera sådana organ.

29. *allmänt nödläge*: en exceptionell situation under en begränsad tid, såsom ett hot mot folkhälsan, ett nödläge till följd av naturkatastrofer eller en större katastrof orsakad av människan, inbegripet en större cybersäkerhetsincident, med negativa konsekvenser för befolkningen i unionen, en medlemsstat eller en del av en medlemsstat, som medför en risk för allvarliga och bestående återverkningar på levnadsvillkoren eller den ekonomiska och finansiella stabiliteten, eller avsevärd och omedelbar värdeminskning av ekonomiska tillgångar i unionen eller berörda medlemsstater, och som fastställs och officiellt utlyses i enlighet med relevanta förfaranden i unionsrätten eller nationell rätt.

30. *kund*: en fysisk eller juridisk person som har ingått ett avtalsförhållande med en leverantör av databehandlingstjänster i syfte att använda en eller flera databehandlingstjänster.

31. *virtuella assistenter*: programvara som kan behandla uppmaningar, uppdrag eller frågor, inbegripet sådana baserade på ljud, skrift, gester eller rörelse, och som baserat på dessa uppmaningar, uppdrag eller frågor ger åtkomst till andra tjänster eller kontrollerar uppkopplade produkters funktioner.

32. *digitala tillgångar*: element i digitalt format, inbegripet applikationer, för vilka kunden har nyttjanderätt, oberoende av avtalsförhållandet med den databehandlingstjänst som kunden avser att byta från.

33. *lokal IKT-infrastruktur*: IKT-infrastruktur och databehandlingsresurser som ägs, hyrs eller leasas av kunden, är belägna i kundens egen datacentral och drivs av kunden eller en tredje part.

34. *byte*: process som inbegriper en ursprunglig leverantör av databehandlingstjänster, en kund till en databehandlingstjänst och, i tillämpliga fall, en destinationsleverantör av databehandlingstjänster, varigenom kunden till en databehandlingstjänst byter från användning av en databehandlingstjänst till användning av en annan databehandlingstjänst av samma tjänstetyp eller en annan tjänst som erbjuds av en annan leverantör av databehandlingstjänster, eller till lokal IKT-infrastruktur, inbegripet genom extrahering, anpassning och uppladdning av data.

35. *uttagsavgifter för data*: avgifter för dataöverföring som tas ut av kunder för att de ska kunna extrahera sina data genom nätverket från IKT-infrastrukturen hos en leverantör av databehandlingstjänster till en annan leverantörs system eller till lokal IKT-infrastruktur.

36. *bytesavgifter*: andra avgifter än standardavgifter eller straffavgifter för förtida uppsägning som en leverantör av databehandlingstjänster tar ut av en kund för de åtgärder som föreskrivs i denna förordning för att byta till en annan leverantörs system eller till lokal IKT-infrastruktur, inbegripet uttagsavgifter för data.

37. *funktionell likvärdighet*: att på grundval av kundens exporterbara data och digitala tillgångar återställa en miniminivå av funktionalitet i miljön för en ny databehandlingstjänst av samma tjänstetyp efter bytesprocessen, där destinationstjänsten för databehandling levererar ett väsentligen jämförbart resultat som svar på samma input för delade funktioner som tillhandahålls kunden enligt avtalet.

38. *exporterbara data*: vid tillämpning av artiklarna 23–31 och 35, in- och utdata, inklusive metadata, som direkt eller indirekt genereras eller samgenereras genom kundens användning av databehandlingstjänsten, med undantag för tillgångar eller data som skyddas genom immateriella rättigheter, eller som utgör en företagshemlighet, som tillhör leverantörer av databehandlingstjänster eller tredje parter.

39. *smart kontrakt*: ett datorprogram som används för automatiserat genomförande av ett avtal eller en del därav med hjälp av en sekvens av elektroniska dataposter och som säkerställer deras integritet och korrektheten hos deras kronologiska ordningsföljd.

40. *interoperabilitet*: förmågan hos två eller fler dataområden eller kommunikationsnät, system, uppkopplade produkter, applikationer, databehandlingstjänster eller komponenter att utbyta och använda data för att utföra sina funktioner.

41. *öppen interoperabilitetsspecifikation*: en teknisk specifikation på informations- och kommunikationsteknikområdet som är resultatinriktad på att uppnå interoperabilitet mellan databehandlingstjänster.

42. *gemensamma specifikationer*: ett dokument, som inte är en standard, vilket omfattar tekniska lösningar som gör det möjligt att uppfylla vissa krav och skyldigheter som fastställs enligt denna förordning.

43. *harmoniserad standard*: en harmoniserad standard enligt definitionen i artikel 2.1 c i förordning (EU) nr 1025/2012.

KAPITEL II

DATADELNING MELLAN FÖRETAG OCH KONSUMENTER OCH MELLAN FÖRETAG

Artikel 3

Skyldighet att göra produktdata och data från tillhörande tjänster tillgängliga för användaren

1. Uppkopplade produkter ska utformas och tillverkas, och tillhörande tjänster ska utformas och tillhandahållas, så att produktdata och data från tillhörande tjänster, inbegripet relevanta metadata som krävs för att tolka och använda dessa data, som standard är direkt tillgängliga för användaren, när detta är relevant och tekniskt möjligt, på ett enkelt, säkert och kostnadsfritt sätt i ett heltäckande, strukturerat, allmänt använt och maskinläsbart format.

2. Innan ett avtal om köp, hyra eller leasing av en uppkopplad produkt ingås ska försäljaren, uthyraren eller leasegivaren, som kan vara tillverkaren, lämna åtminstone följande information till användaren på ett tydligt och begripligt sätt:

a) Typen, formatet och den uppskattade mängden produktdata som den uppkopplade produkten kan generera.

b) Huruvida den uppkopplade produkten kan generera data kontinuerligt och i realtid.

c) Huruvida den uppkopplade produkten kan lagra data på enheten eller på en fjärrserver, inbegripet, i förekommande fall, den planerade lagringstiden.

d) Hur användaren kan få åtkomst till, hämta eller, i relevanta fall, radera datan, inbegripet de tekniska medlen för detta, samt deras användningsvillkor och tjänstekvalitet.

3. Innan ett avtal om tillhandahållande av en tillhörande tjänst ingås ska leverantören av en sådan tjänst lämna åtminstone följande information till användaren på ett tydligt och begripligt sätt:

a) Arten, den uppskattade mängden och insamlingsfrekvensen för de produktdata som den presumtiva datahållaren förväntas erhålla och, i förekommande fall, villkoren för användarens åtkomst till eller hämtning av sådana data, inbegripet den presumtiva datahållarens arrangemang för datalagring och lagringstiden.

b) Arten och den uppskattade mängden av de data från tillhörande tjänster som ska genereras samt villkoren för användarens åtkomst till eller hämtning av sådana data, inbegripet den presumtiva datahållarens arrangemang för datalagring och lagringstiden.

c) Huruvida den presumtiva datahållaren förväntar sig att själv använda lätt åtkomliga data och de ändamål för vilka dessa data ska användas, och om den avser att tillåta en eller flera tredje parter att använda dessa data för ändamål som överenskommits med användaren.

d) Den presumtiva datahållarens och, i tillämpliga fall, andra databehandlingsparters, identitet, såsom dennes företagsnamn och den geografiska adress där denne är etablerad.

e) De kommunikationsmedel som gör det möjligt att snabbt kontakta den presumtiva datahållaren och effektivt kommunicera med denna.

f) Hur användaren kan begära att data delas med en tredje part och, i förekommande fall, avsluta datadelningen.

g) Användarens rätt att lämna in ett klagomål om överträdelse av någon av bestämmelserna i detta kapitel till den behöriga myndighet som utsetts enligt artikel 37.

h) Huruvida en presumtiv datahållare är innehavare av en företagshemlighet som ingår i de data som är åtkomliga från den uppkopplade produkten eller som genereras under tillhandahållandet av en tillhörande tjänst, och, om den presumtiva datahållaren inte är innehavaren av en företagshemlighet, identiteten på innehavaren av en företagshemlighet.

i) Varaktigheten för avtalet mellan användaren och den presumtiva datahållaren samt villkoren för att säga upp ett sådant avtal.

Artikel 4

Användares och datahållares rättigheter och skyldigheter när det gäller att få åtkomst till, använda och tillgängliggöra produktdata och data från tillhörande tjänster

1. Om användaren inte har direkt åtkomst till data från den uppkopplade produkten eller den tillhörande tjänsten ska datahållare utan oskäligt dröjsmål göra lätt åtkomliga data, samt relevanta metadata som är nödvändiga för att tolka och använda dessa data, tillgängliga för användaren, av samma kvalitet som den som är tillgänglig för datahållaren, på ett enkelt, säkert och kostnadsfritt sätt i ett heltäckande, strukturerat, allmänt använt och maskinläsbart format och, i tillämpliga fall och där så är tekniskt genomförbart, kontinuerligt och i realtid. Detta ska göras på grundval av en enkel begäran på elektronisk väg om det är tekniskt möjligt.

2. Användare och datahållare får genom avtal begränsa eller förbjuda åtkomst till, användning eller ytterligare datadelning, om sådan behandling skulle kunna undergräva säkerhetskraven för den uppkopplade produkten, i enlighet med unionsrätten eller nationell rätt, och leda till allvarliga negativa effekter på fysiska personers hälsa, säkerhet eller trygghet. Behöriga myndigheter får tillhandahålla användare och datahållare teknisk expertis i detta sammanhang. Om datahållaren vägrar att dela data enligt denna artikel ska denne underrätta den behöriga myndighet som utsetts enligt artikel 37.

3. Utan att det påverkar användarens rätt att när som helst begära prövning vid en domstol i en medlemsstat får användaren, i samband med en tvist med datahållaren om de avtalsenliga begränsningar eller förbud som avses i punkt 2,

a) i enlighet med artikel 37.5 b lämna in ett klagomål till den behöriga myndigheten, eller

b) komma överens med datahållaren om att hänskjuta ärendet till ett tvistlösningsorgan i enlighet med artikel 10.1.

4. Datahållare får inte göra det orimligt svårt för användaren att göra val eller utöva rättigheter enligt denna artikel, till exempel genom att erbjuda användaren val på ett icke-neutralt sätt eller genom att undergräva eller försämra användarens självständighet, beslutsfattande eller val via strukturen, utformningen, funktionen eller driftssättet för ett digitalt användargränssnitt eller en del därav.

5. För att kontrollera om en fysisk eller juridisk person kan anses vara en användare vid tillämpning av punkt 1 får en datahållare inte kräva att denna person lämnar någon information utöver vad som är nödvändigt. Datahållare får inte spara någon information, i synnerhet inte loggdata, om användarens åtkomst till de data som begärs utöver vad som är nödvändigt för ett korrekt utförande av användarens begäran om åtkomst och för säkerheten och underhållet av datainfrastrukturen.

6. Företagshemligheter ska bevaras och får endast röjas om datahållaren och användaren före utlämnandet vidtar alla nödvändiga åtgärder för att bevara deras konfidentialitet, särskilt avseende tredje parter. Datahållaren, eller om det inte är samma person, innehavaren av en företagshemlighet, ska identifiera de data som skyddas som företagshemligheter, inbegripet i relevanta metadata, och ska komma överens med användaren om de proportionella tekniska och organisatoriska åtgärder som är nödvändiga för att bevara konfidentialiteten för delade data, särskilt i förhållande till tredje parter, såsom standardavtalsvillkor, avtal om konfidentialitet, strikta åtkomstprotokoll, tekniska standarder och tillämpning av uppförandekoder.

7. Om det inte finns någon överenskommelse om de nödvändiga åtgärder som avses i punkt 6, eller om användaren underlåter att genomföra de åtgärder som överenskommits enligt punkt 6 eller äventyrar företagshemligheternas konfidentialitet, får datahållaren hindra eller, i förekommande fall, avbryta delningen av data som identifierats som företagshemligheter. Datahållarens beslut ska vara vederbörligen motiverat och lämnas skriftligen till användaren utan oskäligt dröjsmål. I sådana fall ska datahållaren underrätta den behöriga myndighet som utsetts enligt artikel 37 om att den har hindrat eller avbrutit datadelning och identifiera vilka åtgärder som inte har överenskommits eller genomförts och, i förekommande fall, för vilka företagshemligheter konfidentialiteten har äventyrats.

8. Om en datahållare som är en innehavare av en företagshemlighet kan visa att det är högst sannolikt att denne kommer att lida allvarlig ekonomisk skada till följd av röjandet av företagshemligheter, trots de tekniska och organisatoriska åtgärder som vidtagits av användaren enligt punkt 6 i denna artikel, får den datahållaren, under exceptionella omständigheter och från fall till fall, avslå en begäran om åtkomst till de specifika data som avses. Detta påvisande ska vara vederbörligen motiverat på grundval av objektiva faktorer, särskilt verkställbarheten av skyddet av företagshemligheter i tredjeländer, begärda datas art och grad av konfidentialitet samt den uppkopplade produktens unika och nya karaktär, och ska tillhandahållas användaren skriftligen utan oskäligt dröjsmål. Om datahållaren vägrar att dela data enligt den här punkten ska denne underrätta den behöriga myndighet som utsetts enligt artikel 37.

9. Utan att det påverkar en användares rätt att när som helst begära prövning vid en domstol i en medlemsstat, får en användare som vill bestrida en datahållares beslut att vägra eller att hindra eller avbryta datadelning enligt punkterna 7 och 8

a) i enlighet med artikel 37.5 b lämna in ett klagomål till den behöriga myndigheten, som utan oskäligt dröjsmål ska besluta huruvida och på vilka villkor datadelning ska inledas eller återupptas, eller

b) komma överens med datahållaren om att hänskjuta ärendet till ett tvistlösningsorgan i enlighet med artikel 10.1.

10. Användaren får inte använda de data som erhållits till följd av en begäran som avses i punkt 1 för att utveckla en uppkopplad produkt som konkurrerar med den uppkopplade produkt som dessa data härrör från och inte heller dela dessa data med en tredje part i detta syfte och får inte använda sådana data för att skaffa sig inblick i tillverkarens, eller i förekommande fall datahållarens, ekonomiska situation, tillgångar och produktionsmetoder.

11. Användaren får inte, för att få åtkomst till data, använda tvångsmedel eller missbruka luckor i en datahållares tekniska infrastruktur som utformats för att skydda data.

12. Om användaren inte är den registrerade vars personuppgifter begärs får datahållaren tillgängliggöra personuppgifter som genereras genom användning av en uppkopplad produkt eller tillhörande tjänst för användaren endast om det finns en giltig rättslig grund för behandling enligt artikel 6 i förordning (EU) 2016/679 och, i förekommande fall, om villkoren i artikel 9 i den förordningen och i artikel 5.3 i direktiv 2002/58/EG är uppfyllda.

13. En datahållare får endast använda lätt åtkomliga data som är icke-personuppgifter på grundval av ett avtal med användaren. En datahållare får inte använda sådana data för att få inblick i användarens ekonomiska situation, tillgångar och produktionsmetoder, eller användning av dessa, på något annat sätt som skulle kunna undergräva användarens kommersiella ställning på de marknader där användaren är verksam.

14. Datahållare får inte göra sådana produktdata som är icke-personuppgifter tillgängliga för tredje parter för kommersiella eller icke-kommersiella ändamål annat än för att fullgöra avtalet med användaren. Vid behov ska datahållare genom avtal förbinda tredje parter att inte dela vidare data som de har mottagit från dem.

Artikel 5

Användarens rätt att dela data med tredje parter

1. På begäran av en användare, eller av en part som agerar för en användares räkning, ska datahållaren utan oskäligt dröjsmål för en tredje part tillgängliggöra lätt åtkomliga data samt de relevanta metadata som är nödvändiga för att tolka och använda dessa data, av samma kvalitet som den som är tillgänglig för datahållaren, på ett enkelt och säkert sätt, kostnadsfritt för användaren, i ett heltäckande, strukturerat, allmänt använt och maskinläsbart format och, när så är relevant och tekniskt genomförbart, kontinuerligt och i realtid. Data ska göras tillgänglig av datahållaren för den tredje parten i enlighet med artiklarna 8 och 9.

2. Punkt 1 ska inte gälla lätt åtkomliga data i samband med testning av nya uppkopplade produkter, ämnen eller processer som ännu inte har släppts ut på marknaden, såvida inte tredje parts användning av dem är tillåten enligt avtal.

3. Ett företag som har utsetts till grindvakt enligt artikel 3 i förordning (EU) 2022/1925 ska inte vara en godtagbar tredje part enligt den här artikeln och får därför inte

a) på något som helst sätt anmoda en användare, genom begäran eller kommersiellt incitament, inbegripet genom att erbjuda ekonomisk eller annan ersättning, att göra data som användaren har erhållit till följd av en begäran enligt artikel 4.1 tillgängliga för en av förtagets tjänster,

b) anmoda en användare, genom begäran eller kommersiellt incitament, att begära att datahållaren gör data tillgängliga för en av företagets tjänster enligt punkt 1 i denna artikel,

c) från en användare ta emot data som användaren har erhållit till följd av en begäran enligt artikel 4.1.

4. För att kontrollera om en fysisk eller juridisk person kan anses vara en användare eller en tredje part vid tillämpning av punkt 1 ska användaren eller den tredje parten inte vara skyldig att tillhandahålla någon information utöver vad som är nödvändigt. Datahållare får inte spara någon information om den tredje partens åtkomst till begärda data utöver vad som är nödvändigt för ett korrekt utförande av den tredje partens begäran om åtkomst och för säkerheten och underhållet av datainfrastrukturen.

5. Den tredje parten får inte, för att få åtkomst till data, använda tvångsmedel eller missbruka luckor i en datahållares tekniska infrastruktur som utformats för att skydda data.

6. En datahållare får inte använda lätt åtkomliga data för att få inblick i den tredje partens ekonomiska situation, tillgångar och produktionsmetoder, eller användning av dessa, på något annat sätt som skulle kunna undergräva den tredje partens kommersiella ställning på de marknader där den tredje parten är verksam, såvida inte den tredje parten har gett sitt tillstånd till sådan användning och har teknisk möjlighet att när som helst och på ett enkelt sätt återkalla det tillståndet.

7. Om användaren inte är den registrerade vars personuppgifter begärs får alla personuppgifter som genereras genom användning av en uppkopplad produkt eller tillhörande tjänst, endast göras tillgängliga av datahållaren eller den tredje parten om det finns en giltig rättslig grund för behandlingen enligt artikel 6 i förordning (EU) 2016/679 och, i förekommande fall, om villkoren i artikel 9 i den förordningen och i artikel 5.3 i direktiv 2002/58/EG är uppfyllda.

8. Om datahållaren och den tredje parten underlåter att komma överens om arrangemangen för överföring av data får detta inte hindra eller inkräkta på den registrerades utövande av sina rättigheter enligt förordning (EU) 2016/679, i synnerhet inte när det gäller rätten till dataportabilitet enligt artikel 20 i den förordningen.

9. Företagshemligheter ska bevaras och får endast röjas för tredje parter i den mån sådant röjande är absolut nödvändigt för att uppfylla det syfte som överenskommits mellan användaren och den tredje parten. Datahållaren, eller, om det inte är samma person, innehavaren av en företagshemlighet, ska identifiera de data som skyddas som företagshemligheter, inbegripet i relevanta metadata, och ska komma överens med den tredje parten om alla proportionella tekniska och organisatoriska åtgärder som är nödvändiga för att bevara konfidentialiteten för delade data, såsom standardavtalsvillkor, avtal om konfidentialitet, strikta åtkomstprotokoll, tekniska standarder och tillämpning av uppförandekoder.

10. Om det inte finns någon överenskommelse om de nödvändiga åtgärder som avses i punkt 9 i denna artikel eller om den tredje parten underlåter att genomföra de åtgärder som överenskommits enligt punkt 9 i denna artikel eller äventyrar företagshemligheternas konfidentialitet, får datahållaren hindra eller, i förekommande fall, avbryta delningen av data som identifierats som företagshemligheter. Datahållarens beslut ska vara vederbörligen motiverat och lämnas skriftligen till den tredje parten utan oskäligt dröjsmål. I sådana fall ska datahållaren underrätta den behöriga myndighet som utsetts enligt artikel 37 om att den har hindrat eller avbrutit datadelning och identifiera vilka åtgärder som inte har överenskommits eller genomförts och, i förekommande fall, för vilka företagshemligheter konfidentialiteten har äventyrats.

11. Om en datahållare som är en innehavare av en företagshemlighet kan visa att det är högst sannolikt att denne kommer att lida allvarlig ekonomisk skada till följd av röjandet av företagshemligheter, trots de tekniska och organisatoriska åtgärder som vidtagits av den tredje parten enligt punkt 9 i denna artikel, får den datahållaren, under exceptionella omständigheter och från fall till fall, avslå en begäran om åtkomst till de specifika data som avses. Detta påvisande ska vara vederbörligen motiverat på grundval av objektiva faktorer, särskilt verkställbarheten av skyddet av företagshemligheter i tredjeländer, begärda datas art och grad av konfidentialitet samt den uppkopplade produktens unika och nya karaktär, och ska tillhandahållas den tredje parten skriftligen utan oskäligt dröjsmål. Om datahållaren vägrar att dela data enligt den här punkten ska denne underrätta den behöriga myndighet som utsetts enligt artikel 37.

12. Utan att det påverkar tredje parts rätt att när som helst begära prövning vid en domstol i en medlemsstat, får en tredje part som vill bestrida en datahållares beslut att vägra eller att hindra eller avbryta datadelning enligt punkterna 10 och 11

a) i enlighet med artikel 37.5 b lämna in ett klagomål till den behöriga myndigheten, som utan oskäligt dröjsmål ska besluta huruvida och på vilka villkor datadelningen ska inledas eller återupptas, eller

b) komma överens med datahållaren om att hänskjuta ärendet till ett tvistlösningsorgan i enlighet med artikel 10.1.

13. Den rätt som avses i punkt 1 får inte på ett ogynnsamt sätt påverka registrerades rättigheter enligt tillämplig unionsrätt och nationell rätt om skydd av personuppgifter.

Artikel 6

Skyldigheter för tredje parter som tar emot data på användarens begäran

1. En tredje part ska behandla de data som gjorts tillgängliga för den enligt artikel 5 endast för de ändamål och på de villkor som överenskommits med användaren med förbehåll för unionsrätt och nationell rätt om skyddet av personuppgifter, inbegripet den registrerades rättigheter när det gäller personuppgifter. Den tredje parten ska radera dessa data när de inte längre är nödvändiga för det överenskomna ändamålet, såvida inte annat överenskommits med användaren när det gäller personuppgifter.

2. Den tredje parten får inte

a) göra det orimligt svårt för användaren att göra sina val eller utöva sina rättigheter enligt artikel 5 och den här artikeln, inbegripet genom att erbjuda användaren val på ett icke-neutralt sätt, eller utöva tvång mot, vilseleda eller manipulera användaren eller genom att undergräva eller inskränka användarens självständighet, beslutsfattande eller val, inbegripet genom ett digitalt användargränssnitt eller en del därav,

b) utan hinder av artikel 22.2 a och c i förordning (EU) 2016/679 använda de data som den tar emot för profilering, såvida det inte är nödvändigt för att tillhandahålla den tjänst som begärs av användaren,

c) göra de data som den tar emot tillgängliga för en annan tredje part, såvida inte datan görs tillgängliga på grundval av ett avtal med användaren, och förutsatt att den andra tredje parten vidtar alla nödvändiga åtgärder som överenskommits mellan datahållaren och den tredje parten för att bevara företagshemligheters konfidentialitet,

d) göra de data som den tar emot tillgängliga för ett företag som har utsetts till grindvakt enligt artikel 3 i förordning (EU) 2022/1925,

e) använda de data som den mottar för att utveckla en produkt som konkurrerar med den uppkopplade produkt från vilken de data som åtkommits härrör eller dela dessa data med en annan tredje part för det ändamålet; tredje parter får inte heller använda produktdata eller data från en tillhörande tjänst som är icke-personuppgifter och som gjorts tillgängliga för dem för att få inblick i datahållarens ekonomiska situation, tillgångar och produktionsmetoder, eller användning av dessa,

f) använda de data som den mottar på ett sätt som inverkar negativt på säkerheten för den uppkopplade produkten eller de tillhörande tjänsterna,

g) bortse från specifika åtgärder som överenskommits med en datahållare eller med innehavaren av företagshemligheter enligt artikel 5.9 och äventyra konfidentialiteten för företagshemligheter,

h) hindra en användare som är en konsument, inbegripet på grundval av ett avtal, från att göra mottagna data tillgängliga för andra parter.

Artikel 7

Tillämpningsområdet för skyldigheter vad gäller datadelning mellan företag och konsumenter och mellan företag

1. Skyldigheterna i detta kapitel ska inte gälla data som genereras genom användning av uppkopplade produkter som tillverkas eller utformas, eller tillhörande tjänster som tillhandahålls av, ett mikroföretag eller ett litet företag, förutsatt att det företaget inte har ett partnerföretag eller ett anknutet företag i den mening som avses i artikel 3 i bilagan till rekommendation 2003/361/EG som inte betraktas som ett mikroföretag eller ett litet företag och när det mikroföretaget eller det lilla företaget inte tillverkar eller utformar en uppkopplad produkt eller tillhandahåller en tillhörande tjänst på entreprenad.

Detsamma ska gälla för data som genereras genom användning av uppkopplade produkter som har tillverkats eller tillhörande tjänster som har tillhandahållits av ett företag som har betraktats som ett medelstort företag enligt artikel 2 i bilagan till rekommendation 2003/361/EG i mindre än ett år och för uppkopplade produkter under ett år från den dag då de släpptes ut på marknaden av ett medelstort företag.

2. Avtalsvillkor som till nackdel för användaren utesluter tillämpning av, avviker från eller ändrar verkan av användarens rättigheter enligt detta kapitel ska inte vara bindande för användaren.

KAPITEL III

SKYLDIGHETER FÖR DATAHÅLLARE SOM ÄR SKYLDIGA ATT GÖRA DATA TILLGÄNGLIGA ENLIGT UNIONSRÄTTEN

Artikel 8

Villkor enligt vilka datahållare gör data tillgängliga för datamottagare

1. Om en datahållare inom ramen för förbindelser mellan företag är skyldig att göra data tillgängliga för en datamottagare enligt artikel 5 eller enligt annan tillämplig unionsrätt eller nationell lagstiftning som antagits i enlighet med unionsrätten, ska datahållaren komma överens med en datamottagare om villkoren för att göra data tillgängliga och ska göra detta på rättvisa, rimliga och icke-diskriminerande villkor och på ett öppet sätt i enlighet med detta kapitel och kapitel IV.

2. Ett avtalsvillkor om åtkomst till och användning av data eller om ansvar och rättsmedel vid överträdelse eller uppsägning av datarelaterade skyldigheter ska inte vara bindande om det utgör ett oskäligt avtalsvillkor i den mening som avses i artikel 13 eller om det, till användarens nackdel, utesluter tillämpningen av, avviker från eller ändrar verkan av användarens rättigheter enligt kapitel II.

3. En datahållare får inte, avseende åtgärder som vidtagits för att göra data tillgängliga, diskriminera mellan jämförbara kategorier av datamottagare, inbegripet datahållarens partnerföretag eller anknutna företag, när data görs tillgängliga. Om en datamottagare anser att de förhållanden under vilka data har gjorts tillgängliga för denne är diskriminerande, ska datahållaren utan oskäligt dröjsmål ge datamottagaren information, på dennes motiverade begäran, som visar att det inte har förekommit någon diskriminering.

4. En datahållare får inte, inbegripet på exklusiv grund, göra data tillgängliga för en datamottagare, såvida inte användaren begär detta enligt kapitel II.

5. Datahållare och datamottagare ska inte vara skyldiga att tillhandahålla någon information utöver vad som är nödvändigt för att kontrollera efterlevnaden av de avtalsvillkor som överenskommits för tillgängliggörande av data eller vad som är nödvändigt för uppfyllandet av deras skyldigheter enligt denna förordning eller annan tillämplig unionsrätt eller nationell lagstiftning som antagits i enlighet med unionsrätten.

6. Om inte annat föreskrivs i unionsrätten, inbegripet artiklarna 4.6 och 5.9 i denna förordning, eller i nationell lagstiftning som antagits i enlighet med unionsrätten, ska en skyldighet att göra data tillgängliga för en datamottagare inte medföra någon skyldighet att röja företagshemligheter.

Artikel 9

Ersättning för tillgängliggörande av data

1. Ersättning som en datahållare och en datamottagare kommer överens om för att göra data tillgängliga i förbindelser mellan företag ska vara icke-diskriminerande och rimlig och får inbegripa en marginal.

2. När datahållaren och datamottagaren kommer överens om ersättning ska de särskilt beakta följande:

a) Kostnader för att göra data tillgängliga, inbegripet särskilt de kostnader som är nödvändiga för formatering av data, spridning med elektroniska medel och lagring.

b) Investeringar i insamling och framställning av data, i förekommande fall med beaktande av huruvida andra parter har bidragit till att inhämta, generera eller samla in datan i fråga.

3. Den ersättning som avses i punkt 1 kan också bero på datans volym, format och karaktär.

4. Om datamottagaren är ett mikroföretag eller ett litet eller medelstort företag eller en icke-vinstdrivande forskningsorganisation och om en sådan datamottagare inte har partnerföretag eller anknutna företag som inte betraktas som mikroföretag eller små eller medelstora företag, får den överenskomna ersättningen inte överstiga de kostnader som anges i punkt 2 a.

5. Kommissionen ska anta riktlinjer för beräkningen av rimlig ersättning, med beaktande av råd från Europeiska datainnovationsstyrelsen som avses i artikel 42.

6. Denna artikel ska inte hindra annan unionsrätt eller nationell lagstiftning som antagits i enlighet med unionsrätten från att utesluta ersättning för tillgängliggörande av data eller föreskriva lägre ersättning.

7. Datahållaren ska ge datamottagaren tillräckligt detaljerad information om grunden för beräkningen av ersättningen så att datamottagaren kan bedöma huruvida kraven i punkterna 1–4 är uppfyllda.

Artikel 10

Tvistlösning

1. Användare, datahållare och datamottagare ska ha tillgång till ett tvistlösningsorgan, som certifierats i enlighet med punkt 5 i denna artikel, för att lösa tvister enligt artiklarna 4.3, 4.9 och 5.12 samt tvister avseende rättvisa, rimliga och icke-diskriminerande villkor för tillgängliggörande av data på ett öppet sätt i enlighet med detta kapitel och kapitel IV.

2. Tvistlösningsorganen ska informera de berörda parterna om avgifter eller mekanismer som används för att fastställa avgifter innan dessa parter begär ett beslut.

3. När det gäller tvister som hänskjutits till ett tvistlösningsorgan enligt artiklarna 4.3, 4.9 och 5.12, om tvistlösningsorganet avgör en tvist till förmån för användaren eller datamottagaren, ska datahållaren bära alla de avgifter som tas ut av tvistlösningsorganet och ersätta den användaren eller den datamottagaren för alla andra rimliga kostnader som denne har ådragit sig i samband med tvistlösningen. Om tvistlösningsorganet avgör en tvist till förmån för datahållaren ska användaren eller datamottagaren inte vara skyldig att ersätta några avgifter eller andra utgifter som datahållaren har betalat eller ska betala i samband med tvistlösningen, såvida inte tvistlösningsorganet finner att användaren eller datamottagaren uppenbart har handlat i ond tro.

4. Kunder och leverantörer av databehandlingstjänster ska ha tillgång till ett tvistlösningsorgan, som certifierats i enlighet med punkt 5 i denna artikel, för att lösa tvister som rör överträdelser av kundernas rättigheter och de skyldigheter som leverantörer av databehandlingstjänster har, i enlighet med artiklarna 23–31.

5. Den medlemsstat där tvistlösningsorganet är etablerat ska på begäran av det organet certifiera detta organ, om organet har visat att det uppfyller samtliga följande villkor:

a) Det är opartiskt och oberoende, och ska fatta sina beslut i enlighet med tydliga, icke-diskriminerande och rättvisa förfaranderegler.

b) Det har den sakkunskap som krävs, i synnerhet när det gäller rättvisa, rimliga och icke-diskriminerande villkor, inbegripet ersättning, och om att göra data tillgängliga på ett öppet sätt, vilket innebär att organet på ett effektivt sätt kan fastställa dessa villkor.

c) Det kan enkelt nås genom elektronisk kommunikationsteknik.

d) Det kan anta beslut på ett snabbt, effektivt och kostnadseffektivt sätt på minst ett av unionens officiella språk.

6. Medlemsstaterna ska underrätta kommissionen om de tvistlösningsorgan som certifierats i enlighet med punkt 5. Kommissionen ska offentliggöra en förteckning över dessa organ på en särskild webbplats och hålla den uppdaterad.

7. Ett tvistlösningsorgan ska vägra att behandla en begäran om lösning av en tvist som redan har hänskjutits till ett annat tvistlösningsorgan eller till en domstol i en medlemsstat.

8. Ett tvistlösningsorgan ska ge parterna möjlighet att inom rimlig tid framföra sina synpunkter i frågor som dessa parter har begärt ska prövas vid det organet. I detta sammanhang ska varje part i en tvist förses med inlagorna från den andra parten i tvisten och eventuella utlåtanden från experter. Parterna ska ges möjlighet att lämna synpunkter på sådana inlagor och utlåtanden.

9. Ett tvistlösningsorgan ska fatta sitt beslut i en fråga som hänskjutits till det inom 90 dagar efter mottagandet av en begäran enligt punkterna 1 och 4. Detta beslut ska vara skriftligt eller på ett varaktigt medium och ska åtföljas av en motivering.

10. Tvistlösningsorganen ska utarbeta och offentliggöra årliga verksamhetsrapporter. Sådana årliga rapporter ska innehålla i synnerhet följande information:

a) En sammanställning av utgången av tvister.

b) Den genomsnittliga tid det har tagit att lösa tvister.

c) De vanligaste skälen till tvister.

11. För att underlätta utbytet av information och bästa praxis får ett tvistlösningsorgan besluta att inkludera rekommendationer i den rapport som avses i punkt 10 om hur problem kan undvikas eller lösas.

12. Ett tvistlösningsorgans beslut ska endast vara bindande för parterna om parterna uttryckligen och innan tvistlösningsförfarandet inleds har samtyckt till att beslutet är bindande.

13. Denna artikel påverkar inte parters rätt att söka ett effektivt rättsmedel inför en domstol i en medlemsstat.

Artikel 11

Tekniska skyddsåtgärder om obehörig användning eller obehörigt utlämnande av data

1. En datahållare får vidta lämpliga tekniska skyddsåtgärder, inbegripet smarta kontrakt och kryptering, för att förhindra obehörig åtkomst till data, inbegripet metadata, och för att säkerställa överensstämmelse med artiklarna 4, 5, 6, 8 och 9 samt med de överenskomna avtalsvillkoren för tillgängliggörande av data. Sådana tekniska skyddsåtgärder får varken diskriminera mellan datamottagare eller hindra en användares rätt att erhålla en kopia av eller hämta, använda eller få åtkomst till data eller tillhandahålla tredje parter data enligt artikel 5 eller någon rätt för tredje part enligt unionsrätten eller nationell lagstiftning som antagits i enlighet med unionsrätten. Användare, tredje parter och datamottagare får inte ändra eller avlägsna sådana tekniska skyddsåtgärder såvida inte datahållaren samtycker till detta.

2. Under de omständigheter som avses i punkt 3 ska den tredje parten eller datamottagaren utan oskäligt dröjsmål tillmötesgå begärandena från datahållaren och, i tillämpliga fall och om det inte är samma person, innehavaren av en företagshemlighet eller användaren, om

a) att radera de data som tillhandahållits av datahållaren och eventuella kopior av dessa,

b) att avsluta produktion, erbjudande eller utsläppande på marknaden eller användning av varor, härledda data eller tjänster som framställts på grundval av kunskap som erhållits genom sådana data, eller import, export eller lagring av varor som innebär intrång för dessa ändamål, och förstöra alla varor som innebär intrång, om det finns en allvarlig risk för att den olagliga användningen av dessa data kommer att orsaka datahållaren, innehavaren av en företagshemlighet eller användaren betydande skada eller om en sådan åtgärd inte skulle vara oproportionell med hänsyn till intressena för datahållaren, innehavaren av en företagshemlighet eller användaren,

c) att informera användaren om den obehöriga användningen eller det obehöriga röjandet av data och om de åtgärder som vidtagits för att bringa den obehöriga användningen eller det obehöriga röjandet av dessa data att upphöra,

d) att ersätta den part som lider skada till följd av missbruk eller röjande av sådana data som olagligen åtkommits eller använts.

3. Punkt 2 ska vara tillämplig om en tredje part eller en datamottagare

a) i syfte att erhålla data har lämnat falsk information till en datahållare, använt bedrägliga eller tvingande medel eller missbrukat luckor i datahållarens tekniska infrastruktur som är utformad för att skydda dessa data,

b) har använt de data som gjorts tillgängliga för obehöriga ändamål, inbegripet utveckling av en konkurrerande uppkopplad produkt i den mening som avses i artikel 6.2 e,

c) olagligen har lämnat ut data till en annan part,

d) inte har upprätthållit de tekniska och organisatoriska åtgärder som överenskommits enligt artikel 5.9, eller

e) har ändrat eller avlägsnat tekniska skyddsåtgärder som tillämpas av datahållaren enligt punkt 1 i denna artikel utan datahållarens samtycke.

4. Punkt 2 ska också vara tillämplig om en användare ändrar eller avlägsnar tekniska skyddsåtgärder som datahållaren tillämpar eller inte upprätthåller de tekniska och organisatoriska åtgärder som vidtagits av användaren i samförstånd med datahållaren eller, om det inte är samma person, innehavaren av företagshemligheter, för att bevara företagshemligheter, samt med avseende på varje annan part som tar emot data från användaren i strid med denna förordning.

5. Om datamottagaren handlar i strid med artikel 6.2 a eller b ska användarna ha samma rättigheter som datahållarna enligt punkt 2 i den här artikeln.

Artikel 12

Omfattningen av skyldigheterna för datahållare som enligt unionsrätten är skyldiga att göra data tillgängliga

1. Detta kapitel ska tillämpas om en datahållare i förbindelser mellan företag är skyldig att göra data tillgängliga för en datamottagare enligt artikel 5 eller enligt tillämplig unionsrätt eller nationell lagstiftning som antagits i enlighet med unionsrätten.

2. Ett avtalsvillkor i ett datadelningsavtal som, till nackdel för en part eller, där detta är tillämpligt, till nackdel för användaren, utesluter tillämpningen av detta kapitel, avviker från det eller ändrar dess verkan, ska inte vara bindande för den parten.

KAPITEL IV

OSKÄLIGA AVTALSVILLKOR I SAMBAND MED ÅTKOMST TILL OCH ANVÄNDNING AV DATA MELLAN FÖRETAG

Artikel 13

Oskäliga avtalsvillkor som ensidigt åläggs ett annat företag

1. Ett avtalsvillkor om åtkomst till och användning av data eller om ansvar och rättsmedel vid överträdelse eller uppsägande av datarelaterade skyldigheter som ett företag ensidigt har ålagt ett annat företag ska inte vara bindande för det senare företaget om det är oskäligt.

2. Ett avtalsvillkor som återspeglar tvingande bestämmelser i unionsrätten eller bestämmelser i unionsrätten som skulle vara tillämpliga om frågan inte reglerades i avtalsvillkoren, ska inte anses vara oskäligt.

3. Ett avtalsvillkor är oskäligt om det är av sådan art att dess användning i hög grad avviker från god affärssed vid åtkomst till och användning av data i strid med god tro och god sed.

4. Ett avtalsvillkor ska i synnerhet vara oskäligt med avseende på tillämpningen av punkt 3 om det har till syfte eller verkan att

a) utesluta eller begränsa ansvaret för den part som ensidigt ålagt villkoret för uppsåtliga handlingar eller grov oaktsamhet,

b) utesluta de rättsmedel som står till buds för den part som ensidigt har ålagts villkoret i händelse av underlåtenhet att fullgöra avtalsförpliktelser eller utesluta ansvar för den part som ensidigt ålade avtalsvillkoret vid ett åsidosättande av dessa skyldigheter,

c) ge den part som ensidigt har föreskrivit villkoret ensamrätt att avgöra om de data som lämnas är i överensstämmelse med avtalet eller att tolka något avtalsvillkor.

5. Ett avtalsvillkor ska antas vara oskäligt med avseende på tillämpningen av punkt 3 om det har till syfte eller verkan att

a) på ett olämpligt sätt begränsa rättsmedlen vid underlåtenhet att fullgöra avtalsförpliktelser eller begränsa ansvaret vid ett åsidosättande av dessa skyldigheter eller utvidga ansvaret för det företag som ensidigt har ålagts villkoret,

b) tillåta den part som ensidigt införde villkoret att få åtkomst till och använda den andra avtalsslutande partens data på ett sätt som avsevärt skadar den andra avtalsslutande partens legitima intressen, särskilt när sådana data innehåller kommersiellt känsliga data eller skyddas av företagshemligheter eller immateriella rättigheter,

c) hindra den part som ensidigt har ålagts villkoret att använda de data som den parten har tillhandahållit eller genererat under avtalsperioden, eller att begränsa användningen av sådana data i en sådan omfattning att den parten inte har rätt att använda, samla in, få åtkomst till eller kontrollera sådana data eller utnyttja värdet av sådana data på ett adekvat sätt,

d) hindra den part som ensidigt har ålagts villkoret att säga upp avtalet inom rimlig tid,

e) hindra den part som ensidigt har ålagts villkoret att erhålla en kopia av de data som den parten har tillhandahållit eller genererat under avtalets löptid eller inom en rimlig tidsperiod efter det att avtalet sagts upp,

f) göra det möjligt för den part som ensidigt ålägger villkoret att säga upp avtalet med oskäligt kort varsel, med beaktande av varje rimlig möjlighet för den andra avtalsslutande parten att byta till en alternativ och jämförbar tjänst och den ekonomiska skada som följer av en sådan uppsägning, såvida det inte finns tungt vägande skäl för detta,

g) göra det möjligt för den part som ensidigt ålägger villkoret att väsentligt ändra det pris som anges i avtalet eller andra materiella villkor för de data som ska delas med avseende på deras art, format, kvalitet eller kvantitet, om inget giltigt skäl och ingen rätt för den andra parten att säga upp avtalet vid en sådan ändring anges i avtalet.

Första stycket g ska inte påverka villkor genom vilka den part som ensidigt ålägger villkoret förbehåller sig rätten att ensidigt ändra villkoren i ett avtal med obestämd löptid, förutsatt att det i avtalet anges ett giltigt skäl för sådana ensidiga ändringar, att den part som ensidigt ålägger villkoret är skyldig att underrätta den andra avtalsslutande parten med rimligt varsel om sådana avsedda ändringar och att den andra avtalsslutande parten har rätt att utan kostnad säga upp avtalet vid en ändring.

6. Ett avtalsvillkor ska anses vara ensidigt ålagt i den mening som avses i denna artikel om det har tillhandahållits av en avtalsslutande part och den andra avtalsslutande parten inte har kunnat påverka dess innehåll trots försök att förhandla om det. Det åligger den avtalsslutande part som har tillhandahållit avtalsvillkoret att bevisa att villkoret inte har införts ensidigt. Den avtalspart som har tillhandahållit det omtvistade avtalsvillkoret kan inte göra gällande att villkoret är ett oskäligt avtalsvillkor.

7. Om det oskäliga avtalsvillkoret kan avskiljas från övriga villkor i avtalet ska dessa återstående villkor vara bindande.

8. Denna artikel är inte tillämplig på avtalsvillkor som anger avtalets huvudsakliga syfte eller på prisets lämplighet i förhållande till de data som lämnas i utbyte.

9. Parterna i ett avtal som omfattas av punkt 1 ska inte utesluta tillämpningen av denna artikel, avvika från den eller ändra dess verkan.

KAPITEL V

GÖRA DATA TILLGÄNGLIGA FÖR OFFENTLIGA ORGAN, KOMMISSIONEN, EUROPEISKA CENTRALBANKEN OCH UNIONSORGAN PÅ GRUNDVAL AV ETT EXCEPTIONELLT BEHOV

Artikel 14

Skyldighet att göra data tillgängliga på grundval av ett exceptionellt behov

Om ett offentligt organ, kommissionen, Europeiska centralbanken eller ett unionsorgan visar att det föreligger ett exceptionellt behov, enligt artikel 15, av att använda vissa data, inbegripet de relevanta metadata som är nödvändiga för tolkningen och användningen av dessa data, för att fullgöra sina lagstadgade skyldigheter av allmänt intresse, ska datahållare som är andra juridiska personer än offentliga organ och som innehar dessa data göra dem tillgängliga på vederbörligen motiverad begäran.

Artikel 15

Exceptionellt behov av att använda data

1. Ett exceptionellt behov av att använda vissa data i den mening som avses i detta kapitel ska vara begränsat i tid och omfattning och ska anses föreligga endast under någon av följande omständigheter:

a) Om de begärda data är nödvändiga för att hantera ett allmänt nödläge och det offentliga organet, kommissionen, Europeiska centralbanken eller unionsorganet inte i tid, på ett ändamålsenligt sätt och på likvärdiga villkor kan erhålla sådana data på alternativa sätt.

b) Under omständigheter som inte omfattas av led a och endast när det gäller icke-personuppgifter, om

   i) ett offentligt organ, kommissionen, Europeiska centralbanken eller ett unionsorgan agerar på grundval av unionsrätten eller nationell rätt och har identifierat specifika data, vars avsaknad hindrar den eller det från att utföra en specifik uppgift av allmänt intresse som uttryckligen föreskrivs i lag, såsom framställning av officiell statistik eller begränsning av eller återhämtning från ett allmänt nödläge, och

   ii) det offentliga organet, kommissionen, Europeiska centralbanken eller unionsorganet har uttömt alla andra till buds stående medel för att erhålla sådana data, inbegripet inköp av data på marknaden genom att erbjuda marknadspris, eller genom att förlita sig på befintliga skyldigheter för att göra data tillgängliga eller antagande av nya lagstiftningsåtgärder som skulle kunna säkerställa att data finns tillgängliga i tid.

2. Punkt 1 b ska inte tillämpas på mikroföretag och små företag.

3. Skyldigheten att visa att det offentliga organet inte har kunnat erhålla icke-personuppgifter genom att köpa in dem på marknaden ska inte gälla om den specifika uppgiften av allmänt intresse är framställning av officiell statistik och om inköp av sådana data inte är tillåtet enligt nationell rätt.

Artikel 16

Förhållande till andra skyldigheter att göra data tillgängliga för offentliga organ, kommissionen, Europeiska centralbanken och unionsorgan

1. Detta kapitel ska inte påverka de skyldigheter som fastställs i unionsrätten eller nationell rätt vad gäller rapportering eller att tillmötesgå begäranden om åtkomst till information eller visa eller kontrollera efterlevnaden av rättsliga skyldigheter.

2. Detta kapitel ska inte tillämpas på offentliga organ, kommissionen, Europeiska centralbanken eller unionsorgan som bedriver verksamhet som syftar till att förebygga, förhindra, utreda, upptäcka eller lagföra brott eller administrativa överträdelser eller verkställa straffrättsliga påföljder, eller på tull- eller skatteförvaltning. Detta kapitel påverkar inte tillämplig unionsrätt eller nationell rätt om förebyggande, förhindrande, utredning, upptäckt eller lagföring av brott eller administrativa överträdelser eller verkställighet av straffrättsliga påföljder eller administrativa sanktioner, eller för tull- eller skatteförvaltning.

Artikel 17

Begäran om att data ska göras tillgängliga

1. Ett offentligt organ, kommissionen, Europeiska centralbanken eller ett unionsorgan som begär data enligt artikel 14 ska

a) specificera vilka data som krävs, inbegripet de relevanta metadata som är nödvändiga för att tolka och använda dessa data,

b) visa att de nödvändiga villkor för att det föreligger ett exceptionellt behov enligt artikel 15 för det ändamål för vilket data begärs är uppfyllda,

c) förklara syftet med begäran, den avsedda användningen av begärda data, i tillämpliga fall även av en tredje part i enlighet med punkt 4 i denna artikel, användningens varaktighet, och när så är lämpligt hur behandlingen av personuppgifter ska tillgodose det exceptionella behovet,

d) om möjligt specificera när data förväntas raderas av alla parter som har åtkomst till dem,

e) motivera valet av datahållare till vilken begäran riktas,

f) specificera eventuella andra offentliga organ eller kommissionen, Europeiska centralbanken eller unionsorgan och de tredje parter med vilka begärda data förväntas delas,

g) om personuppgifter begärs, specificera vilka tekniska och organisatoriska åtgärder som är nödvändiga och proportionella för att genomföra dataskyddsprinciperna och de nödvändiga skyddsåtgärderna, såsom pseudonymisering, och huruvida datahållaren kan tillämpa anonymisering innan data görs tillgängliga,

h) ange den rättsliga bestämmelse som tilldelar det begärande offentliga organet, kommissionen, Europeiska centralbanken eller unionsorganet den specifika uppgift av allmänt intresse som är relevant för begäran om data,

i) ange den tidsfrist inom vilken data ska tillgängliggöras och den tidsfrist som avses i artikel 18.2 inom vilken datahållaren får neka eller begära ändring av begäran,

j) göra sitt yttersta för att undvika att ett tillmötesgående av begäran om data leder till att datahållare blir ansvariga för överträdelser av unionsrätten eller nationell rätt.

2. En begäran om data enligt punkt 1 i denna artikel ska

a) göras skriftligen och uttryckas på ett klart, koncist och tydligt språk som kan förstås av datahållaren,

b) vara specifik avseende den typ av data som begärs och avse data som datahållaren har kontroll över vid tidpunkten för begäran,

c) stå i proportion till det exceptionella behovet och vara motiverad, i fråga om detaljnivå och omfattning av begärda data och hur ofta dessa begärda data kommer att tillgås,

d) respektera datahållarens legitima mål och innehålla ett åtagande om att säkerställa skyddet av företagshemligheter i enlighet med artikel 19.3 och beakta de kostnader och ansträngningar som krävs för att göra data tillgängliga,

e) gälla icke-personuppgifter och, endast om detta har visats vara otillräckligt för att tillgodose det exceptionella behovet av att använda data i enlighet med artikel 15.1 a, begära personuppgifter i pseudonymiserad form och fastställa de tekniska och organisatoriska åtgärder som ska vidtas för att skydda dessa data,

f) informera datahållaren om de sanktioner som den behöriga myndighet som utsetts enligt artikel 37 ska ålägga enligt artikel 40 om begäran inte tillmötesgås,

g) om begäran görs av ett offentligt organ, överföras till den datasamordnare som avses i artikel 37 i den medlemsstat där det begärande offentliga organet är etablerat, som utan oskäligt dröjsmål ska offentliggöra begäran på nätet såvida datasamordnaren inte anser att sådant offentliggörande skulle utgöra en risk för den allmänna säkerheten,

h) om begäran görs av kommissionen, Europeiska centralbanken eller ett unionsorgan, utan oskäligt dröjsmål göras tillgänglig på nätet,

i) om personuppgifter begärs, utan oskäligt dröjsmål anmälas till den tillsynsmyndighet som ansvarar för att övervaka tillämpningen av förordning (EU) 2016/679 i den medlemsstat där det offentliga organet är etablerat.

Europeiska centralbanken och unionsorgan ska underrätta kommissionen om sina begäranden.

3. Ett offentligt organ, kommissionen, Europeiska centralbanken eller ett unionsorgan får inte göra data som erhållits enligt detta kapitel tillgängliga för vidareutnyttjande enligt definitionen i artikel 2.2 i förordning (EU) 2022/868 eller artikel 2.11 i direktiv (EU) 2019/1024. Förordning (EU) 2022/868 och direktiv (EU) 2019/1024 ska inte tillämpas på data som innehas av offentliga organ och som erhållits enligt detta kapitel.

4. Punkt 3 i denna artikel hindrar inte ett offentligt organ, kommissionen, Europeiska centralbanken eller ett unionsorgan från att utbyta data som erhållits enligt detta kapitel med andra offentliga organ eller kommissionen, Europeiska centralbanken eller unionsorgan, i syfte att fullgöra de uppgifter som avses i artikel 15, enligt vad som anges i begäran i enlighet med punkt 1 f i den här artikeln, eller att göra dessa data tillgängliga för en tredje part om det eller den genom ett offentligt tillgängligt avtal har delegerat tekniska inspektioner eller andra funktioner till denna tredje part. Skyldigheterna för offentliga organ enligt artikel 19, särskilt skyddsåtgärder för att bevara konfidentialiteten för företagshemligheter, ska även tillämpas på sådana tredje parter. Om ett offentligt organ eller kommissionen, Europeiska centralbanken eller ett unionsorgan överför eller tillgängliggör data enligt den här punkten ska det eller den utan oskäligt dröjsmål underrätta den datahållare från vilken dessa data mottogs.

5. Om datahållaren anser att dess rättigheter enligt detta kapitel har kränkts genom överföringen eller tillgängliggörandet av data, får denne lämna in ett klagomål till den behöriga myndighet som utsetts enligt artikel 37 i den medlemsstat där datahållaren är etablerad.

6. Kommissionen ska utarbeta en mall för begäranden enligt denna artikel.

Artikel 18

Tillmötesgående av begäran om data

1. En datahållare som mottar en begäran om att göra data tillgängliga enligt detta kapitel ska utan oskäligt dröjsmål göra dessa data tillgängliga för det begärande offentliga organet, kommissionen, Europeiska centralbanken eller ett unionsorgan, med beaktande av nödvändiga tekniska, organisatoriska och rättsliga åtgärder.

2. Utan att det påverkar de särskilda behov vad gäller tillgänglighet av data som fastställs i unionsrätten eller nationell rätt får en datahållare avslå eller ansöka om ändring av en begäran om att göra data tillgängliga enligt detta kapitel utan oskäligt dröjsmål och under alla omständigheter senast fem arbetsdagar efter mottagandet av en begäran om data som är nödvändiga för att hantera ett allmänt nödläge och utan oskäligt dröjsmål och, under alla omständigheter, senast 30 arbetsdagar efter mottagandet av en sådan begäran i andra fall av exceptionellt behov, av något av följande skäl:

a) Datahållaren har inte kontroll över de data som begärs.

b) En liknande begäran för samma ändamål har tidigare lämnats in av ett annat offentligt organ eller kommissionen, Europeiska centralbanken eller ett unionsorgan, och datahållaren har inte underrättats om att dessa data har raderats enligt artikel 19.1 c.

c) Begäran uppfyller inte villkoren i artikel 17.1 och 17.2.

3. Om datahållaren beslutar sig för att avslå begäran eller ansöka om ändring av den i enlighet med punkt 2 b, ska denne ange identiteten på det offentliga organ eller kommissionen, Europeiska centralbanken eller det unionsorgan som tidigare lämnat in en begäran för samma ändamål.

4. Om de data som begärs innehåller personuppgifter ska datahållaren anonymisera personuppgifterna på korrekt sätt, såvida det inte för att tillmötesgå begäran om att göra data tillgängliga för ett offentligt organ, kommissionen, Europeiska centralbanken eller ett unionsorgan krävs att personuppgifterna lämnas ut. I sådana fall ska datahållaren pseudonymisera personuppgifterna.

5. Om det offentliga organet, kommissionen, Europeiska centralbanken eller unionsorganet vill överklaga en datahållares vägran att tillhandahålla begärda data eller om datahållaren vill bestrida begäran och ärendet inte kan lösas genom en lämplig ändring av begäran, ska ärendet hänskjutas till den behöriga myndighet som utsetts enligt artikel 37 i den medlemsstat där datahållaren är etablerad.

Artikel 19

Skyldigheter för offentliga organ, kommissionen, Europeiska centralbanken och unionsorgan

1. Ett offentligt organ, kommissionen, Europeiska centralbanken eller ett unionsorgan som tar emot data till följd av en begäran enligt artikel 14

a) får inte använda dessa data på ett sätt som är oförenligt med det ändamål för vilket de begärdes,

b) ska ha genomfört tekniska och organisatoriska åtgärder som bevarar konfidentialiteten och integriteten avseende de data som begärs och säkerheten vid överföring av data, särskilt personuppgifter, och som skyddar de registrerades rättigheter och friheter,

c) ska radera dessa data så snart de inte längre är nödvändiga för det angivna ändamålet och utan oskäligt dröjsmål informera datahållaren och enskilda personer eller organisationer som har tagit emot data enligt artikel 21.1 om att de har raderats, såvida det inte krävs att dessa data arkiveras i enlighet med unionsrätt eller nationell rätt om allmänhetens tillgång till handlingar i samband med insynsskyldigheter.

2. Ett offentligt organ, kommissionen, Europeiska centralbanken, ett unionsorgan eller en tredje part som tar emot data enligt detta kapitel får inte

a) använda data eller insikter om datahållarens ekonomiska situation, tillgångar och produktions- eller driftsmetoder för att utveckla eller förbättra en uppkopplad produkt eller tillhörande tjänst som konkurrerar med datahållarens uppkopplade produkt eller tillhörande tjänst,

b) dela dessa data med en annan tredje part för något av de ändamål som avses i led a.

3. Röjande av företagshemligheter till ett offentligt organ, kommissionen, Europeiska centralbanken eller ett unionsorgan ska endast krävas i den mån det är absolut nödvändigt för att uppnå syftet med en begäran enligt artikel 15. I sådana fall ska datahållaren eller, om det inte rör sig om samma person, innehavaren av en företagshemlighet identifiera de data som skyddas som företagshemligheter, inbegripet relevanta metadata. Det offentliga organet, kommissionen, Europeiska centralbanken eller unionsorganet ska före röjandet av företagshemligheter vidta alla nödvändiga och lämpliga tekniska och organisatoriska åtgärder för att bevara konfidentialiteten för företagshemligheterna, när så är lämpligt även användning av standardavtalsvillkor och tekniska standarder samt tillämpning av uppförandekoder.

4. Ett offentligt organ, kommissionen, Europeiska centralbanken eller ett unionsorgan ska ansvara för säkerheten för de data som de tar emot.

Artikel 20

Ersättning vid situationer då det föreligger ett exceptionellt behov

1. Andra datahållare än mikroföretag och små företag ska kostnadsfritt tillgängliggöra de data som är nödvändiga för att hantera ett allmänt nödläge enligt artikel 15.1 a. Det offentliga organ, kommissionen, Europeiska centralbanken eller det unionsorgan som har tagit emot dessa data ska ge datahållaren offentligt erkännande på begäran av datahållaren.

2. Datahållaren ska ha rätt till skälig ersättning för att göra data tillgängliga i enlighet med en begäran som gjorts enligt artikel 15.1 b. Sådan ersättning ska täcka de tekniska och organisatoriska kostnader som uppstår till följd av tillmötesgåendet av begäran, inbegripet, vid behov, kostnaderna för anonymisering, pseudonymisering, aggregering och teknisk anpassning, och en rimlig marginal. På begäran av det offentliga organet, kommissionen, Europeiska centralbanken eller unionsorganet ska datahållaren tillhandahålla information om underlaget till kostnadsberäkningen och den rimliga marginalen.

3. Punkt 2 ska också vara tillämplig om mikroföretag och små företag begär ersättning för att göra data tillgängliga.

4. Datahållare ska inte ha rätt till ersättning för att göra data tillgängliga i enlighet med en begäran som gjorts enligt artikel 15.1 b, om den specifika uppgiften av allmänt intresse är framställning av officiell statistik och om inköp av data inte är tillåten enligt nationell rätt. Medlemsstaterna ska underrätta kommissionen om inköp av data för framställning av officiell statistik inte är tillåtet enligt nationell rätt.

5. Om det offentliga organet, kommissionen, Europeiska centralbanken eller unionsorganet inte godtar den ersättningsnivå som datahållaren begär, får det eller den lämna in ett klagomål till den behöriga myndighet som utsetts enligt artikel 37 i den medlemsstat där datahållaren är etablerad.

Artikel 21

Delning av data som erhållits i samband med ett exceptionellt behov med forskningsorganisationer eller statistikorgan

1. Ett offentligt organ, kommissionen, Europeiska centralbanken eller ett unionsorgan ska ha rätt att dela data som mottagits enligt detta kapitel

a) med enskilda personer eller organisationer i syfte att bedriva vetenskaplig forskning eller analys som är förenlig med det ändamål för vilket data begärdes, eller

b) med nationella statistikbyråer och Eurostat för framställning av officiell statistik.

2. Enskilda personer eller organisationer som tar emot data enligt punkt 1 ska agera utan vinstsyfte eller inom ramen för ett uppdrag av allmänt intresse som erkänns i unionsrätten eller nationell rätt. Detta omfattar inte organisationer på vilka kommersiella företag har ett betydande inflytande som sannolikt skulle kunna leda till förmånstillträde till forskningsresultaten.

3. Enskilda personer eller organisationer som tar emot data enligt punkt 1 i denna artikel ska fullgöra samma skyldigheter som dem som är tillämpliga på offentliga organ, kommissionen, Europeiska centralbanken eller unionsorgan enligt artiklarna 17.3 och 19.

4. Trots vad som anges i artikel 19.1 c får enskilda personer eller organisationer som tar emot data enligt punkt 1 i den här artikeln behålla de data som mottagits för det ändamål för vilket data begärdes i upp till sex månader efter det att dessa data har raderats av de offentliga organen, kommissionen, Europeiska centralbanken och unionsorgan.

5. Om ett offentligt organ, kommissionen, Europeiska centralbanken eller ett unionsorgan har för avsikt att överföra eller tillgängliggöra data enligt punkt 1 i denna artikel ska det eller den utan oskäligt dröjsmål underrätta den datahållare från vilken dessa data mottogs samt uppge identitet och kontaktuppgifter för den organisation eller enskilda person som tar emot data, ändamålet med överföringen eller tillgängliggörandet av data, den period under vilken data ska användas och de tekniska skyddsåtgärder och organisatoriska åtgärder som har vidtagits för att skydda dessa data, även om det rör sig om personuppgifter eller företagshemligheter. Om datahållaren inte godtar överföringen eller tillgängliggörandet av data, får denne lämna in ett klagomål till den behöriga myndighet som utsetts enligt artikel 37 i den medlemsstat där datahållaren är etablerad.

Artikel 22

Ömsesidigt bistånd och gränsöverskridande samarbete

1. Offentliga organ, kommissionen, Europeiska centralbanken och unionsorgan ska samarbeta och bistå varandra för att genomföra detta kapitel på ett konsekvent sätt.

2. Data som utbyts i samband med begärt bistånd och som tillhandahållits enligt punkt 1 får inte användas på ett sätt som är oförenligt med det ändamål för vilket de begärdes.

3. Om ett offentligt organ avser att begära data från en datahållare som är etablerad i en annan medlemsstat, ska den först underrätta den behöriga myndighet som utsetts enligt artikel 37 i den medlemsstaten om den avsikten. Detta krav ska även gälla för begäranden från kommissionen, Europeiska centralbanken och unionsorgan. Begäran ska granskas av den behöriga myndigheten i den medlemsstat där datahållaren är etablerad.

4. Efter att ha granskat begäran mot bakgrund av kraven enligt artikel 17, ska den relevanta behöriga myndigheten utan oskäligt dröjsmål vidta en av följande åtgärder:

a) Överföra begäran till datahållaren och i tillämpliga fall ge det begärande offentliga organet, kommissionen, Europeiska centralbanken eller unionsorganet råd om det eventuella behovet av att samarbeta med offentliga organ i den medlemsstat där datahållaren är etablerad, i syfte att minska den administrativa bördan för datahållaren när det gäller att tillmötesgå begäran.

b) Avslå begäran av vederbörligen motiverade skäl i enlighet med detta kapitel.

Det begärande offentliga organet, kommissionen, Europeiska centralbanken eller unionsorganet ska beakta råden från och de skäl som anges av den relevanta behöriga myndigheten enligt första stycket innan ytterligare åtgärder vidtas, såsom en inlämning på nytt av begäran, i tillämpliga fall.

KAPITEL VI

BYTE AV DATABEHANDLINGSTJÄNSTER

Artikel 23

Undanröjande av hinder för ett effektivt byte

Leverantörer av databehandlingstjänster ska vidta de åtgärder som föreskrivs i artiklarna 25, 26, 27, 29 och 30 för att göra det möjligt för kunder att byta till en databehandlingstjänst som omfattar samma tjänstetyp och som tillhandahålls av en annan leverantör av databehandlingstjänster, eller till lokal IKT-infrastruktur, eller, i förekommande fall, att använda flera leverantörer av databehandlingstjänster samtidigt. I synnerhet ska leverantörer av databehandlingstjänster inte införa utan i stället undanröja förkommersiella, kommersiella, tekniska, avtalsmässiga och organisatoriska hinder som hindrar kunderna från att

a) säga upp avtalet om databehandlingstjänsten efter den maximala uppsägningstiden och efter det att bytesprocessen har slutförts med framgång, i enlighet med artikel 25,

b) ingå nya avtal med en annan leverantör av databehandlingstjänster som täcker samma tjänstetyp,

c) portera kundens exporterbara data och digitala tillgångar till en annan leverantör av databehandlingstjänster eller till lokal IKT-infrastruktur, även efter att ha utnyttjat ett gratiserbjudande,

d) i enlighet med artikel 24 uppnå funktionell likvärdighet i användningen av den nya databehandlingstjänsten i IKT-miljön hos en annan leverantör av databehandlingstjänster som omfattar samma tjänstetyp,

e) om det är tekniskt möjligt separera de databehandlingstjänster som avses i artikel 30.1 från andra databehandlingstjänster som tillhandahålls av leverantören av databehandlingstjänster.

Artikel 24

Tillämpningsområdet för de tekniska skyldigheterna

Ansvaret för leverantörer av databehandlingstjänster enligt artiklarna 23, 25, 29, 30 och 34 ska endast gälla de tjänster, avtal eller affärsmetoder som tillhandahålls av den ursprungliga leverantören av databehandlingstjänster.

Artikel 25

Avtalsvillkor om byte

1. Kundens rättigheter och leverantörens skyldigheter vad gäller ett byte av leverantör av databehandlingstjänster eller, i tillämpliga fall, till lokal IKT-infrastruktur ska tydligt anges i ett skriftligt avtal. Leverantören av databehandlingstjänster ska göra detta avtal tillgängligt för kunden före undertecknandet av avtalet på ett sätt som gör det möjligt för kunden att lagra och återge avtalet.

2. Utan att det påverkar tillämpningen av direktiv (EU) 2019/770 ska det avtal som avses i punkt 1 i denna artikel innehålla åtminstone följande:

a) Villkor som gör det möjligt för kunden att på begäran byta till en databehandlingstjänst som erbjuds av en annan leverantör av databehandlingstjänster eller att portera alla exporterbara data och digitala tillgångar till lokal IKT-infrastruktur, utan oskäligt dröjsmål och under alla omständigheter senast efter den maximala övergångsperioden på 30 kalenderdagar, som ska inledas efter den maximala uppsägningstid som avses i led d, under vilken tjänsteavtalet fortfarande är tillämpligt och under vilken leverantören av databehandlingstjänster ska

   i) ge kunden och tredje parter som kunden har godkänt rimligt bistånd i bytesprocessen,

ii) iaktta vederbörlig omsorg för att upprätthålla driftskontinuitet och fortsätta att tillhandahålla funktioner eller tjänster enligt avtalet,

iii) tillhandahålla tydlig information om kända risker för kontinuiteten i tillhandahållandet av funktioner eller tjänster från den ursprungliga leverantören av databehandlingstjänster,

iv) säkerställa att en hög säkerhetsnivå upprätthålls under hela bytesprocessen, särskilt säkerheten för data under överföringen och den fortsatta säkerheten för dessa data under den period för datahämtning som avses i led g, i enlighet med tillämplig unionsrätt eller nationell rätt.

b) En skyldighet för leverantören av databehandlingstjänster att stödja den utträdesstrategi för kunden som är relevant för de avtalade tjänsterna, bland annat genom att tillhandahålla all relevant information.

c) Ett villkor som anger att avtalet ska anses vara uppsagt och att kunden ska underrättas om detta i något av följande fall:

i) I tillämpliga fall, efter ett framgångsrikt slutförande av bytesprocessen.

ii) Vid utgången av den maximala uppsägningstid som avses i led d, om kunden inte vill byta utan radera sina exporterbara data och digitala tillgångar när tjänsten upphör.

d) En maximal uppsägningstid för inledande av bytesprocessen, som inte får överstiga två månader.

e) En uttömmande specifikation av alla kategorier av data och digitala tillgångar som kan porteras under bytesprocessen, inklusive åtminstone alla exporterbara data.

f) En uttömmande specifikation av alla kategorier av data som är specifika för att leverantörens databehandlingstjänsten ska fungera internt och som ska undantas från de exporterbara data enligt led e om det finns en risk för överträdelse med avseende på leverantörens företagshemligheter, förutsatt att sådana undantag inte hindrar eller försenar den bytesprocess som föreskrivs i artikel 23.

g) En minimiperiod för datahämtning på minst 30 kalenderdagar, med början efter det att den övergångsperiod som överenskommits mellan kunden och leverantören av databehandlingstjänster har löpt ut, i enlighet med led a i denna punkt och punkt 4.

h) Ett villkor som säkerställer fullständig radering av alla exporterbara data och digitala tillgångar som genereras direkt av kunden eller som direkt berör kunden, efter utgången av den period för datahämtning som avses i led g eller efter utgången av en alternativ överenskommen period vid en senare tidpunkt än den dag då den period för datahämtning som avses i led g löper ut, förutsatt att bytesprocessen har slutförts med framgång.

i) Bytesavgifter som får införas av leverantörer av databehandlingstjänster i enlighet med artikel 29.

3. Det avtal som avses i punkt 1 ska innehålla klausuler enligt vilka kunden får underrätta leverantören av databehandlingstjänster om sitt beslut att vidta en eller flera av följande åtgärder när den maximala uppsägningstid som avses i punkt 2 d löper ut:

a) Byta till en annan leverantör av databehandlingstjänster; kunden ska i så fall tillhandahålla nödvändiga uppgifter om den leverantören.

b) Byta till lokal IKT-infrastruktur.

c) Radera sina exporterbara data och digitala tillgångar.

4. Om den obligatoriska maximala övergångsperiod som föreskrivs i punkt 2 a är tekniskt ogenomförbar ska leverantören av databehandlingstjänster underrätta kunden inom 14 arbetsdagar efter det att begäran om byte gjorts och vederbörligen motivera varför det är tekniskt ogenomförbart samt ange en alternativ övergångsperiod, som inte får överstiga sju månader. I enlighet med punkt 1 ska driftskontinuitet säkerställas under hela den alternativa övergångsperiod.

5. Utan att det påverkar tillämpningen av punkt 4 ska det avtal som avses i punkt 1 innehålla klausuler som ger kunden rätt att förlänga övergångsperioden en gång med en tidsperiod som kunden anser lämpligare för sina egna ändamål.

Artikel 26

Informationsskyldighet för leverantörer av databehandlingstjänster

Leverantören av databehandlingstjänster ska förse kunden med

a) information om tillgängliga förfaranden för byte och portering till databehandlingstjänsten, inbegripet information om tillgängliga metoder och format för byten och portering samt tekniska och andra begränsningar som leverantören av databehandlingstjänster känner till,

b) en hänvisning till ett uppdaterat onlineregister som sköts av leverantören av databehandlingstjänster, med uppgifter om alla datastrukturer och dataformat samt relevanta standarder och öppna interoperabilitetsspecifikationer i vilka de exporterbara data som avses i artikel 25.2 e är tillgängliga.

Artikel 27

Skyldighet att handla i god tro

Alla berörda parter, inbegripet destinationsleverantörer av databehandlingstjänster, ska samarbeta i god tro för att göra bytesprocessen effektiv, möjliggöra snabb överföring av data och bibehålla databehandlingstjänstens kontinuitet.

Artikel 28

Avtalsenliga insynsskyldigheter i fråga om internationell åtkomst och överföring

1. Leverantörer av databehandlingstjänster ska göra följande information tillgänglig på sina webbplatser och hålla den informationen uppdaterad:

a) Vilken jurisdiktion som den IKT-infrastruktur som används för databehandling av deras enskilda tjänster tillhör.

b) En allmän beskrivning av de tekniska, organisatoriska och avtalsmässiga åtgärder som leverantören av databehandlingstjänster vidtagit för att förhindra internationell statlig åtkomst till eller överföring av icke-personuppgifter som innehas i unionen, om en sådan åtkomst eller överföring skulle strida mot unionsrätten eller den berörda medlemsstatens nationella rätt.

2. De webbplatser som avses i punkt 1 ska förtecknas i avtal för alla databehandlingstjänster som erbjuds av leverantörer av databehandlingstjänster.

Artikel 29

Gradvist avskaffande av bytesavgifter

1. Från och med den 12 januari 2027 får leverantörer av databehandlingstjänster inte ta ut några bytesavgifter av kunden för bytesprocessen.

2. Från och med den 11 januari 2024 till och med 12 januari 2027 får leverantörer av databehandlingstjänster ta ut nedsatta bytesavgifter av kunden för bytesprocessen.

3. De nedsatta bytesavgifter som avses i punkt 2 får inte överstiga de kostnader som är direkt kopplade till den berörda bytesprocessen som uppstår för leverantören av databehandlingstjänster.

4. Innan leverantörer av databehandlingstjänster ingår avtal med en kund ska de förse den presumtiva kunden med tydlig information om vilka standardavgifter och straffavgifter för förtida uppsägning som kan komma att utkrävas, samt om de nedsatta bytesavgifterna som kan komma att utkrävas under den tidsperiod som avses i punkt 2.

5. I förekommande fall ska leverantörer av databehandlingstjänster tillhandahålla information till en kund om databehandlingstjänster som inbegriper mycket komplexa eller kostsamma byten eller för vilka det är omöjligt att byta utan betydande störningar i data, digitala tillgångar eller tjänstearkitektur.

6. I tillämpliga fall ska leverantörerna av databehandlingstjänster göra den information som avses i punkterna 4 och 5 allmänt tillgänglig för kunderna via en särskild del av sin webbplats eller på något annat lättillgängligt sätt.

7. Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 45 med avseende på att komplettera denna förordning genom att inrätta en övervakningsmekanism som låter kommissionen övervaka de bytesavgifter som tas ut av leverantörer av databehandlingstjänster på marknaden för att säkerställa att avskaffandet och nedsättningen av bytesavgifter enligt punkterna 1 och 2 i den här artikeln kommer att genomföras i enlighet med de tidsfrister som föreskrivs i de punkterna.

Artikel 30

Tekniska aspekter av byte

1. Leverantörer av databehandlingstjänster som avser skalbara och elastiska datorresurser begränsade till infrastrukturella element såsom servrar, nät och de virtuella resurser som krävs för driften av infrastrukturen, men som inte ger åtkomst till de operativa tjänster, den programvara och de applikationer som lagras, på annat sätt behandlas eller används på dessa infrastrukturkomponenter ska, i enlighet med artikel 27, vidta alla rimliga åtgärder som står i deras makt för att underlätta för kunden att, efter att denna har bytt till en tjänst som omfattar samma tjänstetyp, uppnå funktionell likvärdighet vid användningen av den destinationstjänsten för databehandling. Den ursprungliga leverantören av databehandlingstjänster ska underlätta bytesprocessen genom att tillhandahålla kapacitet, adekvat information, dokumentation, tekniskt stöd och, vid behov, nödvändiga verktyg.

2. Andra leverantörer av databehandlingstjänster än de som avses i punkt 1 ska göra öppna gränssnitt tillgängliga i samma utsträckning för alla sina kunder och de berörda destinationsleverantörerna av databehandlingstjänster och kostnadsfritt i syfte att underlätta bytesprocessen. Dessa gränssnitt ska innehålla tillräcklig information om den berörda tjänsten för att möjliggöra utveckling av programvara för kommunikation med tjänsterna, i syfte att åstadkomma dataportabilitet och interoperabilitet.

3. För andra databehandlingstjänster än de som avses i punkt 1 i denna artikel ska leverantörer av databehandlingstjänster säkerställa kompatibilitet med gemensamma specifikationer som bygger på öppna interoperabilitetsspecifikationer eller harmoniserade standarder för interoperabilitet minst tolv månader efter det att hänvisningarna till dessa gemensamma specifikationer eller harmoniserade standarder för interoperabla databehandlingstjänster offentliggjordes i det centrala unionsregistret över standarder för interoperabla databehandlingstjänster efter offentliggörandet av de underliggande genomförandeakterna i *Europeiska unionens officiella tidning* i enlighet med artikel 35.8.

4. Andra leverantörer av databehandlingstjänster än de som avses i punkt 1 i denna artikel ska uppdatera det onlineregister som avses i artikel 26 b i enlighet med sina skyldigheter enligt punkt 3 i den här artikeln.

5. Vid byten mellan tjänster av samma tjänstetyp, för vilka gemensamma specifikationer eller harmoniserade standarder för interoperabla databehandlingstjänster som avses i punkt 3 i denna artikel inte har offentliggjorts i det centrala unionsregistret över standarder för interoperabla databehandlingstjänster i enlighet med artikel 35.8, ska leverantören av databehandlingstjänsterna på kundens begäran exportera alla exporterbara data i ett strukturerat, allmänt använt och maskinläsbart format.

6. Leverantörer av databehandlingstjänster ska inte vara skyldiga att utveckla ny teknik eller nya tjänster, eller att röja eller överföra digitala tillgångar som skyddas genom immateriella rättigheter eller utgör en företagshemlighet till en kund eller en annan leverantör av databehandlingstjänster eller att äventyra kundens eller leverantörens driftssäkerhet och driftsintegritet.

Artikel 31

Särskild ordning för vissa databehandlingstjänster

1. De skyldigheter som fastställs i artiklarna 23 d, 29, 30.1 och 30.3 ska inte tillämpas på databehandlingstjänster där de flesta huvudfunktioner har skräddarsytts för att tillgodose en enskild kunds särskilda behov eller där alla komponenter har utvecklats för en enskild kunds räkning, och om dessa databehandlingstjänster inte erbjuds i stor kommersiell skala via tjänstekatalogen hos leverantören av databehandlingstjänster.

2. De skyldigheter som fastställs i detta kapitel ska inte tillämpas på databehandlingstjänster som tillhandahålls som en icke-produktionsversion för testnings- och utvärderingsändamål och under en begränsad tidsperiod.

3. Innan ett avtal om tillhandahållande av de databehandlingstjänster som avses i denna artikel ingås ska leverantören av databehandlingstjänster informera den potentiella kunden om vilka skyldigheter i detta kapitel som inte är tillämpliga.

KAPITEL VII

OLAGLIG INTERNATIONELL STATLIG ÅTKOMST TILL OCH ÖVERFÖRING AV ICKE-PERSONUPPGIFTER

Artikel 32

Internationell statlig åtkomst och överföring

1. Leverantörer av databehandlingstjänster ska vidta alla adekvata tekniska, organisatoriska och rättsliga åtgärder, inbegripet avtal, för att förhindra internationell statlig åtkomst och tredjeländers statliga åtkomst till och överföring av icke-personuppgifter som innehas i unionen, om en sådan överföring eller åtkomst skulle strida mot unionsrätten eller den berörda medlemsstatens nationella rätt, utan att det påverkar tillämpningen av punkt 2 eller 3.

2. Beslut eller domar från en domstol i ett tredjeland och beslut från en administrativ myndighet i ett tredjeland där det krävs att en leverantör av databehandlingstjänster överför eller ger åtkomst till icke-personuppgifter som omfattas av denna förordning och som innehas i unionen ska endast erkännas eller genomföras på något som helst sätt om de grundar sig på en internationell överenskommelse, såsom ett fördrag om ömsesidig rättslig hjälp, som gäller mellan det begärande tredjelandet och unionen, eller ett sådant avtal mellan det begärande tredjelandet och en medlemsstat.

3. I de fall då, i avsaknad av en internationell överenskommelse som avses i punkt 2, en leverantör av databehandlingstjänster är adressat för ett beslut eller en dom från en domstol i ett tredjeland eller ett beslut från en administrativ myndighet i ett tredjeland om att överföra eller ge åtkomst till icke-personuppgifter som omfattas av tillämpningsområdet för denna förordning och som innehas i unionen, och efterlevnaden av ett sådant beslut skulle riskera att medföra att adressaten bryter mot unionsrätten eller den berörda medlemsstatens nationella rätt, ska tredjelandsmyndigheten motta eller få åtkomst till sådana data endast om

a) tredjelandets system kräver att skälen till ett sådant beslut och beslutets proportionalitet ska fastställas och föreskriver att beslutet eller domen är av specifik art, exempelvis genom att det fastställs en tillräckligt stark koppling till vissa misstänkta personer eller till överträdelser,

b) adressatens motiverade invändning är föremål för en granskning av en behörig domstol i tredjelandet, och

c) den behöriga domstol i tredjelandet som utfärdar beslutet eller domen eller granskar en administrativ myndighets beslut enligt det tredjelandets rätt har befogenhet att ta vederbörlig hänsyn till de relevanta rättsliga intressena för leverantören av de data som skyddas av unionsrätten eller den berörda medlemsstatens nationella rätt.

Beslutets eller domens adressat får begära ett yttrande från det relevanta nationella organ eller den relevanta nationella myndighet som har behörighet för internationellt samarbete i rättsliga frågor, för att avgöra om de villkor som anges i första stycket är uppfyllda, särskilt när den anser att beslutet kan avse företagshemligheter och andra kommersiellt känsliga data samt innehåll som skyddas av immateriella rättigheter eller att överföringen kan leda till återidentifiering. Det relevanta nationella organet eller den relevanta nationella myndigheten får samråda med kommissionen. Om adressaten anser att beslutet eller domen kan inkräkta på unionens eller dess medlemsstaters nationella säkerhets- eller försvarsintressen ska den begära ett yttrande från det relevanta nationella organet eller den relevanta nationella myndigheten för att avgöra om begärda data rör unionens eller dess medlemsstaters nationella säkerhets- eller försvarsintressen. Om adressaten inte har fått något svar inom en månad, eller om yttrandet av ett sådant organ eller en sådan myndighet visar att de villkor som anges i första stycket inte är uppfyllda, får adressaten avslå begäran om överföring eller åtkomst till icke-personuppgifter av dessa skäl.

Europeiska datainnovationsstyrelsen, som avses i artikel 42, ska ge råd till och bistå kommissionen vid utarbetandet av riktlinjer för bedömningen av huruvida de villkor som avses i första stycket i denna punkt är uppfyllda.

4. Om de villkor som fastställs i punkt 2 eller 3 är uppfyllda ska leverantören av databehandlingstjänster tillhandahålla den minsta mängd data som är tillåten som svar på en begäran, på grundval av en rimlig tolkning av den begäran av den leverantör, det relevanta nationella behöriga organ eller den relevanta behöriga nationella myndighet som avses i punkt 3 andra stycket.

5. Leverantören av databehandlingstjänster ska informera kunden om att det finns en begäran från en myndighet i ett tredjeland om att få åtkomst till dess data innan leverantören tillmötesgår den begäran, utom när begäran tjänar brottsbekämpande ändamål och så länge som detta är nödvändigt för att upprätthålla den brottsbekämpande verksamhetens effektivitet.

KAPITEL VIII

INTEROPERABILITET

Artikel 33

Väsentliga krav med avseende på interoperabilitet för data, datadelningsmekanismer och datadelningstjänster samt gemensamma europeiska dataområden

1. Deltagare i dataområden som erbjuder data eller datatjänster till andra deltagare ska uppfylla följande väsentliga krav för att underlätta interoperabiliteten mellan data, datadelningsmekanismer och datadelningstjänster samt mellan gemensamma europeiska dataområden, som är ändamåls- eller sektorsspecifika eller sektoröverskridande interoperabla ramar för gemensamma standarder och praxisformer för delning eller gemensam behandling av data för bland annat utveckling av nya produkter och tjänster, vetenskaplig forskning eller civilsamhällsinitiativ:

a) Innehåll i datamängden, användningsbegränsningar, licenser, datainsamlingsmetoder, datakvalitet och osäkerhet i data ska beskrivas tillräckligt, när så är tillämpligt, i ett maskinläsbart format, för att mottagaren ska kunna hitta, få åtkomst till och använda data.

b) Datastrukturer, dataformat, vokabulärer, klassificeringssystem, taxonomier och kodförteckningar ska, om sådana finns tillgängliga, beskrivas på ett allmänt tillgängligt och konsekvent sätt.

c) De tekniska medlen för åtkomst till data, såsom programmeringsgränssnitt, och deras användningsvillkor och tjänstekvalitet ska vara tillräckligt beskrivna för att möjliggöra automatisk åtkomst och överföring av data mellan parter, även kontinuerligt, genom bulknedladdning eller i realtid i ett maskinläsbart format, om detta är tekniskt möjligt och inte hindrar den uppkopplade produktens funktionsduglighet.

d) De medel som krävs för att möjliggöra interoperabilitet för verktyg för automatiserat genomförande av datadelningsavtal, såsom smarta kontrakt, ska i tillämpliga fall tillhandahållas.

Kraven kan vara av allmän karaktär eller avse specifika sektorer, samtidigt som sambandet med krav som härrör från annan unionsrätt eller nationell rätt beaktas fullt ut.

2. Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 45 i denna förordning med avseende på att komplettera denna förordning genom att ytterligare specificera de väsentliga krav som fastställs i punkt 1 i den här artikeln, med avseende på de krav som till sin natur inte kan ge den avsedda effekten om de inte specificeras närmare i bindande unionsrättsakter och för att korrekt återspegla den tekniska utvecklingen och marknadsutvecklingen.

Kommissionen ska, när den antar delegerade akter, beakta råd från Europeiska datainnovationsstyrelsen i enlighet med artikel 42 c iii.

3. Deltagare i dataområden som erbjuder data eller datatjänster till andra deltagare i dataområden som uppfyller de harmoniserade standarder eller delar av dem vars hänvisningar är offentliggjorda i *Europeiska unionens officiella tidning* ska förutsättas uppfylla de väsentliga krav som fastställs i punkt 1, i den mån dessa krav omfattas av sådana harmoniserade standarder eller delar av dem.

4. Kommissionen ska enligt artikel 10 i förordning (EU) nr 1025/2012 begära att en eller flera europeiska standardiseringsorganisationer utarbetar harmoniserade standarder som uppfyller de väsentliga krav som fastställs i punkt 1 i den här artikeln.

5. Kommissionen får genom genomförandeakter anta gemensamma specifikationer som omfattar något av eller alla de väsentliga krav som fastställs i punkt 1 om följande villkor är uppfyllda:

a) Kommissionen har enligt artikel 10.1 i förordning (EU) nr 1025/2012 begärt att en eller flera europeiska standardiseringsorganisationer ska utarbeta en harmoniserad standard som uppfyller de väsentliga krav som fastställs i punkt 1 i den här artikeln, och

   i) begäran har inte accepterats,

   ii) de harmoniserade standarder som avser denna begäran har inte levererats inom den tidsfrist som fastställts i enlighet med artikel 10.1 i förordning (EU) nr 1025/2012, eller

   iii) de harmoniserade standarderna uppfyller inte begäran, och

b) ingen hänvisning till harmoniserade standarder som omfattar de relevanta väsentliga krav som fastställs i punkt 1 i denna artikel är offentliggjord i *Europeiska unionens officiella tidning* i enlighet med förordning (EU) nr 1025/2012, och ingen sådan hänvisning förväntas offentliggöras inom rimlig tid.

Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 46.2.

6. Innan kommissionen utarbetar ett utkast till genomförandeakt som avses i punkt 5 i denna artikel ska den underrätta den kommitté som avses i artikel 22 i förordning (EU) nr 1025/2012 om att den anser att villkoren i punkt 5 i den här artikeln är uppfyllda.

7. Vid utarbetandet av utkastet till den genomförandeakt som avses i punkt 5 ska kommissionen beakta råd från Europeiska datainnovationsstyrelsen och synpunkter från andra relevanta organ eller expertgrupper och vederbörligen samråda med alla berörda parter.

8. Deltagare i dataområden som erbjuder data eller datatjänster till andra deltagare i dataområden som uppfyller de gemensamma specifikationer som fastställs genom genomförandeakter som avses i punkt 5 eller delar av dem ska förutsättas överensstämma med de väsentliga krav som fastställs i punkt 1 i den mån dessa krav omfattas av sådana gemensamma specifikationer eller delar av dem.

9. Om en harmoniserad standard antas av en europeisk standardiseringsorganisation och föreslås för kommissionen för offentliggörande av hänvisningen till den i *Europeiska unionens officiella tidning*, ska kommissionen bedöma den harmoniserade standarden i enlighet med förordning (EU) nr 1025/2012. När en hänvisning till en harmoniserad standard offentliggörs i *Europeiska unionens officiella tidning* ska kommissionen upphäva de genomförandeakter som avses i punkt 5 i denna artikel, eller delar av dem som omfattar samma väsentliga krav som omfattas av den harmoniserade standarden.

10. Om en medlemsstat anser att en gemensam specifikation inte helt uppfyller de väsentliga krav som fastställs i punkt 1 ska den underrätta kommissionen om detta genom att lämna en detaljerad förklaring. Kommissionen ska bedöma denna detaljerade förklaring och får vid behov ändra genomförandeakten om fastställande av den gemensamma specifikationen i fråga.

11. Kommissionen får anta riktlinjer med beaktande av förslaget från Europeiska datainnovationsstyrelsen i enlighet med artikel 30 h i förordning (EU) 2022/868 om fastställande av interoperabla ramar för gemensamma standarder och praxisformer för de gemensamma europeiska dataområdenas funktion.

Artikel 34

Interoperabilitet för parallell användning av databehandlingstjänster

1. Kraven i artiklarna 23, 24, 25.2 a ii, a iv, e och f och 30.2–30.5 ska också gälla i tillämpliga delar för leverantörer av databehandlingstjänster för att underlätta interoperabilitet för parallell användning av databehandlingstjänster.

2. När en databehandlingstjänst används parallellt med en annan databehandlingstjänst, får leverantörerna av databehandlingstjänster påföra uttagsavgifter för data, men endast i syfte att vidareföra de kostnader som uppkommit, utan att överskrida dessa kostnader.

Artikel 35

Interoperabilitet för databehandlingstjänster

1. Öppna interoperabilitetsspecifikationer och harmoniserade standarder för interoperabla databehandlingstjänster ska

a) om det är tekniskt möjligt åstadkomma interoperabilitet mellan olika databehandlingstjänster som omfattar samma tjänstetyp,

b) förbättra portabiliteten för digitala tillgångar mellan olika databehandlingstjänster som omfattar samma tjänstetyp,

c) om det är tekniskt möjligt underlätta funktionell likvärdighet mellan olika databehandlingstjänster som avses i artikel 30.1 som omfattar samma tjänstetyp,

d) inte inverka negativt på säkerhet och integritet för databehandlingstjänster och data,

e) vara utformade på ett sådant sätt att det möjliggör tekniska framsteg och införande av nya funktioner och innovation inom databehandlingstjänster.

2. Öppna interoperabilitetsspecifikationer och harmoniserade standarder för interoperabla databehandlingstjänster ska på ett adekvat sätt hantera

a) aspekterna av interoperabilitet i molnet när det gäller transportinteroperabilitet, syntaktisk interoperabilitet, semantisk datainteroperabilitet, beteendeinteroperabilitet och policyinteroperabilitet,

b) aspekterna av dataportabilitet i molnet vad gäller syntaktisk dataportabilitet, semantisk dataportabilitet och portabilitet för datapolicy,

c) aspekterna av applikationer i molnet vad gäller syntaktisk applikationsportabilitet, applikationsportabilitet för instruktioner, applikationsportabilitet för metadata, applikationsportabilitet för beteende och applikationsportabilitet för policy.

3. De öppna interoperabilitetsspecifikationerna ska uppfylla kraven i bilaga II till förordning (EU) nr 1025/2012.

4. Efter att ha beaktat relevanta internationella och europeiska standarder och självregleringsinitiativ får kommissionen i enlighet med artikel 10.1 i förordning (EU) nr 1025/2012 begära att en eller flera europeiska standardiseringsorganisationer utarbetar harmoniserade standarder som uppfyller de väsentliga krav som fastställs i punkterna 1 och 2 i den här artikeln.

5. Kommissionen får genom genomförandeakter anta gemensamma specifikationer på grundval av öppna interoperabilitetsspecifikationer som omfattar alla de väsentliga krav som fastställs i punkterna 1 och 2.

6. Vid utarbetandet av utkastet till den genomförandeakt som avses i punkt 5 i denna artikel ska kommissionen beakta synpunkterna från de relevanta behöriga myndigheter som avses i artikel 37.5 h och andra relevanta organ eller expertgrupper och vederbörligen samråda med alla berörda parter.

7. Om en medlemsstat anser att en gemensam specifikation inte helt uppfyller de väsentliga krav som fastställs i punkterna 1 och 2 ska den underrätta kommissionen om detta genom att lämna en detaljerad förklaring. Kommissionen ska bedöma denna detaljerade förklaring och får vid behov ändra genomförandeakten om fastställande av den gemensamma specifikationen i fråga.

8. Vid tillämpning av artikel 30.3 ska kommissionen genom genomförandeakter offentliggöra hänvisningar till harmoniserade standarder och gemensamma specifikationer för interoperabla databehandlingstjänster i ett centralt unionsregister över standarder för interoperabla databehandlingstjänster.

9. De genomförandeakter som avses i denna artikel ska antas i enlighet med det granskningsförfarande som avses i artikel 46.2.

Artikel 36

Väsentliga krav avseende smarta kontrakt för genomförande av datadelningsavtal

1. Säljaren av en applikation som använder smarta kontrakt eller, i avsaknad av en sådan, den person vars närings- eller yrkesverksamhet inbegriper användning av smarta kontrakt för andra inom ramen för genomförandet av ett avtal eller en del av det om att tillgängliggöra data ska säkerställa att dessa smarta kontrakt efterlever följande väsentliga krav:

a) Robusthet och åtkomstkontroll: Säkerställa att det smarta kontraktet har utformats för att erbjuda åtkomstkontrollmekanismer och en mycket hög grad av robusthet för att undvika funktionsfel och stå emot manipulering från tredje parters sida.

b) Säkerhet vid uppsägning och avbrott: Säkerställa att det finns en mekanism för att avsluta det fortsatta genomförandet av transaktioner och att det smarta kontraktet omfattar interna funktioner som kan återställa eller instruera kontraktet att permanent eller tillfälligt avbryta driften, i synnerhet för att undvika framtida oavsiktliga exekveringar.

c) Dataarkivering och kontinuitet: Säkerställa, under omständigheter då ett smart kontrakt måste avslutas eller avaktiveras, att det finns en möjlighet att arkivera transaktionsuppgifterna, smart avtalslogik och kod för att föra register över tidigare utförda transaktioner (granskningsbarhet).

d) Åtkomstkontroll: Säkerställa att ett smart kontrakt skyddas genom strikta mekanismer för åtkomstkontroll vid skikten för kontroll och smarta kontrakt.

e) Enhetlighet: Säkerställa enhetlighet med villkoren i det datadelningsavtal som det smarta kontraktet genomför.

2. Säljaren av ett smart kontrakt eller, i avsaknad av en sådan, den person vars närings- eller yrkesverksamhet inbegriper användning av smarta kontrakt för andra inom ramen för genomförandet av ett avtal eller en del av det om att tillgängliggöra data ska utföra en bedömning av överensstämmelse i syfte att uppfylla de väsentliga krav som fastställs i punkt 1 och, när dessa krav är uppfyllda, utfärda en EU-försäkran om överensstämmelse.

3. Genom att utarbeta en EU-försäkran om överensstämmelse ska försäljaren av en applikation som använder smarta kontrakt eller, i avsaknad av en sådan, den person vars närings- eller yrkesverksamhet inbegriper användning av smarta kontrakt för andra inom ramen för genomförandet av ett avtal eller en del av det om att tillgängliggöra data vara ansvarig för efterlevnaden av de väsentliga krav som fastställs i punkt 1.

4. Ett smart kontrakt som uppfyller de harmoniserade standarder eller de relevanta delarna av dessa standarder och vars hänvisningar är offentliggjorda i *Europeiska unionens officiella tidning* ska förutsättas uppfylla de väsentliga krav som fastställs i punkt 1, i den mån dessa krav omfattas av sådana harmoniserade standarder eller delar av dem.

5. Kommissionen ska enligt artikel 10 i förordning (EU) nr 1025/2012 begära att en eller flera europeiska standardiseringsorganisationer utarbetar harmoniserade standarder som uppfyller de väsentliga krav som fastställs i punkt 1 i den här artikeln.

6. Kommissionen får, genom genomförandeakter, anta gemensamma specifikationer som omfattar något av eller alla de väsentliga krav som fastställs i punkt 1 om följande villkor är uppfyllda:

a) Kommissionen har enligt artikel 10.1 i förordning (EU) nr 1025/2012 begärt att en eller flera europeiska standardiseringsorganisationer ska utarbeta en harmoniserad standard som uppfyller de väsentliga krav som fastställs i punkt 1 i den här artikeln, och

   i) begäran har inte accepterats,

   ii) de harmoniserade standarder som avser denna begäran har inte levererats inom den tidsfrist som fastställts i enlighet med artikel 10.1 i förordning (EU) nr 1025/2012, eller

   iii) de harmoniserade standarderna uppfyller inte begäran, och

b) ingen hänvisning till harmoniserade standarder som omfattar de relevanta väsentliga krav som fastställs i punkt 1 i denna artikel är offentliggjord i *Europeiska unionens officiella tidning* i enlighet med förordning (EU) nr 1025/2012, och ingen sådan hänvisning förväntas offentliggöras inom rimlig tid.

Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 46.2.

7. Innan kommissionen utarbetar ett utkast till den genomförandeakt som avses i punkt 6 i denna artikel ska den underrätta den kommitté som avses i artikel 22 i förordning (EU) nr 1025/2012 om att den anser att villkoren i punkt 6 i den här artikeln är uppfyllda.

8. Vid utarbetandet av utkastet till den genomförandeakt som avses i punkt 6 ska kommissionen beakta råd från Europeiska datainnovationsstyrelsen och synpunkter från andra relevanta organ eller expertgrupper och vederbörligen samråda med alla berörda parter.

9. Säljaren av ett smart kontrakt eller, i avsaknad av en sådan, den person vars närings- eller yrkesverksamhet inbegriper användning av smarta kontrakt för andra inom ramen för genomförandet av ett avtal eller en del av det om att tillgängliggöra data som uppfyller de gemensamma specifikationer som fastställs genom genomförandeakter som avses i punkt 6 eller delar av dem ska förutsättas överensstämma med de väsentliga krav som fastställs i punkt 1 i den mån dessa krav omfattas av sådana gemensamma specifikationer eller delar av dem.

10. Om en harmoniserad standard antas av en europeisk standardiseringsorganisation och föreslås för kommissionen för offentliggörande av hänvisningen till den i *Europeiska unionens officiella tidning*, ska kommissionen bedöma den harmoniserade standarden i enlighet med förordning (EU) nr 1025/2012. När en hänvisning till en harmoniserad standard offentliggörs i *Europeiska unionens officiella tidning* ska kommissionen upphäva de genomförandeakter som avses i punkt 6 i denna artikel, eller delar av dem som omfattar samma väsentliga krav som de som omfattas av den harmoniserade standarden.

11. Om en medlemsstat anser att en gemensam specifikation inte helt uppfyller de väsentliga krav som fastställs i punkt 1 ska den underrätta kommissionen om detta genom att lämna en detaljerad förklaring. Kommissionen ska bedöma denna detaljerade förklaring och får vid behov ändra genomförandeakten om fastställande av den gemensamma specifikationen i fråga.

KAPITEL IX

GENOMFÖRANDE OCH EFTERLEVNAD

Artikel 37

Behöriga myndigheter och datasamordnare

1. Varje medlemsstat ska utse en eller flera behöriga myndigheter som ska ansvara för tillämpningen och efterlevnaden av denna förordning (behöriga myndigheter). Medlemsstaterna får inrätta en eller flera nya myndigheter eller förlita sig på befintliga myndigheter.

2. Om en medlemsstat utser mer än en behörig myndighet ska den bland dem utse en datasamordnare för att underlätta samarbetet mellan de behöriga myndigheterna och bistå enheter som omfattas av denna förordning i alla frågor som rör dess tillämpning och efterlevnad. De behöriga myndigheterna ska, vid utövandet av de uppgifter och befogenheter som tilldelats dem enligt punkt 5, samarbeta med varandra.

3. De tillsynsmyndigheter som ansvarar för att övervaka tillämpningen av förordning (EU) 2016/679 ska ansvara för att övervaka tillämpningen av den här förordningen när det gäller skyddet av personuppgifter. Kapitlen VI och VII i förordning (EU) 2016/679 ska gälla i tillämpliga delar.

Europeiska datatillsynsmannen ska ansvara för att övervaka tillämpningen av denna förordning i den mån den berör kommissionen, Europeiska centralbanken eller unionsorgan. Där det är relevant ska artikel 62 i förordning (EU) 2018/1725 gälla i tillämpliga delar.

Uppgifterna och befogenheterna för de tillsynsmyndigheter som avses i denna punkt ska utövas med avseende på behandling av personuppgifter.

4. Utan att det påverkar tillämpningen av punkt 1 i denna artikel gäller följande:

a) När det gäller sektorsspecifika frågor som rör åtkomst till och användning av data i samband med tillämpningen av denna förordning ska sektorsmyndigheternas behörighet respekteras.

b) Den behöriga myndighet som ansvarar för tillämpningen och kontrollen av efterlevnaden av artiklarna 23–31, 34 och 35 ska ha erfarenhet på området data och elektroniska kommunikationstjänster.

5. Medlemsstaterna ska säkerställa att uppgifterna och befogenheterna för de behöriga myndigheterna är tydligt definierade och omfattar följande:

a) Öka datakompetensen och medvetenheten bland de användare och enheter som omfattas av denna förordning om deras rättigheter och skyldigheter enligt denna förordning.

b) Hantera klagomål som härrör från påstådda överträdelser av denna förordning, inbegripet vad gäller företagshemligheter, och i lämplig utsträckning undersöka föremålet för klagomålen och regelbundet inom rimlig tid informera de klagande, i tillämpliga fall i enlighet med nationell rätt, om hur utredningen fortskrider och om resultatet av den, särskilt om ytterligare utredning eller samordning med en annan behörig myndighet är nödvändig.

c) Utföra undersökningar om frågor som rör tillämpningen av denna förordning, inbegripet på grundval av information som erhålls från en annan behörig myndighet eller offentlig myndighet.

d) Ålägga effektiva, proportionella och avskräckande ekonomiska sanktioner, som kan inbegripa viten och sanktioner med retroaktiv verkan, eller inleda rättsliga förfaranden för åläggande av böter,

e) Övervaka den tekniska och relevanta kommersiella utveckling som är relevant för tillgängliggörande och användning av data,

f) Samarbeta med behöriga myndigheter i andra medlemsstater och, i förekommande fall, med kommissionen eller Europeiska datainnovationsstyrelsen, för att säkerställa en konsekvent och effektiv tillämpning av denna förordning, inbegripet utbyte av all relevant information på elektronisk väg, utan oskäligt dröjsmål, även avseende punkt 10 i denna artikel.

g) Samarbeta med de relevanta behöriga myndigheter som ansvarar för genomförandet av andra unionsrättsakter eller nationella rättsakter, inbegripet med myndigheter med behörighet på området data och elektroniska kommunikationstjänster, med den tillsynsmyndighet som ansvarar för att övervaka tillämpningen av förordning (EU) 2016/679 eller med sektorsmyndigheter för att säkerställa att den här förordningen verkställs i överensstämmelse med annan unionsrätt och nationell rätt.

h) Samarbeta med de relevanta behöriga myndigheterna för att säkerställa att artiklarna 23–31, artikel 34 och 35 verkställs i överensstämmelse med annan unionsrätt och självreglering som är tillämplig på leverantörer av databehandlingstjänster.

i) Säkerställa att bytesavgifter avskaffas i enlighet med artikel 29.

j) Granska de begäranden om data som gjorts enligt kapitel V.

Om en datasamordnare har utsetts ska denna underlätta det samarbete som avses i första stycket f, g och h och på begäran bistå de behöriga myndigheterna.

6. Datasamordnaren ska, om en sådan behörig myndighet har utsetts,

a) fungera som enda kontaktpunkt för alla frågor som rör tillämpningen av denna förordning,

b) säkerställa att offentliga organs begäranden om att göra data tillgängliga på grund av ett exceptionellt behov enligt kapitel V finns tillgängliga för allmänheten på nätet och främja frivilliga avtal om datadelning mellan offentliga organ och datahållare,

c) årligen informera kommissionen om de avslag som det underrättats om enligt artiklarna 4.2, 4.8 och 5.11.

7. Medlemsstaterna ska meddela kommissionen namnen på de behöriga myndigheterna och deras uppgifter och befogenheter samt, i tillämpliga fall, namnet på datasamordnaren. Kommissionen ska föra ett offentligt register över dessa myndigheter.

8. När de behöriga myndigheterna utför sina uppgifter och utövar sina befogenheter i enlighet med denna förordning ska de vara opartiska och stå fria från all yttre påverkan, direkt eller indirekt, och får varken begära eller ta emot instruktioner i enskilda ärenden från någon annan offentlig myndighet eller någon privat part.

9. Medlemsstaterna ska säkerställa att de behöriga myndigheterna har tillräckliga personalresurser och tekniska resurser och relevant sakkunskap för att de på ett effektivt sätt ska kunna utföra sina uppgifter i enlighet med denna förordning.

10. Enheter som omfattas av tillämpningsområdet för denna förordning ska omfattas av behörigheten för den medlemsstat där de är etablerade. Om enheten är etablerad i fler än en medlemsstat ska den anses omfattas av behörigheten för den medlemsstat där den har sitt huvudsakliga etableringsställe, dvs. där enheten har sitt huvudkontor eller säte från vilket de huvudsakliga finansiella funktionerna och den operativa kontrollen utövas.

11. Varje enhet som omfattas av tillämpningsområdet för denna förordning och som gör uppkopplade produkter tillgängliga eller erbjuder tillhörande tjänster i unionen, och som inte är etablerad i unionen, ska utse en rättslig företrädare i en av medlemsstaterna.

12. För att säkerställa efterlevnaden av denna förordning ska enheter som omfattas av tillämpningsområdet för denna förordning och som gör uppkopplade produkter tillgängliga eller erbjuder tillhörande tjänster i unionen bemyndiga en rättslig företrädare som de behöriga myndigheterna ska vända sig till utöver eller i stället för enheten med avseende på alla frågor som rör denna enhet. Den rättsliga företrädaren ska samarbeta med de behöriga myndigheterna och, på begäran, för dessa på ett övergripande sätt påvisa de åtgärder som vidtagits och de bestämmelser som införts av enheter som omfattas av tillämpningsområdet för denna förordning och som gör uppkopplade produkter tillgängliga eller erbjuder tillhörande tjänster i unionen för att säkerställa efterlevnaden av denna förordning.

13. En enhet som omfattas av tillämpningsområdet för denna förordning och som gör uppkopplade produkter tillgängliga eller erbjuder tillhörande tjänster i unionen ska anses omfattas av den medlemsstats behörighet där dess rättsliga företrädare finns. Att en sådan enhet utser en rättslig företrädare ska inte påverka denna enhets ansvar eller rättsliga åtgärder som kan vidtas mot denna enhet. Fram till dess att en enhet utser en rättslig företrädare i enlighet med denna artikel ska den i tillämpliga fall omfattas av alla medlemsstaters behörighet med avseende på att säkerställa tillämpningen och efterlevnaden av denna förordning. Varje behörig myndighet får utöva sin behörighet, inbegripet genom att ålägga effektiva, proportionella och avskräckande sanktioner, förutsatt att enheten inte är föremål för verkställighetsförfaranden enligt denna förordning avseende samma sakförhållanden vid en annan behörig myndighet.

14. De behöriga myndigheterna ska ha befogenhet att från användare, datahållare eller datamottagare, eller deras rättsliga företrädare, som omfattas av deras medlemsstats behörighet begära all information som krävs för att kontrollera efterlevnaden av denna förordning. Varje begäran om information ska stå i proportion till den underliggande uppgiftens utförande och innehålla en motivering.

15. Om en behörig myndighet i en medlemsstat begär bistånd eller verkställighetsåtgärder från en behörig myndighet i annan medlemsstat ska den lämna en motiverad begäran. En behörig myndighet ska vid mottagandet av en sådan begäran utan oskäligt dröjsmål lämna ett svar med detaljerade uppgifter om de åtgärder som har vidtagit eller som avses att vidtas.

16. Behöriga myndigheter ska respektera principen om konfidentialitet samt om yrkes- och affärshemligheter och ska skydda personuppgifter i enlighet med unionsrätten eller nationell rätt. All information som utbyts inom ramen för en begäran om bistånd och som tillhandahålls enligt denna artikel får användas endast med avseende på det ärende för vilket den har begärts.

Artikel 38

Rätt att lämna in klagomål

1. Utan att det påverkar något annat administrativt prövningsförfarande eller rättsmedel ska fysiska och juridiska personer ha rätt att enskilt eller, i förekommande fall, kollektivt lämna in ett klagomål till den relevanta behöriga myndigheten i den medlemsstat där de har sin hemvist, sin arbetsplats eller sin etableringsort, om de anser att deras rättigheter enligt denna förordning har kränkts. Datasamordnaren ska på begäran lämna all nödvändig information till fysiska och juridiska personer så att de kan lämna in klagomål till den relevanta behöriga myndigheten.

2. Den behöriga myndighet till vilken klagomålet har lämnats in ska i enlighet med nationell rätt underrätta klaganden om hur förfarandet fortskrider och om det beslut som fattats.

3. Behöriga myndigheter ska samarbeta för att effektivt och snabbt hantera och avgöra klagomål, bland annat genom att utan oskäligt dröjsmål utbyta all relevant information på elektronisk väg. Detta samarbete ska inte påverka de samarbetsmekanismer som föreskrivs i kapitlen VI och VII i förordning (EU) 2016/679 och i förordning (EU) 2017/2394.

Artikel 39

Rätten till ett effektivt rättsmedel

1. Utan att det påverkar administrativa rättsmedel eller andra prövningsförfaranden utanför domstol ska berörda fysiska och juridiska personer ha rätt till ett effektivt rättsmedel avseende rättsligt bindande beslut som fattats av behöriga myndigheter.

2. Om en behörig myndighet underlåter att vidta åtgärder med avseende på ett klagomål ska berörda fysiska och juridiska personer, i enlighet med nationell rätt, antingen ha rätt till ett effektivt rättsmedel eller tillgång till omprövning av en opartisk myndighet som besitter lämplig sakkunskap.

3. Förfaranden enligt denna artikel ska inledas vid domstolarna i den medlemsstat där den behöriga myndighet som rättsmedlen avser är belägen, antingen individuellt eller, i förekommande fall, kollektivt av företrädare för en eller flera fysiska eller juridiska personer.

Artikel 40

Sanktioner

1. Medlemsstaterna ska fastställa regler om sanktioner för överträdelse av bestämmelserna i denna förordning och vidta alla nödvändiga åtgärder för att säkerställa att de tillämpas. Sanktionerna ska vara effektiva, proportionella och avskräckande.

2. Senast den 12 september 2025 ska medlemsstaterna till kommissionen anmäla dessa regler och åtgärder samt utan dröjsmål anmäla eventuella ändringar som berör dem. Kommissionen ska regelbundet uppdatera och föra ett lättillgängligt offentligt register över dessa åtgärder.

3. Medlemsstaterna ska beakta rekommendationerna från Europeiska datainnovationsstyrelsen och följande icke uttömmande kriterier för åläggande av sanktioner för överträdelser av denna förordning:

a) Överträdelsens art, allvar, omfattning och varaktighet.

b) Varje åtgärd som den överträdande parten har vidtagit för att begränsa eller avhjälpa den skada som överträdelsen har orsakat.

c) Eventuella tidigare överträdelser som begåtts av den överträdande parten.

d) De ekonomiska fördelar som den överträdande parten har erhållit eller de förluster denna har undvikit genom överträdelsen, i den mån sådana fördelar eller förluster kan fastställas på ett tillförlitligt sätt.

e) Eventuella andra försvårande eller förmildrande omständigheter som är tillämpliga på ärendet.

f) Den överträdande partens årsomsättning i unionen under det föregående räkenskapsåret.

4. För överträdelser av de skyldigheter som fastställs i kapitlen II, III och V i denna förordning får de tillsynsmyndigheter som ansvarar för att övervaka tillämpningen av förordning (EU) 2016/679 inom ramen för sin behörighet påföra administrativa sanktionsavgifter i enlighet med artikel 83 i förordning (EU) 2016/679 på upp till det belopp som avses i artikel 83.5 i den förordningen.

5. För överträdelser av de skyldigheter som fastställs i kapitel V i denna förordning får Europeiska datatillsynsmannen inom ramen för sin behörighet påföra administrativa sanktionsavgifter i enlighet med artikel 66 i förordning (EU) 2018/1725 på upp till det belopp som avses i artikel 66.3 i den förordningen.

Artikel 41

Standardavtalsvillkor och standardavtalsklausuler

Kommissionen ska före den 12 september 2025 utarbeta och rekommendera icke-bindande standardavtalsvillkor för åtkomst till och användning av data, inbegripet villkor om rimlig ersättning och skydd av företagshemligheter, och icke-bindande standardavtalsklausuler för molnavtal för att hjälpa parterna att utarbeta och förhandla fram avtal med rättvisa, rimliga och icke-diskriminerande avtalsenliga rättigheter och skyldigheter.

Artikel 42

Europeiska datainnovationsstyrelsens roll

Europeiska datainnovationsstyrelsen, som inrättats av kommissionen som en expertgrupp enligt artikel 29 i förordning (EU) 2022/868 och i vilken behöriga myndigheter ska vara företrädda, ska stödja en konsekvent tillämpning av den här förordningen genom att

a) ge råd till och bistå kommissionen när det gäller att utveckla en konsekvent praxis hos behöriga myndigheter avseende efterlevnaden av kapitlen II, III, V och VII,

b) underlätta samarbete mellan behöriga myndigheter genom kapacitetsuppbyggnad och informationsutbyte, särskilt genom att fastställa metoder för ett effektivt informationsutbyte om efterlevnaden av rättigheterna och skyldigheterna enligt kapitlen II, III och V i gränsöverskridande fall, inbegripet samordning när det gäller fastställande av sanktioner,

c) ge råd till och bistå kommissionen när det gäller

i) huruvida det ska begäras att sådana harmoniserade standarder som avses i artiklarna 33.4, 35.4 och 36.5 utarbetas,

ii) utarbetandet av de genomförandeakter som avses i artiklarna 33.5, 35.5, 35.8 och 36.6,

iii) utarbetandet av de delegerande akter som avses i artiklarna 29.7 och 33.2, och

iv) antagandet av de riktlinjer om fastställande av interoperabla ramar för gemensamma standarder och praxisformer för de gemensamma europeiska dataområdenas funktion som avses i artikel 33.11.

KAPITEL X

RÄTTEN AV SITT EGET SLAG ENLIGT DIREKTIV 96/9/EG

Artikel 43

Databaser som innehåller vissa data

Rätten av sitt eget slag enligt artikel 7 i direktiv 96/9/EG ska inte tillämpas när data erhålls från eller genereras av en uppkopplad produkt eller en tillhörande tjänst som omfattas av denna förordning, särskilt med avseende på artiklarna 4 och 5 i denna förordning.

KAPITEL XI

SLUTBESTÄMMELSER

Artikel 44

Andra unionsrättsakter som reglerar rättigheter och skyldigheter avseende åtkomst till och användning av data

1. De specifika skyldigheterna att göra data tillgängliga mellan företag, mellan företag och konsumenter, och i undantagsfall mellan företag och offentliga organ, i unionsrättsakter som trädde i kraft senast den 11 januari 2024, och delegerade akter eller genomförandeakter som antagits på grundval av dessa, ska inte påverkas.

2. Denna förordning påverkar inte sådan unionsrätt som, mot bakgrund av behoven inom en sektor, ett gemensamt europeiskt dataområde eller ett område av allmänt intresse, fastställer ytterligare krav, särskilt när det gäller följande:

a) Tekniska aspekter på dataåtkomst.

b) Begränsningar av datahållares rätt att få åtkomst till eller använda vissa data som tillhandahålls av användarna.

c) Aspekter som går utöver åtkomst till och användning av data.

3. Denna förordning, med undantag för kapitel V, påverkar inte tillämpningen av sådan unionsrätt och nationell rätt som föreskriver åtkomst till och godkännande av användning av data för vetenskapliga forskningsändamål.

Artikel 45

Utövande av delegeringen

1. Befogenheten att anta delegerade akter ges till kommissionen med förbehåll för de villkor som anges i denna artikel.

2. Den befogenhet att anta delegerade akter som avses i artiklarna 29.7 och 33.2 ges till kommissionen tills vidare från och med den 11 januari 2024.

3. Den delegering av befogenhet som avses i artiklarna 29.7 och 33.2 får när som helst återkallas av Europaparlamentet eller rådet. Ett beslut om återkallelse innebär att delegeringen av den befogenhet som anges i beslutet upphör att gälla. Beslutet får verkan dagen efter det att det offentliggörs i *Europeiska unionens officiella tidning*, eller vid ett senare i beslutet angivet datum. Det påverkar inte giltigheten av delegerade akter som redan har trätt i kraft.

4. Innan kommissionen antar en delegerad akt ska den samråda med experter som utsetts av varje medlemsstat i enlighet med principerna i det interinstitutionella avtalet av den 13 april 2016 om bättre lagstiftning.

5. Så snart kommissionen antar en delegerad akt ska den samtidigt delge Europaparlamentet och rådet denna.

6. En delegerad akt som antas enligt artikel 29.7 eller 33.2 ska träda i kraft endast om varken Europaparlamentet eller rådet har gjort invändningar mot den delegerade akten inom en period på tre månader från den dag då akten delgavs Europaparlamentet och rådet, eller om både Europaparlamentet och rådet, före utgången av den perioden, har underrättat kommissionen om att de inte kommer att invända. Denna period ska förlängas med tre månader på Europaparlamentets eller rådets initiativ.

Artikel 46

Kommittéförfarande

1. Kommissionen ska biträdas av den kommitté som inrättats genom förordning (EU) 2022/868. Denna kommitté ska vara en kommitté i den mening som avses i förordning (EU) nr 182/2011.

2. När det hänvisas till denna punkt ska artikel 5 i förordning (EU) nr 182/2011 tillämpas.

Artikel 47

Ändring av förordning (EU) 2017/2394

I bilagan till förordning (EU) 2017/2394 ska följande punkt läggas till:

”29. Europaparlamentets och rådets förordning (EU) 2023/2854 av den 13 december 2023 om harmoniserade regler för skälig åtkomst till och användning av data och om ändring av förordning (EU) 2017/2394 och direktiv (EU) 2020/1828 (dataförordningen) (OJ L, 2023/2854, 22.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2854/oj).”

Artikel 48

Ändring av direktiv (EU) 2020/1828

I bilaga I till direktiv (EU) 2020/1828 ska följande punkt läggas till:

"68. Europaparlamentets och rådets förordning (EU) 2023/2854 av den 13 december 2023 om harmoniserade regler för skälig åtkomst till och användning av data och om ändring av förordning (EU) 2017/2394 och direktiv (EU) 2020/1828 (dataförordningen) (EUT L OJ L, 2023/2854, 22.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2854/oj)."

Artikel 49

Utvärdering och översyn

1. Kommissionen ska senast den 12 september 2028 genomföra en utvärdering av denna förordning och lämna en rapport om de viktigaste resultaten till Europaparlamentet, rådet och Europeiska ekonomiska och sociala kommittén. I utvärderingen ska särskilt följande bedömas:

a) Situationer som ska betraktas som situationer då det finns ett exceptionellt behov vid tillämpningen av artikel 15 i denna förordning och tillämpningen av kapitel V i denna förordning i praktiken, särskilt de offentliga organens, kommissionens, Europeiska centralbankens och unionsorganens erfarenheter av tillämpningen av kapitel V i denna förordning, antalet samt resultatet av de förfaranden som inletts hos den behöriga myndigheten enligt artikel 18.5 om tillämpningen av kapitel V i denna förordning, enligt vad som rapporterats av de behöriga myndigheterna, effekterna av andra skyldigheter som fastställs i unionsrätten eller nationell rätt för att tillmötesgå begäranden om åtkomst till information, effekterna av frivilliga mekanismer för datadelning, såsom de som införts av dataaltruismorganisationer som erkänns enligt förordning (EU) 2022/868, på uppnåendet av målen i kapitel V i den här förordningen, och personuppgifternas roll inom ramen för artikel 15 i den här förordningen, inbegripet utvecklingen av integritetsfrämjande teknik.

b) Denna förordnings inverkan på användningen av data i ekonomin, inbegripet på datainnovation, metoder för monetarisering av data och dataförmedlingstjänster samt på datadelning inom de gemensamma europeiska dataområdena.

c) Tillgängligheten till och användningen av olika kategorier och typer av data.

d) Uteslutning av vissa kategorier av företag vad gäller bestämmelserna i artikel 5.

e) Avsaknaden av all påverkan på immateriella rättigheter.

f) Inverkan på företagshemligheter, inbegripet skyddet mot att de olagligen anskaffas, utnyttjas och lämnas ut, samt effekterna av den mekanism som gör det möjligt för datahållaren att avslå användarens begäran enligt artiklarna 4.8 och 5.11, med beaktande, i möjligaste mån, av en eventuell översyn av direktiv (EU) 2016/943.

g) Huruvida den förteckning över oskäliga avtalsvillkor som avses i artikel 13 är uppdaterad mot bakgrund av nya affärsmetoder och den snabba takten i marknadsinnovationen.

h) Ändringar av avtalspraxis hos leverantörer av databehandlingstjänster och huruvida detta leder till tillräcklig efterlevnad av artikel 25.

i) Sänkningen av de avgifter som tas ut av leverantörer av databehandlingstjänster för bytesprocessen, i enlighet med det gradvisa avskaffandet av bytesavgifter enligt artikel 29.

j) Samspelet mellan denna förordning och andra unionsrättsakter av betydelse för dataekonomin.

k) Förhindrandet av olaglig statlig åtkomst till icke-personuppgifter.

l) Effektiviteten hos det system för kontroll av efterlevnad som krävs enligt artikel 37.

m) Inverkan av denna förordning på mikroföretag och små och medelstora företag när det gäller deras innovationskapacitet och tillgången till databehandlingstjänster för användare i unionen samt bördan som de nya skyldigheterna innebär.

2. Kommissionen ska senast den 12 september 2028 genomföra en utvärdering av denna förordning och lämna en rapport om de viktigaste resultaten till Europaparlamentet, rådet och Europeiska ekonomiska och sociala kommittén. I denna utvärdering ska effekterna av artiklarna 23–31, 34 och 35 bedömas, särskilt när det gäller prissättning och mångfalden av databehandlingstjänster som erbjuds inom unionen, med särskilt fokus på leverantörer som är mikroföretag och små och medelstora företag.

3. Medlemsstaterna ska förse kommissionen med de uppgifter som är nödvändiga för att utarbeta de rapporter som avses i punkterna 1 och 2.

4. På grundval av de rapporter som avses i punkterna 1 och 2 kan kommissionen om så är lämpligt lägga fram ett lagstiftningsförslag för Europaparlamentet och rådet i syfte att ändra denna förordning.

Artikel 50

Ikraftträdande och tillämpning

Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

Den ska tillämpas från och med den 12 september 2025.

De skyldigheter som följer av artikel 3.1 ska tillämpas på de uppkopplade produkter och de tillhörande tjänster som släpps ut på marknaden efter den 12 september 2026.

Kapitel III ska endast tillämpas på skyldigheter att göra data tillgängliga enligt unionsrätt eller nationell lagstiftning som antagits i enlighet med unionsrätten som träder i kraft efter den 12 september 2025.

Kapitel IV ska tillämpas på avtal som ingås efter den 12 september 2025..

Kapitel IV ska tillämpas från och med den 12 september 2027 på avtal som ingåtts den 12 september 2025 eller tidigare, under förutsättning att de

a) har ingåtts på obestämd tid, eller

b) löper ut minst 10 år efter den 11 januari 2024.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Strasbourg den 13 december 2023.

På Europaparlamentets vägnar	*På rådets vägnar*
R. METSOLA	P. NAVARRO RÍOS
Ordförande	*Ordförande*

Statens offentliga utredningar 2025

Kronologisk förteckning

1. Skärpta krav för svenskt medborgarskap. Ju.
2. Några frågor om grundläggande fri- och rättigheter. Ju.
3. Skatteincitament för forskning och utveckling. En översyn av FoU-avdraget och expertskattereglerna. Fi.
4. Moderna och enklare skatteregler för arbetslivet. Fi.
5. Avgift för områdessamverkan – och andra åtgärder för trygghet i byggd miljö. LI.
6. Plikten kallar! En modern personalförsörjning av det civila försvaret. Fö.
7. Ny kärnkraft i Sverige – effektivare tillståndsprövning och ändamålsenliga avgifter. KN.
8. Bättre förutsättningar för trygghet och studiero i skolan. U.
9. På språklig grund. U.
10. En förändrad abortlag – för en god, säker och tillgänglig abortvård. S.
11. Straffbarhetsåldern. Ju.
12. AI-kommissionens Färdplan för Sverige. Fi.
13. En effektivare organisering av mindre myndigheter – analys och förslag. Fi.
14. En skärpt miljöstraffrätt och ett effektivt sanktionssystem. KN.
15. Stärkta drivkrafter och möjligheter för biståndsmottagare. Volym 1 och 2. S.
16. Ett nytt regelverk för uppsikt och förvar. Ju.
17. Anpassning av svensk rätt till EU:s avskogningsförordning. LI.
18. Ett likvärdigt betygssystem. Volym 1 och 2. U.
19. Kunskap för alla – nya läroplaner med fokus på undervisning och lärande. U.
20. Kommunal anslutning till Utbetalningsmyndighetens verksamhet. Fi.
21. Miljömålsberedningens förslag om en strategi för hur Sverige ska leva upp till EU:s åtaganden inom biologisk mångfald respektive nettoupptag av växthusgaser från markanvändningssektorn (LULUCF). KN.
22. Förbättrad konkurrens i offentlig och privat verksamhet. KN.
23. Ersättningsregler med brottsoffret i fokus. Ju.
24. Publiken i fokus – reformer för ett starkare filmland. Ku.
25. Arbetslivskriminalitet – upplägg, verktyg och åtgärder, fortsatt arbete. A.
26. Tid för undervisningsuppdraget – åtgärder för god undervisning och läraryrkenas attraktivitet. U.
27. En socionomutbildning i tiden. U.
28. Frihet från våld, förtryck och utnyttjande. En jämställdhetspolitisk strategi mot våld och en stärkt styrning av centrala myndigheter. A.
29. Ökad kvalitet hos Samhall och fler vägar till skyddat arbete. A.
30. Enklare mervärdesskatteregler vid försäljning av begagnade varor och donation av livsmedel. Fi.
31. Utmönstring av permanent uppehållstillstånd och vissa anpassningar till miniminivån enligt EU:s migrations- och asylpakt. Ju.
32. Vissa förändringar av jaktlagstiftningen. LI.
33. Skärpta och tydligare krav på vandel för uppehållstillstånd. Ju.
34. Ett modernare konsumentskydd vid distansavtal. Ju.
35. Etableringsboendelagen – ett nytt system för bosättning för vissa nyanlända. A.

36. Skydd för biologisk mångfald i havsområden utanför nationell jurisdiktion. UD.
37. Skärpta villkor för friskolesektorn. U.
38. Att omhänderta barn och unga. S.
39. Digital teknik på lika villkor. En reglering för socialtjänsten och verksamhet enligt LSS. S.
40. Säkrare tivoli. Ju.
41. Pensionsnivåer och pensionsavgiften – analyser på hundra års sikt. S.
42. Säkerhetsskyddslagen – ytterligare kompletteringar. Ju.
43. Säkerställ tillgången till läkemedel – förordnande och utlämnande i bristsituationer. S.
44. Förbättrat stöd i skolan. U.
45. Ökat informationsutbyte mellan myndigheter – några anslutande frågor. Ju.
46. Tryggare idrottsarrangemang. Ju.
47. Spänning i tillvaron – hur säkrar vi vår framtida elförsörjning? KN.
48. Stärkt pandemiberedskap. S.
49. Säkerhetspolisens behandling av personuppgifter. Ju.
50. En ny nationell myndighet för viltförvaltning. LI.
51. Bättre förutsättningar för klimatanpassning. KN.
52. Ökad insyn i politiska processer. Ju.
53. Kvalificering till socialförsäkring och ekonomiskt bistånd för vissa grupper. S.
54. Ett skärpt regelverk om utvisning på grund av brott. Ju.
55. En reformerad samhällsorientering för bättre integration. A.
56. Stärkt skydd för domstolarnas och domarnas oberoende. Ju.
57. Polisiär beredskap i fred, kris och krig. Ju.
58. En stärkt hästnäring – för företagande, jämställdhet, jämlikhet och folkhälsa. LI.
59. Stärkt lagstiftning mot hedersrelaterat våld och förtryck. Ju.
60. En starkare fondmarknad. Fi.
61. Sveriges internationella adoptionsverksamhet – lärdomar och vägen framåt. Volym 1 och 2. S.
62. Ansvaret för hälso- och sjukvården. Volym 1 Bedömningar och förslag. Volym 2 Underlagsrapporter. S.
63. Stärkt patientsäkerhet genom rätt kompetens – utifrån hälso- och sjukvårdens och tandvårdens behov. S.
64. En ny kontrollorganisation i livsmedelskedjan – för ökad effektivitet, likvärdighet och konkurrenskraft. LI.
65. En mer flexibel hyresmarknad. Ju.
66. En straffreform. Volym 1, 2, 3 och 4. Ju.
67. Arlanda – en viktig port för det svenska välståndet. Åtgärder som stärker konkurrenskraften för Arlanda flygplats. LI.
68. Nya samverkansformer, modern byggnads- och reparationsberedskap – för ökad försörjningsberedskap. KN.
69. Effektivare samverkan för djur- och folkhälsa. LI.
70. Längre liv, längre arbetsliv – förlängd rätt att kvarstå i anställningen. A.
71. Fortsatt utveckling av en nationell läkemedelslista – en del i en ny nationell infrastruktur för datadelning. Del 1 och 2. S.
72. Verktyg för en mer likvärdig resursfördelning till skolan. U.
73. En arbetsmiljöstrategi för ett förändrat arbetsliv. A.
74. Ny reglering för den arbetsmarknadspolitiska verksamheten. A.
75. Folkbokföringsverksamhet, biometri och brottsbekämpning. Fi.
76. Det handlar om oss – så bryter vi utanförskapet och bygger en starkare gemenskap. A.
77. En översyn av den statliga lönegarantin. A.
78. En reformerad underrättelseverksamhet. Fö.
79. Samlade förmågor för ökad cybersäkerhet. Fö.

80. Koordinatbestämda fastighetsgränser. Ju.
81. En ny organisation av ekobrottsbekämpningen. Ju.
82. Sysselsättning och boende på landsbygden – Juridiska personers förvärv av jordbruksmark och en effektiv tillämpning av glesbygdsbestämmelserna. LI.
83. Ett nationellt förbud mot tiggeri. Ju.
84. Hem för barn och unga. För en trygg, säker och meningsfull vård. S.
85. Ökad tydlighet, stärkt samverkan – förutsättningar för framtidens utvecklingspolitik. LI.
86. Redo! En utredning om personalförsörjningen av det militära försvaret. Fö.
87. Straffrättsliga åtgärder mot korruption och tjänstefel. Ju.
88. Tidigt besked om lämplig användning av mark och vatten. KN.
89. En moderniserad fiskelagstiftning. Volym 1 och 2. LI.
90. Förmedling av post till personer med skydd i folkbokföringen. Fi.
91. Nya regler om arv och testamente – bland annat ett testamentsregister i offentlig regi och ett stärkt skydd för efterlevande sambor. Ju.
92. En kulturkanon för Sverige. Ku.
93. En robust skogspolitik för aktivt skogsbruk. Del 1 och 2. LI.
94. En säkrare utrikesförvaltning. UD.
95. Skärpta villkor för anhöriginvandring. Ju.
96. Fler möjligheter till ökat välstånd. Fi.
97. Krishantering och ändrade rörelseregler för försäkringsföretag. Volym I, II, III & IV. Fi.
98. En bättre organisering av fastighetsbildningsverksamheten. LI.
99. Ändring av permanent uppehållstillstånd för vissa utlänningar. Ju.
100. Åtgärder mot illegal ip-tv. Ku.
101. Anpassningar till AI-förordningen – säker användning, effektiv kontroll och stöd för innovation. Fi.
102. Bättre ansvarsfördelning. Ju.
103. En ny produktansvarslag. Ju.
104. Ny kärnkraft i Sverige – ett samlat system för omhändertagande av radioaktivt avfall. KN.
105. Om överföring av Första AP-fondens verksamhet och tillgångar till Tredje och Fjärde AP-fonderna. Fi.
106. Om överföring av Sjätte AP-fondens verksamhet och tillgångar till Andra AP-fonden. Fi.
107. Sveriges nationella klimatmål – uppdaterat etappmål till 2030. KN.
108. Ett datalyft mot fel, fusk och frånvaro. S.
109. Särskilda provokativa åtgärder. Ju.
110. Snabbare bredband i hela landet – åtgärder för effektivare utbyggnad av gigabitinfrastruktur. Fi.
111. Rättssäkerhetens pris. Ju.
112. Verktyg för skydd av EU-medel. Rättsliga förutsättningar för svenska myndigheter att använda Arachne och Edes. Fi.
113. En förbättrad elevhälsa. U.
114. Skärpningar i lagen om särskild kontroll av vissa utlänningar och utlänningslagen. Volym 1 och 2. Ju.
115. Kompletterande bestämmelser till EU:s cyberresiliensförordning. Fi.
116. Distribution av radio och tv i det nya medielandskapet. Ku.
117. Fondandelsbolag – för en mer konkurrenskraftig fondmarknad. Volym 1 och 2. Fi.
118. Ökad och rättvis tillgång till data – kompletterande bestämmelser till EU:s dataförordning. Fi.

Statens offentliga utredningar 2025

Systematisk förteckning

Justitiedepartementet

Skärpta krav för svenskt medborgarskap. [1]

Några frågor om grundläggande fri- och rättigheter. [2]

Straffbarhetsåldern. [11]

Ett nytt regelverk för uppsikt och förvar. [16]

Ersättningsregler med brottsoffret i fokus. [23]

Utmönstring av permanent uppehållstillstånd och vissa anpassningar till miniminivån enligt EU:s migrations- och asylpakt. [31]

Skärpta och tydligare krav på vandel för uppehållstillstånd. [33]

Ett modernare konsumentskydd vid distansavtal. [34]

Säkrare tivoli. [40]

Säkerhetsskyddslagen – ytterligare kompletteringar. [42]

Ökat informationsutbyte mellan myndigheter – några anslutande frågor. [45]

Tryggare idrottsarrangemang. [46]

Säkerhetspolisens behandling av personuppgifter. [49]

Ökad insyn i politiska processer. [52]

Ett skärpt regelverk om utvisning på grund av brott. [54]

Stärkt skydd för domstolarnas och domarnas oberoende. [56]

Polisiär beredskap i fred, kris och krig. [57]

Stärkt lagstiftning mot hedersrelaterat våld och förtryck. [59]

En mer flexibel hyresmarknad. [65]

En straffreform. Volym 1, 2, 3 och 4. [66]

Koordinatbestämda fastighetsgränser. [80]

En ny organisation av ekobrottsbekämpningen. [81]

Ett nationellt förbud mot tiggeri. [83]

Straffrättsliga åtgärder mot korruption och tjänstefel. [87]

Nya regler om arv och testamente – bland annat ett testamentsregister i offentlig regi och ett stärkt skydd för efterlevande sambor. [91]

Skärpta villkor för anhöriginvandring. [95]

Ändring av permanent uppehållstillstånd för vissa utlänningar. [99]

Bättre ansvarsfördelning. [102]

En ny produktansvarslag. [103]

Särskilda provokativa åtgärder. [109]

Rättssäkerhetens pris. [111]

Skärpningar i lagen om särskild kontroll av vissa utlänningar och utlänningslagen. Volym 1 och 2. [114]

Klimat- och näringslivsdepartementet

Ny kärnkraft i Sverige – effektivare tillståndsprövning och ändamålsenliga avgifter. [7]

En skärpt miljöstraffrätt och ett effektivt sanktionssystem. [14]

Miljömålsberedningens förslag om en strategi för hur Sverige ska leva upp till EU:s åtaganden inom biologisk mångfald respektive nettoupptag av växthusgaser från markanvändningssektorn (LULUCF). [21]

Förbättrad konkurrens i offentlig och privat verksamhet. [22]

Spänning i tillvaron – hur säkrar vi vår framtida elförsörjning? [47]

Bättre förutsättningar för klimatanpassning. [51]

Nya samverkansformer, modern byggnads- och reparationsberedskap – för ökad försörjningsberedskap. [68]

Tidigt besked om lämplig användning av mark och vatten. [88]

Ny kärnkraft i Sverige – ett samlat system för omhändertagande av radioaktivt avfall. [104]

Sveriges nationella klimatmål – uppdaterat etappmål till 2030. [107]

Kulturdepartementet

Publiken i fokus – reformer för ett starkare filmland. [24]

En kulturkanon för Sverige. [92]

Åtgärder mot illegal ip-tv. [100]

Distribution av radio och tv i det nya medielandskapet. [116]

Landsbygds- och infrastrukturdepartementet

Avgift för områdessamverkan – och andra åtgärder för trygghet i byggd miljö. [5]

Anpassning av svensk rätt till EU:s avskogningsförordning. [17]

Vissa förändringar av jaktlagstiftningen. [32]

En ny nationell myndighet för viltförvaltning. [50]

En stärkt hästnäring – för företagande, jämställdhet, jämlikhet och folkhälsa. [58]

En ny kontrollorganisation i livsmedelskedjan – för ökad effektivitet, likvärdighet och konkurrenskraft. [64]

Arlanda – en viktig port för det svenska välståndet. Åtgärder som stärker konkurrenskraften för Arlanda flygplats. [67]

Effektivare samverkan för djur- och folkhälsa. [69]

Sysselsättning och boende på landsbygden – Juridiska personers förvärv av jordbruksmark och en effektiv tillämpning av glesbygdsbestämmelserna. [82]

Ökad tydlighet, stärkt samverkan – förutsättningar för framtidens utvecklingspolitik. [85]

En moderniserad fiskelagstiftning. Volym 1 och 2. [89]

En robust skogspolitik för aktivt skogsbruk. Del 1 och 2. [93]

En bättre organisering av fastighetsbildningsverksamheten. [98]

Socialdepartementet

En förändrad abortlag – för en god, säker och tillgänglig abortvård. [10]

Stärkta drivkrafter och möjligheter för biståndsmottagare Volym 1 och 2. [15]

Att omhänderta barn och unga. [38]

Digital teknik på lika villkor. En reglering för socialtjänsten och verksamhet enligt LSS. [39]

Pensionsnivåer och pensionsavgiften – analyser på hundra års sikt. [41]

Säkerställ tillgången till läkemedel – förordnande och utlämnande i bristsituationer. [43]

Stärkt pandemiberedskap. [48]

Kvalificering till socialförsäkring och ekonomiskt bistånd för vissa grupper. [53]

Sveriges internationella adoptionsverksamhet – lärdomar och vägen framåt. Volym 1 och 2. [61]

Ansvaret för hälso- och sjukvården. Volym 1 Bedömningar och förslag. Volym 2 Underlagsrapporter. [62]

Stärkt patientsäkerhet genom rätt kompetens – utifrån hälso- och sjukvårdens och tandvårdens behov. [63]

Fortsatt utveckling av en nationell läkemedelslista – en del i en ny nationell infrastruktur för datadelning. Del 1 och 2. [71]

Hem för barn och unga. För en trygg, säker och meningsfull vård. [84]

Ett datalyft mot fel, fusk och frånvaro. [108]

Utbildningsdepartementet

Bättre förutsättningar för trygghet och studiero i skolan. [8]

På språklig grund. [9]

Ett likvärdigt betygssystem Volym 1 och 2. [18]

Kunskap för alla – nya läroplaner med fokus på undervisning och lärande. [19]

Tid för undervisningsuppdraget – åtgärder för god undervisning och läraryrkenas attraktivitet. [26]

En socionomutbildning i tiden. [27]

Skärpta villkor för friskolesektorn. [37]

Förbättrat stöd i skolan. [44]

Verktyg för en mer likvärdig resursfördelning till skolan. [72]

En förbättrad elevhälsa. [113]

Utrikesdepartementet

Skydd för biologisk mångfald i havsområden utanför nationell jurisdiktion. [36]

En säkrare utrikesförvaltning. [94]