Verktyg för skydd av EU-medel

Rättsliga förutsättningar för svenska myndigheter att använda Arachne och Edes

Betänkande av Utredningen om användningen av vissa verktyg för att skydda EU:s finansiella intressen

Stockholm 2025

STATENS OFFENTLIGA UTREDNINGAR

SOU 2025:112

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 978-91-525-1407-8 (tryck)
ISBN 978-91-525-1408-5 (pdf)
ISSN 0375-250X

Till statsrådet och chefen för Finansdepartementet Elisabeth Svantesson

Regeringen beslutade den 12 december 2024 att ge en särskild utredare i uppdrag att undersöka de rättsliga förutsättningarna för svenska myndigheter att använda riskbedömningsverktyget Arachne och uppfylla kraven enligt den omarbetade budgetförordningen, bland annat skyldigheterna inom ramen för systemet för tidig upptäckt och uteslutning (Edes), för att motverka felaktiga utbetalningar och bedrägerier i samband med hantering av EU-medel.

Till särskild utredare förordnades från och med den 3 februari 2025 rättsliga experten Leena Mildenberger.

Som experter förordnades från och med den 10 februari 2025 stf. enhetschefen vid Statens Jordbruksverk (Jordbruksverket) Annika Boiardt, stabsjuristen vid Ekobrottsmyndigheten Olof Hallström, revisorn vid Ekonomistyrningsverket (ESV) Hoger Ibrahim, verksamhetsexperten vid Polismyndigheten Teresa Klett, departementssekreteraren vid Finansdepartementet Mats Kullander, verksamhetsexperten vid Migrationsverket Jonas Lidström, verksjuristen vid Tillväxtverket Meliha Sevinc Husberg och verksjuristen vid Rådet för Europeiska socialfonden i Sverige (Svenska ESF-rådet) Joel Sjödin. Rättsliga experten Liselotte Westerlind förordnades som expert från och med den 7 april 2025. Från och med den 15 maj 2025 entledigades Teresa Klett från uppdraget och ersattes samma dag med juristen vid Polismyndigheten Mathias Lassinantti Jansson. Från och med den 1 juli 2025 entledigades Mats Kullander från uppdraget och ersattes samma dag med ämnesrådet Ricky Ifwarsson.

Som sekreterare i utredningen anställdes från och med den 4 mars 2025 hyresrådet Per Lindblom.

Arbetet har bedrivits i nära samråd med experterna. Experterna har i allt väsentligt ställt sig bakom de förslag och bedömningar som lämnas.

Härmed överlämnas betänkandet *Verktyg för skydd av EU-medel. Rättsliga förutsättningar för svenska myndigheter att använda Arachne och Edes* (SOU 2025:112). Utredningens uppdrag är med detta slutfört.

Stockholm november 2025

Leena Mildenberger

Per Lindblom

Innehåll

Begrepp och förkortningar

Amif: Asyl-, migrations- och integrationsfonden. (På engelska: Asylum, Migration and Integration Fund.)

Arachne: Ett it-verktyg för riskvärdering och datautvinning som kommissionen har tagit fram och tillhandahåller för att stödja ansvariga myndigheter i kontroller av stödmottagare av EU-medel.

Arachne-stadgan: Arachne, Charter for the introduction, the application and the integration of the Arachne risk scoring tool (senaste tillgängliga version: 2.4).[1]

Attesterande organ: Ett offentligt eller privat organ som utses av varje medlemsstat för att granska medlemsstatens styrningssystem och utbetalande organs årsräkenskaper och prestationsrapportering avseende utgifter med finansiering från EU:s jordbruksfonder.

BAR – Brexit Adjustment Reserve: Brexitjusteringsreserven.

Behörig myndighet: Myndighet som utses av varje medlemsstat för att utfärda, granska och återkalla ackrediteringen av utbetalande organ.

Beskrivning av personuppgiftsbehandlingen för Arachne: Den beskrivning av personuppgiftsbehandling avseende Arachne som kommissionen har anmält till EU:s dataskyddsombuds register.[2]

---

[1] https://employment-social-affairs.ec.europa.eu/policies-and-activities/funding/european-social-fund-plus-esf/what-arachne_en. Hämtat 2025-10-22.
[2] Record for processing of personal data. Title: Risk analysis for fraud prevention and detection in the management of EU funds (ARACHNE SYSTEM). Reference: DPR-EC-00598.4, publicerad den 27 november 2023. https://ec.europa.eu/dpo-register/detail/DPR-EC-00598. Hämtat 2025-10-29.

Beskrivning av personuppgiftsbehandlingen för Edes: Den beskrivning av personuppgiftsbehandling avseende Edes som kommissionen har anmält till EU:s dataskyddsombuds register.[3]

BMVI – Border Management and Visa Instrument: Instrumentet för ekonomiskt stöd för gränsförvaltning och viseringspolitik.

Budgetförordningen (ibland den omarbetade budgetförordningen): Europaparlamentets och rådets förordning (EU, Euratom) 2024/2509 av den 23 september 2024 om finansiella regler för unionens allmänna budget (omarbetning).

Budgetgenomförande: Utförande av verksamheter som rör förvaltning, övervakning, kontroll och revision av budgetanslag i enlighet med de metoder som föreskrivs i artikel 62 i budgetförordningen (enligt definition i artikel 2.7 i budgetförordningen).

CAP – Common Agricultural Policy: EU:s gemensamma jordbrukspolitik. (GJP i svensk förkortning.)

CPR – Common Provisions Regulation: Europaparlamentets och rådets förordning (EU) 2021/1060 av den 24 juni 2021 om fastställande av gemensamma bestämmelser för Europeiska regionala utvecklingsfonden, Europeiska socialfonden+, Sammanhållningsfonden, Fonden för en rättvis omställning och Europeiska havs-, fiskeri- och vattenbruksfonden samt finansiella regler för dessa och för Asyl-, migrations- och integrationsfonden, Fonden för inre säkerhet samt instrumentet för ekonomiskt stöd för gränsförvaltning och viseringspolitik. Avser programperioden 2021–2027.

Dataskyddsförordningen (ibland EU:s dataskyddsförordning): 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).

[3] Record for processing of personal data, Title: Entry of a Data Subject in the Early Detection and Exclusion System (EDES-DB), Reference DPR-EC-04410.2, publicerad den 8 februari 2022. https://ec.europa.eu/dpo-register/detail/DPR-EC-04410. Hämtat 2025-10-29.

Dataskyddsförordningen för EU:s institutioner: 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.

Delad förvaltning: En metod för att genomföra EU-budgeten där kommissionen behåller det yttersta ansvaret för genomförandet men där medlemsstaterna ansvarar för nationella förvaltnings- och kontrollsystem.

Delegerade organ: Organ som utför uppgifter på delegation av ett utbetalande organ. Det utbetalande organet får delegera utförandet av alla uppgifter utom utbetalningar.

Den tidigare budgetförordningen: Europaparlamentets och rådets förordning (EU, Euratom) 2018/1046 av den 18 juli 2018 om finansiella regler för unionens allmänna budget, om ändring av förordningarna (EU) nr 1296/2013, (EU) nr 1301/2013, (EU) nr 1303/2013, (EU) nr 1304/2013, (EU) nr 1309/2013, (EU) nr 1316/2013, (EU) nr 223/2014, (EU) nr 283/2014 och beslut nr 541/2014/EU samt om upphävande av förordning (EU, Euratom) nr 966/2012.

Direkt förvaltning: En metod för att genomföra EU-budgeten där kommissionen på egen hand förvaltar en EU-fond eller ett program, till skillnad från delad förvaltning eller indirekt förvaltning.

ECA – European Court of Auditors: Europeiska unionens revisionsrätt.

Edes – Early Detection and Exclusion System: Systemet för tidig upptäckt och uteslutning. Inrättat av kommissionen för att stärka skyddet av EU:s ekonomiska intressen och säkerställa sund ekonomisk förvaltning.

EGF – European Globalisation Adjustment Fund for Displaced Workers: Europeiska fonden för justering för globaliseringseffekter för uppsagda arbetstagare.

EGFJ: Europeiska garantifonden för jordbruket. (På engelska: European Agricultural Guarantee Fund [EAGF].)

EHFVF: Europeiska havs-, fiskeri- och vattenbruksfonden. (På engelska: European Maritime, Fisheries and Aquaculture Fund [EMFAF]).

Ejflu: Europeiska jordbruksfonden för landsbygdsutveckling. (På engelska: Agricultural Fund for Rural Development [EAFRD].)

Eppo – European Public Prosecutor's Office: Europeiska åklagarmyndigheten.

Eruf: Europeiska regionala utvecklingsfonden. (På engelska: European Regional Development Fund [ERDF].)

ESF+: Europeiska socialfonden+. Föregångaren under programperioden 2014–2020 benämndes Europeiska socialfonden (ESF). (På engelska: European Social Fund Plus.)

ESI-fonder: Europeiska struktur- och investeringsfonderna. De fem fonder som under programperioden 2014–2020 omfattades av gemensamma regler: Eruf, ESF, Efjlu, EHFF och Sammanhållningsfonden (ej verksam i Sverige). Under programperioden 2021–2027 omfattas Ejflu inte längre av CPR. (På engelska: European Structural and Investment Funds, ESIF.)

Ex ante-kontroller: Kontroller som utförs innan en ansökan om EU-medel beviljas och som kan bidra till att EU-medel inte betalas ut i fall då det finns risk för felaktiga utbetalningar, dubbelfinansieringar, bedrägerier, korruption och intressekonflikter.

Ex post-kontroller: Kontroller som utförs efter det att en ansökan om EU-medel har beviljats och som kan bidra till att felaktigheter upptäcks i efterhand.

FRO: Fonden för en rättvis omställning. (På engelska: Just Transition Fund [JTF].)

FTS – Financial Transparency System: Systemet för finansiell öppenhet. Offentlig onlinedatabas över mottagare av finansiering vid direkt och indirekt förvaltning.

Förmedlande organ: En förvaltande myndighet får ange ett eller flera förmedlande organ som ska utföra vissa uppgifter under den förvaltande myndighetens ansvar.

Förvaltande myndighet: Myndighet som utses av medlemsstaterna för att förvalta program med finansiering från fonder som regleras av CPR. Kan också avse den nationella förvaltande myndighet som medlemsstaterna ska utse för sina GJP-planer.

Genomförandemyndighet: Myndighet som inom RRF motsvarar förvaltande myndighet.

GJP: EU:s gemensamma jordbrukspolitik. (CAP i engelsk förkortning.)

IAKS: Förordningsstyrt administrations- och kontrollsystem som tillämpas på areal- och djurbaserade interventioner med finansiering från både EGFJ och Ejflu. (På engelska: Integrated Administration and Control System [IACS].)

Indirekt förvaltning: En metod för att genomföra EU-budgeten där kommissionen anförtror genomförandeuppgifter åt till exempel länder utanför EU och internationella organisationer.

Interoperabilitet: Förmåga som gör det möjligt för nätverks- och informationssystem hos olika aktörer att interagera med varandra genom datadelning med hjälp av elektronisk kommunikation.

Interreg: Program som stöder gränsöverskridande samarbetsprojekt mellan regioner och länder till stöd för regional utveckling.

IMS – Irregularity Management System: Systemet för hantering av oriktigheter. Ett elektroniskt system för informationsutbyte som underlättar rapportering av oriktigheter på olika områden. Det tillhandahålls medlemsstaterna och stödmottagarna av EU-medel.

ISF – Internal Security Fund: Fonden för inre säkerhet.

Olaf: Europeiska byrån för bedrägeribekämpning. (På engelska: European Anti-Fraud Office.)

Personuppgiftspolicy för Arachne: Kommissionens information som riktar sig till den vars personuppgifter behandlas.[4]

Personuppgiftspolicy för Edes: Kommissionens information som riktar sig till den vars personuppgifter behandlas.[5]

Programperiod: Program med finansiering från EU löper över perioder som normalt varar i sju år. Med nuvarande programperiod avses 2021–2027. Föregående programperiod avser 2014–2021. Nuvarande programperiod för EU:s jordbruksutgifter avser 2023–2027 då GJP under föregående period förlängdes med två år.

Revisionsmyndighet: Utses av medlemsstaterna för revision av program med finansiering från fonder som regleras av CPR. Revisionsmyndigheten utför systemrevisioner, insatsrevisioner och räkenskapsrevisioner i syfte att ge kommissionen en oberoende försäkran om att förvaltnings- och kontrollsystemen fungerar effektivt och att utgifterna i de räkenskaper som lämnas till kommissionen är lagliga och korrekta. Uttrycket används också nationellt när det gäller RRF, men i regelverket används ”revisionsorgan”.

RRF – The Recovery and Resilience Facility: EU:s facilitet för återhämtning och resiliens som kanaliserar medel från EU:s krisåterhämtningspaket *Next Generation EU* (Faciliteten för återhämtning och resiliens).

[4] Protection of your personal data, Processing operation: Risk analysis for fraud prevention and detection in the management of European Structural Funds (ARACHNE), Data Controller: DAC, Record reference: DPR-EC-00598. https://employment-social-affairs.ec.europa.eu/policies-and-activities/funding/european-social-fund-plus-esf/what-arachne_en. Hämtat 2025-10-23.
[5] Protection of your personal data, Processing operation: Privacy Statement for the database of the Early Detection and Exclusion System (EDES), Record reference: DPR-EC-04410. https://commission.europa.eu/system/files/2023-06/Privacy_statement-edes-June-2023.pdf. Hämtat 2025-10-23.

Sammanhållningspolitiken: Den europeiska sammanhållningspolitiken har som mål att bidra till ekonomisk, social och territoriell sammanhållning inom unionen. Den motsvaras i EU:s budget av utgiftsområdet Sammanhållning, resiliens och värden. I sammanhållningspolitiken ingår Eruf, ESF+, FRO och Sammanhållningsfonden.

SEFI-rådet: Rådet för skydd av EU:s finansiella intressen.

Utbetalande organ: Myndighet eller organ som utses av en medlemsstat för att förvalta och kontrollera utgifter med finansiering från EU:s jordbruksfonder.

VIES – VAT Information Exchange System: Ett system för utbyte av information om mervärdesskatt och ett sökverktyg som ägs av kommissionen.

Sammanfattning

Uppdraget

Utredningen har haft i uppdrag att undersöka de rättsliga förutsättningarna för svenska myndigheter att använda riskbedömningsverktyget Arachne och uppfylla kraven enligt den omarbetade budgetförordningen, Europaparlamentets och rådets förordning (EU, Euratom) 2024/2509 av den 23 september 2024 om finansiella regler för unionens allmänna budget (omarbetning), bland annat skyldigheterna inom ramen för systemet för tidig upptäckt och uteslutning (Edes), för att motverka felaktiga utbetalningar och bedrägerier i samband med hantering av EU-medel. I uppdraget har ingått att

- kartlägga vilka uppgifter myndigheterna skulle få tillgång till, registrera eller annars utbyta vid en användning av Arachne och inom ramen för Edes, samt vilken tillgång andra aktörer skulle få till uppgifterna,
- kartlägga och bedöma vilka skyldigheter som svenska myndigheter skulle ha vid en användning av Arachne och inom ramen för Edes,
- utifrån kartläggningen bedöma om det finns behov av ändrade regler för att svenska myndigheter ska kunna använda Arachne och uppfylla sina skyldigheter inom ramen för Edes,
- bedöma om det finns behov av ändrade regler för att svenska myndigheter ska kunna uppfylla kraven i den omarbetade budgetförordningen, särskilt i fråga om rapportering av uppgifter för registrering i Arachne,
- lämna nödvändiga författningsförslag.

Det övergripande syftet med uppdraget är att EU:s finansiella intressen ska skyddas. För skyddet av EU:s finansiella intressen är det centralt att motverka felaktiga utbetalningar, bedrägerier, korruption, intressekonflikter, dubbelfinansiering och andra oegentligheter. De svenska myndigheter som deltar i genomförandet av EU:s budget behöver ha ändamålsenliga system för att säkerställa tillgång till den information som behövs för att göra riskbedömningar av stödsökande och slutliga stödmottagare, och för att i efterhand kontrollera dessa.

Centralt för utredningen är innehållet i den omarbetade budgetförordningen. Huvudsakligen ska de delar av budgetförordningen som är relevanta i denna utredning tillämpas på program som antas eller finansieras från och med den 1 januari 2028.

Budgetförordningen medför krav på medlemsstaterna att tillgängliggöra uppgifter för kommissionen, samt att i vissa fall offentliggöra information.

Arachne är ett datautvinnings- och riskvärderingsverktyg som Europeiska kommissionen (härefter kommissionen) har tagit fram för att hjälpa medlemsstaternas myndigheter att kontrollera hur EU-stöd används och förvaltas. Verktyget är i dag frivilligt att använda och detta gäller även enligt den omarbetade budgetförordningen. De som i dag väljer att använda Arachne behöver lämna vissa uppgifter för att Arachne ska fungera som avsett. Lämnandet av uppgifter som ska tillföras Arachne är avsett att från med 2028 ske genom det ovan nämnda kravet på tillgängliggörande som budgetförordningen medför.

Edes är ett system som kommissionen har utvecklat och som syftar till att göra det lättare att tidigt upptäcka personer eller enheter som är ett hot mot unionens ekonomiska intressen, att utesluta personer eller enheter från att ta del av EU-medel och att ålägga ekonomiska sanktioner mot mottagare av EU-medel som befinner sig i en uteslutningssituation. Systemet har hittills enbart omfattat EU-medel under vissa förvaltningsformer. Det kommer att bli obligatoriskt att använda Edes vid hantering av i princip samtliga EU-stöd när det gäller program som antas eller finansieras från och med den 1 januari 2028. Vid svenska myndigheters användning av Edes kommer det att gälla en partiell tillämpning på så sätt att endast vissa av uteslutningsgrunderna gäller.

Utredningen har inte haft i uppdrag att analysera om svenska myndigheter bör eller inte bör använda de system som EU tillhandahåller för att skydda EU:s finansiella intressen i de delar ett sådant användande är eller kommer att vara frivilligt. Utredningens uppdrag är begränsat till att undersöka de rättsliga förutsättningarna för svenska myndigheter att använda Arachne och för att uppfylla kraven enligt den omarbetade budgetförordningen, bland annat när det gäller Edes.

Betänkandet innehåller en kartläggningsdel där det huvudsakligen behandlas vilka svenska myndigheter som får vissa skyldigheter eller kan komma att vidta vissa åtgärder på frivillig basis samt vad detta innebär, särskilt när det gäller hanteringen av information av olika slag. Betänkandet innehåller också en del där det analyseras om det behöver vidtas några åtgärder för att svenska myndigheter ska kunna uppfylla dessa skyldigheter eller för att de ska kunna vidta vissa åtgärder på frivillig väg. Kartläggningen och övervägandena om behov av åtgärder fokuserar på följande moment.

- Lämnande av uppgifter vid ett användande av Arachne (före 2028)
- Tillgängliggörande av obligatoriska uppgifter för kommissionen
- Tillgängliggörande av frivilliga uppgifter för kommissionen
- Offentliggörande av uppgifter på kommissionens webbsida
- Användande av Arachne som verktyg
- Användande av Edes som verktyg.

Utredningens kartläggningsarbete

Fonder som omfattas

Utredningen har till att börja med undersökt vad som gäller för EU-medel som hanteras genom så kallad delad förvaltning, det vill säga gemensamt av kommissionen och Sverige. Betänkandet omfattar i denna del främst bedömningar rörande hanteringen av Europeiska garantifonden för jordbruket, Europeiska jordbruksfonden för landsbygdsutveckling, Europeiska regionala utvecklingsfonden, Europeiska socialfonden+, Europeiska havs-, fiskeri- och vattenbruksfonden, Asyl-, migrations- och integrationsfonden, Fonden för inre

säkerhet, Fonden för en rättvis omställning samt Instrumentet för ekonomiskt stöd för gränsförvaltning och viseringspolitik.

Utredningen har också i viss utsträckning undersökt vad som gäller för direkt förvaltning tillsammans med medlemsstaterna, en förvaltningsform som för närvarande används endast när det gäller Faciliteten för återhämtning och resiliens (RRF).

Även om förhållandena vid förvaltning av RRF behandlas, läggs i detta betänkande störst fokus på de EU-medel som hanteras genom delad förvaltning. Det regelverk som styr förvaltningen av RRF har i praktiken begränsad tillämplighet i tid genom att reformer och investeringar ska ha genomförts till den 31 augusti 2026 och utbetalningar till den 31 december samma år.

Program med finansiering från EU löper över perioder som normalt varar i sju år. Med nuvarande programperiod avses 2021–2027. Nuvarande programperiod för EU:s jordbruksutgifter avser dock 2023–2027. Det kan komma att ske förändringar för den programperiod som börjar 2028 när det gäller vilka fonder som finns och hur de förvaltas.

Myndigheter som omfattas

Flera svenska myndigheter har roller när det gäller genomförandet av EU:s budget och hanteringen av EU-medel. Myndigheter som hanterar EU-medel genom delad förvaltning i dag är bland annat Statens jordbruksverk (Jordbruksverket), Tillväxtverket, Rådet för Européiska socialfonden i Sverige (Svenska ESF-rådet), Migrationsverket, Polismyndigheten och länsstyrelserna. Även till exempel Skogsstyrelsen, Sametinget och Havs- och vattenmyndigheten har funktioner inom delad förvaltning som är relevanta för detta betänkande.

När det gäller RRF finns det totalt 62 så kallade genomförandemyndigheter. Tio myndigheter har fått ett särskilt ansvar för genomförandet och rapporterar in resultatinformation till Ekonomistyrningsverket (ESV), nämligen Boverket, Myndigheten för digital förvaltning, Myndigheten för yrkeshögskolan, Naturvårdsverket, Post- och telestyrelsen, Skolverket, Socialstyrelsen, Statens energimyndighet, Trafikverket samt Universitetskanslersämbetet. Utöver dessa tio myndigheter är även samtliga länsstyrelser och 31 lärosäten genomförandemyndigheter.

ESV har en roll som revisionsmyndighet med ansvar att granska hanteringen av de medel som Sverige tar emot inom ramen för delad förvaltning samt att granska genomförandet av den svenska återhämtningsplanen inom ramen för RRF.

Ekobrottsmyndigheten ansvarar för samordningen av de nationella åtgärderna mot oegentlig och ineffektiv hantering och användning av EU-medel i Sverige.

Även Regeringskansliet har vissa uppgifter relaterade till hanteringen av EU-medel. Landsbygds- och infrastrukturdepartementet har rollen som behörig myndighet för jordbruksfonderna och ansvarar bland annat för att ackreditera utbetalande organ och utse attesterande organ. Finansdepartementet är samordnande myndighet för genomförandet av Sveriges återhämtningsplan inom ramen för RRF.

Den svenska organisationsstrukturen kan komma att förändras i framtiden, bland annat på grund av tillkomsten av nya fonder på EU-nivå. Förändringar i den svenska organisationsstrukturen har också föreslagits av Utredningen om hantering av EU-medel i betänkandet En ny organisation för förvaltning av EU-medel (SOU 2024:22), förslag som bereds i Regeringskansliet.

Tillgängliggörande av obligatoriska uppgifter

Av budgetförordningen följer från och med 2028 ett krav på svenska myndigheter som deltar i genomförandet av EU:s budget att göra viss information tillgänglig för kommissionen. Avsikten är att denna information ska tillföras Arachne. De uppgifter som ska tillgängliggöras avser mottagare av stöd, insatsen och mottagarens verkliga huvudmän. Skyldigheten gäller dock bara sådan information som myndigheterna ska registrera och lagra enligt sektorsspecifika regler, vilket innebär att kraven varierar mellan olika sektorer. De uppgifter som tillgängliggörs kan komma att få betydande spridning, bland annat genom att användare av Arachne i andra länder får tillgång till dem och genom att uppgifterna också kan komma att offentliggöras på en webbsida.

De myndigheter som omfattas av skyldigheten bedöms vara alla myndigheter som tar emot, förvaltar, övervakar, kontrollerar och

reviderar EU-medel, om de har skyldigheter enligt sektorsspecifika regler att registrera och lagra information av aktuellt slag.

Tillgängliggörande av frivilliga uppgifter

Vid sidan av de uppgifter som måste tillgängliggöras för kommissionen möjliggör budgetförordningen ett frivilligt tillgängliggörande av uppgifter. De frivilliga uppgifter som tillgängliggörs kan komma att få betydande spridning, bland annat genom att användare av Arachne i andra länder kan få tillgång till dem. Det finns vissa begränsningar rörande vilka uppgifter som kan lämnas på frivillig basis. Det kan vara bra att vissa uppgifter, som inte är rättsligt obligatoriska, ändå tillgängliggörs och tillförs Arachne, då det kan öka värdet av systemet. Utredningen behandlar vilka uppgifter det kan finnas skäl att tillgängliggöra på frivillig basis men konstaterar att det finns utmaningar när det gäller att identifiera vilka uppgifter det kan vara fråga om.

Offentliggörande av uppgifter

Budgetförordningen innebär en ny skyldighet för svenska myndigheter som hanterar EU-medel inom ramen för förvaltningsformen direkt förvaltning tillsammans med medlemsstaterna. Skyldigheten gäller att säkerställa ett offentliggörande i efterhand av viss information på en centraliserad webbplats. Skyldigheten kommer inte att gälla RRF, som hanteras inom ramen för den förvaltningsformen. Det kan dock inte uteslutas att det under kommande programperioder kommer nya fonder och program som förvaltas på detta sätt. Sverige kommer då att vara skyldigt att uppfylla skyldigheten.

Den information som ska offentliggöras motsvarar vissa av de uppgifter som ska tillgängliggöras för kommissionen. Vidare finns det undantagssituationer då uppgifter inte ska offentliggöras.

Användande av Arachne som verktyg

Utredningen bedömer att följande slags myndigheter kan komma att använda Arachne som verktyg.

- De myndigheter som deltar i genomförandet av budgeten inom ramen för delad förvaltning och därvid har någon roll i tilldelning av medel eller kontroll av utbetalda medel.
- De myndigheter som inom ramen för RRF deltar i genomförandet av budgeten och därvid har någon roll i tilldelning av medel eller kontroll av utbetalda medel, samt de myndigheter som i framtiden eventuellt kommer att på det sättet förvalta EU-fonder med en liknande förvaltningsform, det vill säga genom direkt förvaltning tillsammans med medlemsstaterna.
- De myndigheter som har i uppgift att i efterhand genomföra granskningar eller revisioner av utbetalade stöd, såsom ESV i egenskap av revisionsmyndighet.

Uppgifterna i Arachne består i dagsläget av både så kallade interna data och externa data. Det interna datainnehållet består av uppgifter om program och beviljade stöd från de deltagande medlemsstaterna och uppgifter från kommissionen.

Arachne innehåller också externa data från olika kommersiella databaser, nämligen Orbis och World Compliance. Informationen kan exempelvis avse information om företag och personer. Informationen kan inkludera uppgifter om att personer förekommer på olika listor som andra aktörer har tagit fram med avseende på bland annat politiskt utsatta personer och olika sanktionslistor. Informationen kan även inkludera negativ publicitet om personer och företag.

Arachne genererar automatiskt riskvärderingar rörande stöd som har beviljats. Dessa sparas också i Arachne. Det är också möjligt för en användare att begära att Arachne ska göra en riskvärdering under processen att välja vilka som ska tilldelas EU-medel. Detta sker genom en så kallad förhandsfunktion. Riskvärderingar inom ramen för förhandsfunktionen kan bara göras på begäran av en användare.

Det finns begränsningar när det gäller vilka uppgifter som användare av Arachne får tillgång till. I allmänhet är behörigheten för myndigheter begränsad till uppgifter om de program de själva hanterar.

Användande av Edes som verktyg

Utredningen bedömer att följande slags myndigheter kan komma att använda Edes som verktyg.

- De myndigheter som deltar i genomförandet av budgeten inom ramen för delad förvaltning och därvid har någon roll i tilldelning av medel eller kontroll av utbetalade medel. För de myndigheter som har en roll i tilldening av medel blir det obligatoriskt att tillämpa Edes-regelverket och därmed också att använda Edes-databasen. Vid delad förvaltning är tillämpningen partiell på det sättet att endast vissa uteslutningsgrunder är aktuella.
- De myndigheter som inom ramen för RRF deltar i genomförandet av budgeten och därvid har någon roll i tilldelning av medel eller kontroll av utbetalda medel – på frivillig basis.
- De myndigheter som eventuellt i framtiden kommer att förvalta EU-fonder genom direkt förvaltning tillsammans med medlemsstaterna och därvid har någon roll i tilldelning av medel eller kontroll av utbetalda medel. För de myndigheter som har en roll i tilldelning av medel kommer det att vara obligatoriskt att tillämpa Edes-regelverket och därmed också att använda Edes-databasen. Tillämpningen är partiell på det sättet att endast vissa uteslutningsgrunder är aktuella.
- De myndigheter som har i uppgift att i efterhand genomföra granskningar eller revisioner av utbetalade stöd, såsom ESV. För dessa myndigheter är det inte obligatoriskt att tillämpa Edes-regelverket.

I Edes finns det uppgifter om fall som avser tidig upptäckt, uteslutning och ekonomiska sanktioner. Där finns uppgifter om företag och om personer, och det kan då handla om namn, kontaktuppgifter, identifikationsnummer och födelsedatum. Där finns vidare uppgifter om grunderna bakom en uteslutning eller en sanktion. Grunderna kan exempelvis bestå i vissa allvarliga fel i yrkesutövningen eller av brottsligt beteende av vissa slag.

Utredningen gör bedömningen att svenska myndigheters tillgång till uppgifter i Edes kommer att vara begränsad till uppgifter om uteslutning, och alltså inte omfatta uppgifter om tidig upptäckt

och ekonomiska sanktioner. Tillgången kan också komma att vara begränsad till uppgifter om uteslutning på vissa grunder.

Behovet av åtgärder

Utredningen föreslår en ny bestämmelse i offentlighets- och sekretesslagen

Utredningen har bedömt behovet av ny sekretessreglering när det gäller tillgängliggörande av obligatoriska uppgifter, lämnande av uppgifter i situationer där det inte finns någon rättslig skyldighet att lämna uppgifter, offentliggörande av uppgifter samt användande av Arachne respektive Edes som verktyg.

Utredningen har kommit fram till att det inte krävs några författningsändringar på sekretessområdet när det gäller tillgängliggörande av obligatoriska uppgifter. Utredningen gör samma bedömning när det gäller de situationer då svenska myndigheter kan ha anledning att lämna uppgifter utan att det finns en rättslig skyldighet. Inte heller när det gäller kravet på offentliggörande av uppgifter finns det enligt utredningens bedömning något behov av författningsändringar på sekretessområdet.

När det gäller användande av Arachne och Edes som verktyg gör utredningen bedömningen att uppgifter i systemen kan komma att bli allmänna handlingar hos de svenska myndigheter som använder systemen. Det kan vidare beträffande båda systemen inte uteslutas att det finns behov av sekretesskydd för uppgifter som finns i systemen. Beträffande Edes bedömer utredningen att befintliga sekretessbestämmelser är tillräckliga och i det avseendet finns det inte något behov av författningsändringar.

Beträffande Arachne gör utredningen bedömningen att gällande sekretessregler i stor utsträckning är tillräckliga. Det är enligt utredningens mening ett fullt möjligt alternativ för regeringen att välja att inte gå vidare med något förslag om en ny sekretessbestämmelse. Det kan samtidigt argumenteras för att de oklarheter som finns beträffande möjligheterna att sekretessbelägga uppgifter som härrör från riskvärderingar enligt gällande sekretessbestämmelser kan leda till att viktiga allmänna intressen inte får genomslag. Utredningen lämnar därför ett förslag på hur en sekretessbestämmelse skulle kunna utformas.

Förslaget innebär att sekretess ska gälla för uppgift som härrör från en riskvärdering som har gjorts genom Arachne, om det kan antas att syftet med den förvaltning, övervakning, kontroll och revision som ska ske i enlighet med budgetförordningen motverkas om uppgiften röjs. Den nya bestämmelsen föreslås träda i kraft den 1 januari 2027.

Det krävs inte några författningsändringar på dataskyddsområdet eller ändringar i myndigheternas instruktioner

Utredningen har bedömt behovet av författningsändringar på dataskyddsområdet när det gäller tillgängliggörande av obligatoriska uppgifter, lämnande av uppgifter i situationer där det inte finns någon rättslig skyldighet att lämna uppgifter, offentliggörande av uppgifter samt användande av Arachne respektive Edes som verktyg. Det bedöms inte i något avseende krävas några författningsändringar på dataskyddsområdet. Befintlig dataskyddsreglering ger ett tillräckligt stöd och skydd för den personuppgiftsbehandling som förväntas bli aktuell.

Utredningen har också bedömt behovet av ändringar i myndigheternas instruktioner och har inte funnit något sådant behov utifrån de frågor som utredningen haft att bedöma.

1 Författningsförslag

1.1 Förslag till lag om ändring i offentlighets- och sekretesslagen (2009:400)

Härigenom föreskrivs att det i offentlighets- och sekretesslagen (2009:400) ska införas en ny paragraf, 17 kap. 7 d §, och närmast före 17 kap. 7 d § en ny rubrik av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	17 kap.
	Riskvärderingar vid genomförande av EU:s budget
	7 d § *Sekretess gäller för uppgift som härrör från en riskvärdering som har gjorts genom ett sådant system som avses i artikel 36.2 d i Europaparlamentets och rådets förordning (EU, Euratom) 2024/2509 av den 23 september 2024 om finansiella regler för unionens allmänna budget (omarbetning), om det kan antas att syftet med den förvaltning, övervakning, kontroll och revision som ska ske i enlighet med Europaparlamentets och rådets förordning (EU, Euratom) 2024/2509 motverkas om uppgiften röjs.*

Denna lag träder i kraft den 1 januari 2027.

2 Utredningens uppdrag och arbete

2.1 Utredningens uppdrag

Regeringen beslutade den 12 december 2024 att ge en särskild utredare i uppdrag att undersöka de rättsliga förutsättningarna för svenska myndigheter att använda riskbedömningsverktyget Arachne och uppfylla kraven enligt den omarbetade budgetförordningen[1], bland annat skyldigheterna inom ramen för systemet för tidig upptäckt och uteslutning (Edes), för att motverka felaktiga utbetalningar och bedrägerier i samband med hantering av EU-medel (bilaga 1).

I kommittédirektiven anger regeringen att det är viktigt att de svenska myndigheter som deltar i genomförandet av EU:s budget har ändamålsenliga system för att säkerställa tillgång till den information som behövs för att göra riskbedömningar av stödsökande och slutliga stödmottagare, och för att i efterhand kontrollera dessa. Bristfälliga kontroller av de stödsökande riskerar att leda till felaktiga utbetalningar av EU-medel.

Enligt regeringen saknar myndigheterna i dagsläget tillräckliga möjligheter att strukturerat och regelmässigt utbyta och samköra uppgifter om utbetalda medel och stödsökande respektive slutliga stödmottagare. Detta medför svårigheter att kontrollera riktigheten i vissa ingivna underlag som ligger till grund för beslut om stöd. Ett förbättrat informationsutbyte mellan myndigheterna kan bidra till att förebygga och motverka otillåten dubbelfinansiering och andra typer av bedrägerier.

[1] Europaparlamentets och rådets förordning (EU, Euratom) 2024/2509 av den 23 september 2024 om finansiella regler för unionens allmänna budget (omarbetning).

Utredningens uppdrag beskrivs sammanfattat så att utredaren bland annat ska

- kartlägga vilka uppgifter myndigheterna skulle få tillgång till, registrera eller annars utbyta vid en användning av Arachne och inom ramen för Edes, samt vilken tillgång andra aktörer skulle få till uppgifterna,
- kartlägga och bedöma vilka skyldigheter som svenska myndigheter skulle ha vid en användning av Arachne och inom ramen för Edes,
- utifrån kartläggningen bedöma om det finns behov av ändrade regler för att svenska myndigheter ska kunna använda Arachne och uppfylla sina skyldigheter inom ramen för Edes,
- lämna nödvändiga författningsförslag.

2.2 Utredningens arbetssätt

Fyra möten har ägt rum med utredningens expertgrupp. En anställd vid kommissionen har vid ett av mötena hållit en presentation av Arachne. Därutöver har bilaterala kontakter och kontakter med hela expertgruppen ägt rum.

Utredningen har hållit sig informerad om och beaktat relevant arbete på området som pågår inom Regeringskansliet och EU. Utredningen har vid genomförandet av uppdraget samrått med de delar av Regeringskansliet som ansvarar för hantering av EU-medel, samt övriga berörda myndigheter och organisationer.

2.3 Betänkandets disposition

Betänkandet är indelat i tolv kapitel. I kapitel 1 finns författningsförslag. Kapitel 2 behandlar utredningens uppdrag och arbete. I kapitel 3 finns en övergripande beskrivning av regleringen och organisationen av förvaltningen och kontrollen av EU-medel. Kapitel 4–6 innehåller kartläggningar som bland annat behandlar vilka myndigheter som berörs och vilka slags uppgifter som aktualiseras när det gäller lämnande och offentliggörande av uppgifter (kapitel 4), användande av Arachne som verktyg (kapitel 5) samt användande av Edes som

verktyg (kapitel 6). I kapitel 7 görs en övergripande beskrivning av vad som gäller beträffande offentlighet, sekretess och dataskydd. I kapitel 8 behandlas behovet av åtgärder. Kapitel 9 innehåller en samlad integritetsanalys. Kapitel 10 behandlar frågor om ikraftträdande och behov av övergångsbestämmelser. Kapitel 11 innehåller en konsekvensbeskrivning och kapitel 12 en författningskommentar.

3 Förvaltning och kontroll av EU-medel

3.1 Det är viktigt att motverka felaktig hantering av EU-medel

EU-budgeten samlar resurser på EU-nivå så att det finns nödvändiga medel för att unionen ska nå sina mål och genomföra sin politik. Budgeten finansieras av medlemsländernas EU-avgift. Den kan genomföras på olika sätt och med olika förvaltningsformer. Ansvaret för att budgetmedlen hanteras på rätt sätt åligger flera olika aktörer.

Det pågår arbete med att motverka olika former av oriktigheter vid utbetalningar av allmänna medel, både på EU-nivå och i Sverige. Det som ska motverkas kan vara felaktiga utbetalningar, dubbelfinansieringar, bedrägerier, korruption och intressekonflikter. Det är viktigt att det finns ändamålsenliga verktyg och system för att motverka sådana oriktigheter. I det arbetet är det centralt att myndigheter som förvaltar EU-medel har tillgång till relevant och aktuell information, bland annat om de juridiska och fysiska personer som är aktuella som mottagare av stöd. Sådan information är avgörande för att det ska kunna göras erforderliga kontroller innan stöd betalas ut och för att löpande och efterföljande kontroller, revisioner och granskningar ska kunna göras sedan stöd har betalats ut. Det i sin tur förutsätter ett effektivt och ändamålsenligt informationsutbyte mellan olika aktörer. Frågor om utökat informationsutbyte mellan myndigheter i Sverige har varit i fokus under ett antal år och lett till flera lagändringar på senare tid. På EU-nivå finns flera verktyg för att få tillgång till information av betydelse vid hantering av EU-medel.

3.2 Tre olika former för förvaltning av EU-medel

Det är Europeiska kommissionen (härefter kommissionen) som genomför EU-budgeten och alla program och fonder omfattas av någon av tre förvaltningsformer: direkt, indirekt eller delad förvaltning. Metoderna för genomförande av budgeten framgår av artikel 62 i budgetförordningen.

Vid *direkt förvaltning* förvaltar kommissionen på egen hand en EU-fond eller ett program.

Delad förvaltning innebär att kommissionen behåller det yttersta ansvaret för genomförandet men medlemsstaterna ansvarar för nationella förvaltnings- och kontrollsystem.

Indirekt förvaltning är en metod för att genomföra EU-budgeten där kommissionen anförtror genomförandeuppgifter åt till exempel länder utanför EU eller internationella organisationer.

Som medlem i EU tar Sverige del av EU-medel från unionens gemensamma budget. Huvuddelen av dessa medel förvaltas enligt principen om delad förvaltning, alltså gemensamt av kommissionen och svenska myndigheter. Sverige ansvarar för att bygga upp förvaltnings- och kontrollsystem som garanterar en sund ekonomisk förvaltning av EU:s medel.

När kommissionen genomför budgeten inom ramen för delad förvaltning ska uppgifter som har samband med genomförandet delegeras till medlemsstaterna. När medlemsstaterna utför uppgifter som har samband med genomförandet av budgeten inom ramen för delad förvaltning ska de utse organ som ska ansvara för förvaltningen och kontrollen av unionsmedel. Dessa organ får i sin tur anförtro några av sina uppgifter på andra organ (artikel 63 i budgetförordningen).

Det förekommer också att svenska myndigheter hanterar EU-stöd som förvaltas genom direkt förvaltning tillsammans medlemsstaterna.

3.3 Regelverket kring hanteringen av EU-medel

3.3.1 EU-lagstiftning

EUF-fördraget

Vikten av att skydda EU:s finansiella intressen, bland annat avseende EU-medel, betonas i flera EU-rättsakter. I fördraget om den Europeiska unionens funktionssätt (EUF-fördraget) föreskrivs bland annat att unionen och medlemsstaterna ska bekämpa bedrägerier och all annan olaglig verksamhet som riktar sig mot unionens ekonomiska intressen, att medlemsstaterna ska vidta samma åtgärder för att bekämpa bedrägerier som riktar sig mot unionens ekonomiska intressen som de vidtar för att bekämpa bedrägerier som riktar sig mot deras egna ekonomiska intressen och att medlemsstaterna ska samordna sina åtgärder för att skydda unionens ekonomiska intressen mot bedrägerier. Europaparlamentet och rådet ska i enlighet med det ordinarie lagstiftningsförfarandet besluta om nödvändiga åtgärder som rör förebyggande av och kamp mot bedrägerier som riktar sig mot unionens ekonomiska intressen för att ge effektivt och likvärdigt skydd i medlemsstaterna liksom i unionens institutioner, organ och byråer (artikel 325).

Budgetförordningen

Inom EU har det som berörs ovan vidtagits åtgärder för att stärka skyddet av unionens ekonomiska intressen. I bland annat detta syfte har EU:s budgetförordning omarbetats. Den omarbetade budgetförordningen ska – till stora delar – tillämpas från och med den 30 september 2024. Vissa övergångsbestämmelser innebär att delar av förordningen ska börja tillämpas senare. Huvudsakligen gäller – i de delar som är relevanta i denna utredning – att den omarbetade budgetförordningen endast tillämpas på program som antas eller finansieras från och med den 1 januari 2028. Förordningen benämns härefter i detta betänkande budgetförordningen eller ibland den omarbetade

budgetförordningen. I den mån den tidigare gällande budgetförordningen[1] avses benämns denna den tidigare budgetförordningen.

Budgetförordningen är central för hanteringen av EU:s budget. Den tar bland annat sikte på att förbättra skyddet av budgeten mot oriktigheter, inbegripet bedrägerier, korruption, intressekonflikter och dubbelfinansiering. Det handlar bland annat om åtgärder för att samla in, jämföra och sammanställa information om mottagare och att identifiera de fysiska personer som i slutändan drar nytta av missbruk av EU-medel (se exempelvis skäl 3 och 29 till budgetförordningen).

I förordningen finns bland annat bestämmelser om system för att skydda EU:s finansiella intressen, såsom Arachne och Edes, vilka behandlas närmare nedan, om medlemsstaters och myndigheters tillgängliggörande av uppgifter till kommissionen samt om offentliggörande av uppgifter. Eftersom det är en EU-förordning är den direkt tillämplig.

Budgetförordningen innebär att skärpta krav kan komma att ställas på medlemsländerna. Vilka dessa krav är behandlas mer ingående i detta betänkande.

Sektorsspecifika bestämmelser

Det finns ett antal sektorsspecifika EU-förordningar som reglerar villkor för särskilda politikområden och EU-fonder. I budgetförordningen görs i flera fall hänvisningar till sådana rättsakter. I det följande nämns några centrala sådana förordningar, med fokus på bestämmelser om kontroll och insamling och annan behandling av uppgifter.

[1] Europaparlamentets och rådets förordning (EU, Euratom) 2018/1046 av den 18 juli 2018 om finansiella regler för unionens allmänna budget, om ändring av förordningarna (EU) nr 1296/2013, (EU) nr 1301/2013, (EU) nr 1303/2013, (EU) nr 1304/2013, (EU) nr 1309/2013, (EU) nr 1316/2013, (EU) nr 223/2014, (EU) nr 283/2014 och beslut nr 541/2014/EU samt om upphävande av förordning (EU, Euratom) nr 966/2012.

CPR

En viktig sektorsspecifik reglering är förordningen om gemensamma bestämmelser, den så kallade CPR (Common Provisions Regulation)[2]. Den innehåller gemensamma bestämmelser för ett flertal fonder, nämligen Europeiska regionala utvecklingsfonden (Eruf), Europeiska socialfonden+ (ESF+), Sammanhållningsfonden, Fonden för en rättvis omställning (FRO) samt Europeiska havs-, fiskeri- och vattenbruksfonden (EHFVF). CPR innehåller vidare finansiella regler för nämnda fonder liksom för Asyl-, migrations- och integrationsfonden (Amif), Fonden för inre säkerhet (ISF) samt för Instrumentet för ekonomiskt stöd för gränsförvaltning och viseringspolitik (BMVI).

Förordningen innehåller bland annat bestämmelser om förvaltande myndigheters ansvar, till exempel att ha förvaltnings- och kontrollsystem samt att samla in och publicera uppgifter. Exempelvis föreskrivs i artikel 49.3 att den förvaltande myndigheten ska offentliggöra en förteckning på en webbplats över de insatser som har valts ut för att få stöd från fonderna. I artikel 69.12 finns skyldigheter för medlemsstaterna att rapportera vissa oriktigheter i systemet för hantering av oriktigheter, IMS (Irregularity Management System). Artikel 74.1 c föreskriver att förvaltande myndigheter ska ha effektiva och proportionerliga förfaranden för bedrägeribekämpning.

Regelverket gäller stödgivning som sker eller har skett med stöd av förordningen under programperioden 2021–2027.

CAP-förordningen

Inom ramen för den gemensamma jordbrukspolitiken (GJP) finns den så kallade CAP-förordningen (Common Agricultural Policy)[3]. Den tar sikte på bland annat utbetalande organ och ekonomisk förvaltning när det gäller jordbruksfonderna Europeiska garantifonden

[2] Europaparlamentets och rådets förordning (EU) 2021/1060 av den 24 juni 2021 om fastställande av gemensamma bestämmelser för Europeiska regionala utvecklingsfonden, Europeiska socialfonden+, Sammanhållningsfonden, Fonden för en rättvis omställning och Europeiska havs-, fiskeri- och vattenbruksfonden samt finansiella regler för dessa och för Asyl-, migrations- och integrationsfonden, Fonden för inre säkerhet samt instrumentet för ekonomiskt stöd för gränsförvaltning och viseringspolitik.

[3] Europaparlamentets och rådets förordning (EU) 2021/2116 av den 2 december 2021 om finansiering, förvaltning och övervakning av den gemensamma jordbrukspolitiken och om upphävande av förordning (EU) nr 1306/2013.

för jordbruket (EGFJ) och Europeiska jordbruksfonden för landsbygdsutveckling (Ejflu) och innehåller regler om krav på förvaltnings- och kontrollsystem och skyldigheter att samla in och publicera uppgifter. Som exempel kan nämnas att medlemsstaterna ska inrätta effektiva förvaltnings- och kontrollsystem för att säkerställa att unionslagstiftningen om unionens interventioner efterlevs (artikel 59.2) och säkerställa att det offentliggörs information om mottagare av stöd (artikel 98.1).

Förordningen omfattar programperioden 2021–2027.

RRF-förordningen

Den så kallade RRF-förordningen[4] (The Recovery and Resilience Facility, Faciliteten för återhämtning och resiliens) kanaliserar medel från EU:s krisåterhämtningspaket *Next Generation EU*. Faciliteten genomförs av kommissionen genom direkt förvaltning, men samtidigt tillsammans med medlemsstaterna. Förordningen innehåller likt ovan nämnda förordningar bland annat bestämmelser om skyddsmekanismer för EU-medel och om uppgiftslämnande och offentliggörande. Förordningen har i praktiken begränsad tillämplighet i tid genom att reformer och investeringar ska ha genomförts till den 31 augusti 2026 och utbetalningar till den 31 december samma år. För att medlemsstaterna ska få medel från RRF ska de uppnå mål och delmål som är fastställda och beskrivna i en nationell återhämtningsplan. Den svenska regeringen har beslutat om en sådan återhämtningsplan. Alla åtgärder i Sveriges återhämtningsplan, och vilka mål och delmål som ska nås för varje åtgärd, finns beskrivna i bilagan till Rådets genomförandebeslut om godkännande av bedömningen av Sveriges återhämtnings- och resiliensplan (COM [2024] 557 final). Det har också slutits ett finansieringsavtal mellan Sverige och kommissionen som beskriver hur medlen ska disponeras.

Inom ramen för budgetförordningens systematik faller förvaltningen av RRF under direkt förvaltning. Det är dock fråga om en särskild form av direkt förvaltning, som i detta betänkande kallas för *direkt förvaltning tillsammans med medlemsstaterna*.

[4] Europaparlamentets och rådets förordning (EU) 2021/241 av den 12 februari 2021 om inrättande av faciliteten för återhämtning och resiliens.

Övergripande om de sektorsspecifika regelverken

Samtliga ovan nämnda förordningar hänvisar till ett datautvinningsverktyg, med vilket avses Arachne. Samtliga innehåller också hänvisningar till reglering om skydd för uppgifter och för den personliga integriteten.

Det bör beaktas att ovan nämnda förordningar avser vad som gäller i nuläget och att det inte står klart vad som kommer att gälla under nästa programperiod, alltså från och med 2028. Ändringar avseende såväl fonder som EU-förordningar kan förväntas. Det är dock sannolikt att de grundläggande kraven på myndigheter att motverka felaktigheter och möjligheten att använda Arachne kommer att gälla även i den kommande regleringen. Utredningen bedömer det som sannolikt att sådana funktioner snarare kan komma att stärkas i kommande reglering.

Nedan i tabell 3.1 redogörs samlat för de EU-fonder och instrument som främst är relevanta för denna utredning och vilka sektorsspecifika regler som i dag reglerar de olika fonderna och instrumenten.

Tabell 3.1 Relevanta EU-fonder och instrument med tillhörande sektorsspecifika regelverk

EU-fond	Sektorsspecifikt regelverk
Europeiska garantifonden för jordbruket (EGFJ)	CAP (2021/2116)
Europeiska jordbruksfonden för landsbygdsutveckling (Ejflu)	CAP
Europeiska regionala utvecklingsfonden (Eruf)	CPR (2021/1060)
Europeiska socialfonden+ (ESF+)	CPR
Fonden för en rättvis omställning (FRO)	CPR
Europeiska havs-, fiskeri- och vattenbruksfonden (EHFVF)	CPR
Asyl-, migrations- och integrationsfonden (Amif)	CPR
Fonden för inre säkerhet (ISF)	CPR
Instrumentet för ekonomiskt stöd för gränsförvaltning och viseringspolitik (BMVI)	CPR
Faciliteten för återhämtning och resiliens	RRF (2021/241)

Källa: Egen sammanställning.

3.3.2 Nationell lagstiftning

Ett antal svenska författningar reglerar de närmare förutsättningarna för hanteringen av EU-medel. Några exempel nämns i det följande.

Lagen (1994:1708) om EU:s förordningar om strukturstöd och om stöd till utveckling av landsbygden kompletterar sådana EU-förordningar som innehåller bestämmelser om stöd från Eruf, ESF+, FRO och Ejflu (1 § första stycket). Tillsyn och annan kontroll över att de EU-förordningar som lagen kompletterar följs utövas av den eller de myndigheter som regeringen bestämmer (2 § första stycket).

Förordningen (2022:1379) om förvaltning av program för vissa EU-fonder innehåller bestämmelser för programperioden 2021–2027 om förvaltningen av vissa program (se 1 kap. 1 §). Den innehåller kompletterande bestämmelser till flera EU-förordningar, däribland till den tidigare budgetförordningen och CPR (1 kap. 2 §). Den svenska förordningen pekar ut vilka myndigheter som är förvaltande myndigheter respektive revisionsmyndighet samt anger uppgifter som myndigheterna ska ha, med hänvisning till specifika artiklar i EU-förordningarna.

I förordningen (2022:1826) om EU:s gemensamma jordbrukspolitik pekas Statens jordbruksverk (Jordbruksverket) ut som bland annat utbetalande organ enligt CAP-förordningen (1 kap. 11 §).

Förordningen (2022:1461) om stöd från Europeiska havs-, fiskeri- och vattenbruksfonden samt förordningen (2021:846) om förvaltning av fonden för inre säkerhet och instrumentet för ekonomiskt stöd för gränsförvaltning och viseringspolitik är ytterligare exempel på svensk reglering som kompletterar EU-lagstiftningen.

Myndigheternas instruktioner innehåller också bestämmelser av betydelse för hanteringen av EU-medel i Sverige. Som exempel kan nämnas 6 § förordningen (2009:145) med instruktion för Tillväxtverket enligt vilken Tillväxtverket har det övergripande ansvaret för samordning, förvaltning och utveckling av genomförandet av Eruf och FRO i Sverige. Tillväxtverket har också det ansvar och utför de uppgifter som framgår av förordningen om förvaltning av program för vissa EU-fonder.

Det bör noteras att ovan nämnda författningar förväntas ändras eller ersättas av nya, när den nya programperiodens fonder och mål har fastställts.

3.4 Budgetförordningens reglering av intern kontroll samt övergripande om Arachne och Edes

3.4.1 Intern kontroll av budgetgenomförandet

Budgetförordningen innehåller bestämmelser om intern kontroll av budgetgenomförandet och dessa finns i artikel 36. Artikeln innehåller 11 punkter och föreskriver bland annat följande. Enligt principen om sund ekonomisk förvaltning ska budgeten genomföras med hjälp av en ändamålsenlig och effektiv intern kontroll som är avpassad för respektive metod för genomförande och i enlighet med relevanta sektorsspecifika regler (artikel 36.1). Intern kontroll ska tillämpas på alla förvaltningsnivåer och vara utformad för att ge rimliga garantier för att ett antal uppräknade mål ska uppnås (artikel 36.2). Målen i artikel 36.2 rör i korthet att verksamheter ska präglas av ändamålsenlighet, effektivitet och sparsamhet, att rapporteringen ska vara tillförlitlig, att tillgångar och information ska skyddas, att oriktigheter ska motarbetas (särskilt om detta mål, se avsnitt 3.4.2) och att det ska finnas fullgod riskhantering med avseende på underliggande transaktioners laglighet och korrekthet.

Vidare anges närmare vad en ändamålsenlig intern kontroll i synnerhet ska omfatta (artikel 36.3), vad en effektiv intern kontroll ska grundas på (artikel 36.4), vilken information som unionsinstitutioner och unionsorgan och personer eller enheter som genomför budgeten ska göra tillgänglig för kommissionen vid motverkade av oriktigheter (artikel 36.6 – som behandlas särskilt i flera avsnitt nedan) och närmare om det system som kan användas vid motverkandet av felaktigheter (artikel 36.7). Det anges också att vissa uppgifter om fakta ska översändas till kommissionen (artikel 36.8 – som behandlas särskilt i avsnitt 4.6).

3.4.2 Oriktigheter ska motverkas

Ett av de uppräknade målen i artikel 36.2 i budgetförordningen är att oriktigheter såsom bedrägerier, korruption, intressekonflikter och dubbelfinansiering förebyggs, upptäcks, korrigeras och följs upp (härefter förenklat: att oriktigheter ska motverkas). Detta kan enligt bestämmelsen ske genom den frivilliga användningen av ett gemensamt integrerat och interoperabelt informations- och övervaknings-

system som tillhandahålls av kommissionen. Systemet inbegriper ett gemensamt datautvinnings- och riskgraderingsverktyg. Det möjliggör tillgång till och elektronisk automatisk hämtning, registrering, lagring och analys av data om mottagarna av unionsfinansiering, inbegripet deras verkliga huvudmän, i enlighet med sektorsspecifika regler (artikel 36.2 d).

Systemet och verktyget som avses med denna skrivning är Arachne. Liknande skrivningar finns också i sektorsspecifik reglering såsom i CAP-förordningen och i RRF-förordningen. Vad gäller begreppet verkliga huvudmän hänvisas det till definitionen i artikel 3.6 i EU:s penningtvättsdirektiv från 2015.[5]

En hänvisning till artikel 36.2 d i budgetförordningen kan avse såväl målet att motverka oriktigheter som användandet av Arachne. Det kan noteras att målet att motverka oriktigheter inte är frivilligt, medan användandet av Arachne är frivilligt enligt budgetförordningen.

Budgetförordningen ska tillämpas från och med den 30 september 2024 (artikel 280) men enligt artikel 277.5 ska den skyldighet som anges i artikel 36.2 d (och 36.6) när det gäller tillgång till uppgifter om mottagarna av medel och deras verkliga huvudmän endast tillämpas på program som antas inom och finansieras genom fleråriga budgetramar efter 2027. Kraven i bestämmelserna gäller således inte för de program som löper nu, utan först från och med 2028.

3.4.3 Översiktligt om Arachne

Ett datautvinnings- och riskvärderingsverktyg

Arachne är ett datautvinnings- och riskvärderingsverktyg som kommissionen har tagit fram för att hjälpa medlemsstaternas myndigheter att kontrollera hur EU-stöd som hanteras inom ramen för delad förvaltning används och förvaltas. Det introducerades inför programperioden 2014–2020. Systemet syftar till att bland annat förvaltande myndigheter ska kunna identifiera projekt och kontrakt med hög risk samt identifiera potentiella risker med kopplingar till andra pro-

[5] 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.

jekt. Verktyget är i dag frivilligt att använda och tillhandahålls avgiftsfritt från kommissionen.

Arachne, som det fungerar i dag, kopplar ihop data om projekt och kontrakt från deltagande medlemsstaters nationella projektdatabaser med två kommersiella databaser, en som samlar in offentligt tillgängliga uppgifter om cirka 400 miljoner aktiva och vilande bolag samt 200 miljoner huvudmän från hela världen och en som bland annat innehåller sanktionslistor och listor över politiskt utsatta personer. Uppgifter från databaserna uppdateras varje kvartal. Med hjälp av dessa uppgifter skapas en automatgenererad riskvärdering utifrån ett hundratal riskparametrar. Parametrarna är indelade i sju kategorier, nämligen upphandling, avtalsförvaltning, stödberättigande, resultat, koncentration, rimlighet samt anseende och bedrägeri. Riskindikatorerna hjälper myndigheter att identifiera de mest riskfyllda projekten, stödmottagarna, leverantörerna och avtalen. Riskerna poängsätts med ett värde från 1 till 50.

Genom verktyget kan myndigheter få en uppfattning om eventuella intressekonflikter och risker för dubbelfinansiering från olika fonder och program. I början av 2022 infördes en funktion i verktyget som gör det möjligt att göra riskvärderingar av företag och projekt som ännu inte har fått medel beviljade. Denna funktion kallas i detta betänkande *förhandsfunktionen*. Det innebär att verktyget också kan användas som ett stöd vid handläggning av projektansökningar.

Arachne tillhandahåller information och varnar för risker men tillhandahåller inte bevis för olika felaktigheter. De riskvärderingar som Arachne producerar är inte tänkta att direkt leda till beslut. Systemet ger i stället myndigheterna en möjlighet att med utgångspunkt i riskindikationerna från systemet göra en egen värdering av vilka projekt som ska analyseras vidare (se mer i avsnitt 5.2.2).

De riskvärderingar som görs i Arachne kan avse enskilda projekt, kontrakt eller stödmottagare med mera. Arachne kan endast göra en riskvärdering om alla nödvändiga data har tillförts Arachne och alla nödvändiga externa data finns i de externa databaserna.

När det gäller medlemsstaternas och nationella myndigheters förhållande till Arachne kan det finnas skäl att skilja mellan å ena sidan att använda systemet i meningen att bereda sig tillgång till det och utnyttja den information som finns eller kan tas fram därifrån exempelvis vid riskvärderingar och å andra sidan lämnande av uppgifter till systemet. Det finns också olika behörighetsroller i Arachne,

där en särskild behörighet är att ha rätt att föra in uppgifter i systemet. Behörigheter tilldelas av en lokal administratör.

Principer för tillämpningen av Arachne

Utöver artikel 36.2 d i budgetförordningen finns reglering som tar sikte på Arachne i bland annat artikel 36.6 och 36.7. Skäl 29–32 behandlar också Arachne. Artikel 36.7 är central i fråga om de principer som gäller för Arachne. Där anges vad systemet syftar till, vad det får användas för, att åtkomsten ska vara förenlig med bland annat dataskyddsprinciper och att åtkomsten ska begränsas till vissa aktörer. Vidare behandlas personuppgiftsansvar och lagringsperioder.

För Arachne finns också en stadga (Arachne, Charter for the introduction, the application and the integration of the Arachne risk scoring tool) här benämnd Arachne-stadgan. I detta betänkande används version 2.4, som är den i skrivande stund senaste tillgängliga versionen av stadgan.[6]

Stadgan innehåller ett antal principer men också information. De gemensamma principerna i stadgan ska enligt punkt 1 tillämpas av de programmyndigheter och avdelningar vid kommissionen som ansvarar för genomförandet av bland annat CAP och RRF. Det anges också vilka som innefattas i begreppet programmyndigheter. Genom att använda Arachne accepterar programmyndigheterna att följa principerna i stadgan. När det gäller dataskydd anges bland annat att programmyndigheterna måste följa nationell och EU-rättslig dataskyddslagstiftning.

Arachne är under utveckling och det kan komma att bli obligatoriskt att använda det

När Arachne introducerades inför programperioden 2014–2020 omfattade det enbart fonderna under sammanhållningspolitiken. Numera omfattas fler fonder och användningen har vuxit i takt med att fler länder och användare har anslutit sig. I januari 2025 använde samtliga medlemsstater Arachne för minst en EU-fond, utom Sverige, Danmark, Finland och Tyskland.

[6] https://employment-social-affairs.ec.europa.eu/policies-and-activities/funding/european-social-fund-plus-esf/what-arachne_en. Hämtat 2025-10-22.

Systemet har utvecklats under åren och nya funktioner har tillkommit, bland annat för att kunna användas inom ramen för RRF. Det pågår arbete med att utveckla och modernisera Arachne ytterligare, och kommissionen har tillsatt en expertgrupp med bland annat deltagare från medlemsstaterna i detta syfte. Expertgruppens arbete kommer att pågå under 2025 och 2026. I planerna för verktyget ingår att uppgifter framöver ska kunna överföras automatiserat. En ny version av verktyget tas fram och avses anpassas till den omarbetade budgetförordningen.

Systemet har hittills varit frivilligt att använda och även enligt budgetförordningen är verktyget frivilligt att använda (artikel 36.2 d). Kommissionen ska före utgången av 2027 lägga fram en bedömning av hur Arachne fungerar med avseende på flera kriterier (artikel 36.6 tredje stycket). Europaparlamentet, rådet och kommissionen har gemensamt uttalat att de ska undersöka och på nytt diskutera den obligatoriska användningen av Arachne under den fleråriga budgetramen efter 2027 (se Gemensamt uttalande från Europaparlamentet, rådet och kommissionen om det gemensamma verktyg för datautvinning och riskgradering som föreskrivs i artikel 36 i budgetförordningen i samband med antagandet av förordning 2024/2509 [C/2024/5767]). Det kan alltså inte uteslutas att det blir obligatoriskt för medlemsländerna att använda Arachne i sin handläggning och kontroll av EU-medel i framtiden.

3.4.4 Översiktligt om Edes

Systemet för tidig upptäckt och uteslutning (Edes) är ett system som kommissionen inrättade 2016. Det övergripande syftet är att skydda unionens ekonomiska intressen. Systemet har hittills enbart omfattat EU-medel under direkt och indirekt förvaltning. Budgetförordningen innehåller ett antal förändringar i förhållande till tidigare regelverk. Det kommer att bli obligatoriskt att använda Edes vid hantering av samtliga EU-stöd, förutom avseende RRF, när det gäller program som antas eller finansieras från och med den 1 januari 2028 (se artikel 144.5 och 277 i budgetförordningen). Det är redan i dag i princip möjligt för svenska myndigheter som deltar i budgetgenomförandet att använda Edes.

Edes syftar till att göra det lättare att tidigt upptäcka personer eller enheter som är ett hot mot unionens ekonomiska intressen, att utesluta personer eller enheter från att ta del av EU-medel och att ålägga ekonomiska sanktioner mot mottagare av EU-medel som befinner sig i en uteslutningssituation (artikel 137.1 i budgetförordningen). I allvarliga fall kan information om uteslutningar och sanktioner offentliggöras på en webbplats som hanteras av kommissionen.

Grunderna för uteslutning är listade i budgetförordningen och avser bland annat konkurs- och insolvenssituationer, underlåtenhet att betala skatter eller socialförsäkringsavgifter, allvarliga fel i yrkesutövningen samt slutgiltiga brottmålsdomar rörande vissa brottstyper, såsom viss ekonomisk brottslighet, terroristbrott och människohandel (artikel 138 i budgetförordningen).

Så kallade behöriga utanordnare har flera roller inom ramen för Edes. Det är exempelvis en behörig utanordnare som beslutar om att någon ska uteslutas från att delta i förfaranden för tilldelning eller från att genomföra unionsmedel[7] när det föreligger en uteslutningssituation.

Det finns en panel som bland annat har till uppgift att göra preliminära bedömningar som kan ligga till grund för beslut om uteslutning i situationer där det saknas ett slutgiltigt avgörande.

I Edes-databasen samlas bland annat information om uteslutningar. Personer och enheter som genomför budgeten inom ramen för delad förvaltning ska konsultera Edes-databasen innan de tilldelar unionsmedel eller väljer ut bidragsmottagare. De ska också verkställa de uteslutningar som har registrerats i databasen, vilket innebär att de ska avslå ansökningar om EU-medel.

Edes kommer att utvecklas för att anpassas till det nya tillämpningsområdet.[8]

[7] I den svenska versionen av budgetförordningen har uttrycket ”the implementation of Union funds” översatts med ”förvaltningen av unionsmedel” (i olika grammatiska former). På tyska används uttrycket ”Ausführung von Unionsmitteln”. Enligt utredningen framstår det som mer korrekt att på svenska beskriva detta som ”genomförandet av unionsmedel”. Se exempelvis artiklarna 62.1 första stycket c ix och 152.8 samt skäl 51. Utredningen använder därför begreppet ”genomförande” av unionsmedel när det i den engelska versionen handlar om ”implementation” av sådana medel.

[8] Komm2025/00388-8.

3.4.5 Det kan finnas fördelar med ett användande av Arachne och Edes

Utredningen om hantering av EU-medel har i betänkandet En ny organisation för förvaltning av EU-medel (SOU 2024:22) uttalat sig positivt till ett användande av Arachne och Edes. Utredningen anförde att en anslutning till Arachne kan öka svenska myndigheters förmåga att på ett ändamålsenligt, effektivt och rättssäkert sätt upptäcka dubbelfinansiering, intressekonflikter och oegentligheter. Att regeringen utser en nationell administratör och att förvaltande myndigheter ansluter sig till Edes bedömdes vara ett grundläggande och ändamålsenligt krav för att säkerställa att fondmedel inte utbetalas till uppenbart olämpliga aktörer. Utredningen framförde också att en anslutning till Arachne och Edes medför en rad juridiska frågeställningar, som bör analyseras vidare innan en anslutning kan ske (SOU 2024:22, s. 23 och 448–457).

I betänkandet gjordes en omfattande genomgång av organisationen för förvaltning av EU-medel och den genomgången används i stor utsträckning som grund för den kartläggning och de bedömningar som görs i detta betänkande.

3.5 Organisationen för förvaltning av EU-medel i Sverige

3.5.1 Inledning

I detta avsnitt redogör utredningen översiktligt för organisationen för förvaltning av EU-medel i Sverige och vilka roller som olika myndigheter har i den organisationen. Det kan här nämnas att förändringar kan förväntas för den programperiod som börjar 2028 och att en ny organisation har föreslagits i betänkandet SOU 2024:22. Det kan också komma nya fonder och instrument som behöver hanteras. Som exempel kan nämnas EU:s sociala klimatfond, som ska inrättas 2026 som en del av det så kallade 55 %-paketet (Fit for 55).[9] Utredningen gör inte några överväganden när det gäller vilka fonder och organisationsförändringar som kan vara aktuella framöver, men

[9] https://regeringen.se/regeringens-politik/miljo-och-klimat/genomforandet-av-eus-sociala-klimatfond/. Hämtat 2025-10-16.

beaktar dessa förhållanden i möjligaste mån, i syfte att bedömningar och eventuella förslag ska kunna vara relevanta även i framtiden.

3.5.2 EU-fonder med delad förvaltning samt RRF

EU-medel med delad förvaltning förmedlas till stödmottagare i medlemsstaterna genom nationella program för olika EU-fonder eller samarbetsprogram som rör flera medlemsstater. Programmen löper över perioder som normalt varar i sju år. De flesta av de aktuella fondprogrammen gäller åren 2021–2027. Det nuvarande programmet med finansiering från de två jordbruksfonderna, den så kallade strategiska planen för den gemensamma jordbrukspolitiken (GJP,) gäller dock för åren 2023–2027.

Särskilt följande EU-fonder med delad förvaltning är aktuella i Sverige under den nuvarande programperioden.

- Europeiska garantifonden för jordbruket (EGFJ)
- Europeiska jordbruksfonden för landsbygdsutveckling (Ejflu)
- Europeiska regionala utvecklingsfonden (Eruf)
- Europeiska socialfonden+ (ESF+)
- Fonden för inre säkerhet (ISF)
- Europeiska havs-, fiskeri- och vattenbruksfonden (EHFVF)
- Asyl-, migrations- och integrationsfonden (Amif)
- Fonden för en rättvis omställning (FRO)
- Instrumentet för ekonomiskt stöd för gränsförvaltning och viseringspolitik (BMVI).

Utöver de ovan nämnda fonderna finns det ytterligare fonder med delad förvaltning, nämligen till att börja med den tillfälliga så kallade Brexitjusteringsreserven (BAR) som inrättades för att kompensera företag och myndigheter i vissa sektorer för negativa effekter av Storbritanniens utträde ur EU. Den är numera avslutad men kontroller kan utföras under ytterligare cirka fyra år. Även Europeiska fonden för justering för globaliseringseffekter för uppsagda arbetstagare (EGF) kan nämnas. EGF ska stödja sådana socioekonomiska om-

vandlingar som uppstår till följd av globaliseringen och tekniska och miljömässiga förändringar genom att hjälpa uppsagda arbetstagare och egenföretagare vars verksamhet har upphört att anpassa sig till strukturförändringar. EGF skiljer sig från EU:s struktur- och investeringsfonder bland annat på så sätt att de sistnämnda arbetar strategiskt och långsiktigt för att föregripa och hantera de sociala konsekvenserna av näringslivsförändringar, till exempel genom livslångt lärande. EGF ger däremot ett tidsbegränsat individuellt engångsstöd. EGF ska utgöra en krisfond som fungerar reaktivt. EGF upphör att gälla efter 2027 (se Commission staff working document, A dynamic EU budget for the priorities of the future: the Multiannual Financial Framework 2028-2034, SWD [2025] 570 final/2, s. 34).

Ett antal svenska myndigheter är vidare involverade i hanteringen av EU:s facilitet för återhämtning och resiliens (RRF) som kanaliserar medel från EU:s krisåterhämtningspaket *Next Generation EU*. RRF förvaltas direkt av kommissionen, men åtgärderna som Sverige söker finansiellt stöd för beslutas inom ramen för den ordinarie svenska budgetprocessen. Det är således fråga om direkt förvaltning tillsammans med medlemsstaterna (se avsnitt 3.3.1).

3.5.3 Myndigheter som hanterar EU-medel genom delad förvaltning

Ansvaret för hantering av medel från EU-fonder med delad förvaltning är fördelat på ett antal svenska myndigheter. I detta betänkande behandlas särskilt åtta myndigheter som har roller som förvaltande myndigheter eller utbetalande organ under programperioden 2021–2027. Rollen som benämns utbetalande organ tar sikte på Jordbruksverket när det gäller CAP-förordningen, se 1 kap. 11 § förordningen om EU:s gemensamma jordbrukspolitik.

De myndigheter som hanterar EU-medel inom ramen för delad förvaltning och som behandlas särskilt här är Jordbruksverket, Tillväxtverket, Rådet för Europeiska socialfonden i Sverige (Svenska ESF-rådet), Migrationsverket och Polismyndigheten samt länsstyrelserna i Jämtlands, Västerbottens och Norrbottens län (se till exempel förordningen om förvaltning av program för vissa EU-fonder).

Tabell 3.2 Ansvariga myndigheter för vissa fondprogram med delad förvaltning

Fondprogram och myndigheter avser programperioden 2021–2027 och GJP 2023–2027

Finansiering från	Förvaltande myndighet	Utbetalande organ	Delegerade organ	Förmedlande organ
EGFJ	Jordbruksverket	Jordbruksverket	Länsstyrelserna	
Ejflu	Jordbruksverket	Jordbruksverket	Länsstyrelserna Sametinget Skogsstyrelsen	
EHFVF	Jordbruksverket			Fem länsstyrelser Havs- och vattenmyndigheten
Eruf	Tillväxtverket Länsstyrelserna i Jämtlands, Västerbottens och Norrbottens län			
FRO	Tillväxtverket			
ESF+	Svenska ESF-rådet			
Amif	Migrationsverket			
BMVI	Polismyndigheten			
ISF	Polismyndigheten			

Källa: SOU 2024:22, s. 115 och egen sammanställning.

3.5.4 Myndigheter som hanterar medel genom direkt förvaltning tillsammans med medlemsstaterna – RRF

På EU-nivå regleras som nämns ovan EU:s facilitet för återhämtning och resiliens (RRF) genom RRF-förordningen. RRF är ett resultatbaserat instrument där utbetalning av medel sker i efterhand när åtgärderna har genomförts. Medlemsstater ansöker om medel genom att lämna in betalningsansökningar. Vissa svenska myndigheter lämnar uppgifter till Ekonomistyrningsverket (ESV) inom ramen för rapportering i enlighet med artikel 22.2 d i RRF-förordningen.

Ett antal svenska myndigheter hanterar och handlägger ärenden avseende medel från RRF. ESV och Ekobrottsmyndigheten har fått i uppdrag att stödja övriga myndigheter vid deras genomförande av Sveriges återhämtningsplan.

Det finns totalt 62 så kallade genomförandemyndigheter. Tio myndigheter har fått ett särskilt ansvar för genomförandet och rap-

porterar in resultatinformation till ESV. Vilka dessa myndigheter är och vilka åtgärder inom ramen för RRF respektive myndighet ansvarar för framgår av tabell 3.3 nedan. Utöver dessa tio myndigheter är även samtliga länsstyrelser och 31 lärosäten genomförandemyndigheter.

Tabell 3.3 De tio särskilt ansvariga myndigheterna och åtgärder inom ramen för RRF

Myndighet	Åtgärder som myndigheten ansvarar för
Boverket	Stöd till energieffektivisering av flerbostadshus Investeringsstöd för hyresbostäder och bostäder för studerande
Myndigheten för digital förvaltning	Förvaltningsgemensam digital infrastruktur
Myndigheten för yrkeshögskolan	Fler platser inom yrkeshögskolan
Naturvårdsverket	Klimatklivet Skydd av värdefull natur
Post- och telestyrelsen	Bredbandsutbyggnad
Skolverket	Fler platser i regional yrkesinriktad vuxenutbildning (yrkesvux)
Socialstyrelsen	Äldreomsorgslyftet
Statens energimyndighet	Industriklivet
Trafikverket	Järnvägssatsningar
Universitetskanslersämbetet	Resurser för att möta efterfrågan på utbildning vid universitet och högskolor

Källa: ESV[10].

3.5.5 Ekonomistyrningsverket är revisionsmyndighet

ESV har enligt sin instruktion bland annat i uppgift att utveckla och förvalta den ekonomiska styrningen av den statliga verksamheten samt utföra revision av Sveriges hantering av EU-medel och främja en effektiv och korrekt hantering av dessa medel (1 § förordningen [2016:1023] med instruktion för Ekonomistyrningsverket). Det kan noteras att ESV och Statskontoret ska slås samman under det gemensamma namnet Statskontoret. Organisationsförändringen ska träda i kraft den 1 januari 2026. Uppgiften att utföra revision av Sveriges hantering av EU-medel och främja en effektiv och korrekt hantering av dessa kommer då att framgå av 1 § förordningen (2025:681) med instruktion för Statskontoret. Eftersom organisationsföränd-

[10] https://www.esv.se/statistik-och-data/statistik/mottagare-av-rrf-medel/ansvariga-myndigheter-och-atgarder/. Hämtat 2025-10-28.

ringen ännu inte har ägt rum använder utredningen i detta betänkande namnet ESV på myndigheten.

Regeringen har utsett ESV till centraliserad nationell revisionsmyndighet i Sverige med ansvaret att granska de EU-medel som Sverige tar emot inom den delade förvaltningen. Det betyder att ESV på regeringens uppdrag ansvarar för att granska att ansvariga myndigheter hanterar medlen i enlighet med EU:s och nationella regelverk, samt att pengarna som de ansvariga myndigheterna betalar ut används till rätt saker och på ett effektivt sätt. Det gör myndigheten genom att granska både hur myndigheterna förvaltar fonderna och att utbetalningar för enskilda projekt och insatser är korrekta.

ESV har även utsetts till revisionsmyndighet och har fått i uppdrag att granska genomförandet av den svenska återhämtningsplanen inom ramen för RRF. Revisionsuppdraget omfattar hela förvaltnings- och kontrollsystemet för genomförandet av RRF i Sverige.

3.5.6 Ekobrottsmyndigheten har en samordnande roll

Ekobrottsmyndigheten är en åklagarmyndighet som ansvarar för bekämpning av ekonomisk brottslighet. Myndigheten ska bland annat se till att personer som begår ekonomiska brott blir föremål för brottsutredning och lagföring, arbeta för att begränsa vinsterna av brott och brottslig verksamhet och delta i det myndighetsgemensamma arbetet mot den grova och organiserade brottsligheten samt mot arbetslivskriminalitet. Myndigheten ska följa och analysera utvecklingen och rättstillämpningen när det gäller ekonomisk brottslighet och utarbeta förslag till åtgärder och samordna åtgärder mot ekonomisk brottslighet, se 1, 2 och 5 §§ förordningen (2015:744) med instruktion för Ekobrottsmyndigheten.

Ekobrottsmyndigheten ansvarar för samordningen av de nationella åtgärderna mot bedrägerier, missbruk och annan oegentlig och ineffektiv hantering och användning av EU-relaterade medel i Sverige (6 § förordningen med instruktion för Ekobrottsmyndigheten).

Ekobrottsmyndigheten ska även vara sambandscentral för bedrägeribekämpning i frågor som rör Europeiska byrån för bedrägeribekämpning (Olaf). Rollen som sambandscentral innebär att myndigheten ska ta emot anmälningar från Olaf om utredningar i Sverige och därefter hänvisa till behörig myndighet (13 § förordningen med

instruktion för Ekobrottsmyndigheten). Ekobrottsmyndigheten är vidare behörig myndighet vid Olaf:s kontroller och inspektioner i Sverige om inte någon annan myndighet har utsetts (13 a § förordningen med instruktion för Ekobrottsmyndigheten). Myndigheten bistår Olaf i de utredningar som byrån genomför i Sverige.

Rådet för skydd av EU:s finansiella intressen (SEFI-rådet) ansvarar för att samordna åtgärder i Sverige mot bedrägerier och andra missbruk av EU-relaterade medel. Bland annat ska rådet främja en effektiv och korrekt hantering av EU-medel i Sverige och göra det enklare för berörda myndigheter att samarbeta kring att förebygga, upptäcka, utreda och vidta åtgärder när det finns misstanke om att EU-relaterade medel används på fel sätt. Ekobrottsmyndigheten ansvarar för rådets kanslifunktioner och är ständig ordförande i rådet, se förordningen (2015:745) om rådet för skydd av Europeiska unionens finansiella intressen.

3.5.7 Departement har roller som behörig och samordnande myndighet

Regeringskansliet har uppgifter relaterade till hanteringen av EU-medel. När det gäller särskilt utpekade roller kan nämnas att Landsbygds- och infrastrukturdepartementet har rollen som behörig myndighet för jordbruksfonderna och ansvarar bland annat för att ackreditera utbetalande organ och utse attesterande organ. Departementet är direkt utpekat i 1 kap. 9 § förordningen om EU:s gemensamma jordbrukspolitik som behörig myndighet enligt artikel 8 i CAP-förordningen. Finansdepartementet är samordnande myndighet för genomförandet av Sveriges återhämtningsplan som finansieras av RRF och har det övergripande ansvaret för att övervaka genomförandet av planen. Den samordnande myndigheten ansvarar bland annat för att rapportera uppnådda resultat till kommissionen samt bereda Sveriges betalningsansökningar, inklusive den samlade förvaltningsförklaringen. Den samordnande myndigheten ansvarar vidare för att ta fram svar till kommissionen på förfrågningar om information och tillgång till uppgifter om bland annat slutmottagare.

3.5.8 Organisationsstrukturen kan förändras och nya fonder kan tillkomma

Utredningen om hantering av EU-medel har föreslagit ett antal ändringar avseende vilka myndigheter som ska förvalta medel från olika fonder (SOU 2024:22). Utredningen har också lämnat förslag om att SEFI-rådets strategiska roll ska stärkas. Förslagen bereds i Regeringskansliet.

3.5.9 Exempel på hur begreppen fond, program och projekt används

Inom ramen för förvaltningen av EU-medel används flera olika begrepp, såsom fonder, faciliteter, program, planer och stöd. För att underlätta förståelsen för hur de olika begreppen förhåller sig till varandra lämnas här några exempel.

Europeiska havs-, fiskeri- och vattenbruksfonden (EHFVF) är en *fond* på EU-nivå som finansierar projekt och investeringar som leder till konkurrenskraftiga företag inom fiske och vattenbruk samt en hållbar förvaltning av haven. Varje land i EU tar fram ett eget *program* utifrån de ramar som ges av europeiska havs-, fiskeri- och vattenbruksförordningen[11], som beslutats av kommissionen. I programmet Havs-, fiskeri- och vattenbruksprogrammet 2021–2027 beskriver Sverige vad pengarna ska främja, vilka mål som ska uppnås och vilka stöd som ska finnas. Inom ramen för Havs-, fiskeri- och vattenbruksprogrammet 2021–2027 finns flera olika *stöd*, exempelvis Hållbart fiske och Hållbara vattenbruk. Närmare information finns på Jordbruksverkets hemsida.[12] Det förekommer variationer i hur begreppen används beträffande olika områden.

[11] Europaparlamentets och rådets förordning (EU) 2021/1139 av den 7 juli 2021 om Europeiska havs-, fiskeri- och vattenbruksfonden och om ändring av förordning (EU) 2017/1004.
[12] https://jordbruksverket.se/stod/eus-politik-for-jordbruk-och-fiske/havs--fiskeri--och-vattenbruksprogrammet. Hämtat 2025-06-25.

4 Lämnande och offentliggörande av uppgifter

4.1 Vissa utgångspunkter

4.1.1 Övergripande om lämnande och offentliggörande av uppgifter i dag och från och med 2028

För att oriktigheter med EU-medel ska kunna motverkas behöver det finnas information om de EU-medel som redan har beviljats av myndigheterna i medlemsländerna. Sådan information behöver därför lämnas av medlemsländerna och det sker också enligt olika regelverk i dag. För att Arachne ska fungera på ett bra sätt behöver också information om beviljade EU-medel finnas i det systemet. I dag fungerar det så att medlemsländerna som använder Arachne för in sådan information i systemet. Att de som väljer att använda Arachne på detta sätt ska lämna uppgifter framgår i dag av Arachne-stadgan (Arachne, Charter for the introduction, the application and the integration of the Arachne risk scoring tool, punkt 11). En användare av Arachne som önskar använda den så kallade förhandsfunktionen i Arachne behöver i dag särskilt lämna vissa uppgifter genom systemet och detta kommer – såvitt kan bedömas i nuläget – även att gälla efter 2028.

Budgetförordningen innebär en förändring av regleringen när det gäller lämnande av uppgifter om beviljade EU-medel. Från och med 2028 blir det obligatoriskt för medlemsländerna att tillgängliggöra viss information, se artikel 36.6 och 277 i budgetförordningen. Tanken är att uppgifter som tillgängliggörs enligt denna artikel ska tillföras Arachne. Även i artikel 36.8 – som avser rapportering av oriktigheter via IMS – behandlas uppgiftslämnande till kommissionen.

Det finns en skillnad mellan nödvändiga och valfria uppgifter, både vid den skyldighet att tillgängliggöra uppgifter som gäller från

och med 2028 och vid det uppgiftslämnande som i dag sker vid ett frivilligt användande av Arachne. När det gäller skyldigheten att tillgängliggöra uppgifter enligt artikel 36.6 använder utredningen ibland begreppen (rättsligt) obligatoriska respektive frivilliga uppgifter. När det gäller det uppgiftslämnande som i dag sker vid användande av Arachne använder utredningen ibland begreppen (funktionellt) nödvändiga respektive valfria uppgifter.

Både den omarbetade och den tidigare budgetförordningen innehåller i artikel 38 bestämmelser om offentliggörande av information. Den omarbetade budgetförordningen innehåller också – till skillnad från den tidigare – en bestämmelse om att medlemsstaterna under vissa förutsättningar ska säkerställa visst offentliggörande i efterhand (artikel 38.4 tredje stycket i budgetförordningen).

Sammanfattningsvis behandlas i detta betänkande följande fall av lämnande av uppgifter som det kan bli aktuellt för svenska myndigheter att utföra.

- Lämnande av uppgifter vid ett användande av Arachne:
  - Funktionellt nödvändiga uppgifter (vid ett användande före 2028)
  - Inte funktionellt nödvändiga uppgifter (vid ett användande före 2028)
  - Uppgifter inom ramen för förhandsfunktionen (före och efter 2028)
- Tillgängliggörande av uppgifter enligt artikel 36.6 (efter 2028):
  - Rättsligt obligatoriska uppgifter
  - Frivilliga uppgifter.

Saken kan också uttryckas så att utredningen behandlar ett enda fall av rättsligt obligatoriskt lämnande av uppgifter, nämligen tillgängliggörande av obligatoriska uppgifter enligt artikel 36.6. Beträffande övriga ovan nämnda fall av uppgiftslämnande finns det ingen rättslig skyldighet att lämna uppgifterna. Utredningen gör denna uppdelning när behovet av åtgärder utreds (se avsnitt 8.2 och 8.3).

När det gäller Edes innebär budgetförordningen inte något nytt krav på medlemsländerna att lämna uppgifter (se avsnitt 4.6).

4.1.2 Utredningens uppdrag

Utredningen har bland annat i uppdrag att kartlägga och beskriva vilka uppgifter som ska eller får registreras eller annars utbytas i Arachne och inom ramen för Edes, samt i vilken utsträckning som aktörer utanför den egna myndigheten skulle få tillgång till uppgifterna. När det gäller utbyte av uppgifter finns det skäl att nämna att Arachne inte främst beskrivs som ett verktyg för utbyte av uppgifter. Eftersom Arachne bland annat är ett datautvinningsverktyg kan det ändå bidra till att underlätta för myndigheter att få del av uppgifter som andra har.

Utredningen har också i uppdrag att bedöma om det finns behov av ändrade regler för att svenska myndigheter ska kunna uppfylla de krav som ställs i budgetförordningen, särskilt i fråga om rapportering av uppgifter för registrering i Arachne.

I detta kapitel behandlas lämnande av uppgifter vid en användning av Arachne (avsnitt 4.3), ett nytt krav på tillgängliggörande av uppgifter till kommissionen (avsnitt 4.4), tillgängliggörande av frivilliga uppgifter till kommissionen (avsnitt 4.5), frågan om Edes medför några nya krav på lämnande av uppgifter (avsnitt 4.6) samt ett nytt krav på offentliggörande av uppgifter som träffar medlemsstaterna (avsnitt 4.7). I avsnitt 4.8 behandlas frågan om externa aktörers tillgång till lämnade uppgifter.

Bedömningar av behov av författningsändringar eller andra åtgärder med anledning av dessa frågor finns i kapitel 8.

Inledningsvis berörs svenska myndigheters uppgiftslämnande till kommissionen i dag.

4.2 Myndigheter lämnar uppgifter till kommissionen i dag

Utredningens uppdrag är att utreda vilket uppgiftslämnande som följer av budgetförordningen samt vid en användning av Arachne och Edes. I det sammanhanget är det också av relevans att översiktligt beskriva visst uppgiftslämnande som redan sker.

Sektorsspecifika förordningar som CAP-förordningen, CPR och RRF-förordningen innehåller flera krav på tillgängliggörande eller annat uppgiftslämnande till kommissionen avseende EU-medel. Det gäller bland annat sådana uppgifter som är aktuella i denna utredning.

Uppgiftslämnande sker på olika sätt, bland annat med användning av befintliga EU-system såsom IMS och rapporteringssystemet SFC. Uppgifter tillgängliggörs också av svenska myndigheter genom offentliggörande på webbsidor, varifrån kommissionen hämtar in uppgifter.

Som exempel kan nämnas att Migrationsverket, Tillväxtverket och andra myndigheter som har att tillämpa CPR-regelverket rapporterar oriktigheter som de har upptäckt avseende utbetalningar i enlighet med artikel 69 och bilaga XII i CPR, vilket sker genom IMS. Det rör oriktigheter, återkrav eller åtalsanmälningar med belopp som överstiger 10 000 euro (EU-finansierad andel). Rapporteringen sker en gång per kvartal.

När det gäller rapportering av stöd publicerar Migrationsverket en förteckning av insatser i enlighet med artikel 49 i CPR, på sin webbsida och rapporterar in denna till kommissionen. Svenska ESF-rådet lägger upp övergripande information per projekt på en dedikerad hemsida (projektbanken), vilken tas in och sammanställs av kommissionen. För överföringar används kommissionens rapporteringssystem SFC. Även Tillväxtverket lägger upp information om projekt på sin hemsida. Överföring av uppgifter om beviljade belopp och uppnådda indikatorutfall på aggregerad nivå för hela program sker genom SFC.

Jordbruksverket lämnar uppgifter till kommissionen rörande oriktigheter via IMS bland annat med tillämpning av förordning (EU) 2024/205[1]. Verket lämnar också uppgifter till kommissionen om projekt, utbetalningar till stödmottagare och räkenskaper via SFC. När det gäller rapportering av stöd publicerar Jordbruksverket uppgifter på sin webbplats i enlighet med artikel 98 i CAP-förordningen, och rapporterar in dessa uppgifter till kommissionen.

ESV sänder revisionsrapporter till kommissionen men lämnar uppgifter om slutmottagare till kommissionen och andra EU-institutioner först efter begäran. Vad gäller RRF har ESV dock tagit fram en portal där uppgifter om de 100 största slutmottagarna av RRF-medel laddas upp enligt artikel 25 a i RRF-förordningen.

[1] Kommissionens delegerade förordning (EU) 2024/205 av den 18 december 2023 om komplettering av Europaparlamentets och rådets förordning (EU) 2021/2116 med särskilda bestämmelser om rapportering av oriktigheter avseende Europeiska garantifonden för jordbruket och Europeiska jordbruksfonden för landsbygdsutveckling och om upphävande av kommissionens delegerade förordning (EU) 2015/1971.

Ekobrottsmyndigheten har inte några skyldigheter att lämna uppgifter till kommissionen enligt ovan nämnda bestämmelser. Visst uppgiftslämnande sker till Olaf. Ekobrottsmyndigheten är behörig myndighet för att förse Olaf med information och transaktionsregister enligt artikel 7.3 a i förordning (EU, Euratom) nr 883/2013[2] (se 13 a § [2015:744] förordningen med instruktion för Ekobrottsmyndigheten).

Det följer också en skyldighet för bland andra medlemsländerna att informera Olaf om sådant som kan ha samband med eventuella fall av bedrägeri, korruption eller annan olaglig verksamhet som riktar sig mot unionens ekonomiska intressen (se artikel 8 i förordning [EU, Euratom] nr 883/2013). Det finns också bestämmelser om att medlemsstaterna ska inrapportera alla brottsliga handlingar till Europeiska åklagarmyndigheten (Eppo) i fråga om vilka Eppo skulle kunna utöva sin behörighet (se artikel 24 i förordning [EU] 2017/1939).[3]

Även budgetförordningen innehåller bestämmelser om rapportering av uppgifter till kommissionen, liksom den tidigare gällande budgetförordningen.

Svenska myndigheter har således stor vana av att lämna uppgifter avseende EU-stöd.

4.3 Lämnande av uppgifter vid användande av Arachne

4.3.1 Inledning

Arachne är redan i dag frivilligt för medlemsstaterna att använda. För att kunna använda systemet förutsätts det för närvarande att myndigheterna lämnar uppgifter till kommissionen om beviljade medel. Det handlar delvis om motsvarande uppgiftslämnande som från och med 2028 kommer att regleras genom skyldigheten att tillgängliggöra uppgifter enligt artikel 36.6 i budgetförordningen. För det fall svenska myndigheter avser att använda Arachne innan den skyldigheten träder i kraft kommer de alltså att behöva lämna upp-

[2] Europaparlamentets och rådets förordning (EU, Euratom) nr 883/2013 av den 11 september 2013 om utredningar som utförs av Europeiska byrån för bedrägeribekämpning (Olaf) och om upphävande av Europaparlamentets och rådets förordning (EG) nr 1073/1999 och rådets förordning (Euratom) nr 1074/1999.

[3] Rådets förordning (EU) 2017/1939 av den 12 oktober 2017 om genomförande av fördjupat samarbete om inrättande av Europeiska åklagarmyndigheten.

gifter genom att ladda upp dem i Arachne. Det kan i denna del vara fråga om följande tre situationer av uppgiftslämnande.

- Funktionellt nödvändiga uppgifter om beviljade medel
- Inte funktionellt nödvändiga uppgifter om beviljade medel
- Uppgifter till grund för en förhandskontroll inför eventuellt beviljande av projekt.

Vilka myndigheter som kan komma att använda Arachne som verktyg och därmed få tillgång till uppgifter som finns där behandlas i avsnitt 5.3.

4.3.2 Uppgifter om beviljade medel

Uppgifter som ska respektive kan lämnas enligt Arachne-stadgan

För det fall svenska myndigheter önskar använda Arachne före 2028 behöver de lämna vissa uppgifter om medel som redan har beviljats, något som framgår av Arachne-stadgan (punkt 11). Det sker för närvarande genom att data laddas upp genom användande av en så kallad XML-fil. De uppgifter som kan laddas upp motsvaras av olika förangivna datafält. Vissa uppgiftsslag, som motsvarar datafält, kan sägas vara *funktionellt nödvändiga*. Med detta avses att de behövs för att Arachne ska kunna fungera som avsett och generera riskvärderingar. Andra uppgiftsslag är *inte funktionellt nödvändiga* utan valfria.

Enligt Arachne-stadgan finns det totalt 105 möjliga datafält som kan laddas upp till Arachne för respektive program. Som utredningen uppfattar det saknas det möjlighet att lämna information i form av fritext. När medlemsstaterna väljer att använda Arachne är enligt stadgan följande sju datafält gällande *projektinformation* nödvändiga för att Arachne ska kunna generera riskvärderingar: projekt-id, projektnamn, status, generaldirektorat, projekttyp, mottagare (id och namn) samt projektkostnad.

Detta lämnande av uppgifter om beviljade medel fyller i princip samma syfte som det tillgängliggörande av uppgifter som blir obligatoriskt enligt artikel 36.6 i budgetförordningen från och med 2028. I huvudsak synes det handla om motsvarande uppgifter som är funk-

tionellt nödvändiga i dag som kommer att bli obligatoriska uppgifter enligt artikel 36.6. Det kan dock finnas vissa avvikelser.

Medlemsstaterna rekommenderas att lämna även uppgifter som kanske inte är funktionellt nödvändiga.

Uppgifter som ska respektive kan lämnas inom ett visst område – ett exempel

Vilka filer som behöver laddas upp kan variera mellan olika fonder. Utredningen utgår här från ett exempel, som avser fonderna ISF, Amif och BMVI. Som referensram för uppgiftsslagen använder utredningen den XML-fil som i dag kan användas av medlemsstater för att föra in uppgifter i Arachne.

Inledningsvis behöver filens funktioner beskrivas övergripande. Beroende på bland annat vilka fonder som uppgiftslämnandet avser visar filen olika flikar (som i det följande beskrivs som kategorier). Inom varje kategori finns ett antal fält som kan fyllas i och som motsvarar ett uppgiftsslag. Färgsättningen visar i vilken utsträckning *kategorin* innehåller nödvändiga delar eller om ett *fält* är nödvändigt att fylla i. Röda fält är funktionellt nödvändiga. Gröna fält indikerar att de ska fyllas i om man väljer att fylla i uppgifter inom den kategori som fälten tillhör. Andra fält är grå. Dessa fält är inte i någon mening nödvändiga att fylla i utan helt valfria.

I aktuellt exempel finns det funktionellt nödvändiga (röda) fält under följande kategorier.

- *Allmän information* (med nödvändiga fält för källa, datum, författare, program/plan-id, myndighet, valuta och medlemsstat)
- *Projektinformation* (med nödvändiga fält för projekt-id, projektnamn, status, generaldirektorat, projekttyp, mottagare och projektkostnad, härutöver valfria fält, se mer nedan)
- *Information om enheter* – som här tar sikte på mottagare (med nödvändiga fält för enhetens id, namn och land, härutöver frivilliga fält, se mer nedan).

Som framgår av punktuppställningen finns det valfria fält inom ovan nämnda kategorier. När det gäller *projektinformation* kan nämnas till exempel närmare uppgifter om mottagaren såsom om koncern-

tillhörighet, omsättning och antal anställda. Såvitt gäller *information om enheter* kan nämnas momsregistreringsnummer, adressuppgifter och omsättning.

Utöver vad som finns under de nödvändiga kategorierna finns det ett stort antal fält inom ytterligare – valfria – kategorier. Kategorierna är i aktuellt exempel följande.

- Kontrakt (Contracts)
- Underleverantörer (SubContracts)
- Utgifter/kostnader (Expenses)
- Verklig huvudman (Beneficial Owner)
- Anknutna personer (Related People)
- Projektpartners (Project-Partners)
- Medlemmar i konsortiet (Consortium Members)
- Tjänsteleverantörer (Service Providers)
- Nyckelexperter (Key Experts).

Fälten som finns inom dessa kategorier avser närmare uppgifter, såsom id-uppgifter, belopp, för- och efternamn, födelsedatum och funktion.

4.3.3 Lämnande av uppgifter vid användning av Arachnes förhandsfunktion

Arachne innehåller en så kallad förhandsfunktion (the ex-ante functionality), som ger användare möjlighet att – under processen med att välja vilka som ska tilldelas EU-medel – göra en värdering av vilka risker det skulle innebära om en viss enhet skulle tilldelas EU-medel (se vidare avsnitt 5.2.1).

Inom ramen för förhandsfunktionen laddar användaren upp viss information till Arachne. Detta kan göras antingen genom att användare skapar en så kallad XML-fil eller genom att använda en särskild funktion för redigering av data (Dataset editor). När informationen har laddats upp gör Arachne en riskvärdering utifrån underlaget över natten.

Det finns inte någon skyldighet för svenska myndigheter att använda Arachne och det är givetvis även frivilligt att använda förhandsfunktionen. Om myndigheterna väljer att använda funktionen är det dock – som Arachne är utformat i dag – vissa uppgifter som är nödvändiga att ladda upp för att Arachne ska kunna göra en riskvärdering inom ramen för förhandsfunktionen. Användare har därutöver möjlighet att ange ytterligare uppgifter.

För att kunna använda förhandsfunktionen behöver användare till att börja med lämna viss *allmän information*. Det finns funktionellt nödvändiga fält för källa, datum, författare, program/plan-id, myndighet, valuta och medlemsstat.

Vidare finns det funktionellt nödvändiga fält för viss *projektinformation* med nödvändiga fält för projekt-id, projektnamn och mottagare. Det kan också lämnas ytterligare icke nödvändig projektinformation om startdatum och slutdatum samt projektkostnad.

Det finns också funktionellt nödvändiga fält för *information om enheter* (som här tar sikte på mottagare) med nödvändiga fält för enhetens id, namn, land och verklig huvudman. Det kan också lämnas ytterligare icke nödvändig information om enheterna.

Utöver de funktionellt nödvändiga uppgiftskategorierna kan ytterligare uppgifter lämnas inom (bland annat) följande – valfria – kategorier.

- Kontrakt (Contracts)
- Anknutna personer (Related People)
- Projektpartners (Project-Partners)
- Medlemmar i konsortiet (Consortium Members)
- Nyckelexperter (Key Experts).

Fälten som finns inom dessa kategorier avser närmare uppgifter om kategorierna, såsom id-uppgifter, belopp, för- och efternamn, födelsedatum och funktion.

Utredningen konstaterar att de uppgifter som ska och kan lämnas inom ramen för förhandsfunktionen delvis motsvarar de uppgifter om beviljade medel som de myndigheter som använder Arachne i dag ska och kan tillföra systemet.

4.4 Ett nytt krav på tillgängliggörande av uppgifter från och med 2028

4.4.1 Om artikel 36.6 i budgetförordningen

Från och med 2028 blir det obligatoriskt för medlemsländerna att tillgängliggöra vissa uppgifter för kommissionen, vilka är avsedda att användas i Arachne, även om det alltjämt kommer att vara frivilligt att använda Arachne. Detta framgår av artikel 36.6 i budgetförordningen, som innehåller skyldigheter för ett antal aktörer att göra viss information tillgänglig för kommissionen, i ett särskilt format. Bestämmelsen inleds med en hänvisning till målet i artikel 36.2 d att förebygga, upptäcka, korrigera och följa upp oriktigheter och dubbelfinansiering.

Enligt bestämmelsens första stycke ska unionsinstitutioner och unionsorgan och personer eller enheter som genomför budgeten enligt artikel 62.1 göra viss information tillgänglig för kommissionen elektroniskt i ett interoperabelt och maskinläsbart format. I punkten räknas uppgifter upp som gäller *mottagaren* (artikel 36.6 första stycket a), *insatsen* (artikel 36.6 första stycket b) och mottagarens *verkliga huvudman* (artikel 36.6 första stycket c).

Enligt artikel 36.6 andra stycket ska medlemsstaterna ge kommissionen tillgång till den information som anges i första stycket endast om de är skyldiga att registrera och lagra sådan information i enlighet med sektorsspecifika regler. Om en sådan skyldighet inte ingår i de sektorsspecifika reglerna får medlemsstaterna på frivillig basis ge kommissionen tillgång till den information som de förfogar över som avses i första stycket.

Enligt övergångsbestämmelsen i artikel 277.5 ska den skyldighet som anges i artikel (36.2 d och) 36.6 när det gäller tillgång till uppgifter om mottagarna av medel och deras verkliga huvudmän endast tillämpas på program som antas inom och finansieras genom fleråriga budgetramar efter 2027. Det kan noteras att uppgift om insatsen inte nämns i övergångsbestämmelsen. En anledning till detta är sannolikt att det redan finns skyldigheter att lämna uppgifter om insatsen. Skyldigheterna enligt nämnda artiklar bedöms av utredningen inträda vid samma tidpunkt beträffande samtliga slags uppgifter.

Övriga delar av artikel 36.6 handlar bland annat om att kommissionen ska göra en utvärdering av Arachne och att användningen av Arachne är frivillig.

4.4.2 Vilka svenska myndigheter omfattas av skyldigheten?

Vilka riktar sig skyldigheten till?

Skyldigheten i artikel 36.6 första stycket i budgetförordningen att göra uppgifter tillgängliga för kommissionen riktar sig till ”unionsinstitutioner och unionsorgan och personer eller enheter som genomför budgeten enligt artikel 62.1”. Med *budgetgenomförande* avses utförande av verksamheter som rör förvaltning, övervakning, kontroll och revision av budgetanslag i enlighet med de metoder som föreskrivs i artikel 62 (artikel 2.7).

Artikel 62.1 anger metoder för genomförande av budgeten, såsom genom direkt förvaltning som sker genom kommissionens egna avdelningar eller via utsedda genomförandeorgan (artikel 62.1 första stycket a), delad förvaltning som sker med medlemsstaterna (artikel 62.1 första stycket b) eller indirekt förvaltning där genomförandeuppgifter anförtros åt till exempel tredjeländer, internationella organisationer eller offentligrättsliga organ (artikel 62.1 första stycket c).

Skyldigheten i artikel 36.6 första stycket avser flera aktörer och omfattar medlemsstater. Artikel 36.6 andra stycket, som begränsar skyldigheten enligt första stycket, riktar sig enbart till medlemsstater. Hänvisningen till medlemsstaterna får antas gälla även medlemsstaternas myndigheter. Vad gäller de situationer som bestämmelsen omfattar framgår att det gäller när medlemsstaterna ”tar emot och genomför budgeten enligt artikel 62.1”.

Enligt utredningens mening bör utgångspunkten vara att samtliga enheter som har någon roll i att avgöra vem som ska ta emot stöd eller i att i efterhand vidta kontroller av utbetalade stöd anses delta i budgetgenomförandet.

Då det hänvisas till artikel 62.1 i både första och andra stycket av artikel 36.6 omfattas alla förvaltningsformer, och därmed för svenskt vidkommande såväl delad förvaltning som direkt förvaltning tillsammans med medlemsstaterna.

Vilka svenska myndigheter omfattas?

Kretsen av myndigheter som omfattas av skyldigheten att tillgängliggöra uppgifter kan utifrån ovan förda resonemang bedömas vara relativt stor. Det behöver dock beaktas att medlemsländernas och

de nationella myndigheternas skyldigheter är begränsade till fall då skyldigheter följer av sektorsspecifika regler, och bara om det finns en skyldighet att registrera och lagra sådan information enligt sektorsspecifika regler (artikel 36.6 andra stycket). Detta innebär att inte alla som genomför budgeten omfattas av skyldigheten i artikel 36.6.

En fråga är om kretsen svenska myndigheter kan avgränsas på något tydligt sätt. Enligt utredningens mening kan de myndigheter som omfattas av skyldigheten beskrivas som sådana myndigheter som tar emot, förvaltar, övervakar, kontrollerar och reviderar EU-medel, om de har skyldigheter enligt sektorsspecifika regler att registrera och lagra sådan information som avses i artikel 36.6 i budgetförordningen. Beskrivningen träffar utbetalande organ och förvaltande myndigheter enligt dagens sektorsspecifika regelverk, i dag därmed bland annat Jordbruksverket, Migrationsverket, Polismyndigheten, Svenska ESF-rådet samt Tillväxtverket och länsstyrelserna i Jämtlands, Västerbottens och Norrbottens län.

När det gäller RRF-regelverket ska reformer och investeringar ha genomförts till den 31 augusti 2026 och utbetalningar till den 31 december samma år. Då skyldigheterna enligt artikel 36.6 inträder först beträffande program som antas inom och finansieras genom fleråriga budgetramar efter 2027 (artikel 277), omfattas inte enligt utredningens uppfattning myndigheter enligt RRF av skyldigheten att tillgängliggöra uppgifter för kommissionen. Det kan dock komma nya program inom ramen för förvaltningsformen direkt förvaltning tillsammans med medlemsstaterna, som kan medföra att andra myndigheter blir skyldiga att tillgängliggöra information.

Som exempel på myndigheter som har roller när det gäller delad förvaltning men som inte bedöms få en skyldighet att tillgängliggöra uppgifter enligt artikel 36.6 enligt gällande reglering kan nämnas ESV och Ekobrottsmyndigheten. ESV har i uppgift att övervaka och utöva revision men omfattas inte av någon skyldighet enligt sektorsspecifika regler att lagra och registrera sådana uppgifter som nu är aktuella. Ekobrottsmyndighetens uppgifter medför inte heller några sådana skyldigheter.

Beträffande sådana uppgifter som inte är *rättsligt obligatoriska* att tillgängliggöra enligt artikel 36.6, kan det finnas *möjlighet* att tillgängliggöra uppgifter. Frågor om detta behandlas i avsnitt 4.5 nedan. För rättsliga frågor avseende frivilligt uppgiftslämnande, se avsnitt 8.3.

Slutsatser om vilka myndigheter som kommer att vara skyldiga att tillgängliggöra uppgifter

Utredningen anser alltså att myndigheter som omfattas av skyldigheten att tillgängliggöra uppgifter enligt artikel 36.6 kan sammanfattas som myndigheter som tar emot, förvaltar, övervakar, kontrollerar och reviderar EU-medel, om de har skyldigheter enligt sektorsspecifika regler att registrera och lagra sådan information som avses i artikel 36.6 i budgetförordningen.

4.4.3 Vilka uppgifter omfattas av skyldigheten?

Kort om vilka kategorier av uppgifter som skyldigheten gäller

Skyldigheten enligt artikel 36.6 i budgetförordningen är konstruerad på det sättet att det delvis hänvisas till artikel 38 när det gäller att fastställa vilka uppgifter som ska göras tillgängliga. Artikel 38 gäller enligt sin rubrik offentliggörande av information om mottagare samt annan information och den tar huvudsakligen sikte på vad kommissionen ska göra.

Till att börja med gäller skyldigheten enligt artikel 36.6 första stycket vissa uppgifter *om mottagaren*, nämligen all information som förtecknas i artikel 38.2 a, b och c och 38.6 andra stycket och, om det rör sig om en fysisk person, även födelsedatum (artikel 36.6 första stycket a).

Vidare gäller skyldigheten vissa uppgifter *om insatsen*, nämligen all information som förtecknas i artikel 38.2 d och e samt insatsens unika identifieringskod (artikel 36.6 första stycket b).

Därutöver gäller skyldigheten uppgifter som inte nämns i artikel 38, nämligen *om mottagarens verkliga huvudmän* när mottagaren inte är en fysisk person: förnamn, efternamn, födelsedatum och registreringsnummer för mervärdesskatt eller skatteregistreringsnummer om sådana finns, eller en annan unik identifieringskod på landsnivå.

I det följande redogörs för nu relevanta delar av artikel 38.

Uppgifter om mottagare och åtgärden – artikel 38.2 och 38.6 andra stycket

Artikel 38 i budgetförordningen är uppbyggd så att information som kommissionen ska offentliggöra räknas upp i artikel 38.2. Informationen ska enligt den bestämmelsen offentliggöras i ett öppet, interoperabelt och maskinläsbart format som gör det möjligt att sortera, göra sökningar, hämta, jämföra och återanvända uppgifter, med vederbörlig hänsyn till kraven på konfidentialitet och säkerhet, i synnerhet skyddet av personuppgifter.

Informationen avser:

- Om mottagaren är en fysisk eller juridisk person (artikel 38.2 a)
- Mottagarens fullständiga juridiska namn för juridiska personer och deras registreringsnummer för mervärdesskatt eller skatteregistreringsnummer om sådana finns tillgängliga eller en annan unik identifieringskod fastställd på landsnivå, mottagarens för- och efternamn för fysiska personer (artikel 38.2 b)
- Var mottagaren finns, det vill säga
  - mottagarens adress, om mottagaren är en juridisk person,
  - regionen på Nuts 2-nivå[4], om mottagaren är en fysisk person med hemvist i unionen, eller landet, om mottagaren är en fysisk person och inte har hemvist i unionen (artikel 38.2 c)
- Det belopp för vilket ett åtagande gjorts och, om det rör sig om ett åtagande med flera mottagare, fördelningen av detta belopp per mottagare, om den finns tillgänglig (artikel 38.2 d)
- Åtgärdens art och ändamål (artikel 38.2 e).

När det gäller mottagare hänvisar artikel 36.6 till artikel 38.6 andra stycket. Där anges att uppgifterna även ska omfatta fysiska personers registreringsnummer för mervärdesskatt eller skatteregistreringsnummer, om sådana finns tillgängliga, eller en annan unik identifikationskod som fastställts på nationell nivå i syfte att förbättra kvaliteten på de uppgifter som överförs utan att de används för offentliggörande. För mer om artikel 38.6, se under nästa rubrik.

[4] Nuts är den regionala indelning som används inom EU för statistikredovisning. I Sverige utgörs Nuts-2 av åtta riksområden.

Kommissionen ska använda uppgifter som finns i Arachne samt offentliggöra uppgifter om unik identifikationskod – artikel 38.6

Då uppgifter som ska tillgängliggöras enligt artikel 36.6 är avsedda att föras in i Arachne finns det här skäl att ta upp att även artikel 38 har koppling till Arachne. Första stycket i artikel 38.6 lyder: ”Vid tillämpning av punkt 1 första och andra styckena i denna artikel och utan att det påverkar tillämpningen av punkterna 3 och 4 i denna artikel och sektorsspecifika regler, ska kommissionen använda de relevanta uppgifter som lagras i det system som avses i artikel 36.2 d för att föra in på den centraliserade webbplats som avses i punkt 1 i den här artikeln de uppgifter som avses i punkt 2 i den här artikeln.” Utredningen förstår det så att när kommissionen offentliggör uppgifter på den centraliserade webbplatsen ska kommissionen använda de uppgifter som redan finns i Arachne.

Som nämns under föregående rubrik ska enligt artikel 38.6 andra stycket uppgifterna dessutom även omfatta fysiska personers registreringsnummer för mervärdesskatt eller skatteregistreringsnummer, om sådana finns tillgängliga, eller en annan unik identifikationskod som fastställts på nationell nivå i syfte att förbättra kvaliteten på de uppgifter som överförs utan att de används för offentliggörande. Utredningen förstår detta så att om det finns information om registreringsnummer eller dylikt i Arachne, ska kommissionen använda den informationen i utförandet av sin uppgift, men den ska inte offentliggöras på webbplatsen.

Det kan nämnas att även vad gäller denna bestämmelse finns övergångsbestämmelser. Enligt artikel 277.6 ska (artikel 38.4 tredje stycket och) artikel 38.6 endast tillämpas på program som antas inom ramen för och finansieras genom fleråriga budgetramar efter 2027.

Undantag från offentliggörande – artikel 38.3

Artikel 38.3 första stycket anger situationer där informationen inte ska offentliggöras, och inte heller lämnas in för offentliggörande i enlighet med artikel 38.6. Det handlar något förenklat om

a) utbildningsstöd till fysiska personer och andra direktstöd som betalas ut till fysiska personer som är mest behövande,

b) kontrakt till mycket lågt värde som tilldelats utvalda experter samt kontrakt till mycket lågt värde underskridande det belopp som avses i punkt 14.4 i bilaga I till budgetförordningen,

c) ekonomiskt stöd som tillhandahålls genom finansieringsinstrument eller budgetgarantier till ett belopp som understiger 500 000 euro,

d) situationer då ett offentliggörande innebär en risk för berörda personers eller enheters fri- och rättigheter enligt Europeiska unionens stadga om de grundläggande rättigheterna eller kan skada mottagarnas affärsintressen,

e) situationer då det inte krävs för offentliggörande i sektorsspecifika regler om budgeten genomförs genom delad förvaltning.

När det gäller fysiska personer ska utlämnandet av den information som avses i artikel 38.2 baseras på relevanta kriterier såsom åtgärdens frekvens eller typ och de berörda beloppen (artikel 38.3 tredje stycket).

En särskild fråga är om de undantag som gäller för offentliggörande enligt artikel 38.3 också får betydelse vid en tolkning av skyldigheten i artikel 36.6 andra stycket. Frågan här är alltså om skyldigheten att göra uppgifter tillgängliga för kommissionen är förenad med motsvarande undantag som följer av artikel 38.3. Utredningen tolkar det så att skyldigheten att göra uppgifter tillgängliga för kommissionen kan omfatta fler uppgifter än de som kommissionen ska offentliggöra. Hänvisningsmetoden i artikel 36.6 är konstruerad så att skyldigheten att göra uppgifter tillgängliga avser ”information som förtecknas” i vissa punkter i artikel 38.2. I själva punkterna framgår det inte att undantagen enligt artikel 38.3 är tillämpliga. Vidare framstår det som rimligt att det kan finnas skäl att inom ramen för Arachne ha tillgång till mer information än vad som bör offentliggöras och därmed blir mer lättillgänglig, exempelvis på grund av dataskyddsregleringen. Utredningens slutsats är att undantagen i artikel 38.3 inte påverkar artikel 36.6 andra stycket.

4.4.4 Skyldigheten gäller bara när det finns sektorsspecifika regler

Inledning

Artikel 36.6 andra stycket i budgetförordningen medför en begränsning av vilka uppgifter som behöver tillgängliggöras. Där framgår att medlemsstaterna ska ge kommissionen tillgång till den information som anges i första stycket endast om de är skyldiga att registrera och lagra sådan information i enlighet med sektorsspecifika regler. Svenska myndigheter behöver således bara lämna uppgifter om en skyldighet finns enligt annan reglering att lagra och registrera sådan information.

Kraven varierar beroende på sektorsspecifik reglering

Medlemsstaterna, och därmed de nationella myndigheterna, är i flera avseenden skyldiga att registrera och lagra sådan information som avses i artikel 36.6 enligt sektorsspecifika regler. Sådana sektorsspecifika regler finns i dag i CPR, som gäller för Eruf, ESF+, FRO, EHFVF, Amif, ISF och BMVI, samt i CAP-förordningen. Av dessa rättsakter följer skyldigheter att registrera och lagra uppgifter på det sätt som framgår i tabell 4.1. I de delar det finns sådana skyldigheter i de sektorsspecifika reglerna finns det också en skyldighet för myndigheterna att göra sådana uppgifter tillgängliga för kommissionen enligt artikel 36.6 i budgetförordningen.

Kraven varierar beroende på sektorsspecifik reglering. När det gäller jordbruksfonderna finns det i CAP exempelvis inte några krav på att lagra och registrera uppgifter om verklig huvudman.

Det bör noteras att de sektorsspecifika reglerna som nu nämns gäller för nuvarande programperiod. Vad som kommer att gälla för kommande programperiod, och därmed från och med den tidpunkt då skyldigheten att tillgängliggöra information för kommissionen enligt budgetförordningen börjar gälla, är inte känt. Nu gällande reglering får därmed betraktas som en referensram.

Utredningen utvecklar i det följande närmare vad som gäller enligt CPR. Enligt artikel 72.1 e i CPR ska förvaltande myndigheter bland annat elektroniskt registrera och lagra de uppgifter om varje insats som behövs för övervakning, utvärdering, ekonomisk för-

valtning, kontroller och revisioner i enlighet med bilaga XVII samt säkerställa uppgifternas säkerhet, integritet och konfidentialitet och autentisering av användare. Bilaga XVII har två kolumner. I vänsterkolumnen anges typen av uppgift, även kallat datafält. I högerkolumnen anges fonder för vilka uppgifterna i fråga inte krävs. Om en fond inte anges i högerkolumnen är alltså uppgiften obligatorisk för den fonden. Bilagan innehåller 142 olika datafält, alltså typer av uppgifter. Uppgifterna är angivna i olika kategorier. Datafält 1–8 avser uppgifter om stödmottagaren. Bland annat ska uppgift om namn och identifieringskod för varje stödmottagare, uppgift om huruvida stödmottagaren är ett offentligrättsligt eller privaträttsligt organ, juridisk person eller fysisk person anges för samtliga fonder. Vissa datafält avser uppgifter om insatsen, exempelvis namn på insatsen och dess identifieringskod samt en kort beskrivning av insatsen.

Tabell 4.1 Krav på lagring i nu gällande sektorsspecifik reglering i förhållande till kraven på tillgängliggörande i budgetförordningen

Med angivande av artiklar i budgetförordningen, CPR och CAP

Uppgift	BF	CPR	CAP
Om mottagaren			
Om mottagaren är en fysisk eller juridisk person	36.6.a + 38.2 a	72.1 e, Bil.XVII rad 2	98.2 + 49.3 a–b CPR
Mottagarens namn och, för juridisk person, unik identifieringskod	36.6.a + 38.2 b och 38.6 2 st	72.1 e, Bil.XVII rad 1–2 49.3 a–b	98.2 + 49.3 a–b CPR
Födelsedatum för fysisk person	36.6.a	72.1 e, Bil.XVII rad 2	
Var mottagaren finns, det vill säga i) mottagarens adress, om mottagaren är en juridisk person, ii) regionen på Nuts 2-nivå, om mottagaren är en fysisk person med hemvist i unionen, eller landet, om mottagaren är en fysisk person och inte har hemvist i unionen	36.6.a + 38.2 c	72.1 e, Bil.XVII rad 7 + 49.3 m	
Om åtgärden			
Det belopp för vilket ett åtagande gjorts och, om det rör sig om ett åtagande med flera mottagare, fördelningen av detta belopp per mottagare, om den finns tillgänglig	36.6 b + 38.2 d	72.1 e, Bil.XVII rad 56–58 + 49.3 h	98.2 + 49.3 h CPR
Åtgärdens art och ändamål	36.6 b + 38.2 e	72.1 e, Bil.XVII rad 10 + 49.3 e	98.2 + 49.3 e CPR
Insatsens unika identifieringskod	36.6 b	72.1 e, Bil.XVII rad 9 + 49.3	98.2 + 49.3 CPR
Om verklig huvudman			
Om mottagarens verkliga huvudmän när mottagaren inte är en fysisk person: förnamn, efternamn, födelsedatum, och registreringsnummer för mervärdesskatt eller skatteregistreringsnummer om sådana finns, eller en annan unik identifieringskod på landsnivå	36.6 c	72.1 e, Bil.XVII rad 3	

Källa: Egen sammanställning.

Slutsatser om vilka uppgifter som behöver tillgängliggöras

Sammanfattningsvis anger artikel 36.6 första stycket i budgetförordningen en yttersta ram för vilka uppgifter som behöver tillgängliggöras för kommissionen. Skyldigheten kan vara mer begränsad i förhållande till den yttersta ramen, genom att det också krävs att det finns en skyldighet att registrera och lagra uppgifterna enligt gällande sektorsspecifik reglering. Exempelvis finns det beträffande vissa fonder inte krav på tillgängliggörande av uppgifter om verklig huvudman.

Den yttersta ramen är vissa närmare uppgifter om:

- Mottagaren
- Åtgärden
- Mottagarens verkliga huvudman.

Vad som kommer att gälla enligt kommande sektorsspecifik reglering är inte känt. Viss vägledning om vilka uppgifter som kan komma att vara obligatoriska att lämna kan möjligen fås utifrån de uppgifter om beviljade medel som i dag är funktionellt nödvändiga att lämna av de som väljer att använda Arachne, se avsnitt 4.3.2.

4.4.5 Uppgifter från medlemsländerna kommer att tillföras Arachne

Det framgår inte uttryckligen i budgetförordningen att de uppgifter som ska tillgängliggöras för kommissionen enligt artikel 36.6 i budgetförordningen ska tillföras Arachne, men avsikten är att så ska ske. Det framgår exempelvis av en vitbok från kommissionen om en översyn av bedrägeribekämpningsstrukturen att uppgifter som samlas in av medlemsstaternas myndigheter beträffande alla fonder kommer att ingå i det EU-omfattande verktyget Arachne+ (COM [2025] 546 final, s. 7).

Det är sannolikt att medlemsstaterna rent tekniskt kommer att använda sig av Arachne för att tillgängliggöra uppgifterna för kommissionen eller att tillgängliggörandet framöver kommer att ske genom automatiserad överföring. Av skäl 30 till budgetförordningen framgår att Arachne bör bygga på interoperabilitet, varigenom uppgifter om mottagare av unionsmedel automatiskt och i realtid bör

hämtas från bland annat relevanta nationella databaser och interna system för relevanta nationella organ och myndigheter. Det är dock oklart hur detta rent praktiskt kommer att gå till framöver, då systemet är under utveckling. Oavsett hur överföringen rent tekniskt kommer att utföras, står det klart att artikel 36.6 är nära knuten till Arachnes funktionalitet.

I Arachne-stadgan beskrivs hur uppgifter i dag kan överföras från medlemsstaterna till Arachne. Uppgifter kan extraheras av programmyndigheterna från deras lokala datoriserade system och laddas upp till en särskild server hos kommissionen (punkt 6.2). I punkt 11 i Arachne-stadgan, som handlar om överföring av data, anges att programmyndigheterna överför datafält i enlighet med kraven i Arachne. Det anges också att – utöver datafälten i de nämnda bilagorna – programmyndigheterna på frivillig basis kan utöka antalet datafält att laddas upp till Arachne.

4.5 Tillgängliggörande av frivilliga uppgifter

4.5.1 Frivilligt tillgängliggörande enligt budgetförordningen från och med 2028

Budgetförordningen möjliggör tillgängliggörande av frivilliga uppgifter

I avsnitt 4.4 finns en kartläggning och en beskrivning av vilka uppgifter som det från och med 2028 kommer att finnas en skyldighet enligt budgetförordningen för svenska myndigheter att göra tillgängliga för kommissionen.

I artikel 36.6 andra stycket i budgetförordningen anges att om en sådan skyldighet inte ingår i de sektorsspecifika reglerna, får medlemsstaterna på frivillig basis ge kommissionen tillgång till den information som de förfogar över som avses i första stycket. Det finns därmed en reglering som uttryckligen tillåter ytterligare uppgiftslämnande. Dessa uppgifter kallas här för frivilliga uppgifter.

En fråga är om det finns några begränsningar när det gäller vilka uppgifter som omfattas av bestämmelsen. Det kan noteras att artikel 36.6 andra stycket i budgetförordningen bara behandlar sådana uppgifter som avses i första stycket. Det bör tolkas så att medlemsstaterna på frivillig basis kan ge kommissionen tillgång till alla slags

uppgifter som avses i första stycket, det vill säga sådana uppgifter som beskrivs i punkterna a–c i första stycket och som rör mottagare, insatsen och verkliga huvudmän. Som utredningen uppfattar det behandlar inte bestämmelsen frivilligt tillgängliggörande av uppgifter av andra slag.

Som utredningen uppfattar saken tar regleringen till att börja med sikte på uppgifter som i och för sig omfattas av artikel 36.6 första stycket i budgetförordningen, men som inte omfattas av någon sektorsspecifik reglering tillämplig på den berörda myndigheten. Vidare kan det konstateras att beskrivningarna av de obligatoriska uppgifterna är tämligen övergripande och att det bör vara möjligt att uppfylla kraven i artikel 36.6 utan att ange så mycket detaljer om exempelvis åtgärdens art och ändamål. De ytterligare och mer detaljerade uppgifter som tillgängliggörs kan därmed också sägas höra till kategorin frivilliga uppgifter, i den meningen att de inte är rättsligt obligatoriska.

I praktiken kan möjligheten att tillgängliggöra uppgifter vara begränsad beroende på de användargränssnitt som används vid tillgängliggörandet. Hur användargränssnittet kommer att vara utformat från och med 2028 är ännu okänt. I sammanhanget kan nämnas att det inom ramen för den information som användare av Arachne i dag lämnar finns begränsningar på så sätt att information för närvarande endast kan lämnas i form av vissa förangivna uppgiftsfält i en datafil. Som utredningen uppfattar det saknas det möjlighet att lämna information i form av fritext. Därmed finns det praktiska begränsningar i fråga om vilka frivilliga uppgifter som kan tillgängliggöras.

Frivilligt tillgängliggörande kan vara bra för att målet att motverka oriktigheter ska uppnås

Om fler uppgifter än de som är rättsligt obligatoriska skulle tillgängliggöras för kommissionen och tillföras Arachne, skulle det kunna öka värdet av att använda systemet. Det skulle kunna befaras att en ordning där endast de rättsligt obligatoriska uppgifterna tillförs systemet innebär att Arachne blir mindre effektivt som riskvärderingssystem och att resultatet av riskvärderingarna blir mindre användbara i praktiken. Detta är också ett av skälen till att utredningen har i uppdrag att utreda frågor som rör frivilligt uppgiftslämnande.

4.5.2 Vilka ytterligare uppgifter kan vara av värde att tillgängliggöra?

Vilka uppgifter som är av värde att tillgängliggöra kan variera

En central fråga är vilka ytterligare uppgifter som kan vara av värde att göra tillgängliga utöver de uppgifter som kommer att vara rättsligt obligatoriska enligt artikel 36.6 i budgetförordningen. Vägledning till detta kan sökas i bland annat syftet med tillgängliggörandet av uppgifter till kommissionen och användningen av Arachne, nämligen att motverka felaktigheter, såsom att hitta dubbelfinansieringar och intressekonflikter. Vägledning kan också sökas i de förangivna fält som i dag kan användas för att föra in uppgifter om beviljade medel i Arachne. Kommissionen rekommenderar att samtliga tillgängliga fält fylls i för bästa utfall och användning av Arachne (se Arachne, Frequently asked questions, version 2.3, den 19 augusti 2022, fråga 13).

Det finns flera utmaningar när det gäller att identifiera vilka ytterligare uppgifter som kan vara värdefulla att göra tillgängliga. Arachne är under utveckling och förändring. Även sektorsspecifik reglering är under utveckling och förändring. Därutöver skiljer sig uppgiftsslag och behov mellan olika stöd och myndigheter. Stöden på CAP-området skiljer sig mycket från stöden inom CPR-området. Till detta kommer att det pågår arbete inom olika expertgrupper inom EU såväl avseende förhandling av nya rättsakter som mer detaljerade frågor såsom om olika riskfaktorer.

När det gäller att få vägledning utifrån de förangivna fälten finns ytterligare utmaningar. Vissa risker är sannolikt viktigare att kunna upptäcka vid svenska myndigheters arbete med att motverka felaktigheter med EU-medel än på generell EU-nivå. Detta medför svårigheter att värdera och rangordna betydelsen av att frivilligt lämna olika uppgiftsslag.

Det kan också vara svårt att utifrån de uppgifter som är funktionellt nödvändiga avgöra vilka uppgifter som kommer att vara obligatoriska respektive frivilliga att tillgängliggöra enligt artikel 36.6 i budgetförordningen. Det synes i nuläget nämligen vara så att de funktionellt nödvändiga fälten i Arachne inte helt motsvarar de rättsligt obligatoriska uppgifterna enligt artikel 36.6 i budgetförordningen.

En annan utmaning är att de uppgiftsfält som finns i Arachne inte helt motsvaras av uppgiftsfält i bilagan till gällande CPR eller

i CAP-förordningen, även om de huvudsakligen är lika. Det kan innebära att det finns möjlighet att genom uppgiftsfälten i Arachnes användargränssnitt lämna in uppgifter som inte har någon motsvarighet i någon sektorsspecifik reglering. Det kan också innebära att det inte är möjligt att lämna uppgifter som omfattas av sådan reglering.

De funktionellt nödvändiga fälten i Arachne synes förändras över tid och det kan förväntas att de kommer att samordnas med skyldigheterna i artikel 36.6 när de börjar att gälla från och med 2028.

Exempel på frivilliga uppgifter som det kan finnas skäl att tillgängliggöra

Trots de osäkerhetsmoment och utmaningar som nämns ovan lyfter utredningen i det följande vissa uppgiftsslag som skulle kunna vara av värde och relevanta att tillgängliggöra, utöver de rättsligt obligatoriska. Utredningen utgår här från ett exempel, som avser fonderna ISF, Amif och BMVI. Som referensram för uppgiftsslagen använder utredningen den XML-fil som i dag kan användas av medlemsstater för att föra in uppgifter i Arachne om beviljade medel. Utformningen av XML-filen i exemplet beskrivs närmare i avsnitt 4.3.2.

I aktuellt exempel finns det funktionellt nödvändiga fält under följande kategorier.

- *Allmän information* (med funktionellt nödvändiga fält för källa, datum, författare, program/plan-id, myndighet, valuta och medlemsstat)
- *Projektinformation* (med nödvändiga fält för projekt-id, projektnamn, status, generaldirektorat, projekttyp, mottagare och projektkostnad)
- *Information om enheter* (med nödvändiga fält för enhetens id, namn och land).

Vad som anges i punktlistan ovan motsvaras i huvudsak av uppgifter som kan vara rättsligt obligatoriska att tillgängliggöra enligt artikel 36.6 i budgetförordningen. Det finns även frivilliga fält inom ovan nämnda kategorier. När det gäller *projektinformation* kan nämnas till exempel närmare uppgifter om mottagaren såsom om koncerntillhörighet, omsättning och antal anställda. Såvitt gäller *information*

om enheter kan nämnas momsregistreringsnummer, adressuppgifter och omsättning. För en ändamålsenlig användning av Arachne skulle samtliga fält som nämns ovan kunna vara av värde att föra in uppgifter i, oavsett om de är nödvändiga eller valfria.

Utöver vad som finns under de nödvändiga kategorierna finns det ett stort antal fält inom ytterligare – inte funktionellt nödvändiga – kategorier. Kategorierna är i aktuellt exempel följande.

- Kontrakt (Contracts)
- Underleverantörer (SubContracts)
- Utgifter/kostnader (Expenses)
- Verklig huvudman (Beneficial Owner)
- Anknutna personer (Related People)
- Projektpartners (Project-Partners)
- Medlemmar i konsortiet (Consortium Members)
- Tjänsteleverantörer (Service Providers)
- Nyckelexperter (Key Experts).

Fälten inom dessa kategorier avser närmare uppgifter, såsom id-uppgifter, belopp, för- och efternamn, födelsedatum och funktion. Även uppgifter av dessa slag bör kunna vara av värde att tillgängliggöra för kommissionen på frivillig basis, sedan skyldigheten börjat gälla 2028. På motsvarande sätt kan det – vid ett eventuellt frivilligt användande av Arachne dessförinnan – finnas skäl att föra in sådana ytterligare uppgifter i Arachne. Det är dock – på grund av ovan nämnda osäkerhetsfaktorer – inte möjligt att med säkerhet ange exakt vilka uppgifter som det kan finnas anledning att tillgängliggöra eller annars föra in i Arachne på frivillig basis.

Vad gäller de rättsliga förutsättningarna enligt nationell rätt att lämna uppgifter av nu aktuellt slag, behandlas sådana frågor i avsnitt 8.3.

4.5.3 Även myndigheter som inte har någon skyldighet att tillgängliggöra uppgifter bör kunna göra det

En särskild fråga är om ett tillgängliggörande skulle kunna utföras av en myndighet som inte kommer att ha några skyldigheter att lämna uppgifter enligt artikel 36.6 i budgetförordningen. Utredningen bedömer att så kan vara fallet. Här kan nämnas den ordning som gäller där ESV tar emot rapporter om resultatinformation från andra myndigheter inom ramen för RRF. Myndigheter enligt RRF omfattas inte av skyldigheten enligt artikel 36.6 att tillgängliggöra uppgifter för kommissionen (se avsnitt 4.4.2). Inom ramen för ett frivilligt uppgiftslämnande bör det dock vara möjligt för ESV att tillgängliggöra dessa uppgifter för kommissionen, att föras in i Arachne. När det gäller RRF kan det nämligen vara ändamålsenligt att låta den myndighet som redan har samlat in relevanta uppgifter om RRF:s genomförande att ansvara för eventuell inmatning av uppgifter i Arachne för att viss efterkontroll ska kunna göras. Ett sådant förfarande skulle också medföra att uppgifter om RRF finns i Arachne, vilket kan bidra till att förhindra till exempel dubbelfinansiering gentemot andra program. De rättsliga förutsättningarna för ett sådant frivilligt uppgiftslämnande som nu nämns behandlas i avsnitt 8.3.

4.6 Inget nytt krav på tillgängliggörande av uppgifter när det gäller Edes

4.6.1 Om innehållet i artikel 36.8 och kopplingen till Edes

I artikel 36.8 i budgetförordningen finns bestämmelser om bland annat lämnande av information till kommissionen om domar och beslut.

Av artikeln framgår något förenklat att personer och enheter som genomför budgeten inom ramen för delad förvaltning och direkt förvaltning tillsammans med medlemsstaterna ska sända viss information till kommissionen om fakta och resultat som fastställts endast i samband med slutgiltiga domar eller slutgiltiga administrativa beslut när de får kännedom om sådan information. Översändandet ska ske via en officiell kanal, såsom IMS. Bestämmelsen gäller vid tillämpning av artikel 36.2 d, artikel 144.2 och artikel 147, och utöver tillämpliga sektorsspecifika regler.

För samma ändamål ska medlemsstaterna översända all annan nödvändig information som kommissionen begär, i synnerhet information som rör den administrativa uppföljningen.

I artikel 144.2 anges vilka uppgifter som Edes ska bygga på och varifrån dessa uppgifter ska komma (se närmare avsnitt 6.2.6). Systemet ska baseras på faktiska omständigheter och slutsatser som lämnas till kommissionen, särskilt av vissa enheter som räknas upp i artikel 144.2.

Artikel 144.2 d är av särskilt intresse för Sverige. Den gäller både vid delad förvaltning och vid direkt förvaltning tillsammans med medlemsstaterna. Bestämmelsen tar sikte på uppgifter av visst slag, något förenklat faktiska omständigheter och slutsatser som fastställs i slutliga domar och beslut. Edes ska baseras på sådana uppgifter bara om överlämnande av uppgifter till kommissionen krävs enligt sektorsspecifika regler.

Artikel 147 handlar om överlämnande av uppgifter avsedda för Edes. Artikel 147.1 anger att uppgifter som begärts från de enheter som avses i artikel 144.2 d ska i enlighet med artikel 36.8 och sektorsspecifika regler överföras till kommissionen.

Det ovan sagda visar att artikel 36.8 tar särskilt sikte på uppgifter som ska lämnas till kommissionen för att de ska ingå i Edes-databasen. En särskild fråga är om denna bestämmelse innebär några nya skyldigheter för Sverige eller svenska myndigheter, och som behöver beaktas när det gäller vilka åtgärder som kan krävas inom ramen för denna utredning.

4.6.2 För vilka gäller kraven i artikel 36.8?

I artikel 277 i budgetförordningen finns vissa övergångsbestämmelser. Av artikel 277.1 framgår, något förenklat, att skyldigheten som anges i artikel 36.8, när det gäller tillämpningen av Edes på delad förvaltning och direkt förvaltning tillsammans med medlemsstaterna, som huvudregel endast ska tillämpas på program som antas eller finansieras från och med den 1 januari 2028.

Flera svenska myndigheter deltar i budgetgenomförandet inom ramen för delad förvaltning. Eftersom RRF – som förvaltas inom ramen för direkt förvaltning tillsammans med medlemsstaterna – har begränsad tillämplighet i tid och Edes-databasen ska användas

i samband med tilldelning av kontrakt eller urval av bidragsmottagare (artikel 144.5), kommer artikel 36.8 avseende just denna facilitet inte att aktualiseras. Däremot kan bestämmelsen aktualiseras för eventuella nya fonder med samma upplägg.

För svenskt vidkommande omfattar bestämmelsen därmed, såvitt är känt för utredningen i dagsläget, endast myndigheter som deltar i delad förvaltning.

4.6.3 Ingen ny skyldighet för medlemsstaterna

Som framgår ovan ska Edes – något förenklat – bygga på uppgifter om slutgiltiga domar och administrativa beslut som lämnas till kommissionen från medlemsstater, bara *om överlämnandet av uppgifter krävs enligt sektorsspecifika regler*.

Mot denna bakgrund drar utredningen slutsatsen att det av artikel 36.8 inte följer någon skyldighet för Sverige eller svenska myndigheter, som inte redan följer av sektorsspecifika regler. Man kan säga att artikel 144.2 d erinrar om medlemsstaternas skyldighet att lämna uppgifter till kommissionen.

4.7 Ett nytt krav på offentliggörande av uppgifter från och med 2028

4.7.1 Om artikel 38 i budgetförordningen

Artikel 38 i budgetförordningen handlar enligt dess rubrik om offentliggörande av information om mottagare samt annan information. Kommissionen ska ge tillgång till information på en centraliserad webbplats om mottagare av medel som finansieras av budgeten och det räknas i artikeln upp vilken information som ska offentliggöras. Flera delar av artikeln behandlas i avsnitt 4.4.

Artikeln riktar sig huvudsakligen till kommissionen men artikel 38.4 handlar om andra aktörer. Artikel 38.4 första stycket tar sikte på indirekt förvaltning och återges inte här, då den inte bedöms ha någon betydelse för nu aktuella frågor. Övriga delar av artikel 38.4 behandlas dock närmare i det följande i syfte att klargöra om de innebär några krav för Sverige eller svenska myndigheter som behöver beaktas inom ramen för denna utredning.

4.7.2 En upplysning om skyldigheter att offentliggöra information enligt sektorsspecifika regler

Enligt *artikel 38.4 andra stycket* i budgetförordningen ska organ som har utsetts enligt artikel 63.3 offentliggöra information i enlighet med sektorsspecifika regler. Dessa sektorsspecifika regler får, i enlighet med den relevanta rättsliga grunden, avvika från artikel 38.2 och 38.3 med beaktande av den berörda sektorns särdrag.

När det gäller ”organ som utsetts enligt artikel 63.3” kan följande sägas. Av artikel 63.3 följer att medlemsstaterna – i enlighet med kriterierna och förfarandena i sektorsspecifika regler – ska utse organ som ska ansvara för förvaltningen och kontrollen av unionsmedel. Detta har skett till exempel genom att förvaltande myndigheter och revisionsmyndighet har pekats ut genom nationell rätt, se till exempel 1 kap. 4–7 §§ förordningen (2022:1379) om förvaltning av program för vissa EU-fonder.

Utredningen uppfattar artikel 38.4 andra stycket så att den utgör en bestämmelse som erinrar om att sådana organ som utsetts enligt artikel 63.3 har skyldigheter att offentliggöra uppgifter enligt sektorsspecifika regler. Vidare framgår av stycket att sådana sektorsspecifika regler får avvika från det som regleras om information som ska offentliggöras enligt artikel 38.2 och 38.3. En motsvarande reglering finns i artikel 38.4 i den tidigare budgetförordningen. Artikel 38.4 andra stycket innebär alltså inte några nya skyldigheter som behöver beaktas inom ramen för denna utredning.

4.7.3 En ny skyldighet för medlemsstater vid direkt förvaltning

Enligt *artikel 38.4 tredje stycket* i budgetförordningen ska medlemsstater som tar emot och genomför unionsmedel[5] enligt artikel 62.1 första stycket a säkerställa offentliggörande i efterhand av information om deras mottagare på en sådan centraliserad webbplats som avses artikel 38.1 i enlighet med vad som sägs i artikel 38.2–3. Av

[5] I den svenska versionen av budgetförordningen har uttrycket ”the implementation of Union funds” översatts med ”förvaltningen av unionsmedel” (i olika grammatiska former). På tyska används uttrycket ”Ausführung von Unionsmitteln”. Enligt utredningen framstår det som mer korrekt att på svenska beskriva detta som ”genomförandet av unionsmedel”. Se exempelvis artiklarna 62.1 första stycket c ix och 152.8 samt skäl 51. Utredningen använder därför begreppet ”genomförande” av unionsmedel när det i den engelska versionen handlar om ”implementation” av sådana medel.

övergångsbestämmelsen i artikel 277.6 följer att artikel 38.4 tredje stycket endast ska tillämpas på program som antas inom ramen för och finansieras genom fleråriga budgetramar efter 2027.

Utredningen uppfattar bestämmelsen så att den är tillämplig vid hantering av EU-medel inom ramen för förvaltningsformen direkt förvaltning tillsammans med medlemsstaterna. RRF hanteras inom ramen för den förvaltningsformen. RRF-förordningen har i praktiken begränsad tillämplighet i tid genom att reformer och investeringar ska ha genomförts till den 31 augusti 2026 och utbetalningar till den 31 december samma år. Mot bakgrund av övergångsbestämmelsen i artikel 277.6 ska artikel 38.4 tredje stycket inte tillämpas på RRF. Det kan dock inte uteslutas att det under kommande programperioder kommer nya fonder och program som Sverige förvaltar inom ramen för förvaltningsformen direkt förvaltning tillsammans med medlemsstaterna. Bestämmelsen kan då bli relevant för Sverige, genom att Sverige då kommer att vara skyldigt att uppfylla det som sägs i bestämmelsen.

Bestämmelsen är formulerad så att medlemsstater ska säkerställa offentliggörande i efterhand av information om deras mottagare på en centraliserad webbplats. Det kan noteras att bestämmelsen inte hade någon motsvarighet i den tidigare budgetförordningen. I skäl 41 till den omarbetade budgetförordningen anges att medlemsstater som tar emot och genomför unionsmedel inom ramen för direkt förvaltning bör tillhandahålla information om sina mottagare i enlighet med budgetförordningen.

Enligt utredningen får bestämmelsen uppfattas som en skyldighet för medlemsstater att – inom ramen för EU-medel som förvaltas enligt direkt förvaltning tillsammans med medlemsstaterna – se till att viss information offentliggörs på den centraliserade webbplatsen. Denna skyldighet synes vara oberoende av innehållet i sektorsspecifika regler.

Den information som ska offentliggöras beskrivs genom en hänvisning till artikel 38.2–3. Artikel 38.2 innehåller en uppräkning av uppgifter som rör mottagare (artikel 38.2 a–c) och om åtgärden (artikel 38.2 d–e). Artikel 38.3 innehåller undantagssituationer då uppgifterna inte ska offentliggöras. Innehållet i dessa bestämmelser behandlas närmare i avsnitt 4.4.3.

Frågan om behov av åtgärder för att Sverige ska kunna uppfylla skyldigheten att säkerställa offentliggörande enligt artikel 38.4 tredje stycket behandlas i avsnitt 8.4.

4.8 Externa aktörers tillgång till lämnade uppgifter

4.8.1 Uppdraget i denna del

Inom ramen för uppdraget att kartlägga och beskriva vilka uppgifter som ska eller får registreras eller annars utbytas i Arachne och inom ramen för Edes, ska utredningen också kartlägga och beskriva i vilken utsträckning som aktörer utanför den egna myndigheten skulle få tillgång till uppgifterna.

Myndigheter som väljer att använda Arachne före 2028 ska ladda upp vissa uppgifter till systemet. Även de uppgifter som kommer att tillgängliggöras enligt artikel 36.6 i budgetförordningen (både obligatoriska och frivilliga uppgifter) avses att föras in i Arachne. Uppdraget i denna del bör därför främst ta sikte på vilken tillgång externa aktörer kan få till uppgifter i Arachne.

När det gäller Edes bedömer utredningen att svenska myndigheter inte på grund av några krav i budgetförordningen kommer att utföra något uppgiftslämnande för tillförande till Edes-databasen. Artikel 36.8 bedöms inte medföra några sådana krav (se avsnitt 4.6). Utredningen tar i detta avsnitt ändå upp några frågor kopplade till Edes.

4.8.2 Olika aktörer kommer att få tillgång till uppgifter via Arachne

Artikel 36.6 i budgetförordningen nämner kommissionen som mottagare, och därmed är kommissionen en av dem som kommer att få tillgång till uppgifter som lämnas med stöd av den artikeln. Genom att uppgifterna kommer att tillföras Arachne, vars databas är tillgänglig för flera aktörer, är det dock inte bara kommissionen som kommer att vara den slutliga mottagaren, trots att bestämmelsen endast nämner tillgängliggörande för kommissionen.

Tillgången till uppgifter som finns i Arachne regleras bland annat i artikel 36.7 andra stycket i budgetförordningen. Enligt bestämmelsen ska åtkomsten till de uppgifter som behandlas av Arachne över-

ensstämma med tillämpliga dataskyddsregler samt respektera principerna om nödvändighet och proportionalitet. Åtkomsten ska begränsas till unionsinstitutioner och organ som genomför budgeten, de medlemsstater som genomför budgeten enligt delad förvaltning, de medlemsstater som tar emot och genomför unionsmedel inom ramen för direkt förvaltning, de personer eller enheter som genomför budgeten inom ramen för indirekt förvaltning samt unionens utrednings-, kontroll- och revisionsorgan, däribland Olaf, revisionsrätten och Eppo, inom ramen för utövandet av deras respektive befogenheter.

Uppgifter som är tillgängliga via Arachne ska göras tillgängliga för Europaparlamentet och rådet från fall till fall i den utsträckning som är nödvändig och står i proportion till utövandet av deras respektive befogenheter, i samband med förfarandet för beviljande av ansvarsfrihet för kommissionen. Sammanfattningsvis kommer andra medlemsstater, deras myndigheter och vissa EU-institutioner att kunna få tillgång till uppgifter som finns i Arachne, under olika förutsättningar.

Arachne-stadgan beskriver närmare vad som avses med programmyndigheter som omfattas av stadgan och kan därmed sägas till viss del precisera vilka nationella myndigheter som kan komma att använda Arachne (se mer i avsnitt 5.3.1). När det gäller styrningen av tillgången till uppgifter ska det säkerställas att den som begär tillgång är del av förvaltnings- eller kontrollsystemet avseende ett specifikt program.

Vidare ger Arachne-stadgan vissa upplysningar om tillgången för EU-organ såsom Olaf, Europeiska unionens revisionsrätt (ECA) och Eppo. Det ges också information om uppgifter som kommissionen kan komma att ta del av. Kommissionen har tillgång till både resultat av riskvärderingar och företagens databas.

I EU:s dataskyddsombuds register över personuppgiftsbehandling finns personuppgiftsbehandlingen avseende Arachne förtecknad, här benämnd beskrivningen av personuppgiftsbehandlingen för Arachne[6]. I den ges också information om tillgång för myndigheter och andra aktörer. Vidare framgår att uppgifter kan överföras till Storbritannien, vilket innebär en tredjelandsöverföring (punkt 6).

[6] Record for processing of personal data, Title: Risk analysis for fraud prevention and detection in the management of EU funds (ARACHNE SYSTEM). Reference: DPR-EC-00598.4, publicerad den 27 november 2023. https://ec.europa.eu/dpo-register/detail/DPR-EC-00598. Hämtat 2025-10-29.

Det finns också frågor och svar avseende Arachne som ger vissa upplysningar (Arachne, Frequently asked questions, version 2.3, den 19 augusti 2022). Som exempel kan nämnas att i de flesta fall har användare i en medlemsstat bara åtkomsträttigheter till program eller planer inom den medlemsstaten, men viss information från andra medlemsstater är tillgänglig, till exempel när ett företag är involverat i flera projekt. En medlemsstat kan också välja att medge andra medlemsstater tillgång till uppgifter om egna program eller planer, vilket kan vara relevant till exempel gällande Interregprogrammen (se fråga 9).

4.8.3 Lämnade uppgifter kommer att få en omfattande spridning

Ovanstående innebär att uppgifter som svenska myndigheter lämnar kommer att få en omfattande spridning. Även om svenska myndigheter i viss mån kommer att kunna påverka vilka som kan få del av uppgifter som de har lämnat – till exempel genom att bevilja andra medlemsstater tillgång till uppgifter om egna program eller planer – bör utgångspunkten vara att utlämnande myndighet inte längre har kontroll över uppgifterna när de har tillgängliggjorts för kommissionen eller förts in i *Arachne*.

Som framgår av avsnitt 4.7 kommer kommissionen enligt artikel 38 att offentliggöra viss information, som härrör från Arachne, och motsvarande kan bli aktuellt även för myndigheter inom ramen för direkt förvaltning tillsammans med medlemsstaterna. Det betyder att uppgifter som svenska myndigheter har lämnat kan komma att offentliggöras och därmed också ges spridning utanför användarkretsen av Arachne. Transparens i fråga om mottagare av EU-medel är av stor vikt och betonas bland annat i budgetförordningens skäl 33 och 34.

När det gäller *Edes* kommer uppgifter att föras in i Edes-databasen. Edes baseras på uppgifter som bland annat rapporteras in av myndigheter via IMS enligt annan reglering än budgetförordningen. Därmed kan det förvisso förväntas att även svenska myndigheters uppgifter kan komma att finnas i Edes-databasen och därmed få en omfattande spridning. Uppgifterna förs dock inte in i Edes direkt av medlemsländerna, utan till exempel av behöriga utanordnare. Som nämns innebär inte heller budgetförordningen några nya krav

på svenska myndigheter att lämna uppgifter för användande i Edes. Frågor som rör dessa uppgifters spridning ligger därmed utanför utredningens uppdrag.

5 Användande av Arachne som verktyg

5.1 Utredningens uppdrag

Utredningens uppdrag som behandlas i detta kapitel är att beskriva vilka myndigheter som kan komma att använda Arachne samt kartlägga och beskriva vilken typ av åtkomst som myndigheterna skulle få vid en användning av Arachne. Utredningen har också i uppdrag att kartlägga vilka regler som styr användningen av Arachne och bedöma vilka skyldigheter som berörda myndigheter skulle få vid en användning av verktyget, vilket sker delvis i detta kapitel.

När det gäller medlemsstaternas och nationella myndigheters förhållande till Arachne bör man skilja mellan å ena sidan att använda systemet i meningen att bereda sig tillgång till det och utnyttja den information som finns där eller kan tas fram därifrån exempelvis vid riskvärderingar och å andra sidan lämnande av uppgifter genom att data tillförs Arachne för att systemet ska kunna generera riskvärderingar. Detta kapitel avser användning av Arachne på det förstnämnda sättet. Frågor som rör lämnande av uppgifter behandlas i kapitel 4 ovan.

Användningen av Arachne är i dag frivillig, så även enligt den omarbetade budgetförordningen. Det är möjligt att det i framtiden blir obligatoriskt för medlemsstaterna att använda systemet. Under alla förhållanden kan det vara ändamålsenligt för svenska myndigheter att använda systemet, även om det inte är obligatoriskt. Utredningen behöver därför ta ställning till vad ett användande av Arachne som verktyg skulle innebära, bland annat när det gäller vilka myndigheter som skulle kunna komma att använda systemet och vilka uppgifter de därvid skulle få tillgång till. Eftersom Arachne är ett existerande verktyg och därmed tillgängligt för användning redan i dag, utgår det EU-rättsliga regelverket och relevanta källor från

att systemet redan används. Även om myndigheter måste tillgängliggöra uppgifter enligt artikel 36.6 i budgetförordningen först från och med 2028, omfattar utredningens bedömningar i flera delar en möjlig användning av Arachne redan före 2028.

I kapitel 7 behandlas regleringen om offentlighet, sekretess och dataskydd, som påverkar användningen av Arachne och innebär skyldigheter för berörda myndigheter vid en användning av verktyget. I avsnitt 8.5 görs överväganden om behovet av åtgärder för att svenska myndigheter ska kunna använda Arachne.

5.2 Närmare om Arachne

5.2.1 Arachne består av olika delar

Arachne är enligt budgetförordningen ett gemensamt integrerat och interoperabelt informations- och övervakningssystem, inbegripet ett gemensamt datautvinnings- och riskgraderingsverktyg, som tillhandahålls av kommissionen och som möjliggör tillgång till och elektronisk automatisk hämtning, registrering, lagring och analys av data om mottagarna av unionsfinansiering, inbegripet deras verkliga huvudmän (artikel 36.2 d). Systemet Arachne innefattar alltså olika delar. Arachne kan förenklat beskrivas som en databas som innehåller information (datautvinningsdelen av verktyget) och ett verktyg för att göra riskvärderingar (riskvärderingsdelen). I viss mån kan dessa delar överlappa bland annat på så sätt att datautvinning kan ske i syfte att risker ska kunna värderas. I syfte att ge en bild av hur Arachne fungerar ges i det följande något förenklade beskrivningar av systemets olika delar.

Datautvinningsdelen

Datautvinningsdelen av Arachne kan beskrivas som de delar där en användare kan ta del av information utan att Arachne gör någon värdering av de risker som informationen kan indikera. Arachne möjliggör i dag sökningar på exempelvis olika projekt, kontrakt, företag och personer. Det är också möjligt att söka på förhållanden mellan olika enheter. Detta möjliggör sökningar på juridiska och organisatoriska kopplingar mellan olika aktörer.

Riskvärderingsdelen

Begreppet riskvärdering

Det kan i sammanhanget nämnas att olika näraliggande begrepp används i budgetförordningen och i andra relevanta källor för att beskriva Arachnes funktion att behandla risker och att presentera ett resultat av den processen, bland annat riskgradering, riskbedömning och riskvärdering. Det kan särskilt uppmärksammas att det i Arachnestadgan (Arachne, Charter for the introduction, the application and the integration of the Arachne risk scoring tool) finns texter som handlar om resultat av riskberäkningar (risk calculations). Utredningen använder huvudsakligen ordet riskvärdering som beskrivning av den process som sker i Arachne automatiskt eller på begäran av en användare och som behandlar olika risker, samt resultatet av den processen.

Riskvärderingar som Arachne genererar automatiskt – redan beviljade medel

Vissa riskvärderingar genereras automatiskt i Arachne. Arachne värderar risker utifrån ett hundratal riskparametrar. Dessa riskvärderingar avser redan beviljade medel, det vill säga fall där exempelvis ett stöd har godkänts beträffande en viss insats och en viss mottagare. Parametrarna är indelade i sju kategorier, nämligen upphandling, avtalsförvaltning, stödberättigande, resultat, koncentration, rimlighet samt anseende och bedrägeri. Riskindikatorerna hjälper förvaltande myndigheter att identifiera de mest riskfyllda projekten, stödmottagarna, leverantörerna och avtalen.

Användaren kan ta del av det sammanlagda värdet för de olika riskerna som hör till en viss kategori eller värdet för varje risk för sig. Risken anges genom en siffra, där en högre siffra innebär en högre risk, samt genom färgkodning, från grön via gul till röd, där röd innebär högst risk.

Användare kan ta del av gjorda riskvärderingar som nås efter inloggning. Användargränssnittet för Arachne kan anpassas av användaren. Användare kan ta del av information om riskvärderingarna via olika informationspaneler (på engelska Dashboards). På dessa informationspaneler visas olika riskindikatorer och vilka poäng eller värden

som är kopplade till respektive riskindikator. Det finns informationspaneler för respektive projekt, kontrakt, stödmottagare och entreprenör. Användaren kan fokusera på specifik information genom att använda olika filter och navigeringsalternativ.

Användare kan ta del av en sammanfattning av riskerna, en ”overall score”. Genom att klicka på olika flikar och ikoner kan användare komma till andra sidor inom Arachne där det finns mer detaljerad information, i flera led. Viss information är sådan som har tillförts Arachne från medlemsländers myndigheter. Informationen är utökad med information från databasen Orbis. Om det förekommer kopplingar till andra bolag får användaren tillgång till information om dessa bolag och ägare med flera personer som har kopplingar till dessa bolag. Sådan information kan komma från Orbis.

Användare kan också få del av externa länkar, exempelvis om någon person förekommer på en lista med personer i politiskt utsatt ställning (en så kallad PEP-lista, se närmare avsnitt 5.4.2) eller verkställighetslista. Arachne innehåller då länkar till de internetsidor där aktuell information finns allmänt tillgänglig.

Det finns också en modul för *ärendehantering* (Case management), där information om ett visst projekt kan erhållas, inklusive riskutvecklingen över tid för projektet. Vilka funktioner som är tillgängliga för en användare kan variera beroende på vilken roll användaren tilldelats av den lokala administratören.

Via en särskild meny kan en användare ta del av *historisk information* om hur riskvärderingen för ett visst projekt eller kontrakt har utvecklats. Genom denna meny kan användaren ta fram riskvärderingar som har gjorts i Arachne vid tidigare tidpunkter. Data från en tidigare riskvärdering kan exporteras till exempelvis en excel-fil.

Då Arachne är under utveckling kan funktioner och dess användargränssnitt komma att förändras.

Riskvärderingar som begärs av en användare inom ramen för förhandsfunktionen – ex ante

Arachne innehåller en så kallad förhandsfunktion (the ex-ante functionality), som ger användare möjlighet att – under processen att välja vilka som ska tilldelas EU-medel – göra en värdering av vilka risker det skulle innebära om en viss enhet skulle tilldelas EU-medel.

Riskvärderingar inom ramen för förhandsfunktionen kan bara göras på begäran av en användare. Arachne genererar således inte sådana riskvärderingar automatiskt. Endast användare som har tilldelats behörighet kan begära sådana riskvärderingar. Till skillnad från de riskvärderingar som Arachne genererar automatiskt sker inte heller någon automatisk löpande uppdatering av riskvärderingar inom ramen för förhandsfunktionen. Sådana riskvärderingar går bara att göra beträffande projekt, inte mottagare, kontrakt eller entreprenörer.

Det går till så att användaren laddar upp viss information om projektet, potentiell mottagare, eventuell verklig huvudman, entreprenör och projektkostnad till Arachne. Detta kan göras antingen genom att användare skapar en så kallad XML-fil eller genom att använda en särskild funktion för redigering av data (Dataset editor). När informationen har laddats upp gör Arachne en riskvärdering utifrån underlaget över natten. Morgonen därpå finns riskvärderingen tillgänglig i Arachne. En begäran om en sådan riskvärdering loggas i Arachne.

Informationspanelen där resultatet av riskvärderingen presenteras (the ex-ante dashboard) liknar informationspanelen för riskvärderingar som Arachne genererat automatiskt för ett projekt och det är på liknande sätt möjligt för användare att navigera och ta del av mer detaljerad information. Vid en sådan riskvärdering ges inte utfall beträffande alla riskindikatorer som är aktuella i de riskvärderingar som Arachne genererar automatiskt. De tillgängliga kategorierna är avtalsförvaltning, koncentration samt anseende och bedrägeri. Därutöver finns information om datum för uppladdningen av data och riskvärderingen och om den användare som laddat upp data och begärt riskvärderingen. Tidigare gjorda riskvärderingar inom ramen för förhandsfunktionen är sökbara på bland annat dessa kriterier.

En användare har tillgång till de egna tidigare gjorda riskvärderingarna. Gjorda riskvärderingar blir – som utredningen uppfattat det – tillgängliga också för medarbetare som har samma behörighet som användaren. Informationen raderas inte men lagringstiden får – liksom för Arachne i övrigt – inte överstiga tio år (artikel 36.7 fjärde stycket i budgetförordningen). Sådana uppgifter som användare laddar upp inom ramen för förhandsfunktionen tillförs inte Arachne på ett sådant sätt att de ligger till grund för sådana riskvärderingar som Arachne genererar automatiskt.

5.2.2 Endast indikationer på risker – ej krav på agerande från myndigheterna

Arachne är ett hjälpmedel. Verktyget syftar inte till att bedöma stödmottagares individuella beteenden eller till att stödmottagare ska uteslutas per automatik. Verktyget avser att varna för risker för att ge mer underlag för förvaltningskontroller, men det ger *inga bevis* för att fel, oegentligheter eller bedrägerier föreligger. Detta framgår direkt av kommissionens webbsida om Arachne.[1]

Myndigheter kan också ta hänsyn till riskvärderingar i sina strategier för bedrägeribekämpning och kontrollförfaranden.

Eftersom Arachne endast är ett hjälpmedel kan kommissionen – om myndigheter underlåter att agera – endast uppmuntra dem att använda Arachne och kontrollera att andra proportionella och effektiva åtgärder för bedrägeribekämpning genomförs (se Arachne, FAQ on data protection and related issues, Status as of 10th July 2024[2]).

5.2.3 Arachne är under utveckling och är tänkt att bygga på interoperabilitet

Som framgår av avsnitt 3.4.3 har Arachne utvecklats under åren och är fortsatt under utveckling. Utöver vad som anges i det avsnittet kan nämnas att budgetförordningens skäl 29–32 beskriver hur systemet är tänkt att fungera. Som utredningen uppfattar det beskrivs både sådana förändringar som den omarbetade budgetförordningen innebär och vad en framtida utveckling av systemet kan medföra. Av de nämnda skälen framgår att elektronisk registrering och lagring av uppgifter om mottagarna av unionsfinansiering, inbegripet deras verkliga huvudmän, i Arachne bör underlätta riskbedömning för urval, tilldelning, ekonomisk förvaltning, övervakning, utredning, kontroll och revision och bidra till att effektivt förebygga, upptäcka, korrigera och följa upp oriktigheter, inte minst bedrägerier, korruption, intressekonflikter och dubbelfinansiering.

Enligt de nämnda skälen bör Arachne också utvecklas i syfte att undvika dubbelrapportering och minska den administrativa bördan för medlemsstaterna och andra genomförandeenheter. Kommissionen

[1] https://employment-social-affairs.ec.europa.eu/policies-and-activities/funding/european-social-fund-plus-esf/what-arachne_en. Hämtat 2025-10-23.
[2] https://employment-social-affairs.ec.europa.eu/policies-and-activities/funding/european-social-fund-plus-esf/what-arachne_en. Hämtat 2025-10-23.

bör ansvara för utveckling, förvaltning och övervakning av systemet. Det bör bygga på interoperabilitet, varigenom aktuell information och uppgifter om mottagare av unionsmedel bör hämtas automatiskt från och överföras till det systemet, i realtid när så är möjligt.

5.3 Vilka svenska myndigheter kan komma att använda Arachne?

5.3.1 Vissa utgångspunkter

Som framgår av avsnitt 5.1 ska utredningen beskriva vilka myndigheter som kan komma att använda Arachne. Det är dock inte möjligt för utredningen att ange en uttömmande uppräkning av vilka myndigheter som kan komma att använda Arachne. En frivillig användning av Arachne är möjlig redan i dag. Eftersom användningen av Arachne är frivillig även i den omarbetade budgetförordningen finns ingen reglering som pekar ut vilka aktörer som *ska* använda systemet. Utredningen om hantering av EU-medel har föreslagit ett antal ändringar avseende vilka myndigheter som ska förvalta medel från olika fonder (SOU 2024:22). Förslagen bereds i Regeringskansliet. Vidare kommer nya sektorsspecifika regler inför den nya programperioden och därmed kan potentiellt nya berörda myndigheter tillkomma.

Budgetförordningen ger ändå en del vägledning om vilka som kan komma att använda systemet. Enligt artikel 36.7 i budgetförordningen ska åtkomsten till uppgifter i Arachne begränsas till vissa mottagare, bland andra unionsinstitutioner och organ som genomför budgeten samt de medlemsstater som genomför budgeten inom ramen för delad förvaltning och som tar emot och genomför unionsmedel genom direkt förvaltning tillsammans med medlemsstaterna.

Enligt utredningens mening bör utgångspunkten vara att samtliga enheter som har någon roll i att avgöra vem som ska ta emot stöd eller i att i efterhand vidta kontroller av utbetalade stöd har nytta av att använda de system som finns tillgängliga. Däremot bör det i allmänhet saknas anledning för en enhet att använda Arachne om enheten inte har en sådan roll utan till exempel endast verkställer en utbetalning av ett redan beslutat stöd. Inte heller myndigheter som endast mottar stöd har någon anledning att kunna använda Arachne. En annan utgångspunkt bör vara att myndigheter kan kom-

ma att använda Arachne inom ramen för ärendehandläggning – exempelvis ett ärende om återkrav av felaktigt utbetalat stöd – eller inom ramen för så kallat faktiskt handlande, vilket i nu aktuella fall exempelvis kan vara när myndigheter ska välja vilka stöd som bör bli föremål för en närmare kontroll.

Arachne-stadgan utgår från en pågående användning av Arachne. Stadgan ger också vägledning i fråga om tänkta användare av Arachne. I stadgan används begreppet ”programmyndigheterna” för att beskriva dem som åtar sig att följa principerna i dokumentet. I punkten 1 anges vilka som avses med programmyndigheter, uppdelat på följande fonder och program.

a) ESI-fonderna: Förvaltande myndigheter, förmedlande organ, attesterande myndigheter och revisionsmyndigheter

b) CAP: Utbetalande organ och revisionsmyndigheter

c) RRF: Samordnings- och genomförandeorgan och revisionsmyndigheter

d) Andra myndigheter som är involverade i genomförandet av BAR och EGF.

I punkt 2 i stadgan anges att ESI-fondernas programmyndigheter godtar att införliva riskvärderingsverktyget Arachne som en av sina åtgärder för att motverka bedrägerier enligt bland annat CPR, att samordnings- och genomförandeorganen för RRF gör motsvarande enligt kraven i RRF-förordningen och att utbetalande organ för CAP gör detta enligt CAP-förordningen. Av punkt 3 i stadgan framgår att programmyndigheterna som får tillgång till resultaten av Arachnes riskberäkningar bara ska använda dessa för förvaltningskontroller (management verifications), kontroller (controls) och revisioner (audits). Resultaten ska inte användas för personliga intressen eller några andra ändamål. Dessa skrivningar talar för att kretsen som använder Arachne bör begränsas till dem som verkligen har behov av verktyget i sin handläggning eller sitt kontrollarbete.

Även punkt 10 ger vägledning, där det talas om skyldigheter för förvaltande myndigheter att vidta åtgärder enligt CPR och motsvarande för samordnings- och genomförandeorganen för RRF enligt RRF-förordningen och utbetalande organ enligt CAP-förordningen. Det sägs också att efter officiella instruktioner från dessa myndig-

heter kommer kommissionen att ge lokala administratörsrättigheter till utsedda användare. De lokala administratörerna ska ha rätt att bevilja tillgång till Arachne för lokala användare hos förvaltande myndigheter, attesterande myndigheter, revisionsmyndigheter och förmedlande organ för ESI-fonderna, samordnings- och genomförandeorgan för RRF, utbetalande organ för CAP och andra myndigheter som är involverade i genomförandet av BAR och EGF. Den lokala administratören ska säkerställa att de som begär tillgång till systemet verkligen är en del av förvaltningen och kontrollen av det aktuella programmet.

Nedan görs mot denna bakgrund en genomgång av myndigheter i Sverige som bedöms kunna ha användning av Arachne som ett led i att uppfylla målet i budgetförordningen att motverka oriktigheter och som har någon roll i att avgöra vem som ska ta emot stöd eller i att i efterhand vidta kontroller av utbetalade stöd.

Som nämns ovan lämnar inte utredningen någon uttömmande uppräkning av vilka myndigheter som kan komma att använda Arachne. Utredningen gör dock övergripande bedömningar om vilka slags myndigheter det bör vara fråga om. Utifrån dessa bedömningar bör det gå att dra slutsatser om det finns anledning för olika myndigheter att använda Arachne, utifrån de uppgifter de har och eventuellt kan komma att få. Utredningen fokuserar särskilt på vissa myndigheter som bedöms vara särskilt centrala för en användning av Arachne. Dessa myndigheter bedöms också sannolikt vara aktuella för att delta i genomförandet av EU:s budget även under kommande programperiod och har varierande roller i budgetgenomförandet.

5.3.2 Myndigheter som hanterar EU-medel genom delad förvaltning

Förvaltande myndigheter och utbetalande organ är myndigheter som på nationell nivå ansvarar för att EU-medel hanteras på rätt sätt och därmed har särskilda skyldigheter att skydda EU:s budget, som Arachne är ett stödjande system för. Därmed förväntas dessa myndigheter ha nytta av att använda systemet. I det här betänkandet väljer utredningen att utgå från nu gällande fördelning av ansvar för medel och fonder.

Som beskrivs i avsnitt 3.5 förvaltar främst följande svenska myndigheter i dag EU-medel genom delad förvaltning: Jordbruksverket,

Migrationsverket, Polismyndigheten, Svenska ESF-rådet, Tillväxtverket samt länsstyrelserna i Jämtlands, Västerbottens och Norrbottens län. Vad som kommer att gälla för den programperiod som börjar 2028 står dock inte klart. Enligt utredningen tyder för närvarande inget på något annat än att dessa åtta myndigheter kommer att vara förvaltande myndigheter och utbetalande organ avseende EU-fonder även under kommande programperiod.

Flera myndigheter har delegerats uppgifter från förvaltande myndigheter. Jordbruksverket har till exempel delegerat uppgifter som handläggning och kontroll av ersättningsanspråk till länsstyrelserna, Skogsstyrelsen och Sametinget. Det förhållandet att ansvaret ligger kvar på Jordbruksverket skulle kunna tala för att dessa myndigheter (så kallade delegerade organ) i den egenskapen inte skulle behöva eller ha anledning att använda Arachne. Som utredningen uppfattar saken kan dock dessa myndigheter ha en sådan självständig roll i besluten om ersättning att de skulle ha nytta av att använda Arachne i sin handläggning.

Som annat exempel kan nämnas att Havs- och vattenmyndigheten är förmedlande organ för havs-, fiskeri- och vattenbruksprogrammet. Myndigheten bedöms i denna roll ha nytta av att använda Arachne.

5.3.3 Myndigheter som hanterar medel genom direkt förvaltning tillsammans med medlemsstaterna

Inom förvaltningsformen direkt förvaltning förvaltar kommissionen på egen hand EU-fonder. Det innebär som huvudregel att i de fallen har medlemsstaterna och deras myndigheter inte skäl att använda Arachne.

RRF förvaltas dock genom direkt förvaltning tillsammans med medlemsstaterna. De 62 genomförandemyndigheterna för RRF består av tio rapporterande myndigheter, samtliga länsstyrelser och 31 lärosäten. De tio rapporterande myndigheterna är Boverket, Myndigheten för digital förvaltning, Myndigheten för yrkeshögskolan, Naturvårdsverket, Post- och telestyrelsen, Skolverket, Socialstyrelsen, Statens energimyndighet, Trafikverket samt Universitetskanslersämbetet (se vidare avsnitt 3.5.4 och tabell 3.3). Det kan nämnas att regeringen har gett dessa tio myndigheter i uppdrag att besvara ett antal frågor som avser deras eventuella användning av Arachne. Regeringsuppdragen redovisades i slutet av 2024. Myndigheterna

har analyserat hur de kan använda Arachne och redogjort för sin syn på de rättsliga förutsättningarna att använda Arachne, utifrån respektive myndighets reglering.

Länsstyrelserna ansvarar för handläggning, beslutsfattande och uppföljning till exempel avseende stöd som Boverket har ett särskilt ansvar för.

Svaret på frågan i vilken mån som genomförandemyndigheterna kan ha anledning att använda Arachne är delvis beroende av om respektive myndighet kan sägas ha någon roll i att avgöra vem som ska ta emot stöd eller i att i efterhand vidta kontroller av utbetalade stöd. Som utredningen uppfattar det kan förhållandena se olika ut inom ramen för olika åtgärder inom RRF och saken bör bedömas från fall till fall.

I allmänhet bör de rapporterande myndigheterna ha en sådan roll att de kan ha anledning att använda Arachne. Detsamma gäller länsstyrelserna. Utredningen har inte identifierat behov för lärosätena att använda Arachne inom ramen för RRF.

Det bör observeras att Arachne kan sägas ha en endast begränsad användningstid avseende RRF-medel, eftersom reformer och investeringar från RRF-medlen ska ha genomförts till den 31 augusti 2026 och utbetalningar till den 31 december samma år. Från och med 2027 kommer det därför endast bli fråga om ett användande för kontroller ex post.

Det kan inte uteslutas att det framöver tillkommer andra EU-fonder som har en liknande särskild förvaltningsform. Även de myndigheter som förvaltar dessa fonder kan då få anledning att använda Arachne.

5.3.4 Ekonomistyrningsverket

Som utsedd revisionsmyndighet ansvarar ESV för att granska att myndigheter hanterar EU-medel i enlighet med både EU:s och Sveriges regelverk. ESV gör detta genom att granska både hur myndigheterna förvaltar fonderna och att utbetalningar för enskilda projekt och insatser är korrekta. ESV ska också granska genomförandet av den svenska återhämtningsplanen inom ramen för RRF.

Med anledning av sina uppdrag bedömer utredningen att ESV har skäl att använda Arachne, till exempel vid sina revisioner.

5.3.5 Ekobrottsmyndigheten och Polismyndigheten

Ekobrottsmyndigheten och Polismyndigheten är brottsbekämpande myndigheter och det är av stort intresse för dessa aktörer att det finns effektiva system som motverkar felaktiga utbetalningar och bedrägerier. Det kan dock nämnas att Eppo är EU:s oberoende åklagarmyndighet som ska skydda EU:s budget och väcka talan när det gäller brott som skadar EU:s ekonomiska intressen, och brottsanmälan kan göras direkt till Eppo. Eppo utreder och lagför brott och fungerar som åklagare vid de behöriga domstolarna i de medlemsländer som deltar i det fördjupade samarbetet om Eppo.

Frågan kan ställas om Ekobrottsmyndigheten och Polismyndigheten har skäl att använda Arachne. Artikel 36.7 andra stycket i budgetförordningen anger vilka aktörer som åtkomsten till uppgifter i Arachne ska begränsas till. Den bestämmelsen nämner inte nationella brottsbekämpande myndigheter. Av Arachne-stadgan framgår att rätt till åtkomst bara får ges till den som är en del av förvaltnings- eller kontrollsystemet avseende ett program, se punkt 10. Motsvarande framgår också av kommissionens frågor och svar om Arachne, där en fråga avser huruvida myndigheter som inte är direkt involverade i genomförandet av vissa fonder men deltar i kontroll eller revision av fondmedlen kan få tillgång till Arachne. Frågan exemplifierades med brottsbekämpande myndigheter och överordnad revisionsmyndighet (Arachne, Frequently asked questions, version 2.3, den 19 augusti 2022, fråga 2).

Utredningen bedömer därför, som nu gällande regelverk ser ut, att varken Ekobrottsmyndigheten eller Polismyndigheten i sin brottsbekämpande roll tillhör de myndigheter som kan komma att få tillgång till och använda Arachne. Även om det skulle kunna finnas ett stort intresse för myndigheterna att få direkt tillgång till uppgifter i Arachne har de inte rätt till åtkomst till systemet.

En eventuell framtida möjlighet till användning är inte helt utesluten.

I vilken mån som uppgifter kan lämnas över till de brottsbekämpande myndigheterna från andra myndigheter som använder Arachne får bedömas från fall till fall utifrån regelverken om sekretess och dataskydd, och utreds inte närmare här.

5.3.6 Departement som behörig eller samordnande myndighet

Landsbygds- och infrastrukturdepartementet har en roll som behörig myndighet enligt förordningen (2022:1826) om EU:s gemensamma jordbrukspolitik. Departementet har i den rollen som uppgift att bland annat övervaka att Jordbruksverket sköter sina uppgifter avseende jordbruksfonderna. För detta tar departementet del av bland annat ESV:s rapporter. Departementets kontrollarbete sker enligt utredningens mening inte på en sådan nivå att departementet har skäl att bedöma enskilda projekt genom en användning av Arachne. Rollen som behörig myndighet medför inte heller sådana uppgifter som ger skäl att använda Arachne.

Inte heller Finansdepartementets roll som samordnande myndighet för genomförandet av återhämtningsplanen inom ramen för RRF innebär något behov att använda Arachne.

Utredningen har således inte funnit skäl för Regeringskansliet att i dag eller enligt gällande regelverk och kontrollstruktur använda Arachne. Framtida förändringar i departementens roller eller i regleringen om tillgång till Arachne kan medföra en annan bedömning.

5.3.7 Slutsatser om vilka myndigheter som kan komma att använda Arachne

Sammanfattningsvis bedömer utredningen att följande slags myndigheter kan komma att använda Arachne.

- De myndigheter som deltar i genomförandet av budgeten inom ramen för delad förvaltning och därvid har någon roll i tilldelning av medel eller kontroll av utbetalda medel.
- De myndigheter som inom ramen för RRF deltar i genomförandet av budgeten och därvid har någon roll i tilldelning av medel eller kontroll av utbetalda medel, samt de myndigheter som i framtiden eventuellt kommer att på det sättet förvalta EU-fonder med en liknande förvaltningsform, det vill säga genom direkt förvaltning tillsammans med medlemsstaterna.
- De myndigheter som har i uppgift att i efterhand genomföra granskningar eller revisioner av utbetalade stöd, såsom ESV i egenskap av revisionsmyndighet.

5.4 Åtkomst till uppgifter vid användande av Arachne

5.4.1 Uppdraget i denna del

Utredningens uppdrag i denna del beskrivs så att utredaren ska kartlägga och beskriva vilken typ av åtkomst de aktuella myndigheterna, vid användning av Arachne, skulle få till uppgifter i Arachne när dessa används som ett led i handläggningen av ärenden eller vid kontrollåtgärder, med beaktande av eventuella begränsningar avseende vilka sökningar som får göras i systemet eller för vilka ändamål personuppgiftsbehandling får ske. När det gäller uppdraget att beskriva typ av åtkomst uppfattar utredningen det så att det avser vilka slags uppgifter myndigheterna skulle få tillgång till.

För att kunna avgöra vilken åtkomst till uppgifter som svenska myndigheter skulle få vid en användning av Arachne är det lämpligt att först klarlägga vilka uppgifter det totalt sett finns inom systemet. Därefter bör det analyseras om svenska myndigheter har åtkomst till denna totala uppgiftsmängd, eller om användarbegränsningar och liknande skulle begränsa åtkomsten.

Det bör noteras att det nu är fråga om svenska myndigheters tillgång till uppgifter vid användning av Arachne. Även avsnitt 4.8 behandlar frågor om åtkomst till uppgifter men där behandlas uppdraget som rör åtkomst som andra aktörer kan få till uppgifter som svenska myndigheter lämnar. Båda avsnitten berör i stor utsträckning samma bestämmelser i budgetförordningen och information i andra relevanta källor.

5.4.2 Vilka uppgifter finns totalt sett i Arachne?

Arachne innehåller uppgifter med olika ursprung

Uppgifterna i Arachne består i dagsläget av både så kallade interna data och externa data. Det interna datainnehållet består av data från de deltagande medlemsstaterna och från kommissionen. Vidare innehåller Arachne externa data från olika kommersiella databaser, nämligen Orbis och World Compliance.

Uppgifter från medlemsstaterna

Till att börja med innehåller Arachne data från medlemsstaterna om beviljade medel. Det framgår av punkt 11 i Arachne-stadgan att programmyndigheterna ska ombesörja överföring av data i enlighet med kraven i Arachne och enligt specifikation i vissa angivna sektorsspecifika förordningar. Det ska ske i XML-format, på regelbunden basis, minst var tredje månad. I punkten anges också att programmyndigheterna på frivillig basis får utöka mängden datafält och därmed överföra ytterligare data till Arachne.

Användningen är i dag frivillig och det är först genom artikel 36.6 i budgetförordningen som det kan sägas beredas väg för ett mer strukturerat uppgiftslämnande och därmed strukturerat införande av uppgifter i Arachne. Uppgifterna i Arachne från medlemsstaterna är i dag därmed inte på något sätt heltäckande.

Som utredningen uppfattar det är avsikten att uppgiftslämnandet när det gäller beviljade medel framöver ska ske i form av tillgängliggörande av uppgifter till kommissionen i enlighet med artikel 36.6 i budgetförordningen (se avsnitt 4.4.5). Arachne kommer då att innehålla de uppgifter som medlemsstaterna tillgängliggör, både rättsligt obligatoriska och frivilliga uppgifter. Vilken information som är obligatorisk att lämna enligt artikel 36.6 varierar i viss mån på grund av de olika sektorsspecifika regelverken, på det sätt som framgår av tabell 4.1.

I tabell 4.1 saknas hänvisningar till RRF, eftersom artikel 36.6 inte medför någon skyldighet att tillgängliggöra uppgifter enligt det regelverket då reformer och investeringar från RRF-medlen ska ha genomförts innan skyldigheterna i artikel 36.6 ska börja tillämpas. Uppgifter som medlemsstaterna ska registrera och lagra enligt RRF-förordningen skulle kunna finnas eller föras in i Arachne på frivillig basis, det vill säga även om en sådan skyldighet inte finns. De uppgifterna framgår nedan av tabell 5.1. Beträffande RRF kan det också vara aktuellt att utföra kontroller i efterhand och det kan då vara relevant att använda Arachne.

Tabell 5.1 Krav på lagring i RRF i förhållande till kraven på tillgängliggörande i budgetförordningen

Med angivande av artiklar i budgetförordningen och RRF

Uppgift	BF	RRF
Om mottagaren		
Om mottagaren är en fysisk eller juridisk person	36.6.a + 38.2 a	
Mottagarens namn och, för juridisk person, unik identifieringskod	36.6.a + 38.2 b och 38.6 2 st	22.2 d(i) 25a.2 a–b
Födelsedatum för fysisk person	36.6.a	
Var mottagaren finns, det vill säga i) mottagarens adress, om mottagaren är en juridisk person, ii) regionen på Nuts 2-nivå, om mottagaren är en fysisk person med hemvist i unionen, eller landet, om mottagaren är en fysisk person och inte har hemvist i unionen	36.6.a + 38.2 c	
Om åtgärden		
Det belopp för vilket ett åtagande gjorts och, om det rör sig om ett åtagande med flera mottagare, fördelningen av detta belopp per mottagare, om den finns tillgänglig	36.6 b + 38.2 d	22.2 d(iv) 25a.2 c
Åtgärdens art och ändamål	36.6 b + 38.2 e	
Insatsens unika identifieringskod	36.6 b	
Om verklig huvudman		
Om mottagarens verkliga huvudmän när mottagaren inte är en fysisk person: förnamn, efternamn, födelsedatum, och registreringsnummer för mervärdesskatt eller skatteregistreringsnummer om sådana finns, eller en annan unik identifieringskod på landsnivå	36.6 c	22.2d(iii)

Källa: Egen sammanställning.

Den information som kan lämnas på frivillig basis är begränsad till de förangivna datafält som finns tillgängliga för överföring och motsvarar till viss del de typer av uppgifter som anges i artikel 36.6. Se avsnitt 4.5.1 närmare om detta. Till de frivilliga uppgifter som medlemsländerna kan lämna hör uppgifter om ”related people”, vilket kan översättas med anknutna personer. Det kan handla om personer som är anställda hos myndigheter som prövar ansökningar om stöd. Uppgifter om sådana personer kan användas i Arachne för att göra riskvärderingar.

Det kan i sammanhanget nämnas att sådana uppgifter som användare laddar upp i Arachne inom ramen för den så kallade förhandsfunktionen inte tillförs Arachne på ett sådant sätt att de ligger till grund för andra användares riskvärderingar. Gjorda riskvärderingar inom ramen för förhandsfunktionen blir dock tillgängliga också för medarbetare som har samma behörighet som användaren (se avsnitt 5.2.1).

Sammanfattningsvis innehåller Arachne den information som har lämnats av medlemsländerna. Från och med 2028 kommer det att handla om dels den information som medlemsländerna måste lämna enligt artikel 36.6 i budgetförordningen, dels den information som medlemsländerna lämnar på frivillig basis.

Uppgifter från kommissionen

Arachne omfattar också data från FTS (the Financial Transparency System), som innehåller uppgifter om mottagare av medel som lämnas av kommissionen när det gäller fonder som är föremål för indirekt och direkt förvaltning samt den europeiska utvecklingsfonden (EUF, på engelska the European Development Fund). Den sistnämnda fonden har varit ett instrument för att finansiera utvecklingssamarbete med länder i Afrika, Västindien och Stillahavsområdet samt utomeuropeiska länder och territorier.

Arachne innehåller också information från kommissionens system för utbyte av information om mervärdesskatt. Systemet kallas VIES, vilket är en förkortning för VAT Information Exchange System. Genom VIES är det möjligt att kontrollera om ett momsregistreringsnummer är giltigt. VIES är inte en databas utan ett sökverktyg och vid sökning i VIES hämtas uppgifterna från nationella momsdatabaser.

VIES skickar en förfrågan om registreringsnummer till den relevanta nationella databasen för att kontrollera om numret finns registrerat där. Om så är fallet meddelar VIES att numret är giltigt, annars att det är ogiltigt. VIES informerar bara om ett registreringsnummers giltighet vid tidpunkten för kontrollen. Beroende på landets dataskyddsregler visas eventuellt också näringsidkarens namn och adress så som de är angivna i den nationella databasen (se lagråds-

remissen Åtgärder mot mervärdesskattebedrägerier, lämnad till Lagrådet den 9 oktober 2025, s. 21).

Uppgifter från databasen Orbis

Orbis är en global kommersiell databas som innehåller information om cirka 550 miljoner företag. Informationen avser bland annat finansiell information som omsättning och solvensgrad samt indikatorer som rör finansiell trovärdighet och konkursrisk. Databasen innehåller vidare information om cirka 450 miljoner personer, exempelvis ägare och styrelseledamöter, och omfattar uppgifter om namn, födelsedatum samt funktioner och under vilka perioder personerna innehaft funktionerna. Det går också att se vilka kopplingar som finns mellan olika bolag och olika personer. Exempelvis går det att se hur många bolag en person har koppling till. Databasen innehåller även historiska data.

Information i Orbis härrör från offentlig information såsom årsredovisningar och balansräkningar som har lämnats in till myndigheter. Detaljnivån på uppgifterna varierar mellan olika länder och beroende på företagens storlek. Databasen uppdateras i Arachne var tredje månad. Alla data i Orbis är i dag tillgängliga för sökningar i Arachne. I framtiden är – som utredningen uppfattat det – avsikten att data i Orbis endast ska vara tillgängliga för användare beträffande sådana projekt som användaren hanterar.

Uppgifter från databasen World Compliance

Databasen bygger på uppgifter från olika källor

Arachne innehåller också uppgifter från databasen World Compliance, som tillhandahålls kommersiellt av LexisNexis Risk Solutions, Inc. I databasen samlas, aggregeras och centraliseras cirka 2,5 miljoner profiler från olika källor. Källorna härrör från myndigheter i olika länder, med undantag för information om negativ publicitet, se nedan. Databasen uppdateras i Arachne var tredje månad. Denna databas kan sägas innehålla känsligare information än Orbis.

PEP – politiskt utsatta personer

Databasen World Compliance innehåller uppgifter om personer med så kallad PEP-status. PEP är en förkortning för Politically Exposed Persons, på svenska ofta kallade personer i politiskt utsatt ställning. Begreppet definieras i 1 kap. 8 § lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism (penningtvättslagen) som en fysisk person som har eller har haft en viktig offentlig funktion i en stat eller i en internationell organisation (definitionen har sitt ursprung i det EU-rättsliga regelverket mot penningtvätt, se prop. 2008/09:70 s. 183).

Databasen innehåller också information om de politiskt utsatta personernas familjemedlemmar och nära medarbetare.

Sanktionslistor och verkställighetslistor

Databasen innehåller vidare uppgifter om sanktioner och samlar in information från flera sanktionslistor över hela världen, bland annat från EU och FN. Det kan exempelvis handla om en myndighets lista på företag som brutit mot upphandlingsregler.

Dessutom innehåller databasen vad som på engelska kallas en Enforcement List, vilket kan översättas till en verkställighetslista. Den innehåller uppgifter från material från myndigheter över hela världen som avser exempelvis varningar och åtgärder som har vidtagits mot individer och företag. Det handlar bland annat om EU:s terroristförteckning och underlag från Interpol och amerikanska FBI.

Negativ publicitet

Databasen innehåller också information om så kallad Adverse Media, vilket kan översättas med negativ publicitet. I detta avseende omfattar World Compliance en egen databas med profiler som i nyhetsmedia har länkats till olaglig verksamhet från över 30 000 flöden över hela världen.

Hur information från databasen erhålls

Det går inte att söka på enskilda personer eller företag för att se om information om dem finns på de olika listorna. Om en person eller ett företag är involverat i ett projekt som en myndighet hanterar framgår det i riskvärderingar som görs genom Arachne. Det finns riskindikatorer som tar sikte på förekomst i de olika listorna som ingår i databasen. Förekommer en person eller ett företag exempelvis i en artikel som ingår i databasen om negativ publicitet får myndigheten tillgång till den artikeln.

Gjorda riskvärderingar sparas i Arachne

Ett uppgiftsslag som finns i Arachne och som är centralt i detta betänkande är så kallade riskvärderingar (se om begreppet i avsnitt 5.2.1).

Enligt utredningen får i begreppet anses ingå både de ”poäng” eller värden som en viss aktör får beträffande en viss riskindikator samt den bakomliggande informationen som ligger till grund för värderingen. Det innebär att den information som en användare får del av om kopplingar till andra bolag samt om de bolag och personer som berörs ingår, liksom den information som nås via länkar till externa källor. Även information från databaserna Orbis och World Compliance kan alltså ingå i riskvärderingen.

Arachne, som det fungerar för närvarande, gör löpande veckovisa riskvärderingar för pågående projekt. Även de historiska resultaten av gjorda riskvärderingar sparas i Arachne. Det innebär att det går att ta fram information om vilka riskerna var beträffande ett visst projekt vid en viss tidpunkt i det förflutna, något som kan vara användbart exempelvis vid efterhandskontroller.

Även gjorda riskvärderingar inom ramen för den så kallade förhandsfunktionen sparas i Arachne, men åtkomsten till dem är mer begränsad.

5.4.3 Vilka begränsningar i åtkomsten ställs upp?

Begränsningar som avser dataskyddsregelverket

Artikel 36.7 andra stycket i budgetförordningen innehåller bestämmelser som begränsar åtkomsten till uppgifter i Arachne. Där anges till att börja med att åtkomsten till de uppgifter som behandlas av Arachne ska överensstämma med tillämpliga dataskyddsregler. Vidare anges att åtkomsten ska respektera principerna om nödvändighet och proportionalitet. Här kan frågan ställas om därmed avses något annat än dessa principer inom dataskyddsregelverket. Ordet nödvändig används i anslutning till flera av de rättsliga grunderna i artikel 6 i EU:s dataskyddsförordning[3], här benämnd dataskyddsförordningen. En behandling ska exempelvis enligt artikel 6.1 c vara nödvändig för att fullgöra en rättslig förpliktelse. Flera av dataskyddsförordningens bestämmelser innebär också krav på proportionalitet, se exempelvis artiklarna 6.3 och 35.7 om konsekvensbedömning. Utredningen gör bedömningen att det som sägs i artikel 36.7 andra stycket i budgetförordningen tar sikte på principerna om nödvändighet och proportionalitet inom ramen för dataskyddsregelverket och alltså inte har någon därutöver självständig betydelse.

Dataskyddsregelverket kan sägas innebära generella begränsningar i åtkomsten till uppgifter i Arachne. Exempelvis finns det ett förbud i svensk rätt mot sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter. Förenligheten med dataskyddsregelverket vid en användning av Arachne behandlas i avsnitt 8.5.8.

Begränsningar som tar sikte på vissa mottagare

Vissa mottagare pekas ut i artikel 36.7 i budgetförordningen

Förutom de ovan nämnda hänvisningarna till dataskyddsregelverket anges i artikel 36.7 andra stycket också att åtkomsten till uppgifter i Arachne ska begränsas till vissa typer av mottagare. Bland dem som åtkomsten ska begränsas till, såvitt berör svenska aktörer, är de medlemsstater som genomför budgeten med delad förvaltning (enligt artikel 62.1 första stycket b) och de medlemsstater som tar emot och

[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).

genomför unionsmedel vid direkt förvaltning (enligt artikel 62.1 första stycket a).

Utredningen konstaterar därför att medlemsländer som förvaltar EU-medel med delad förvaltning tillhör de som kan få ta del av uppgifter i Arachne. Även medlemsländer som tillsammans med kommissionen hanterar EU-medel vid direkt förvaltning kan ta del av uppgifterna, vilket har betydelse för RRF.

Användare har i allmänhet begränsad behörighet till uppgifter som kommer från andra medlemsländer

Användare av Arachne har bara tillgång till de uppgifter för vilka de har fått behörighet av en lokal administratör. Av Arachne-stadgan framgår att rätt till åtkomst till Arachne bara får ges till den som är en del av förvaltnings- eller kontrollsystemet avseende ett program, se punkt 10. Motsvarande framgår också av frågor och svar om Arachne (Arachne, Frequently asked questions, version 2.3, den 19 augusti 2022, fråga 2). Svenska myndigheter som använder Arachne kommer alltså inte att ha obegränsad tillgång till uppgifter som laddas upp av andra medlemsstater.

Myndigheterna kan, i vissa fall, få en begränsad tillgång till ytterligare uppgifter från andra medlemsstater genom Arachne. Om ett företag är involverat i flera projekt som genomförs i olika medlemsstater kommer myndigheterna från varje medlemsstat att kunna ta del av vissa begränsade data från den andra medlemsstaten med hjälp av vissa riskindikatorer (Arachne, Frequently asked questions, version 2.3, den 19 augusti 2022, fråga 9).

Så som Arachne fungerar i dag har användare obegränsad tillgång och möjlighet att söka i den externa databasen Orbis. Detta är avsett att ändras i den kommande version som kallas Arachne+ på så sätt att information från den externa databasen endast kommer att vara tillgänglig för användare i de fall ett visst företag eller en viss person förekommer i ett projekt beträffande vilket användaren har rätt att få information. När det gäller den externa databasen World Compliance har användare inte direkt tillgång till den, utan endast via riskvärderingar som avser egna projekt (se avsnitt 5.4.2).

Sammanfattande slutsatser om begränsningar i åtkomsten

Dataskyddsregelverket kan sägas innebära generella begränsningar i åtkomsten till uppgifter i Arachne. Det finns vidare begränsningar som tar sikte på att vissa användare endast ska få tillgång till vissa uppgifter i Arachne. Det finns vissa oklarheter när det gäller vilka användare som får vilken tillgång och hur detta kommer att se ut efter 2028. Detta beror bland annat på att det är lokala administratörer som fördelar behörigheterna. Det beror också på att det ännu finns oklarheter om hur systemet kommer att vara utformat. Det framstår som naturligt att Arachne kommer att innehålla tekniska sökbegränsningar som innebär att användare inte får tillgång till annat än vad de har rätt att få del av. Det följer av dataskyddsregelverkets princip om uppgiftsminimering att tillgången till personuppgifter inte ska vara för omfattande i förhållande till de ändamål för vilka de behandlas. Av principen om ändamålsbegränsning följer att personuppgifter ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och att de inte senare får behandlas på ett sätt som är oförenligt med dessa ändamål (se vidare avsnitt 7.2). Det är dock ännu oklart exakt hur sökbegränsningarna kommer att se ut i kommande version av Arachne och i vilken mån det kommer att vara möjligt för användare att få tillgång till uppgifter som de inte har rätt att behandla.

6 Användande av Edes som verktyg

6.1 Utredningens uppdrag

Tillämpningen av Edes-regelverket kommer att bli obligatorisk från och med den 1 januari 2028 även när svenska myndigheter deltar i genomförandet av EU:s budget, bland annat vid delad förvaltning. Utredningen behöver därför ta ställning till vad ett användande av Edes-databasen skulle innebära, bland annat när det gäller vilka myndigheter som skulle kunna komma att konsultera databasen och vilka uppgifter de därvid skulle få tillgång till.

Utredningens uppdrag som behandlas i detta kapitel är att beskriva vilka myndigheter som kan komma att använda Edes-databasen samt kartlägga och beskriva vilken typ av åtkomst de aktuella myndigheterna skulle få till uppgifter i Edes-databasen, när dessa används som ett led i handläggningen av ärenden eller vid kontrollåtgärder, med beaktande av eventuella begränsningar avseende vilka sökningar som får göras i systemet eller för vilka ändamål personuppgiftsbehandling får ske. Utredningen har också i uppdrag att bedöma vilka skyldigheter som berörda myndigheter skulle få inom ramen för Edes. Detta sker delvis i detta kapitel.

I kapitel 4 berörs utredningens uppdrag som omfattar uppgiftslämnande och utredningen gör där bedömningen att Edes inte medför något nytt krav på tillgängliggörande av uppgifter. I kapitel 7 behandlas regleringen om offentlighet, sekretess och dataskydd som bland annat styr användningen av Edes och innebär skyldigheter för berörda myndigheter vid en användning av verktyget. I avsnitt 8.6 görs överväganden om behovet av åtgärder för att svenska myndigheter ska kunna uppfylla sina skyldigheter inom ramen för Edes.

Det är vid sidan av medlemsländerna och nationella myndigheter många aktörer som vidtar åtgärder inom ramen för Edes, exempel-

vis så kallade utanordnare vid kommissionen. Det finns vidare vissa skyldigheter som medlemsstaterna har inom ramen för Edes som ligger utanför utredningens uppdrag. Det handlar exempelvis om att medlemsländer är skyldiga att se till att betalningsansökningar som avser en person eller enhet som befinner sig i en uteslutningssituation inte lämnas in till kommissionen för ersättning (artikel 138.2 tredje stycket i budgetförordningen). Det finns alltså flera frågor, som rör Edes, men som utredningen inte behandlar närmare i detta betänkande.

6.2 Närmare om Edes

6.2.1 Syftet med Edes

Det övergripande syftet med Edes är att skydda unionens ekonomiska intressen. Edes syftar till att göra det lättare att tidigt upptäcka personer eller enheter som är ett hot mot unionens ekonomiska intressen, att utesluta personer eller enheter från att ta del av EU-medel och att ålägga ekonomiska sanktioner mot mottagare av EU-medel som befinner sig i en uteslutningssituation (artikel 137.1 i budgetförordningen).

6.2.2 Det finns oklarheter gällande regleringen av Edes

Under arbetet med detta betänkande har flera frågor uppkommit rörande Edes som gäller tolkningen av vissa bestämmelser i budgetförordningen och hur systemet är tänkt att fungera från och med 2028. Utredningen har ställt frågor om detta till det så kallade Edesteamet vid kommissionen, som dock har förklarat att de inte kan besvara frågorna, med hänvisning till att de är i ett tidigt stadium när det gäller att utveckla strategier och processer för det kommande systemet, som också ska vara tillämpligt på delad förvaltning.[1] De har också angett att etablerandet av det kommande systemet kan leda till förändringar i det befintliga systemet. Enligt dem är det inte heller meningsfullt för dem att ge utredningen information om det befintliga systemet eftersom det kan komma att förändras. När de har utformat strategier och processer planerar de att ta kontakt med intres-

[1] Komm2025/00388-7 och Komm2025/00388-8.

senterna med information om hur systemet kommer att fungera. Mot denna bakgrund finns det alltså vissa oklarheter när det gäller Edes som inte har kunnat klargöras under arbetet med denna utredning. Beskrivningarna och bedömningarna som tar sikte på Edes utgår därmed från vad som i dag är känt för utredningen.

6.2.3 Uteslutningssituationerna

En funktion inom ramen för Edes är möjligheten att utesluta personer eller enheter från att delta i förfaranden för tilldelning av EU-medel eller från att genomföra unionsmedel[2], om de befinner sig i en eller flera så kallade uteslutningssituationer. Dessa beskrivs i artikel 138.1 i budgetförordningen och redogörs i det följande för i något förenklad form. De punkter som är i kursiv stil är av särskilt intresse för Sverige, då de gäller vid så kallad partiell tillämpning (se vidare nedan).

a) Personen eller enheten befinner sig i konkurs eller är föremål för insolvens- eller likvidationsförfaranden, är föremål för tvångsförvaltning och vissa liknande situationer.

b) Personen eller enheten har underlåtit att betala skatter eller socialförsäkringsavgifter.

c) Det har genom en slutgiltig dom eller ett slutgiltigt administrativt beslut fastställts att personen eller enheten har gjort sig skyldig till ett allvarligt fel i yrkesutövningen, och särskilt genom att

    i) på ett bedrägligt sätt eller genom oaktsamhet lämna vilseledande uppgifter som vissa underlag,

    ii) ingå en överenskommelse med andra personer eller enheter i syfte att snedvrida konkurrensen,

    iii) göra intrång i immateriella rättigheter,

[2] I flera artiklar och skäl i den svenska versionen av budgetförordningen har uttrycket ”the implementation of Union funds” översatts med ”förvaltningen av unionsmedel” (i olika grammatiska former). På tyska används uttrycket ”Ausführung von Unionsmitteln”. Enligt utredningen framstår det som mer korrekt att på svenska beskriva detta som ”genomförandet av unionsmedel”. Se exempelvis artiklarna 62.1 första stycket c ix och 152.8 samt skäl 51. Utredningen använder därför begreppet ”genomförande” av unionsmedel när det i den engelska versionen handlar om ”implementation” av sådana medel.

iv) otillbörligt påverka eller försöka att otillbörligt påverka beslutsprocessen för att få tillgång till unionsmedel genom att lämna oriktiga uppgifter och därigenom dra nytta av en intressekonflikt,

v) försöka erhålla konfidentiella uppgifter som kan ge otillbörliga fördelar under förfarandet för tilldelning,

vi) uppmana till diskriminering, hat eller våld mot en grupp av personer eller mot en medlem av en grupp, eller liknande verksamhet, om sådana fel har en inverkan på personens eller enhetens integritet som negativt påverkar eller konkret riskerar att påverka fullgörandet av det rättsliga åtagandet.

d) Det har genom en slutgiltig dom fastställts att personen eller enheten gjort sig skyldig till något av följande:

i) Bedrägeri

ii) Korruption

iii) Beteende som rör en kriminell organisation

iv) Penningtvätt eller finansiering av terrorism

v) Terroristbrott eller brott med anknytning till terroristverksamhet, eller anstiftan, medhjälp eller försök till sådana brott

vi) Barnarbete eller andra människohandelsbrott.

e) Personen eller enheten har under genomförandet av ett rättsligt åtagande som finansieras genom budgeten brustit betydligt i fullgörandet av sina huvudsakliga skyldigheter, vilket har

i) lett till att ett rättsligt åtagande hävts i förtid,

ii) lett till tillämpning av avtalsviten eller andra kontraktsenliga sanktioner, eller

iii) upptäckts av en utanordnare, Olaf, revisionsrätten eller Eppo vid kontroller, revisioner eller utredningar.

f) Det har genom en slutgiltig dom eller ett slutgiltigt administrativt beslut fastställts att personen eller enheten har gjort sig skyldig till oriktigheter i den mening som avses i artikel 1.2 i rådets förordning (EG, Euratom) nr 2988/95 av den 18 december 1995 om skydd av Europeiska gemenskapernas finansiella intressen.

g) Det har genom en slutgiltig dom eller ett slutgiltigt administrativt beslut fastställts att personen eller enheten har skapat en enhet i en annan jurisdiktion i syfte att kringgå skattemässiga, sociala eller andra rättsliga skyldigheter.

h) Det har genom en slutgiltig dom eller ett slutgiltigt administrativt beslut fastställts att en enhet har skapats med den avsikt som avses i led g.

i) Enheten eller personen har avsiktligt och utan godtagbara skäl motsatt sig en utredning, kontroll eller revision som utförts av en utanordnare eller dennes företrädare eller revisor, Olaf, Eppo eller revisionsrätten.

6.2.4 Partiell tillämplighet av Edes

När det gäller svenska myndigheters användande av Edes är uteslutningssituationerna något färre än den fullständiga uppräkningen ovan. Budgetförordningen föreskriver nämligen vad som kallas *en partiell tillämplighet* av systemet för uteslutning i vissa fall. Budgetförordningens reglering av detta är enligt utredningens mening inte helt klar.

Enligt artikel 130 i budgetförordningen ska systemet för uteslutning tillämpas på unionsmedel som betalas ut inom ramen för *delad förvaltning*, med avseende på varje person eller enhet som ansöker om eller tar emot dessa unionsmedel, på de villkor som anges i bland annat artikel 138.2. I stället för artikel 138.1 – där uteslutningsgrunderna anges – ska därmed artikel 138.2 tillämpas när det gäller delad förvaltning. Artikel 138.2 pekar ut endast vissa av situationerna i artikel 138.1. Det handlar om punkterna 1 c iv och d, som står i kursiverad stil ovan.

Även artikel 137 tar upp systemets tillämpning när det gäller olika förvaltningsformer, bland annat delad förvaltning. Enligt artikel 137.2 fjärde stycket ska, när det gäller delad förvaltning, uteslutningssystemet tillämpas på a) varje person eller enhet som ansöker om finansiering inom ramen för ett program med delad förvaltning, som valts ut för sådan finansiering eller som tar emot sådan finansiering, b) enheter vars kapacitet den person eller enhet som avses i led a avser att anlita, eller underleverantörer till en sådan person eller enhet och

c) verkliga huvudmän och eventuella anknutna enheter till den uteslutna enhet som avses i artikel 138.6.

Vid direkt och indirekt förvaltning är kretsen som systemet ska tillämpas på vidare (artikel 137.2 första stycket).

Det kan noteras att den artikel som tar sikte på partiell tillämplighet av Edes (artikel 130) endast behandlar delad förvaltning. Enligt utredningens mening synes tillämpningen av Edes vara på liknande sätt partiell även när det gäller förvaltningsformen *direkt förvaltning tillsammans med medlemsstaterna*. Beträffande den förvaltningsformen finns nämligen en särskild reglering i artikel 137.2, som handlar om vilka aktörer Edes ska tillämpas på. Enligt artikel 137.2 första stycket i ska Edes tillämpas på varje person eller enhet som mottar medel, om budgeten genomförs enligt förvaltningsformen direkt förvaltning tillsammans med medlemsstaterna. I dessa fall ska artikel 138.2 tillämpas. Av artikel 138.2 följer att uteslutningar, när budgeten genomförs enligt förvaltningsformen direkt förvaltning tillsammans med medlemsstaterna, endast ska ske enligt samma begränsade antal uteslutningsgrunder som gäller beträffande delad förvaltning. Vidare framgår av övergångsbestämmelserna i artikel 277.1 att skyldigheterna enligt Edes-regelverket ska tillämpas först från och med 2028, både när det gäller delad förvaltning och direkt förvaltning tillsammans med medlemsstaterna.

Utredningen uppfattar det sammanfattningsvis så att den partiella tillämpningen av Edes – som innebär att uteslutning bara kan ske på vissa uteslutningsgrunder – gäller både vid delad förvaltning och vid direkt förvaltning tillsammans med medlemsstaterna. Saken kan uttryckas så att tillämpningen av Edes är partiell på detta sätt när medlemsstater – såsom Sverige – deltar i budgetgenomförandet. Det kan också noteras att förvaltningsformen direkt förvaltning tillsammans med medlemsstaterna inte behandlas i den tidigare budgetförordningen på det sätt som sker i den omarbetade budgetförordningen.

6.2.5 Beslut om uteslutning, ekonomisk sanktion och offentliggörande

Ett beslut om uteslutning ska fattas av en så kallad behörig utanordnare, om en person eller enhet befinner sig i någon av de angivna uteslutningssituationerna (artikel 138.1 i budgetförordningen). I de fall uteslutningsgrunden inte baseras på en slutlig dom eller ett admi-

nistrativt beslut ska beslutet om uteslutning fattas på grundval av en preliminär bedömning med beaktande av en rekommendation som ska lämnas av en särskild panel (artikel 137 och 145).

I artikel 141 finns bestämmelser om en uteslutnings varaktighet och preskriptionstid. I de fall uteslutningens varaktighet inte har fastställts i en dom eller beslut i en medlemsstat kan uteslutningen gälla i upp till fem år.

Bestämmelser om ekonomiska sanktioner finns i artikel 140. För att uppnå en avskräckande verkan får den behöriga utanordnaren under vissa förutsättningar utfärda en ekonomisk sanktion mot den person eller enhet som befinner sig i en uteslutningssituation. I vissa fall får en ekonomisk sanktion åläggas som ett alternativ till ett beslut om att utesluta mottagaren, om en uteslutning vore oproportionerlig.

Om det krävs för att förstärka uteslutningens eller den ekonomiska sanktionens avskräckande verkan kan information om uteslutningen och sanktionen offentliggöras på kommissionens webbplats, inklusive namnet på personen eller enheten som har uteslutits (artikel 142).

6.2.6 Vilka uppgifter finns i Edes?

Varifrån kommer uppgifterna?

Enligt artikel 144.2 i budgetförordningen ska Edes baseras på vissa faktiska omständigheter och slutsatser och på uppgifter som lämnas till kommissionen, särskilt av vissa aktörer, något förenklat av följande.

a) Eppo och Olaf

b) Utanordnare vid kommissionen, vid en europeisk byrå som inrättats av kommissionen eller vid ett genomförandeorgan

c) En unionsinstitution eller vissa andra EU-organ

d) Vissa enheter som genomför EU:s budget, vid delad förvaltning och inom ramen för direkt förvaltning tillsammans med medlemsstaterna, när det gäller faktiska omständigheter och slutsatser som fastställts endast i samband med slutgiltiga domar eller slutgiltiga administrativa beslut samt upptäckta bedrägerier eller orik-

tigheter och uppföljning av dessa, om överlämnande av uppgifter krävs enligt sektorsspecifika regler

e) Personer eller enheter som genomför unionsmedel enligt indirekt förvaltning.

Punkten d) är av särskilt intresse för Sverige. Den gäller både vid delad förvaltning och vid direkt förvaltning tillsammans med medlemsstaterna. I avsnitt 4.6 framgår utredningens bedömning att budgetförordningen inte innebär några nya skyldigheter för medlemsstaterna att överlämna uppgifter till kommissionen för att de ska tillföras Edes. De uppgifter från medlemsstater som Edes ska baseras på gäller slutliga domar och beslut med mera och bara om överlämnandet redan krävs enligt sektorsspecifika regler.

Uppgifter i Edes

Uppgifter som utbyts inom ramen för Edes ska enligt artikel 144.1 i budgetförordningen centraliseras i en databas som inrättas av kommissionen, Edes-databasen. I Edes-databasen ska den så kallade behöriga utanordnaren föra in uppgifter om fall som avser tidig upptäckt, uteslutning eller ekonomiska sanktioner. Innan uppgifter förs in i databasen ska den berörda personen eller enheten som huvudregel underrättas.

Att uppgifter om beslut om uteslutning och ekonomiska sanktioner ska registreras i databasen framgår också av artikel 137.3. Av sistnämnda artikel framgår att det i vissa fall också ska registreras uppgifter om vissa personer som avses i artikel 138.5. Det handlar bland annat om situationen att uteslutning av en person eller enhet (den berörda personen eller enheten) sker på grund av att en fysisk eller juridisk person som ingår i ledningsorganet för den berörda personen eller enheten befinner sig i en uteslutningssituation av visst slag.

I artikel 144.3 finns närmare bestämmelser om vad uppgifterna som lämnas till kommissionen ska inbegripa, i de fall skyldigheten att lämna uppgifter inte följer av sektorsspecifika regler. Det handlar då förenklat om uppgift om den berörda enhetens eller personens identitet, en sammanfattning av de risker som upptäckts eller av faktiska omständigheter, uppgifter som skulle kunna vara till hjälp för utanordnare när de genomför kontroller eller fattar ett beslut

om uteslutning eller om ekonomiska sanktioner samt uppgifter om åtgärder som krävs för att säkerställa konfidentialiteten för inlämnade uppgifter.

Av *personuppgiftspolicyn för Edes*[3] framgår att det kan finnas bland annat följande typer av uppgifter om fysiska personer, bland annat om mottagare av stöd.

- Information för att identifiera en person: namn, adress, identifikationsnummer, födelsedatum
- Information om eventuell koppling till en juridisk person som förekommer i kommissionens system
- Information om uteslutning eller finansiell sanktion
- Orsakerna till uteslutningen eller sanktionen (enligt artikel 136.1 tidigare budgetförordningen 2018/1046, jfr artikel 138 i budgetförordningen)
- Information om giltighetstiden för en uteslutning eller en tidig upptäckt: tid då den startar respektive upphör
- Information om panelen: om ärendet hänförts dit, tidpunkt för panelen med mera
- Storleken på en eventuell finansiell sanktion
- Information om den ansvarige utanordnaren
- Kontaktperson för ärendet.

När det gäller personer som ingår i ledningsgruppen med mera för juridiska personer som tar emot stöd kan det handla om följande information.

- Information för att identifiera en person: namn, adress, identifikationsnummer, födelsedatum

[3] Protection of your personal data, Processing operation: Privacy Statement for the database of the Early Detection and Exclusion System (EDES), Record reference: DPR-EC-04410. Personuppgiftspolicyn är inte daterad och utredningen har inte kunnat identifiera ett entydigt datum för dess framtagande. Det dokument den hänvisar till - Beskrivning av personuppgiftsbehandlingen för Edes – är daterad den 8 februari 2022. I vart fall tar den inte sikte på den omförhandlade budgetförordningen.
https://commission.europa.eu/system/files/2023-06/Privacy_statement-edes-June-2023.pdf. Hämtat 2025-10-23.

- Information om kopplingen till den juridiska personen och den fysiska personens roll där.

Eftersom uppgift om grunderna för beslut om uteslutning finns i Edes kan där också finnas uppgifter om domar i brottmål. Det kan handla om underlåtenhet att betala skatt, allvarlig misskötsamhet, bedrägerier med mera. När det inte finns någon lagakraftvunnen dom eller liknande kan beslut om uteslutning baseras på preliminära uppgifter.

Det är oklart exakt vilka uppgifter som kommer att finnas i Edes-databasen rörande beslut om uteslutning

Ovan redogörs det på ett översiktligt plan för vilka uppgifter som kan förväntas finnas i Edes. I korthet handlar det om namn och andra kontaktuppgifter, grunden för uteslutning, längden på uteslutningen och storleken på eventuell sanktion.

En särskild fråga är vad som i detta sammanhang avses med beslut om uteslutning. Hur detaljerade uppgifter om grunderna för en uteslutning, exempelvis om brottsligt beteende, kommer svenska myndigheter att få tillgång till? Utredningen har ställt frågor om detta till Edes-teamet vid kommissionen men har inte fått några klargörande svar.[4] Det finns därmed vissa oklarheter när det gäller exakt vilka uppgifter som kommer att vara tillgängliga för svenska myndigheter när det gäller beslut om uteslutning.

Uppgifter som ska lämnas enligt sektorsspecifika regler

Artikel 144.3 – som närmare anger vad uppgifterna som lämnas till kommissionen från vissa aktörer för att tillföras Edes-databasen ska inbegripa – gäller endast i de fall skyldigheten att lämna uppgifter inte följer av sektorsspecifika regler. Eftersom Sveriges skyldighet att lämna uppgifter som ska tillföras Edes är begränsad till fall där överlämnande krävs enligt sektorsspecifika regler, gäller det som sägs i artikel 144.3 inte för Sverige eller svenska myndigheter, och inte heller för andra medlemsländer och deras myndigheter när genomförandet av EU:s budget sker enligt delad förvaltning eller direkt

[4] Komm2025/00388-7 och Komm2025/00388-8.

förvaltning som sker tillsammans med medlemsländerna. Budgetförordningen ger alltså inte någon avgörande ledning för vilka uppgifter som ska lämnas – och som Edes därmed ska innehålla – i dessa fall. Det svaret får i stället sökas i de sektorsspecifika bestämmelserna. Det bör i sammanhanget nämnas att det är svårt att överblicka vilka uppgifter som därvid kan bli aktuella, bland annat eftersom de sektorsspecifika reglerna förväntas bli ändrade inför kommande programperiod.

Som exempel på vad som gäller enligt nuvarande regelverk kan följande nämnas. I artikel 69.12 i CPR finns skyldigheter för medlemsstaterna att rapportera vissa oriktigheter i systemet för hantering av oriktigheter, IMS. De uppgifter som ska lämnas framgår i bilaga XII till CPR. I bilagan framgår att det ska rapporteras oriktigheter som har varit föremål för en första skriftlig bedömning där en behörig administrativ eller rättslig myndighet på grundval av konkreta fakta har dragit slutsatsen att det föreligger en oriktighet, oberoende av möjligheten att denna slutsats senare kan behöva revideras eller dras tillbaka till följd av utvecklingen under det administrativa eller rättsliga förfarandet. Vidare ska, något förenklat, oriktigheter som leder till att administrativa eller rättsliga förfaranden inleds på nationell nivå för att fastställa förekomsten av bedrägerier eller andra brott rapporteras. Dessutom ska medlemsstaterna rapportera oriktigheter som föregår en konkurs samt särskilda oriktigheter eller grupper av oriktigheter på begäran av kommissionen. Vissa oriktigheter är undantagna från rapporteringskravet, bland annat oriktigheter som understiger ett visst belopp. I bilagan finns också bestämmelser om användning och behandling av information som rapporteras.

6.2.7 Vilka får tillgång till uppgifter i Edes och hur begränsas tillgången för olika aktörer?

Alla aktörer som deltar i budgetgenomförandet kan få tillgång till Edes-databasen – redan i dag

Enligt artikel 144.5 första stycket i budgetförordningen ska alla personer och enheter som deltar i genomförandet av budgeten i enlighet med artikel 62 av kommissionen *beviljas tillgång* till uppgifterna om beslut om uteslutning enligt artikel 138, så att de i samband med tilldelning av kontrakt eller urval av bidragsmottagare som ska genom-

föra unionsmedel kan kontrollera om det finns uppgifter om uteslutning i Edes. Utredningen förutsätter att detta avser tillgång till uppgifter i Edes-databasen (i vart fall när det gäller uppgifter om uteslutning, se vidare nedan).

Artikel 144.5 första stycket innehåller alltså två led. I det första ledet hänvisas till ”alla personer och enheter som deltar i genomförandet av budgeten”. Enligt utredningens mening bör utgångspunkten vara att samtliga enheter som har någon roll i att avgöra vem som ska ta emot stöd eller i att i efterhand vidta kontroller av utbetalade stöd anses delta i budgetgenomförandet (jfr artikel 2.7 i budgetförordningen). I det första ledet omfattas alltså såväl myndigheter som behöver göra ex ante-kontroller som myndigheter som behöver göra ex post-kontroller. En särskild fråga är om det andra ledet i artikel 144.5 första stycket innebär att kretsen som ska ges tillgång snävas av till de enheter som har någon roll vid tilldelning av kontrakt eller urval av bidragsmottagare, alltså sådana enheter som har anledning att göra ex ante-kontroller. Utredningen har ställt frågan till Edesteamet vid kommissionen, men har inte fått något klargörande svar.[5]

Utredningen gör bedömningen att artikel 144.5 inte utgör någon sådan åtkomstbegränsning. Den inledande bisatsen anger tydligt att alla som deltar i genomförandet av budgeten ska beviljas tillgång. Något hinder för enheter som deltar i genomförandet av budgeten att få tillgång till Edes-databasen bör bland annat därför inte anses följa av bestämmelsen. En annan sak är att skyldigheten att använda Edes kan vara på visst sätt begränsad, se följande avsnitt.

Det kan noteras att artikel 144.5 i budgetförordningen huvudsakligen motsvarar artikel 142.5 i den tidigare budgetförordningen. Det som sägs ovan om möjlighet att få tillgång till uppgifter – vilket gäller också de svenska myndigheter som deltar i budgetgenomförandet – har alltså gällt även enligt den tidigare budgetförordningen. Det framgår också av beskrivningen av personuppgiftsbehandlingen för Edes[6], där det anges vilka som enligt den tidigare budgetförordningen kan ta emot uppgifter från Edes. I den uppräkningen ingår behöriga personer från alla enheter som deltar i budgetgenomförandet.

[5] Komm2025/00388-7 och Komm2025/00388-8.
[6] Record for processing of personal data, Title: Entry of a Data Subject in the Early Detection and Exclusion System (EDES-DB), Reference DPR-EC-04410.2, publicerad den 8 februari 2022. https://ec.europa.eu/dpo-register/detail/DPR-EC-04410. Hämtat 2025-10-29.

Tillgången för svenska myndigheter är begränsad till uppgifter om beslut om uteslutning

En särskild fråga gäller om tillgången som svenska myndigheter får till Edes – i egenskap av aktörer som deltar i budgetgenomförandet – avser endast beslut om uteslutning eller även andra uppgifter som finns i databasen. Utredningen har ställt frågor till Edes-teamet vid kommissionen om innebörden av den partiella tillämpningen av Edes samt om tillgången till uppgifter i databasen men har inte fått några klargörande svar.[7]

Artikel 144.5 första stycket i budgetförordningen anger att alla personer och enheter som deltar i genomförandet av budgeten i enlighet med artikel 62 av kommissionen ska beviljas tillgång till uppgifterna om *beslut om uteslutning*, så att de i samband med tilldelning av kontrakt eller urval av bidragsmottagare som ska genomföra unionsmedel kan kontrollera om det finns uppgifter om uteslutning i Edes.

Enligt utredningens mening talar strukturen i budgetförordningen för att tillgången är begränsad till beslut om uteslutning för exempelvis medlemsländernas myndigheter.

Av artikel 144.4 synes framgå att bland annat utanordnare vid kommissionen får tillgång till alla uppgifter i Edes-databasen, inte bara sådant som rör uteslutning. I samma riktning talar den personuppgiftspolicy för Edes[8] som avser den tidigare budgetförordningen (vilken i relevanta delar huvudsakligen motsvarar den omarbetade budgetförordningen). Det anges där att aktörer som deltar i budgetgenomförandet enligt artikel 62 b och c (det vill säga beträffande delad och indirekt förvaltning) får tillgång till beslut om uteslutning. Vidare anges det där att personer inom kommissionen, dess genomförandeorgan, övriga unionsinstitutioner med flera får tillgång till – förutom beslut om uteslutning – även information om tidig upptäckt och om sanktioner.

I samma riktning – att tillgången är begränsad till beslut om uteslutning för exempelvis medlemsländernas myndigheter – talar även en ändamålsbaserad tolkning. Det är kommissionens utanordnare

[7] Komm2025/00388-7 och Komm2025/00388-8.

[8] Protection of your personal data, Processing operation: Privacy Statement for the database of the Early Detection and Exclusion System (EDES), Data Controller: Directorate General for Budget – Central Financial Service - Unit BUDG.D.1, Record reference: DPR-EC-04410. Personuppgiftspolicyn är inte daterad och utredningen har inte kunnat identifiera ett entydigt datum för dess framtagande. https://commission.europa.eu/system/files/2023-06/Privacy_statement-edes-June-2023.pdf. Hämtat 2025-10-29.

som fattar beslut om att registrera uppgifter rörande tidig upptäckt, att utesluta personer eller enheter och att ålägga mottagare sanktioner (se artikel 137.3 i budgetförordningen). Utanordnare har generellt ett större behov än svenska myndigheter av uppgifter av ett mer osäkert slag när det gäller misstankar om missförhållanden och liknande. Tillgången till sådana uppgifter kan vara ett led i ställningstaganden om utredningar om uteslutningssituationer föreligger.

De skyldigheter som personer och enheter som deltar i genomförandet av budgeten har – såsom svenska myndigheter – synes främst vara kopplade till att verkställa beslut om uteslutning, det vill säga att inte bevilja stöd till en person eller enhet som befinner sig i en uteslutningssitution, samt att se till att betalningsansökningar som avser sådana personer och enheter inte lämnas till kommissionen för ersättning (se artiklarna 138.2 tredje stycket och 144.5 andra stycket). Det följer av principerna bakom dataskyddsregelverket att personuppgifter inte ska behandlas där det saknas anledning till det. Detta talar för att tillgången för svenska myndigheter är begränsad till uppgifter om uteslutning.

Sammantaget bedömer utredningen att det mesta talar för att budgetförordningen ska tolkas så att tillgången till Edes-databasen för svenska myndigheter är begränsad till uppgifter om beslut om uteslutning. Detta synes vara innebörden av den centrala bestämmelse som direkt tar sikte på tillgång till uppgifter i Edes-databasen, artikel 144.5 första stycket.

Tillgången kan komma att vara begränsad till beslut om uteslutning på vissa grunder

Som utvecklas i avsnitt 6.2.4 gäller det enligt budgetförordningen en partiell tillämplighet av Edes när medlemsstater deltar i budgetgenomförandet, antingen genom delad förvaltning eller direkt förvaltning tillsammans med medlemsstaterna. Vid partiell tillämplighet är bara vissa av uteslutningsgrunderna aktuella, nämligen bara de som anges i artikel 138.2. Detta talar för att medlemsstaterna endast får tillgång till uppgifter om uteslutning enligt vissa grunder men inte alla.

Det är också möjligt att tillgången vid delad förvaltning och direkt förvaltning tillsammans med medlemsstaterna inte är begränsad till uteslutningar på vissa grunder. Det kan noteras att det av den tidi-

gare budgetförordningen framgår att alla enheter som deltar i genomförandet av budgeten genom delad förvaltning får ha tillgång till information om beslut om uteslutning och det synes i denna del inte finnas någon begränsning till vissa uteslutningsgrunder (se personuppgiftspolicyn för Edes, s. 7). Detta framstår också som naturligt eftersom den uppdelning mellan olika uteslutningsgrunder som partiell tillämpning innebär är ny i den omarbetade budgetförordningen. Att medlemsländer genom den nya budgetförordningen skulle få tillgång till mindre information kan framstå som främmande, eftersom ett syfte med den omarbetade budgetförordningen är att stärka systemet för tidig upptäckt och uteslutning för att skydda unionens ekonomiska intressen (skäl 107).

Artikel 144.5 första stycket i budgetförordningen – den bestämmelse som synes reglera förutsättningarna för tillgång till Edes-databasen – innebär inte någon uttrycklig begränsning när det gäller grunden för beslut om uteslutning. Detta talar för att även aktörer som deltar i genomförandet av EU:s budget inom ramen för delad förvaltning och direkt förvaltning tillsammans med medlemsstaterna får tillgång till beslut om uteslutning som skett på samtliga grunder samtidigt som uteslutning endast får ske på vissa grunder.

Det kan dock också argumenteras för att avsikten får antas vara att medlemsstaterna endast ska ha tillgång till beslut om uteslutning på vissa mer allvarliga grunder. För en sådan tolkning kan möjligtvis tala att principerna bakom dataskyddsregelverket innebär att man inte ska ha tillgång till mer uppgifter än vad man behöver för att fullgöra sina arbetsuppgifter. Eftersom medlemsstaterna – inom ramen för Edes – endast har i uppgift att verkställa beslut om uteslutning på vissa grunder saknas det anledning för dem att få tillgång till andra uppgifter än sådana beslut om uteslutning. Sammantaget gör därför utredningen bedömningen att tillgången till beslut om uteslutning för svenska myndigheter kan komma att vara begränsad till beslut om uteslutning på vissa grunder, nämligen de som anges i artikel 138.2.

Tillgången kan begränsas på grund av dataskyddsregelverket

Enligt artikel 144.1 första stycket i budgetförordningen ska uppgifter som utbyts inom ramen för Edes och som centraliseras i databasen behandlas i enlighet med rätten till integritet och övriga rättig-

heter som fastställs i den dataskyddsreglering som gäller för EU:s institutioner[9]. Dataskyddsregelverket kan sägas innebära generella begränsningar i åtkomsten till uppgifter i Edes som träffar alla som använder Edes. Exempelvis finns det i svensk rätt ett förbud mot sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter.

Det framstår som naturligt att Edes kommer att innehålla tekniska sökbegränsningar som innebär att användare inte får tillgång till annat än vad de har rätt att få del av. En sådan ordning följer av dataskyddsregelverkets principer om uppgiftsminimering och ändamålsbegränsning (se vidare avsnitt 7.2). Det är dock ännu oklart exakt hur sökbegränsningarna ser ut och kommer att se ut i Edes och i vilken mån det kommer att vara möjligt för användare att få tillgång till uppgifter som de inte har rätt att behandla.

Förenligheten med dataskyddsregelverket när det gäller användningen av Edes behandlas i avsnitt 8.6.7.

6.2.8 Vilka träffas av skyldigheten att tillämpa Edes-regelverket?

Obligatorisk tillämpning av Edes-regelverket från och med 2028

Enligt den tidigare budgetförordningen ställs krav på en tillämpning av Edes-regelverket vid direkt och indirekt förvaltning (se artikel 135 i den tidigare budgetförordningen). Den omarbetade budgetförordningen ställer krav på att Edes från och med den 1 januari 2028 ska tillämpas även vid delad förvaltning och vid direkt förvaltning tillsammans med medlemsstaterna (se artiklarna 130, 137.2 fjärde stycket och artikel 277.1). Det kan nämnas att den tidigare budgetförordningen inte synes behandla förvaltningsformen direkt förvaltning tillsammans med medlemsstaterna, på det sätt som den omarbetade budgetförordningen gör.

Som framgår ovan kan alla aktörer som deltar i budgetgenomförandet få tillgång till Edes-databasen redan i dag och svenska myndigheter är alltså redan oförhindrade att använda Edes på frivillig basis.

[9] 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.

Skyldigheten att tillämpa Edes-regelverket kommer att gälla aktörer som har en roll vid tilldelning eller urval

I artikel 277.1 i budgetförordningen – som handlar om när tillämpningen av Edes-regelverket blir obligatorisk vid vissa förvaltningsformer – hänvisas till ”skyldigheterna” enligt vissa bestämmelser, bland annat artikel 144.5. Det kan konstateras att det i första stycket av artikel 144.5 inte anges någon skyldighet utan endast en beskrivning av vilka aktörer som ska beviljas tillgång till uppgifterna om beslut av uteslutning. I artikel 144.5 andra stycket beskrivs dock en skyldighet, nämligen att vissa aktörer ska *verkställa* beslut om uteslutning med avseende på den person eller enhet som ansöker om eller väljs ut för att genomföra unionsmedel (för indirekt förvaltning anges annat, som inte är relevant för denna utredning). Utredningen uppfattar ”verkställa beslut” som att en ansökan eller tilldelning ska avslås.

Den skyldighet som är särskilt reglerad i artikel 144.5 är således skyldigheten att verkställa beslut om uteslutning med avseende på den person eller enhet som ansöker om eller väljs ut för att genomföra unionsmedel. För att kunna verkställa sådana beslut behöver aktören känna till att besluten finns och behöver därför också konsultera Edes-databasen innan kontrakt tilldelas eller urval av bidragsmottagare sker. Indirekt följer således en skyldighet att använda Edes på ett sådant sätt.

Skyldigheten att tillämpa Edes-regelverket bedöms dock vara begränsad till aktörer som är i en position att ta ställning till frågor om tilldelning av kontrakt eller urval av bidragsmottagare. Skyldigheten kommer alltså i praktiken inte att omfatta alla som deltar i genomförandet av budgeten vid delad eller direkt förvaltning, även om samtliga sådana aktörer omfattas av ordalydelsen av artikel 144.5 andra stycket.

6.2.9 Bestämmelser som rör så kallade utanordnare innebär inte några skyldigheter för Sverige

En särskild fråga gäller tolkningen av begreppet behörig utanordnare i budgetförordningen. Funktionen har viktiga roller inom Edes. Begreppet används bland annat för den funktion som ska fatta beslut om uteslutning och ekonomiska sanktioner, se bland annat artik-

larna 137.3, 138, 139 och 140. Utredningen har ställt frågor om detta till Edes-teamet vid kommissionen och har därvid gett uttryck för tolkningen att begreppet avser en funktion vid kommissionen och inte hos medlemsländerna.[10] Kommissionen har inte gett något klargörande svar på frågorna och har inte heller invänt mot den framförda tolkningen.[11]

Det kan konstateras att det anges i artikel 73 att varje unionsinstitution ska fungera som utanordnare. Varje unionsinstitution ska delegera utanordnarens funktioner till anställda på lämplig nivå och utanordnarens befogenheter får bara delegeras eller vidaredelegeras till anställda. Med anställda avses här personer anställda vid unionen (det vill säga personer som omfattas av tjänsteföreskrifterna för tjänstemän i Europeiska unionen och anställningsvillkor för övriga anställda vid unionen, jfr skäl 66).

Sammantaget gör utredningen bedömningen att begreppet utanordnare avser en funktion inom kommissionen. De artiklar som tar sikte på behöriga utanordnare bedöms alltså inte innebära några skyldigheter för eller krav på Sverige eller svenska myndigheter.

6.3 Svenska myndigheter som kan komma att använda Edes

6.3.1 Vissa utgångspunkter

Utredningen har i uppdrag att beskriva vilka myndigheter som kan komma att använda Edes-databasen. På motsvarande sätt som redogörs för i avsnitt 5.3.1 avseende Arachne är det inte möjligt för utredningen att ange en uttömmande uppräkning av vilka myndigheter som kan komma att använda Edes. En frivillig användning är möjlig redan i dag. Förändringar kan förväntas för den programperiod som börjar 2028 då det kan komma nya fonder och instrument som behöver hanteras. Utredningen gör dock övergripande bedömningar om vilka slags myndigheter det bör vara fråga om. Utifrån dessa bedömningar bör det gå att dra slutsatser om det finns anledning för olika myndigheter att använda Edes, utifrån de uppgifter de har och eventuellt kan komma att få.

[10] Komm2025/00388-7.
[11] Komm2025/00388-8.

Av avsnitt 6.2 följer att utredningen gör följande övergripande bedömningar när det gäller kravet att använda Edes och vilka åtkomstbegränsningar som finns och kommer att finnas. Den obligatoriska tillämpningen av Edes-regelverket gäller endast aktörer som har en roll vid tilldelning eller urval. Alla aktörer kan dock använda Edes på frivillig basis, redan i dag. Tillgången till uppgifter i Edes är begränsad på flera sätt. Dataskyddsregelverket kan sägas innebära generella begränsningar i åtkomsten till uppgifter i Edes. Det finns vidare begränsningar som bedöms innebära att svenska myndigheter endast får tillgång till beslut om uteslutning och tillgången kan dessutom komma att vara begränsad till uppgifter om uteslutning på vissa grunder.

I det följande görs vissa överväganden om huruvida vissa myndigheter och kategorier av myndigheter kan komma att använda Edes-databasen.

6.3.2 Myndigheter som förvaltar EU-medel genom delad förvaltning

Enligt artikel 144.5 första stycket i budgetförordningen ska alla personer och enheter som deltar i genomförandet av budgeten av kommissionen beviljas tillgång till uppgifter om beslut om uteslutning. Bland annat omfattas därmed personer och enheter som deltar i genomförandet av budgeten genom delad förvaltning. Detta bör – inom ramen för delad förvaltning – omfatta i princip samtliga myndigheter som har någon roll i att avgöra vem som ska ta emot stöd eller att i efterhand vidta kontroller av utbetalade stöd (på motsvarande resonemang som avseende Arachne, se avsnitt 5.3.2). Detta träffar bland annat Jordbruksverket, Migrationsverket, Polismyndigheten, Svenska ESF-rådet, Tillväxtverket samt länsstyrelserna i Jämtlands, Västerbottens och Norrbottens län. Vidare bör det omfatta de myndigheter som har delegerats uppgifter från förvaltande myndigheter och har en tillräckligt självständig roll i besluten om ersättning, nämligen länsstyrelserna, Skogsstyrelsen och Sametinget.

Även Havs- och vattenmyndigheten (förmedlande organ för havsfiskeri- och vattenbruksprogrammet) bedöms delta i budgetgenomförandet på ett sådant sätt att myndigheten bör beviljas tillgång till Edes.

6.3.3 Myndigheter som hanterar medel genom direkt förvaltning tillsammans med medlemsstaterna

En särskild fråga är i vilken mån svenska myndigheter kan komma att använda Edes inom ramen för förvaltningsformen direkt förvaltning tillsammans med medlemsstaterna. I dagsläget är det endast RRF som förvaltas genom den förvaltningsformen.

Det finns reglering om Edes-databasen i budgetförordningen som tar sikte på dess tillämplighet i relation till RRF. I övergångsbestämmelserna anges att Edes-systemet inte tillämpas på RRF och att detta ska gälla utan att det påverkar sektorsspecifika regler och frivillig tillämpning (artikel 277.2). Som utredningen uppfattar saken innebär detta att en frivillig användning av Edes när det gäller RRF är möjlig. Syftet med en användning av Edes är att medel inte ska gå till aktörer som inte har rätt till det. Enligt utredningen kan det alltså finnas anledning – och vara tillåtet enligt budgetförordningen – att använda Edes inom ramen för RRF på frivillig basis. Det handlar om dels de tio rapporterande myndigheterna Boverket, Myndigheten för digital förvaltning, Myndigheten för yrkeshögskolan, Naturvårdsverket, Post- och telestyrelsen, Skolverket, Socialstyrelsen, Statens energimyndighet, Trafikverket och Universitetskanslersämbetet (se vidare avsnitt 3.5.4 och tabell 3.3), dels länsstyrelserna när de ansvarar för handläggning, beslutsfattande och uppföljning (se avsnitt 5.3.3). RRF-myndigheternas eventuella användning av Edes från och med 2027 kan förväntas avse uppföljnings- och granskningsverksamhet av redan beslutade och utbetalade stöd. De kan inte förväntas använda Edes på så sätt att de verkställer beslut om uteslutning (genom att inte betala ut ett stöd), eftersom reformer och investeringar inom ramen för RRF ska vara genomförda vid den tidpunkten.

Som nämns i avsnitt 3.5.1 kan förändringar förväntas för den programperiod som börjar 2028 och det kan komma nya fonder och instrument som behöver hanteras. Om det kommer nya fonder som förvaltas genom direkt förvaltning tillsammans med medlemsstaterna bör Edes kunna användas av de myndigheter som hanterar dessa. Det följer av att alla som deltar i genomförandet av budgeten i enlighet med artikel 62 ska beviljas tillgång till Edes (artikel 144.5).

Även beträffande förvaltningsformen direkt förvaltning tillsammans med medlemsstaterna synes det vara fråga om en slags partiell tillämpning (se vidare avsnitt 6.2.4).

6.3.4 Ekonomistyrningsverket

ESV kan sägas delta i genomförandet av budgeten, på det sätt som beskrivs vad gäller Arachne (se avsnitt 5.3.4). ESV har visserligen inte någon roll när det gäller att avgöra vem som ska ta emot stöd men däremot när det gäller att i efterhand vidta granskningar av utbetalade stöd. ESV kan därför också i och för sig anses ha anledning att använda Edes vid sina revisioner, men inte i syfte att verkställa uteslutningsbeslut. Som utvecklas i avsnitt 6.2.7 anser utredningen inte att artikel 144.5 utgör någon åtkomstbegränsning på ett sätt som skulle utesluta att ESV får tillgång till Edes. ESV bör därmed kunna komma att använda Edes.

6.3.5 Ekobrottsmyndigheten

Utredningen uppfattar Ekobrottsmyndighetens och SEFI-rådets roller så att det inte finns skäl för dem att använda Edes direkt, och att de inte heller omfattas av Edes-regelverket på ett sådant sätt att de bör medges tillgång till Edes-databasen. Det är dock av stort intresse för dessa aktörer att det finns effektiva system som motverkar felaktiga utbetalningar och bedrägerier avseende EU-medel. Det kan dock påminnas om att Eppo är EU:s oberoende åklagarmyndighet som ska skydda EU:s budget och väcka talan när det gäller brott som skadar EU:s ekonomiska intressen, och brottsanmälan kan göras direkt till Eppo (se avsnitt 5.3.5).

6.3.6 Slutsatser om vilka myndigheter som kan komma att använda Edes

Sammanfattningsvis bedömer utredningen att följande slags myndigheter kan komma att använda Edes.

- De myndigheter som deltar i genomförandet av budgeten inom ramen för delad förvaltning och därvid har någon roll i tilldelning av medel eller kontroll av utbetalade medel. För de myndigheter som har en roll i tilldelning av medel blir det obligatoriskt att tillämpa Edes-regelverket och därmed också att använda Edes-databasen. Vid delad förvaltning är tillämpningen partiell på det sättet att endast vissa uteslutningsgrunder är aktuella.

- De myndigheter som inom ramen för RRF deltar i genomförandet av budgeten och därvid har någon roll i tilldelning av medel eller kontroll av utbetalda medel – på frivillig basis.
- De myndigheter som eventuellt i framtiden kommer att förvalta EU-fonder genom direkt förvaltning tillsammans med medlemsstaterna och därvid har någon roll i tilldelning av medel eller kontroll av utbetalda medel. För de myndigheter som har en roll i tilldelning av medel kommer det att vara obligatoriskt att tillämpa Edes-regelverket och därmed också att använda Edes-databasen. Tillämpningen är partiell på det sättet att endast vissa uteslutningsgrunder är aktuella.
- De myndigheter som har i uppgift att i efterhand genomföra granskningar eller revisioner av utbetalade stöd, såsom ESV. För dessa myndigheter är det inte obligatoriskt att tillämpa Edes-regelverket.

7 Övergripande om offentlighet, sekretess och dataskydd

7.1 Övergripande om offentlighet, sekretess och ärendehantering

7.1.1 Om offentlighet och allmänna handlingar

Offentlighetsprincipen kommer till uttryck på olika sätt, exempelvis genom yttrande- och meddelarfrihet för tjänstemän, genom domstolsoffentlighet och genom offentlighet vid beslutande församlingars sammanträden. När det mer allmänt talas om offentlighetsprincipen syftas dock i första hand på reglerna om allmänna handlingars offentlighet.

Rätten att ta del av allmänna handlingar är ett viktigt medel för kontroll av offentliga organs verksamhet. Handlingsoffentligheten har bland annat till syfte att garantera rättssäkerheten och effektiviteten i förvaltningen och folkstyret (prop. 2008/09:150 s. 272). De grundläggande bestämmelserna om allmänna handlingars offentlighet finns i 2 kap. tryckfrihetsförordningen, TF, och genomsyrar all offentlig verksamhet i Sverige. Enligt 2 kap. 1 § TF ska var och en ha rätt att ta del av allmänna handlingar.

Rätten att ta del av allmänna handlingar får bara begränsas om det krävs med hänsyn till vissa i 2 kap. 2 § TF angivna grunder, så kallade sekretessgrunder. En sådan begränsning ska anges noga i en bestämmelse i en särskild lag eller, om det anses lämpligare i ett visst fall, i en annan lag som den särskilda lagen hänvisar till. Den särskilda lagen som avses är offentlighets- och sekretesslagen (2009:400), OSL.

7.1.2 Allmänt om sekretess och sekretessgenombrott

I offentlighets- och sekretesslagen finns bestämmelser om sekretess som begränsar rätten att ta del av allmänna handlingar och som reglerar tystnadsplikt i det allmännas verksamhet. Lagens tillämpningsområde omfattar de organ som ingår i den offentligrättsliga statliga och kommunala organisationen. Det innebär att offentlighets- och sekretesslagen inte är tillämplig på exempelvis unionsorgan inom EU:s organisation (jfr prop. 2023/24:87 s. 58).

Sekretess innebär ett förbud att röja en uppgift, oavsett om det sker genom utlämnande av en allmän handling eller genom att uppgifter röjs muntligen eller på något annat sätt (3 kap. 1 § OSL). Sekretess gäller mot enskilda och mot andra myndigheter samt mellan självständiga verksamhetsgrenar inom myndigheter (8 kap. 1 och 2 §§ OSL). En uppgift för vilken sekretess gäller får som huvudregel inte heller röjas för en utländsk myndighet eller en mellanfolklig organisation (8 kap. 3 § OSL).

Sekretessen är i normala fall reglerad för ett avgränsat tillämpningsområde och gäller för vissa angivna uppgifter, i en viss typ av ärenden, i en viss typ av verksamhet eller hos en viss myndighet. De sekretessbestämmelser som främst aktualiseras i aktuella situationer behandlas i avsnitt 7.1.7.

I offentlighets- och sekretesslagen finns också flera bestämmelser med innebörden att sekretess inte hindrar att uppgifter lämnas, så kallade sekretessbrytande bestämmelser. De sekretessbrytande bestämmelserna kan möjliggöra utlämnande av uppgifter till såväl enskilda som myndigheter. Utgångspunkten är att det är svenska myndigheter som omfattas av myndighetsbegreppet i offentlighets- och sekretesslagen och att sekretessbrytande bestämmelser inte ger stöd för att ge exempelvis unionsorgan tillgång till sekretessbelagda uppgifter (jfr prop. 2023/24:87 s. 66).

I 10 kap. 28 § OSL finns en bestämmelse som innebär att sekretess inte hindrar att en uppgift lämnas till en annan svensk myndighet, om uppgiftsskyldighet följer av lag eller förordning. Det innebär att det kan finnas sekretessbrytande bestämmelser även i andra författningar. Som exempel kan nämnas lagen (2025:170) om skyldighet att lämna uppgifter till de brottsbekämpande myndigheterna och lagen (2024:307) om uppgiftsskyldighet för att motverka fel-

aktiga utbetalningar från välfärdssystemen samt fusk, regelöverträdelser och brottslighet i arbetslivet.

När det gäller uppgiftslämnande till utlandet anges i tidigare nämnda 8 kap. 3 § OSL under vilka förutsättningar sekretessbelagda uppgifter får lämnas ut till en utländsk myndighet eller en mellanfolklig organisation. Bestämmelsen tar sikte på rätten för svenska myndigheter att lämna ut uppgifter och innebär att en uppgift för vilken sekretess gäller får lämnas ut om utlämnande sker i enlighet med särskild föreskrift i lag eller förordning. En uppgift får också lämnas ut om uppgiften i motsvarande fall skulle få lämnas ut till en svensk myndighet och det enligt den utlämnande myndighetens prövning står klart att det är förenligt med svenska intressen att uppgiften lämnas till den utländska myndigheten eller den mellanfolkliga organisationen.

Under de senaste åren har det pågått arbete med att se över lagstiftning som hindrar informationsutbyte och uppgiftslämnande mellan svenska myndigheter, särskilt på det brottsbekämpande området och området för motverkande av felaktigheter. Av intresse för denna utredning är till exempel propositionen Ökat informationsutbyte mellan myndigheter – en ny sekretessbrytande bestämmelse (prop. 2024/25:180), där regeringen föreslår vissa förändringar i offentlighets- och sekretesslagen. Sekretess till skydd för enskilda ska inte hindra att uppgifter lämnas mellan myndigheter om det behövs för vissa syften. I propositionen föreslås att uppgifter ska kunna lämnas om det behövs bland annat för att förebygga, förhindra, upptäcka eller utreda felaktiga utbetalningar, och förebygga, förhindra, upptäcka eller utreda fusk och olika typer av överträdelser. Därför föreslås i propositionen en ny sekretessbrytande bestämmelse, 10 kap. 15 a § OSL. Förslaget rör inte bara felaktiga utbetalningar från välfärdssystemen utan det finns även ett omfattande behov av förbättrade möjligheter till informationsutbyte mellan myndigheter i samband med hanteringen av EU-relaterade medel (prop. s. 27). Riksdagen har den 22 oktober 2025 antagit förslaget. Lagändringarna ska träda i kraft den 1 december 2025.

7.1.3 Allmänna handlingar och ärendehandläggning

Förvaltningslagen (2017:900) gäller för handläggning av ärenden hos förvaltningsmyndigheterna och handläggning av förvaltningsärenden hos domstolarna (1 § första stycket). 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 § OSL (10 § förvaltningslagen). En myndighet som får uppgifter på något annat sätt än genom en handling ska snarast dokumentera dem, om de kan ha betydelse för ett beslut i ärendet. Det ska framgå av dokumentationen när den har gjorts och av vem (27 § förvaltningslagen).

Även offentlighets- och sekretesslagen innehåller bestämmelser om myndigheters hantering av allmänna handlingar, bland annat med koppling till ärendehandläggning. Om en myndighet för handläggning av ett mål eller ärende använder sig av en upptagning för automatiserad behandling, ska upptagningen tillföras handlingarna i målet eller ärendet i läsbar form, om det inte finns särskilda skäl mot det (4 kap. 3 § OSL).

7.1.4 Allmänt om offentlighet och sekretess inom EU-samarbetet

Frågor om offentlighet och sekretess kan aktualiseras i förhållandet mellan Sverige och EU:s institutioner och mellan Sverige och andra medlemsländer inom ramen för EU-samarbetet.

Sverige har traditionellt värnat den svenska offentlighetsprincipen samt arbetat för ökad öppenhet inom EU:s institutioner. Bland annat har Sverige arbetat aktivt för att den så kallade öppenhetsförordningens[1] bestämmelser ska tolkas och tillämpas på ett så öppenhetsvänligt sätt som möjligt (se bland annat prop. 2012/13:192 s. 19). De flesta medlemsstater har dock en helt annan tradition än Sverige när det gäller handlingsoffentlighet (prop. 2012/13:192 s. 23).

Sverige måste inom ramen för det internationella samarbetet kunna tillmötesgå behovet av skydd för utländska myndigheters verksamhet, precis som svenska myndigheter måste kunna kräva att mellanfolkliga organ och myndigheter i andra stater hanterar information

[1] Europaparlamentets och rådets förordning (EG) nr 1049/2001 av den 30 maj 2001 om allmänhetens tillgång till Europaparlamentets, rådets och kommissionens handlingar.

från Sverige på ett sätt som inte skadar svenska myndigheters verksamhet. Sverige kan till exempel inte hävda att sådana uppgifter som i andra staters nationella verksamhet hade omfattats av sekretess till skydd för allmänna intressen ska vara offentliga om de lämnats till en svensk myndighet inom ramen för ett internationellt samarbete, till exempel från en myndighet i en annan medlemsstat i EU. Vidare finns det ett behov av att säkerställa att Sverige kan skydda uppgifter om enskildas förhållanden som överlämnats till svenska myndigheter från andra stater eller mellanfolkliga organisationer, eftersom ett otillräckligt sekretesskydd även i detta avseende kan försvåra det internationella samarbetet (prop. 2012/13:192 s. 24).

Om andra stater och mellanfolkliga organisationer inte skulle kunna förlita sig på att svenska myndigheter kan fullgöra sin skyldighet att i enlighet med avtal eller rättsakter sekretessbelägga uppgifter som utbyts inom ramen för samarbetet, finns en uppenbar risk att dessa skulle bli mindre benägna att lämna uppgifter till Sverige. Detta skulle få negativa effekter för Sveriges möjligheter att delta i det internationella samarbetet och därmed i förlängningen försämra svenska myndigheters möjlighet att till exempel bedriva en effektiv tillsyn (prop. 2012/13:192 s. 25).

En följd av EU-medlemskapet är att Sverige har överlåtit sin normgivningskompetens och möjlighet att ingå internationella överenskommelser till EU inom vissa områden. Detta innebär att Sverige inte alltid kan ensidigt bestämma vilka informationsutbyten med andra stater som landet ska delta i eller under vilka förutsättningar informationsutbytet ska ske (prop. 2012/13:192 s. 23 och 24).

Inom EU-samarbetet tillämpas ibland den så kallade principen om vetorätt för ursprungsinnehavaren vid internationella överenskommelser som omfattar informationsutbyte (se prop. 2012/13:192 s. 17, samt under rubriken *Vilka möjligheter finns det att säkerställa att motsvarande skydd består efter utlämnande till andra aktörer?* i avsnitt 8.2.5).

Det kan i sammanhanget också nämnas att det inte är möjligt att överföra sekretess från en utländsk myndighet eller mellanfolklig organisation. Vidare är de sekretessbrytande reglerna i 10 kap. OSL och i lagens fjärde och femte avdelningar inte direkt tillämpliga i förhållande till utländska myndigheter och mellanfolkliga organisationer.

7.1.5 Det kommer att ske utlämnande av uppgifter

Utredningens bedömning: Såväl myndigheters tillgängliggörande enligt artikel 36.6 som offentliggörande av uppgifter enligt artikel 38.4 tredje stycket i budgetförordningen kommer att innebära ett utlämnande i rättslig mening. Även uppladdning av uppgifter i Arachne innebär ett utlämnande i rättslig mening.

Skälen för utredningens bedömning: I avsnitt 4.1.1 anges de fall av lämnande och offentliggörande av uppgifter som kan bli aktuella för svenska myndigheter och som behandlas i detta betänkande:

- Lämnande av uppgifter vid ett användande av Arachne:
  - Funktionellt nödvändiga uppgifter (vid ett användande före 2028)
  - Inte funktionellt nödvändiga uppgifter (vid ett användande före 2028)
  - Uppgifter inom ramen för förhandsfunktionen (före och efter 2028)
- Tillgängliggörande av uppgifter enligt artikel 36.6 i budgetförordningen (efter 2028):
  - Rättsligt obligatoriska uppgifter
  - Frivilliga uppgifter
- Offentliggörande av uppgifter enligt artikel 38.4 tredje stycket i budgetförordningen (efter 2028).

Frågan är om ovan nämnda förfaranden innebär ett utlämnande i rättslig mening.

Det uppgiftslämnande som kan ske vid ett *användande av Arachne* kan bestå i att funktionellt nödvändiga och inte funktionellt nödvändiga uppgifter laddas upp direkt i Arachne. Denna uppladdning av uppgifter i Arachne är enligt utredningens bedömning ett utlämnande i rättslig mening. Detsamma gäller vid uppladdning av uppgifter i Arachne inom ramen för förhandsfunktionen.

Arachne innehåller också sökfunktioner, då det till exempel är möjligt att söka på ett projektnamn eller ett företagsnamn. När ett

projekt- eller företagsnamn på det sättet skrivs in i systemet är det enligt utredningens mening inte fråga om något utlämnande av uppgifter från en myndighet. Det är inte fråga om att en uppgift från en myndighet laddas upp i eller förs över till Arachne, utan att ett sökbegrepp används i syfte att få del av uppgifter eller information.

När det gäller information till kommissionen enligt artikel 36.6 i budgetförordningen används i artikeln uttrycken *”göra tillgänglig”* och ”ge tillgång till”. Det anges alltså inte uttryckligen att uppgifter ska lämnas ut till kommissionen. Enligt utredningen står det dock klart att formuleringarna medför att det kommer att ske ett utlämnande av uppgifter från myndigheter i rättslig mening. Detta gäller även om det inte är klart på vilket sätt rent tekniskt som tillgängliggörandet kommer att ske.

Enligt utredningen kommer även ett *offentliggörande av uppgifter* enligt artikel 38.4 tredje stycket i budgetförordningen, om detta skulle bli aktuellt, att innebära ett utlämnande i rättslig mening.

När det gäller *Edes* konstaterar utredningen att det inte krävs något uppgiftslämnande från svenska myndigheter utifrån budgetförordningens reglering (se avsnitt 4.6). Det följer alltså inte några nya utlämnandesituationer av en tillämpning av Edes-regelverket eller ett användande av Edes och utredningen behandlar därför inte heller några sådana frågor.

Sammanfattningsvis konstaterar utredningen att de förfaranden som beskrivs i ovan punktlista kommer att medföra att uppgifter lämnas ut i rättslig mening. I den mån det är fråga om uppgifter som annars är sekretessbelagda kan de som utgångspunkt inte lämnas ut till kommissionen eller andra aktörer med mindre än att det finns någon tillämplig sekretessbrytande eller motsvarande bestämmelse. Dessa frågor behandlas i avsnitten för respektive uppgiftslämnande och system i kapitel 8 samt i avsnitt 7.1.7. Uttrycket ”annars sekretessbelagd uppgift” behandlas närmare i avsnitt 8.2.4.

7.1.6 Frågor om allmänna handlingar och sekretess aktualiseras

Utredningens bedömning: Svenska myndigheters uppgiftslämnande, offentliggörande av uppgifter samt användning av Arachne och Edes aktualiserar frågor om allmänna handlingar och sekretess.

Skälen för utredningens bedömning: För att uppgifter ska kunna lämnas ut krävs bland annat att sekretess inte hindrar ett sådant uppgiftslämnande. Uppgifter kan laddas upp i Arachne i dag. De uppgifter som ska eller kan tillgängliggöras enligt artikel 36.6 i budgetförordningen är också avsedda att föras in i Arachne.

Såväl Arachne som Edes-databasen utgör databaser som svenska myndigheter kommer att beredas åtkomst till. Då svenska myndigheter får åtkomst till uppgifter i dessa databaser uppkommer frågor om i vilken utsträckning de kan komma att betraktas som inkomna och förvarade handlingar hos de mottagande myndigheterna, varigenom andra aktörer kan få rätt att ta del av uppgifterna.

Bestämmelserna i tryckfrihetsförordningen om allmänna handlingar, bestämmelser i offentlighets- och sekretesslagen om handlingars offentlighet och sekretess aktualiseras därför. Vidare kan användningen av databaserna ske som ett led i ärendehandläggning och uppgifter som används kan bli en del av ett ärende. Då kan även partinsynsfrågor aktualiseras.

Även det offentliggörande av uppgifter som kan bli aktuellt enligt artikel 38.4 tredje stycket i budgetförordningen aktualiserar frågor om sekretess.

7.1.7 Sekretessbestämmelser som kan aktualiseras

Flera sekretessbestämmelser skulle kunna aktualiseras

Under arbetet med detta betänkande och även i viss mån inom ramen för arbetet bedrivet av Utredningen om hantering av EU-medel har det, bland annat av berörda myndigheter, lyfts fram i vilken utsträckning sekretessbestämmelser kan aktualiseras vid myndigheternas tillgängliggörande av uppgifter för kommissionen eller vid ett användande av Arachne som ett verktyg. Motsvarande frågeställningar har också lyfts fram rörande en tillämpning av Edes (SOU 2024:22, s. 452–457).

Även inom ramen för de regeringsuppdrag som RRF-myndigheterna Boverket, Myndigheten för digital förvaltning, Myndigheten för yrkeshögskolan, Naturvårdsverket, Post- och telestyrelsen, Skolverket, Socialstyrelsen, Statens energimyndighet, Trafikverket samt Universitetskanslersämbetet fått (se avsnitt 5.3.3), har de bland annat lyft frågor om sekretess vid deras eventuella användning av Arachne. Därvid har vissa sekretessbestämmelser diskuterats särskilt. I vilken mån och på vilket sätt olika sekretessbestämmelser aktualiseras behandlas närmare i kapitel 8. I det följande ges en översiktlig beskrivning av de sekretessbestämmelser som har en särskilt central betydelse för de frågor som behandlas i detta betänkande.

Sekretess till skydd för rikets säkerhet eller dess förhållande till andra stater eller mellanfolkliga organisationer

Eftersom de förhållanden som utredningen har att behandla innebär att uppgifter hanteras i förhållande till EU:s institutioner och andra medlemsländer behöver överväganden göras utifrån bestämmelserna i 15 kap. OSL om sekretess till skydd för rikets säkerhet eller dess förhållande till andra stater eller mellanfolkliga organisationer.

Utrikessekretessen regleras i 15 kap. 1 § första stycket OSL, som anger att sekretess gäller för uppgift som rör Sveriges förbindelser med en annan stat eller i övrigt rör annan stat, mellanfolklig organisation, myndighet, medborgare eller juridisk person i annan stat eller statslös, om det kan antas att det stör Sveriges mellanfolkliga förbindelser eller på annat sätt skadar landet om uppgiften röjs.

I 15 kap. 1 a § OSL behandlas sekretess i det internationella samarbetet. Enligt första stycket gäller sekretess 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 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. Enligt tredje stycket gäller, om sekretess gäller enligt första eller andra stycket, att de sekretessbrytande bestämmelserna i 10 kap. 5 c §, 15–27 §§ och 28 § första stycket OSL inte får tillämpas.

15 kap. 1 b § OSL tar sikte på utrikessekretess vid direktåtkomst. Enligt bestämmelsen gäller sekretess för uppgift som en myndighet har elektronisk tillgång till i en upptagning för automatiserad behandling hos en annan stat eller mellanfolklig organisation, om myndigheten inte får behandla uppgiften enligt en bindande EU-rättsakt eller ett av Sverige eller EU ingånget avtal med en annan stat eller mellanfolklig organisation.

Försvarssekretessen, som regleras i 15 kap. 2 § OSL, behöver också beaktas. Den sekretessen gäller för uppgift som rör verksamhet för att försvara landet eller planläggning eller annan förberedelse av sådan verksamhet eller som i övrigt rör totalförsvaret, om det kan antas att det skadar landets försvar eller på annat sätt vållar fara för rikets säkerhet om uppgiften röjs (första stycket första meningen).

Sekretess till skydd främst för myndigheters verksamhet för inspektion, kontroll eller annan tillsyn

Myndigheternas arbete med att kontrollera att EU-medel hanteras korrekt är centralt i denna utredning. Bestämmelserna om sekretess till skydd främst för myndigheters verksamhet för inspektion, kontroll eller annan tillsyn i 17 kap. OSL behöver därför också beaktas.

17 kap. 1 § OSL gäller sekretess vid förberedelser för inspektion, revision eller annan granskning. Enligt bestämmelsen gäller sekretess för uppgift om planläggning eller andra förberedelser för sådan inspektion, revision eller annan granskning som en myndighet ska göra, om det kan antas att syftet med granskningsverksamheten motverkas om uppgiften röjs. I ett avgörande från Kammarrätten i Stockholm har Försäkringskassans riskprofiler och uppgifterna som hänförde sig till arbetet med dessa vid granskning och kontroll av förmånsärenden ansetts omfattas av sekretess enligt bestämmelsen (Kammarrätten i Stockholms dom den 4 februari 2022 i mål nr 8358-21). Utformningen av skaderekvisitet innebär att uppgifter som ska användas vid flera granskningstillfällen, till exempel checklistor för revision, som utgångspunkt inte får lämnas ut så länge uppgifterna används i granskningsverksamheten. När de inte längre ska användas i denna verksamhet ska sådana uppgifter lämnas ut (Lenberg m.fl. Offentlighets- och sekretesslagen, Norstedts Juridik, JUNO Version 31, Publicerad digitalt den 17 juni 2025, kommentaren till 17 kap. 1 § OSL). Det bör noteras att det behöver göras en bedömning av

om syftet med granskningsverksamheten motverkas av om uppgiften röjs och den saken kan bedömas olika beroende på vem ett utlämnande sker till.

Av 17 kap. 1 b § OSL framgår att sekretess gäller för uppgift om metoder, modeller och riskfaktorer som hänför sig till dataanalyser och urval för att förebygga, förhindra och upptäcka felaktiga utbetalningar, om det kan antas att det allmännas syfte med verksamheten motverkas om uppgiften röjs. Paragrafen tillkom i samband med framtagandet av reglering för den nya Utbetalningsmyndighetens verksamhet. Bestämmelsen omfattar exempelvis uppgifter om vilka riskfaktorer som en myndighet har tagit fram för att identifiera misstänkt felaktiga utbetalningar, men även uppgifter om hur dataanalyser eller urvalsmodeller har utformats eller utvecklats kan sekretessbeläggas med stöd av bestämmelsen (prop. 2022/23:34 s. 215). Sekretessen gäller för dessa uppgifter oavsett i vilken verksamhet som de förekommer. Sekretessen gäller – liksom beträffande 17 kap. 1 § – så länge den metod, modell eller riskfaktor som uppgiften är hänförlig till används i verksamheten. När dessa inte längre används upphör sekretessen och uppgifter om dem ska följaktligen lämnas ut på begäran (prop. 2022/23:34 s. 215 och 216).

Särskilt om uppgifter om fysiska personer

I 21 kap. OSL finns bestämmelser till skydd för uppgift om enskilds personliga förhållanden oavsett i vilket sammanhang uppgiften förekommer.

Uppgifter om fysiska personers namn, personnummer och adress är normalt offentliga. Under vissa förutsättningar och efter särskild ansökan kan en person få sina personuppgifter av detta slag skyddade genom att en sekretessmarkering förs in i folkbokföringssystemet. En sådan sekretessmarkering i folkbokföringen har ingen annan betydelse än att vara en varningssignal om behovet av en noggrann sekretessprövning innan en sekretessmarkerad uppgift lämnas ut.

Enligt 21 kap. 3 § första stycket OSL gäller sekretess för uppgift om enskilds bostadsadress eller annan jämförbar uppgift som kan lämna upplysning om var den enskilde bor stadigvarande eller tillfälligt, den enskildes telefonnummer, e-postadress eller annan jämförbar uppgift som kan användas för att komma i kontakt med denne.

Sekretessen enligt första stycket gäller bara om det av särskild anledning kan antas att den enskilde eller någon närstående till denne kan komma att utsättas för hot eller våld eller lida annat allvarligt men om uppgiften röjs. Bestämmelsen har alltså ett rakt kvalificerat skaderekvisit, vilket innebär att presumtionen är att typiskt sett harmlösa uppgifter kan lämnas ut utan någon närmare skadebedömning i det enskilda fallet (se Lenberg m.fl., Offentlighets- och sekretesslagen, JUNO Version 31, Publicerad digitalt den 17 juni 2025, kommentaren till 21 kap. 3 § OSL). Liksom övriga sekretessbestämmelser i 21 kap. OSL gäller sekretessen i 21 kap. 3 § oavsett var uppgiften befinner sig och varje myndighet har att pröva sekretessen vid ett utlämnande.

Även om en uppgift inte omfattas av sekretess enligt någon annan bestämmelse i offentlighets- och sekretesslagen omfattas uppgiften av sekretess, om det kan antas att uppgiften efter ett utlämnande kommer att behandlas i strid med dataskyddsförordningen, lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning, härefter dataskyddslagen, eller 6 § lagen (2003:460) om etikprövning av forskning som avser människor. Detta följer av 21 kap. 7 § OSL. Detta utgör ett generellt förbud att lämna ut personuppgifter, om det kan antas att personuppgiften efter utlämnandet kommer att behandlas i strid med den nämnda dataskyddsregleringen. Bedömningen tar alltså inte sikte på om myndighetens eget utlämnande av uppgifter skulle strida mot nämnda regleringar (Lenberg m.fl., Offentlighets- och sekretesslagen, Norstedts Juridik, JUNO Version 31, Publicerad digitalt den 17 juni 2025, kommentaren till 21 kap. 7 § OSL).

Sekretess vid tillsyn med mera för uppgift om en enskilds affärs- eller driftförhållanden – 30 kap. 23 § OSL

Bestämmelser om sekretess vid tillsyn, stödverksamhet och liknande finns i 30 kap. 23 § OSL. Med stöd av bestämmelsen kan sekretess gälla för uppgift om en enskilds affärs- eller driftförhållanden, uppfinningar eller forskningsresultat, om det kan antas att den enskilde lider skada om uppgiften röjs. Sekretess kan även gälla för uppgift om andra ekonomiska eller personliga förhållanden för den som har trätt i affärsförbindelse eller liknande förbindelse med den som är föremål för myndighetens verksamhet. När det gäller uppgifter av

sistnämnda slag (andra punkten) uppställs inte något skaderekvisit, vilket innebär att sekretessen är absolut.

För att sekretess ska gälla enligt 30 kap. 23 § förutsätts att regeringen har meddelat föreskrifter om det. Relevanta bestämmelser finns i 9 § offentlighets- och sekretessförordningen (2009:641), OSF, som i sin tur hänvisar till förordningens bilaga där det närmare anges i vilka fall sådan sekretess gäller.

Av punkten 106 i bilagan framgår att sekretessen gäller i verksamhet som består i utredning, tillsyn och stödverksamhet enligt förordningen (2022:1379) om förvaltning av program för vissa EU-fonder och förordningen (2022:1826) om EU:s gemensamma jordbrukspolitik. Enligt punkten 107 gäller sekretess i verksamhet som består i utredning, tillsyn och stödverksamhet bland annat enligt lagen (1994:1708) om EU:s förordningar om strukturstöd och om stöd till utveckling av landsbygden. Därigenom omfattas förvaltning av EGFJ, EjFlu, Eruf, ESF + och FRO av sekretessregleringen.

Av punkten 24 framgår att sekretess gäller i verksamhet som består i utredning, planering, tillståndsgivning, tillsyn och stöd inom jordbrukets, rennäringens och fiskets områden hos bland andra Jordbruksverket, Havs- och vattenmyndigheten, Sametinget och länsstyrelser, dock inte för beslut i ärenden med vissa undantag. Genom punkten 24 gäller sekretess vid förvaltning av EHFVF (och stöd enligt förordningen [2022:1461] om stöd från Europeiska havs-, fiskeri- och vattenbruksfonden).

Av punkten 9 i samma bilaga framgår att sekretess gäller i verksamhet som består i utredning, planering, tillståndsgivning, tillsyn och stödverksamhet hos Tillväxtverket. Enligt punkten 88 gäller sekretessen i verksamhet som består i utredning, planering och stödverksamhet hos länsstyrelser i frågor som rör näringslivet, dock inte för beslut i ärenden.

Verksamhet som avser ISF, BMVI och Amif omfattas inte av sekretess enligt bilagan till offentlighets- och sekretessförordningen. Anledningen till detta synes vara att stöden inte avser produktion, handel, transportverksamhet eller näringslivet i övrigt.

7.2 Övergripande om behandling av personuppgifter

7.2.1 Den personliga integriteten skyddas genom flera olika regelverk

Den personliga integriteten skyddas bland annat genom bestämmelser i regeringsformen, den europeiska konventionen av den 4 november 1950 om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) och Europeiska unionens stadga om de grundläggande rättigheterna (EU:s rättighetsstadga), samt dataskyddsförordningen.

I 1 kap. 2 § regeringsformen slås det fast att den offentliga makten ska utövas med respekt bland annat för den enskilda människans frihet och att det allmänna ska värna den enskildes privatliv och familjeliv (första och fjärde styckena). Enligt 2 kap. 6 § andra stycket regeringsformen är var och en gentemot det allmänna skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Skyddet får begränsas genom lag under vissa förutsättningar, bland annat de som anges i 2 kap. 21 § regeringsformen (2 kap. 20 §). Skyddet får inte begränsas genom förordning.

Behandling av personuppgifter berör rätten till respekt för privatlivet enligt artikel 8.1 i Europakonventionen. Enligt denna artikel har var och en rätt till skydd för sitt privat- och familjeliv, sitt hem och sin korrespondens. Europakonventionen gäller som svensk lag, se 1 § lagen (1994:1219) om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna. Enligt 2 kap. 19 § regeringsformen får inte lag eller annan föreskrift meddelas i strid med Sveriges åtaganden på grund av Europakonventionen.

I artiklarna 3, 7 och 8 i EU:s rättighetsstadga slås det fast att var och en har rätt till fysisk och mental integritet, respekt för sitt privat- och familjeliv, sin bostad och sina kommunikationer samt skydd av de personuppgifter som rör honom eller henne. Av artikel 52.3 i stadgan följer att i den mån stadgan omfattar rättigheter som motsvarar sådana som garanteras av Europakonventionen ska de ha samma innebörd och räckvidd som enligt konventionen, men att bestämmelsen inte hindrar unionsrätten från att tillförsäkra ett mer långtgående skydd.

7.2.2 EU:s dataskyddslagstiftning

Dataskyddsförordningen är en generell dataskyddslagstiftning. I förordningen fastställs bestämmelser om skydd för fysiska personer med avseende på behandlingen av personuppgifter och om det fria flödet av personuppgifter (artikel 1.1). Eftersom det är en EU-förordning är den direkt tillämplig. I skäl 14 anges att förordningen inte omfattar behandling av personuppgifter rörande juridiska personer, exempelvis uppgifter om namn på och typ av juridisk person samt kontaktuppgifter. Förordningen gäller således inte vid behandling av uppgifter om juridiska personer.

I artikel 6 uttrycks det grundläggande kravet att det ska finnas en giltig rättslig grund för varje behandling av personuppgifter. Bland de rättsliga grunderna kan nämnas att utföra en uppgift av allmänt intresse (artikel 6.1 e).

I artikel 5 ställs ett antal allmänna, men centrala, principer för behandlingen upp. Däribland kan nämnas principen om laglighet, korrekthet och öppenhet, principen om uppgiftsminimering samt principen om ändamålsbegränsning, som inbegriper finalitetsprincipen och som innebär att personuppgifter ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare får behandlas på ett sätt som är oförenligt med dessa ändamål. Vissa kategorier av personuppgifter kringgärdas av ett särskilt skydd.

Det är den personuppgiftsansvarige som ska säkerställa behandlingens förenlighet med dataskyddsregleringen och den ska bland annat genomföra lämpliga tekniska och organisatoriska skyddsåtgärder till exempel genom krav på inbyggt dataskydd och dataskydd som standard och på lämplig säkerhetsnivå (artikel 24, 25 och 32).

Som framgår av såväl förordningens fullständiga namn som dess första artikel är ett syfte med förordningen att underlätta det fria flödet av personuppgifter. Det fria flödet av personuppgifter inom unionen får varken begränsas eller förbjudas av skäl som rör skyddet för fysiska personer med avseende på behandlingen av personuppgifter (artikel 1.3).

Dataskyddsförordningen gäller inte sådan personuppgiftsbehandling som behöriga myndigheter utför i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, i vilket även ingår att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten (artikel 2.2 d). Sådan behandling

omfattas av tillämpningsområdet för EU:s dataskyddsdirektiv[2], här benämnt dataskyddsdirektivet.

När EU:s institutioner behandlar personuppgifter gäller dataskyddsförordningen för EU:s institutioner. Den innehåller flera bestämmelser som liknar dem i dataskyddsförordningen.

Dataskyddsförordningen benämns ofta GDPR (General Data Protection Regulation), och dataskyddsförordningen för EU:s institutioner benämns ofta EUDPR.

Det finns också dataskyddsbestämmelser i annan EU-rättslig reglering. Sådana bestämmelser finns till exempel i budgetförordningen.

7.2.3 Nationell reglering som kompletterar EU:s dataskyddslagstiftning

Även om dataskyddsförordningen är direkt tillämplig i medlemsstaterna förutsätter och möjliggör den kompletterande bestämmelser i nationell rätt. Så har också skett i svensk rätt. Förordningen kompletteras av dataskyddslagen och förordningen (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning.

Härutöver finns ett mycket stort antal sektorsspecifika författningar, ofta kallade registerförfattningar. De reglerar till exempel myndigheters eller verksamheters personuppgiftsbehandling eller behandling som sker i särskilda register. De kompletterar ofta såväl dataskyddsförordningen som dataskyddslagen. Många myndigheter saknar dock sådan särreglering och behandlar personuppgifter enbart med stöd av den generella regleringen, det vill säga dataskyddsförordningen och dataskyddslagen.

Dataskyddsdirektivet har i svensk rätt genomförts genom brottsdatalagen (2018:1177), som i sin tur i flera fall kompletteras av ett antal sektorsspecifika lagar, såsom lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område.

[2] Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF.

7.2.4 Dataskyddsförordningen och dataskyddslagen är tillämplig lagstiftning

Utredningens bedömning: Dataskyddsförordningen och dataskyddslagen kommer att vara tillämpliga vid svenska myndigheters behandling av personuppgifter.

Skälen för utredningens bedömning

Personuppgifter kommer att behandlas

Bland de uppgifter som kan komma att laddas upp i Arachne eller tillgängliggöras enligt artikel 36.6 i budgetförordningen kan det finnas personuppgifter, det vill säga uppgifter som direkt eller indirekt kan hänföras till en fysisk person (varje upplysning som avser en identifierad eller identifierbar fysisk person, se artikel 4.1 i dataskyddsförordningen). Det kan till exempel vara fråga om uppgifter om stödmottagare som utgör enskild firma eller uppgift om verklig huvudman som är en fysisk person. Det kan också finnas kontaktuppgifter som avser en fysisk person. Personuppgifter kan också finnas bland de uppgifter som svenska myndigheter kan komma att offentliggöra enligt artikel 38.4 tredje stycket i budgetförordningen eller kommer att kunna ta del av genom åtkomst till Arachne och Edes.

Vid behandling av personuppgifter behöver dataskyddsregelverket beaktas. Med behandling avses bland annat insamling, registrering, lagring, bearbetning eller ändring, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt (se t.ex. artikel 4.2 i dataskyddsförordningen).

I artikel 36.6 i budgetförordningen används formuleringar om att information ska göras tillgänglig och att det ska ges tillgång till information. Utredningen bedömer att detta i dataskyddsrättslig mening blir fråga om ett utlämnande av personuppgifter (jfr avsnitt 7.1.5 ovan om offentlighet och sekretess).

Vad gäller Arachne används i artikel 36.2 d formuleringar om att möjliggöra tillgång till och elektronisk automatisk hämtning, registrering, lagring och analys av data. I artikel 36.7 används formuleringar om åtkomst till uppgifter och om uppgifter som är tillgängliga via systemet. Vad gäller Edes anges i artikel 144.5 att vissa aktörer ska beviljas tillgång till vissa uppgifter så att de kan kontrollera om det finns

uppgifter av visst slag. Även sådana åtgärder som nu nämns utgör behandling, i dessa fall till exempel läsning, sökning och bearbetning.

Dataskyddsförordningen och dataskyddslagen kommer att vara tillämplig reglering

Den generella regleringen vid behandling av personuppgifter är dataskyddsförordningen. Det materiella tillämpningsområdet för förordningen omfattar sådan behandling av personuppgifter som helt eller delvis företas på automatisk väg samt annan behandling av personuppgifter som ingår i eller kommer att ingå i ett register (se artikel 2.1).

Det finns vissa undantag från tillämpningsområdet. Exempelvis ska behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av unionsrätten inte heller omfattas av förordningens bestämmelser (se artikel 2.2 a). Genom dataskyddslagen har dock förordningens tillämpningsområde på nationell nivå utvidgats till att även omfatta behandling av personuppgifter i verksamhet som inte omfattas av unionsrätten, med vissa specifika undantag (se 1 kap. 2 och 3 §§ dataskyddslagen).

Dataskyddsförordningen gäller vidare inte sådan personuppgiftsbehandling som omfattas av tillämpningsområdet för dataskyddsdirektivet. Det direktivet är, förenklat beskrivet, tillämpligt vid behöriga myndigheters (enligt en särskild definition) personuppgiftsbehandling när den sker i brottsbekämpande syfte (artikel 2.1 dataskyddsdirektivet, se mer under särskild rubrik nedan).

Den personuppgiftsbehandling som kommer att ske som en följd av artikel 36.6 i budgetförordningen utgör ett led i en verksamhet som omfattas av unionsrätten. Detsamma gäller den personuppgiftsbehandling som kan komma att ske som en följd av en användning av Arachne eller Edes, och om offentliggörande av personuppgifter skulle bli aktuellt enligt artikel 38.4 tredje stycket. Behandlingen kommer också att ske automatiserat.

Behandlingen av personuppgifter vid tillgängliggörande enligt artikel 36.6 eller offentliggörande enligt artikel 38.4 kommer vidare enligt utredningens bedömning inte att ske av behöriga myndigheter i dataskyddsdirektivets mening eller i ett sådant syfte att dataskyddsdirektivet blir tillämpligt. Detta bedömer utredningen, utifrån vad som är känt i dag, inte heller kommer att ske när svenska myndig-

heter använder sig av Arachne och Edes. Detta behandlas närmare under särskild rubrik nedan.

Även i budgetförordningen förutsätts att dataskyddsförordningen är tillämplig reglering vid medlemsstaternas och deras myndigheters personuppgiftsbehandling. Som exempel kan nämnas att artikel 5 i budgetförordningen som behandlar skydd för personuppgifter anger att förordningen inte påverkar tillämpningen av dataskyddsförordningen eller dataskyddsförordningen för EU:s institutioner, och att artikel 63 som gäller förvaltningsformen delad förvaltning föreskriver att all behandling ska vara förenlig med dataskyddsförordningen (artikel 63.4 andra stycket budgetförordningen). Även skäl 39 och 129 till budgetförordningen nämner dataskyddsförordningen. Budgetförordningen saknar helt hänvisningar till dataskyddsdirektivet. Motsvarande gäller för tillhörande sektorsspecifik reglering i till exempel CAP-förordningen, CPR och RRF-förordningen.

Dataskyddsförordningen är därmed tillämplig dataskyddsreglering när svenska myndigheter kommer att behandla personuppgifter enligt budgetförordningen och tillhörande sektorsspecifik EU-rättslig reglering. Detta innebär också att den nationella lagstiftning som hör till dataskyddsförordningen är tillämplig, det vill säga dataskyddslagen och tillhörande förordning.

Finns det ytterligare nationell dataskyddsreglering att beakta?

Det finns i stor omfattning sektorsspecifik dataskyddsreglering, som kompletterar dataskyddsförordningen och dataskyddslagen. En särskild fråga är om det finns särskild nationell reglering på dataskyddsområdet, som är tillämplig vid den personuppgiftsbehandling som nu är aktuell. Om så är fallet behöver även den regleringen beaktas i utredningens arbete.

Under arbetet med detta betänkande och tidigare nämnda regeringsuppdrag till RRF-myndigheterna har det, bland annat av berörda myndigheter, tagits upp frågor om tillämplig dataskyddslagstiftning. De myndigheter som utredningen bedömer bli skyldiga att tillgängliggöra uppgifter enligt artikel 36.6 i budgetförordningen och de myndigheter som omfattas av utredningens bedömningar om Arachne och Edes saknar sektorsspecifik dataskyddsreglering när det gäller den behandling som nu är i fråga. Utredningen har inte identifierat

några registerförfattningar för berörda myndigheter som avser nu aktuell slags behandling.

Det finns således inte några särskilda, nationella registerförfattningar som kompletterar dataskyddsförordningen eller dataskyddslagen i detta sammanhang som beaktas inom ramen för denna utredning.

Kan dataskyddsdirektivet och brottsdatalagen vara tillämplig reglering i något fall?

Ovan framgår att utredningen bedömer att dataskyddsdirektivet inte är tillämplig dataskyddsreglering vid nu aktuell personuppgiftsbehandling. Eftersom motverkande av oriktigheter kan ha beröringspunkter med brottsbekämpande verksamhet kan det finnas skäl att närmare behandla frågan om gränsdragningen mellan dataskyddsförordningen och dataskyddslagen å ena sidan, och dataskyddsdirektivet och brottsdatalagen å andra sidan.

Dataskyddsförordningen gäller inte sådan personuppgiftsbehandling som omfattas av tillämpningsområdet för dataskyddsdirektivet. Dataskyddsdirektivet är tillämpligt på behandling av personuppgifter som utförs av behöriga myndigheter i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten (artikel 2.1 jämförd med artikel 1.1 i dataskyddsdirektivet). Brottsdatalagen genomför dataskyddsdirektivet i svensk rätt och gäller med vissa undantag bland annat vid behandling av personuppgifter som utförs av behöriga myndigheter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller verkställa straffrättsliga påföljder (se 1 kap. 1, 2 och 4 §§).

Av avgörande betydelse för att denna reglering ska vara tillämplig är att behandlingen utförs av en behörig myndighet. I 1 kap. 6 § brottsdatalagen definieras behörig myndighet som

1. en myndighet som har till uppgift att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder, eller upprätthålla allmän ordning och säkerhet, när den behandlar personuppgifter för ett sådant syfte, eller

2. en annan aktör som har anförtrotts myndighetsutövning för ett syfte som anges i 1, när den behandlar personuppgifter för ett sådant syfte.

Detta innebär att grundläggande krav för att dataskyddsdirektivet och brottsdatalagen ska vara tillämpliga är att den som behandlar personuppgifterna är en behörig myndighet och i egenskap av sådan behörig myndighet behandlar personuppgifter för något av de i lagen angivna syftena (se också SOU 2017:29, s. 181 och 182 samt prop. 2017/18:232 s. 111 och 112).

Ekobrottsmyndigheten och Polismyndigheten är exempel på myndigheter som i stor utsträckning i egenskap av behörig myndighet behandlar personuppgifter, förenklat beskrivet, i brottsbekämpande syfte. När dessa myndigheter behandlar personuppgifter i brottsbekämpande syfte och gör det i egenskap av behörig myndighet, är brottsdatalagen tillämplig dataskyddslagstiftning, tillsammans med relevant sektorsspecifik lagstiftning.

När det gäller deras brottsbekämpande verksamhet uppfattar utredningen att båda myndigheterna förvisso skulle kunna ha intresse av att kunna ta del av uppgifter från nu aktuella system (se till exempel avsnitt 5.3.5). Om de skulle beredas tillgång till Arachne och Edes och därvid behandlade personuppgifter, till exempel genom sökning eller läsning, i brottsbekämpande syfte, eller förde in personuppgifter i samma syfte, skulle brottsdatalagen vara tillämplig vid den behandlingen.

Som framgår av avsnitt 5.3.5 bedöms dock Ekobrottsmyndigheten och Polismyndigheten i egenskap av brottsbekämpande myndigheter inte komma att vara användare av Arachne, då de inte på det sätt som avses i budgetförordningen kan anses delta i genomförandet av budgeten när de utför sina brottsbekämpande uppdrag (se dock nedan om Polismyndigheten som förvaltande myndighet). När det gäller Edes framgår av avsnitt 6.2 att Ekobrottsmyndigheten och Polismyndigheten i sina brottsbekämpande roller inte ingår bland de myndigheter som bedöms kunna få tillgång till Edes-databasen. Utredningen bedömer också att dessa myndigheter inte i egenskap av brottsbekämpande myndigheter kommer att tillgängliggöra uppgifter enligt artikel 36.6 i budgetförordningen (se till exempel avsnitt 4.4.2). Därmed kan inte utredningen se att dessa myndigheter, såvitt är känt i dagsläget om möjliga användare av eller syften med användning av

systemen, kommer att behandla personuppgifter med stöd av brottsdatalagen.

Båda myndigheterna utför även personuppgiftsbehandling som omfattas av dataskyddsförordningen, då de inte bara behandlar personuppgifter i brottsbekämpande syfte. Polismyndigheten ingår bland de förvaltande myndigheterna enligt budgetförordningen och handlägger och kontrollerar EU-medel från vissa fonder. Vid den personuppgiftsbehandling som sker då agerar Polismyndigheten inte utifrån sina brottsbekämpande uppdrag. Brottsdatalagen är inte tillämplig vid den personuppgiftsbehandlingen. Det är i stället dataskyddsförordningen och dataskyddslagen.

Att motverka oriktigheter, som till exempel att genom kontrollfunktioner motverka felaktig hantering av EU-medel, kan i och för sig medföra att brottslighet förebyggs och också upptäcks. Många åtgärder som vidtas inom ramen för kontrollverksamhet kan ha brottsförebyggande effekter. Det är dock inte att likställa med att brottsdatalagen är tillämplig. I förarbetena till brottsdatalagen ges viss vägledning kring gränsdragningen mellan regelverkens tillämpningsområde, varvid anges att kontrollverksamhet ligger utanför lagens tillämpningsområde (se t.ex. SOU 2017:29, s. 198–203 och prop. 2017/18:232 s. 113). Detta är i överensstämmelse med utredningens bedömning att dataskyddsförordningen och dataskyddslagen är tillämplig reglering vid nu aktuell personuppgiftsbehandling.

Utredningen ser inte i nuläget att några andra myndigheter som behandlar personuppgifter på ett sådant sätt att brottsdatalagen är tillämplig, kommer att använda Arachne (inklusive att vid en sådan användning ladda upp uppgifter i Arachne) eller Edes, eller tillgängliggöra uppgifter enligt artikel 36.6 eller offentliggöra uppgifter enligt artikel 38.4 tredje stycket i budgetförordningen. Då bedömningen av vilken dataskyddsreglering som blir tillämplig avgörs av syftet med personuppgiftsbehandlingen och det är tillämpande myndigheter som har att bedöma den frågan, kan utredningen inte helt utesluta att det i något fall görs en annan bedömning. Det kan inte heller helt uteslutas att så kan bli fallet någon gång framöver, till exempel om regleringen i budgetförordningen förändras eller kretsen som får åtkomst till systemen förändras. Vidare kan praxis eller synen på vad som innefattas i brottdatalagens tillämpningsområde utvecklas.

Det bör observeras att ovanstående bedömningar avser den personuppgiftsbehandling som omfattas av utredningens uppdrag. Om

uppgifter som härrör från Arachne eller Edes skulle komma till exempel Ekobrottsmyndigheten tillhanda och där användas i brottsbekämpande syfte, kan brottsdatalagen vara tillämplig vid den behandlingen. Sådana frågor ligger utanför utredningens uppdrag.

Gränsdragningen till dataskyddsförordningen för EU:s institutioner

Enligt artikel 2.3 i dataskyddsförordningen är förordning (EG) nr 45/2001[3] tillämplig på den behandling av personuppgifter som sker i EU:s institutioner, organ och byråer. Förordning 45/2001 har upphävts och ersatts av dataskyddsförordningen för EU:s institutioner, som enligt artikel 2 är tillämplig på unionsinstitutioners och unionsorgans behandling av personuppgifter, utom – under vissa förutsättningar – viss behandling av Europol och Eppo. Enligt artikel 99 i den förordningen ska hänvisningar till den upphävda förordningen anses som hänvisningar till dataskyddsförordningen för EU:s institutioner.

Vad gäller nu aktuell personuppgiftsbehandling kommer därför dataskyddsförordningen för EU:s institutioner att vara tillämplig när kommissionen tar emot och behandlar uppgifter som svenska myndigheter tillgängliggör för eller på annat sätt lämnar till kommissionen. Då Arachne kommer att användas av såväl EU:s institutioner och organ som nationella myndigheter kan gränsdragningsfrågor om vem som ansvarar för vilken personuppgiftsbehandling uppkomma. Utredningen återkommer till vissa sådana frågor i kommande avsnitt.

7.2.5 Rättsliga grunder och principer för behandlingen som kan aktualiseras

Rättsliga grunder som kan aktualiseras

De vanligaste rättsliga grunderna för myndigheter

All personuppgiftsbehandling behöver vila på en rättslig grund för att vara laglig (artikel 6.1 i dataskyddsförordningen). De rättsliga grunderna räknas upp i artikel 6.1 a–f.

[3] Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter.

De rättsliga grunder som i huvudsak aktualiseras för myndigheter är behandling som är nödvändig för att *fullgöra en rättslig förpliktelse* som åvilar den personuppgiftsansvarige (artikel 6.1 c) och behandling som är nödvändig för att *utföra en uppgift av allmänt intresse* eller som ett led i den personuppgiftsansvariges myndighetsutövning (artikel 6.1 e).

Andra rättsliga grunder är om personuppgifter behandlas med stöd av den registrerades samtycke (artikel 6.1 a), om behandlingen är nödvändig för att fullgöra ett avtal (artikel 6.1 b), för att skydda intressen som är av grundläggande betydelse för en fysisk person (artikel 6.1 d), eller utifrån en intresseavvägning mellan den personuppgiftsansvariges eller tredje parts berättigade intressen och den registrerades intressen och grundläggande fri- och rättigheter (artikel 6.1 f). Den sistnämnda rättsliga grunden gäller inte för behandling som utförs av offentliga myndigheter när de fullgör sina uppgifter (artikel 6.1 andra stycket).

Uppräkningen i artikel 6.1 är uttömmande. Om ingen av de grunder som anges där är tillämplig är behandlingen inte laglig och får därmed inte utföras. De rättsliga grunderna är i viss mån överlappande och flera rättsliga grunder kan därför vara tillämpliga avseende en och samma behandling.

För att en behandling av personuppgifter ska vara tillåten enligt artikel 6.1 b–f måste den vara *nödvändig* i förhållande till den rättsliga grunden. Innebörden av detta krav beskrivs närmare i avsnitt 8.2.6.

Grunderna för behandling enligt artikel 6.1 c och e omfattas av ytterligare krav

Vad gäller grunderna rättslig förpliktelse (artikel 6.1 c) och uppgift av allmänt intresse (artikel 6.1 e) finns ytterligare krav i artikel 6.3. Enligt första stycket i den punkten ska de grunder för behandlingen som avses i artikel 6.1 c och e fastställas i enlighet med unionsrätten eller en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av. Detta innebär inte att den rättsliga grunden nödvändigtvis måste fastställas i eller i enlighet med en av riksdagen beslutad lag. Däremot måste grunden vara fastställd i laga ordning på ett konstitutionellt korrekt sätt. Grunden ska även vara tydlig och precis, och dess tillämpning ska vara förutsebar för personer som omfattas

av den (se skäl 41 till dataskyddsförordningen och prop. 2017/18:105 s. 51 och 52).

Enligt artikel 6.3 andra stycket ska vidare syftet med behandlingen fastställas i den rättsliga grunden eller, i fråga om behandling enligt artikel 6.1 e, vara nödvändigt för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning. Artikel 6.3 ställer också krav på att, i fråga om grunden för personuppgiftsbehandling, unionsrätten eller medlemsstaternas nationella rätt ska uppfylla ett mål av allmänt intresse och vara proportionell mot det legitima mål som eftersträvas.

Dataskyddslagens bestämmelser om rättslig grund enligt artikel 6.1 c och e

Enligt artikel 6.2 i dataskyddsförordningen får medlemsstaterna behålla eller införa mer specifika bestämmelser för att anpassa tillämpningen med hänsyn till behandling för att efterleva punkt 1 c och e genom att närmare fastställa specifika krav för uppgiftsbehandlingen och andra åtgärder för att säkerställa en laglig och rättvis behandling. Så har också skett i svensk lagstiftning. I dataskyddslagen finns bestämmelser om de två ovan nämnda grunderna. I 2 kap. 1 § dataskyddslagen anges att personuppgifter får behandlas med stöd av artikel 6.1 c i dataskyddsförordningen, 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.

Enligt 2 kap. 2 § dataskyddslagen får personuppgifter behandlas med stöd av artikel 6.1 e i dataskyddsförordningen, om behandlingen är nödvändig för att utföra en uppgift av allmänt intresse som följer av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning, eller som ett led i den personuppgiftsansvariges myndighetsutövning enligt lag eller annan författning.

De grundläggande principerna i artikel 5 som måste uppfyllas

Vilka är principerna?

I artikel 5 i dataskyddsförordningen ställs ett antal allmänna, men centrala, principer för behandlingen av personuppgifter upp. Artiklarna 6 och 5 är grundläggande och kumulativa. Det innebär att någon av de rättsliga grunderna i artikel 6 måste vara tillämplig, samtidigt som samtliga principer i artikel 5 ska följas.

Principerna finns i artikel 5.1 och är följande.

a) Personuppgifter ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade (*principen om laglighet, korrekthet och öppenhet*).

b) Personuppgifter ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål. De får inte senare behandlas på ett sätt som är oförenligt med dessa ändamål (*principen om ändamålsbegränsning,* som inbegriper *finalitetsprincipen*).

c) Personuppgifter ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas (*principen om uppgiftsminimering*).

d) Personuppgifter ska vara riktiga och, om nödvändigt, uppdaterade. Alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål (*principen om riktighet*).

e) Personuppgifter får inte förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas (*principen om lagringsminimering*).

f) Personuppgifter ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse (*principen om integritet och konfidentialitet*).

Det är den personuppgiftsansvarige som ska ansvara för och kunna visa att principerna efterlevs (artikel 5.2).

Särskilt om finalitetsprincipen

Som framgår av punktuppställningen ovan är finalitetsprincipen en del av principen om ändamålsbegränsning (artikel 5.1 b). Finalitetsprincipen kommer även till uttryck i artikel 6.4, där det anges vad som i vissa fall ska beaktas vid en bedömning av personuppgiftsbehandlingens förenlighet med finalitetsprincipen. Om en behandling för andra ändamål än det ändamål för vilket personuppgifterna samlades in inte grundar sig på den registrerades samtycke eller på unionsrätten eller medlemsstaternas nationella rätt som utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle för att skydda vissa mål som anges i artikel 23.1, ska den personuppgiftsansvarige bland annat beakta följande för att fastställa huruvida en behandling för andra ändamål är förenlig med det ändamål för vilket personuppgifterna ursprungligen samlades in:

a) Kopplingar mellan de ändamål för vilka personuppgifterna har samlats in och ändamålen med den avsedda ytterligare behandlingen

b) Det sammanhang inom vilket personuppgifterna har samlats in, särskilt förhållandet mellan de registrerade och den personuppgiftsansvarige

c) Personuppgifternas art, särskilt huruvida särskilda kategorier av personuppgifter behandlas i enlighet med artikel 9 eller huruvida personuppgifter om fällande domar i brottmål och överträdelser behandlas i enlighet med artikel 10

d) Eventuella konsekvenser för registrerade av den planerade fortsatta behandlingen

e) Förekomsten av lämpliga skyddsåtgärder, vilket kan inbegripa kryptering eller pseudonymisering.

8 Behovet av åtgärder

8.1 Utredningens uppdrag och vissa utgångspunkter

I detta kapitel görs bedömningar om i vilken mån det på nationell nivå finns behov av författningsändringar eller andra åtgärder i vissa avseenden. Först behandlas behovet av åtgärder för att Sverige ska kunna uppfylla det krav på tillgängliggörande av uppgifter till kommissionen som från och med 2028 kommer att gälla enligt artikel 36.6 i budgetförordningen, se avsnitt 8.2.

I avsnitt 8.3 behandlas behovet av åtgärder för att svenska myndigheter ska kunna lämna uppgifter i de fall det inte finns en rättslig skyldighet att göra det. Det handlar till att börja med om tillgängliggörande av frivilliga uppgifter enligt artikel 36.6 i budgetförordningen. Vidare handlar det om ett sådant lämnande av uppgifter som ett frivilligt användande av Arachne aktualiserar, dels vid ett sådant lämnande av uppgifter om redan beviljade medel som eventuellt sker före 2028, dels vid användande av den så kallade förhandsfunktionen.

Frågan om det finns några hinder för Sverige att uppfylla skyldigheten att offentliggöra vissa uppgifter behandlas i avsnitt 8.4. I avsnitt 8.5 behandlas behovet av åtgärder för att svenska myndigheter ska kunna använda Arachne som verktyg, i betydelsen att de bereder sig tillgång till uppgifter i databasen och använder systemet som ett riskvärderingsverktyg. Behovet av åtgärder för att svenska myndigheter ska kunna använda Edes som verktyg behandlas i avsnitt 8.6.

Utredningens uppdrag som avser kartläggning och bedömning av de regler som styr användningen av Arachne behandlas också delvis i detta kapitel, liksom de skyldigheter som berörda myndigheter kan få inom ramen för den regleringen och regleringen om Edes. De uppdragen behandlas också delvis i kapitel 5 och 6 (där med fokus på budgetförordningens reglering av de två systemen) samt i kapitel 7 (angående regleringen om offentlighet, sekretess och dataskydd).

Utredningen har i uppdrag att kartlägga vilken personuppgiftsbehandling som en anslutning till Arachne och Edes skulle medföra, vilket behandlas i detta kapitel samt i avsnitt 7.2 och kapitel 9. Även flera delar av uppdragen att kartlägga det skydd för personuppgifter som finns i nämnda system, värdera eventuella risker som kommissionens dataskyddsombud har identifierat, utreda om det finns behov av nya eller ändrade bestämmelser för att möjliggöra den personuppgiftsbehandling som en användning av systemen medför samt lämna nödvändiga författningsförslag behandlas i de avsnitten. Utredningen behandlar motsvarande frågor avseende den personuppgiftsbehandling som olika former av uppgiftslämnande förväntas medföra.

En EU-förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater. Det betyder att en förordning ska tillämpas direkt av nationella myndigheter på samma sätt som lagar och andra nationella föreskrifter. Medlemsstaterna är skyldiga att se till att det inte finns nationella bestämmelser som står i strid med en EU-förordning. En fråga som är reglerad i en EU-förordning får som huvudregel inte regleras nationellt. Detta innebär bland annat att den omständigheten att den generella unionsrättsakten om dataskydd är en förordning, och inte ett direktiv, innebär omfattande begränsningar av möjligheten att införa eller behålla nationella bestämmelser om dataskydd. Dataskyddsförordningen både förutsätter och medger dock nationella bestämmelser som kompletterar eller föreskriver undantag från förordningens regler. Bestämmelser får också återges när det är nödvändigt för att den nationella regleringen ska bli begriplig eller sammanhållen (jfr prop. 2017/18:105 s. 21).

8.2 Tillgängliggörande av obligatoriska uppgifter

8.2.1 Uppdraget i denna del

Artikel 36.6 i budgetförordningen medför såväl skyldigheter som möjligheter att tillgängliggöra uppgifter för kommissionen. I detta avsnitt behandlas de rättsliga frågor som uppkommer med anledning av de delar av artikel 36.6 som medför en *skyldighet* att tillgängliggöra uppgifter, det vill säga rättsligt obligatoriskt uppgiftslämnande.

Här behandlas därmed utredningens uppdrag att bedöma om det finns behov av ändrade regler för att svenska myndigheter ska kunna

uppfylla de krav som ställs i budgetförordningen, särskilt i fråga om rapportering av uppgifter för registrering i Arachne, och att lämna författningsförslag, om så är nödvändigt.

Utredningen har också i uppdrag att utifrån den gjorda kartläggningen avseende Arachne utreda och analysera om det bland de data som ska registreras i Arachne finns uppgifter som skulle kunna omfattas av sekretess, och om det finns rättsliga förutsättningar för svenska myndigheter att registrera eller annars utbyta dessa, samt att analysera och bedöma vilket skydd eventuella sekretessbelagda uppgifter skulle ha i samband med andra medlemsstaters och EU-institutioners användning av Arachne. Även om detta avsnitt avser obligatoriskt tillgängliggörande enligt artikel 36.6 medför det faktum att uppgifterna är avsedda att föras in i Arachne att dessa uppdrag också lämpligen behandlas i detta avsnitt. Även uppdraget att lämna nödvändiga författningsförslag i detta avseende behandlas här, liksom uppdraget som rör hur Arachnes funktionalitet och användning påverkas om eventuella sekretessbelagda uppgifter inte kan registreras.

Vad gäller nyss nämnda uppdrag att utreda och analysera om det finns rättsliga förutsättningar för svenska myndigheter att registrera eller annars utbyta uppgifter, kan det nämnas att Arachne inte främst beskrivs som ett system för utbyte av uppgifter. Arachne är dock ett verktyg för bland annat datautvinning och som sådant har det funktioner som kan underlätta för myndigheter att få del av uppgifter från andra myndigheter.

8.2.2 Några utgångspunkter

Som framgår av avsnitt 4.4.2 kan de myndigheter som kommer att omfattas av skyldigheten att tillgängliggöra uppgifter enligt artikel 36.6 i budgetförordningen sammanfattas som myndigheter som tar emot, förvaltar, övervakar, kontrollerar och reviderar EU-medel, om de har skyldigheter enligt sektorsspecifika regler att registrera och lagra sådan information som avses i artikel 36.6 i budgetförordningen. Med nu gällande sektorsspecifika regler på området för delad förvaltning träffar skyldigheten främst Jordbruksverket, Migrationsverket, Polismyndigheten, Svenska ESF-rådet och Tillväxtverket samt länsstyrelserna i Jämtlands, Västerbottens och Norrbottens län. Utredningens bedömningar i detta avsnitt utgår från dessa myndigheter.

Det kan här upprepas att myndigheterna som omfattas av RRF inte kommer att vara skyldiga att tillgängliggöra uppgifter enligt artikel 36.6 (se bland annat avsnitt 4.4.2). Därmed är det inte aktuellt att bedöma behovet av åtgärder när det gäller RRF-myndigheterna.

8.2.3 Obligatoriska uppgifter kommer i regel inte att omfattas av sekretess

Utredningens bedömning: De uppgifter som svenska myndigheter ska tillgängliggöra för kommissionen enligt artikel 36.6 i budgetförordningen kommer i regel inte att omfattas av sekretess. Det kan dock inte uteslutas att vissa uppgifter undantagsvis skulle kunna vara sekretessbelagda i det enskilda fallet.

Skälen för utredningens bedömning

Uppgifterna som ska tillgängliggöras kommer som huvudregel inte att omfattas av sekretess

Som utredningen redogör för i avsnitt 4.4.3 handlar de uppgifter som ska tillgängliggöras enligt artikel 36.6 i budgetförordningen om stödmottagare, åtgärden och verkliga huvudmän. Sådana slags uppgifter lämnas i stor utsträckning redan i dag till kommissionen eller offentliggörs direkt på utlämnande myndighets hemsida. Uppgifterna behöver enligt budgetförordningen bara tillgängliggöras i den utsträckning de behöver lagras och registreras enligt sektorsspecifika regler. Det betyder att det närmare innehållet i skyldigheten bestäms genom annan reglering än budgetförordningen, samtidigt som den yttersta gränsen för vilka typer av uppgifter som omfattas av skyldigheten bestäms av budgetförordningen.

Utredningen om hantering av EU-medel anförde i betänkandet *En ny organisation för förvaltning av EU-medel* (SOU 2024:22) att majoriteten av de rättsligt obligatoriska uppgifterna förefaller vara av sådan karaktär att de antingen redan är offentliga eller i vart fall inte omfattas av sekretess. Enligt den utredningen krävs det emellertid att en myndighet gör en prövning av huruvida delning är möjligt innan information läggs in i Arachne. Utredningen redogjorde för att bland annat Tillväxtverket hade anfört att det kan bli svårt att

dela sekretessbelagda uppgifter i Arachne om uppgifterna därmed blir tillgängliga inte bara för den egna myndigheten och kommissionen, utan för samtliga förvaltande myndigheter runt om i unionen som är anslutna till verktyget (se SOU 2024:22, s. 455 och 456).

I expertgruppen i denna utredning har det framkommit att det i allmänhet inte synes finnas några rättsliga hinder mot att tillgängliggöra uppgifter för kommissionen inom det rättsligt obligatoriska området, samtidigt som vissa tveksamheter framförts. Dessa tveksamheter har bland annat gällt möjligheten att tillgängliggöra födelsedatum på fysiska personer och uppgifter om personer med skyddade personuppgifter. Vidare har det framförts att det kan innebära problem om insatsens art och ändamål behöver anges på ett mer detaljerat sätt.

När det gäller vilka sekretessbestämmelser som skulle kunna aktualiseras har vissa diskuterats särskilt. Det handlar bland annat om sekretess till skydd för rikets säkerhet eller dess förhållande till andra stater eller mellanfolkliga organisationer som regleras i 15 kap. offentlighets- och sekretesslagen (2009:400), OSL, om sekretess till skydd främst för myndigheters verksamhet för inspektion, kontroll eller annan tillsyn i 17 kap. 1–1 a §§ och sekretess vid tillsyn med mera för uppgift om en enskilds affärs- eller driftförhållanden enligt 30 kap. 23 § OSL. Dessa sekretessbestämmelser beskrivs översiktligt i avsnitt 7.1.7. Bestämmelsen i 21 kap. 7 § OSL, som behandlas närmare i det avsnittet, kan nämnas särskilt här. Den innebär att även om en uppgift inte omfattas av sekretess enligt någon annan bestämmelse i offentlighets- och sekretesslagen omfattas uppgiften av sekretess om det kan antas att uppgiften efter ett utlämnande kommer att behandlas i strid med dataskyddsregelverket. Det är dock utredningens bedömning att bestämmelsen inte bör aktualiseras i fråga om tillgängliggörande enligt artikel 36.6 i budgetförordningen. Det är ett grundläggande krav att åtkomsten till de uppgifter som behandlas i Arachne ska överensstämma med tillämpliga dataskyddsregler (se artikel 36.7 andra stycket i budgetförordningen). Det saknas därför anledning att anta att de uppgifter som tillgängliggörs för kommissionen enligt artikel 36.6, vilka är avsedda att tillföras Arachne, efter ett utlämnande kommer att behandlas i strid med dataskyddsregelverket.

Enligt utredningens mening kommer de uppgifter som ska tillgängliggöras för kommissionen enligt artikel 36.6 i budgetförordningen i de flesta fall över huvud taget inte att omfattas av någon

tillämplig sekretessbestämmelse (även om undantag kan förekomma, vilket behandlas nedan). Det finns då i sekretesshänseende inga hinder mot att dessa uppgifter tillgängliggörs och lämnas ut.

Vidare innebär det förhållandet att en uppgift omfattas av tillämpningsområdet för en sekretessbestämmelse inte i sig att uppgiften är sekretessbelagd i det enskilda fallet. Det krävs också att sekretessbestämmelsens skaderekvisit är uppfyllt, såvida det inte är fråga om absolut sekretess. Enligt utredningens mening är utgångspunkten att skyldigheten i artikel 36.6 är utformad på ett sådant sätt att endast uppgifter som i regel är harmlösa och kan lämnas ut utan stöd av en sekretessbrytande bestämmelse omfattas. Det innebär att uppgifterna i regel kan tillgängliggöras för kommissionen, även om uppgifterna skulle omfattas av tillämpningsområdet för en sekretessbestämmelse. Detta utvecklas nedan bland annat vad gäller uppgifter om fysiska personers namn, personnummer, adress med mera.

Tillgängliggörandet bör ofta kunna ske utan att vissa uppgifter lämnas ut – men undantag kan finnas

Som framgår ovan kommer många av de uppgifter som ska tillgängliggöras redan att vara offentliga. I vilken utsträckning uppgifter som är sekretessreglerade behöver tillgängliggöras beror till viss del på en tolkning av skyldigheten i artikel 36.6 i budgetförordningen när det gäller hur detaljerade uppgifterna behöver vara. Följande exempel kan nämnas, som tar utgångspunkt i regleringen av de uppgifter som ska tillgängliggöras om insatsen enligt artikel 36.6 första stycket b, nämligen bland annat det belopp för vilket ett åtagande har gjorts (artikel 38.2 d) och åtgärdens art och ändamål (artikel 38.2 e).

När det gäller åtgärdens art och ändamål får det anses något oklart hur detaljerade uppgifter som behöver lämnas. Det kan tänkas att jordbruksstöd lämnas för projekt som har betydelse för Sveriges tillgång till livsmedel under kris- och krigstider. Det kan inte uteslutas att det i förhållandena bakom sådana projekt finns information som omfattas av försvarssekretess enligt 15 kap. 2 § OSL. Enligt den bestämmelsen gäller sekretess för uppgift som rör verksamhet för att försvara landet eller planläggning eller annan förberedelse av sådan verksamhet eller som i övrigt rör totalförsvaret, om det kan antas att det skadar landets försvar eller på annat sätt vållar fara för rikets säkerhet om uppgiften röjs.

Det kan dock inte ur de krav som ställs i artikel 36.6 i budgetförordningen utläsas att uppgifter behöver lämnas på en sådan detaljnivå att sådana skyddsvärda förhållanden som skisseras ovan måste röjas. Det framstår som troligt att åtgärdens art och ändamål i allmänhet kan beskrivas på ett sådant sätt att skyddsvärd information inte röjs. Det kan inte heller antas vara syftet med budgetförordningens bestämmelser att denna typ av känslig information ska röjas. En sådan ordning kan inte anses ligga i kommissionens eller medlemsstaternas intresse.

Det kan emellertid noteras att uppgift om det belopp för vilket ett åtagande har gjorts ingår bland de uppgifter som ska tillgängliggöras, givetvis under förutsättning att en skyldighet att registrera och lagra sådan information följer av sektorsspecifika regler (se artikel 36.6 b och 38.2 d i budgetförordningen). En uppgift om total projektkostnad skulle, i kombination med andra uppgifter, kunna avslöja information om stödmottagares ekonomiska planer. Sådana uppgifter kan omfattas av sekretess om det kan antas att den enskilde lider skada om uppgiften röjs. Detta skulle kunna aktualisera en tillämpning av 30 kap. 23 § OSL. Som utvecklas i avsnitt 7.1.7 krävs det, för att sekretess ska gälla enligt 30 kap. 23 § OSL, att regeringen har meddelat föreskrifter om det, vilket har skett inom aktuellt område, se 9 § offentlighets- och sekretessförordningen (2009:641), OSF. Enligt utredningen är det svårt att bedöma hur vanligt det skulle vara att röjande av en uppgift om projektkostnad skulle medföra ett sådant men. Det kan noteras att sådana uppgifter som utgångspunkt ingår bland de uppgifter som ska offentliggöras enligt artikel 38.2 i budgetförordningen, även om en möjlighet till undantag finns i artikel 38.3.

Generellt bör det alltså finnas goda förutsättningar för myndigheterna att tillgängliggöra uppgifter inom det obligatoriska området på ett sådant sätt att uppgifter som är sekretessbelagda inte lämnas ut, men det kan också finnas undantagsfall då annars sekretessbelagda uppgifter behöver tillgängliggöras (se avsnitt 8.2.4 om uttrycket ”annars sekretessbelagd uppgift”).

Särskilt om uppgift om fysiska personers namn, personnummer, adress med mera

Uppgifter om fysiska personers namn, personnummer och adress är normalt offentliga.

Frågan kan ställas om det med anledning av bestämmelsen i artikel 36.6 i budgetförordningen kan bli nödvändigt för någon svensk myndighet att tillgängliggöra uppgifter om en enskild person som efter en sekretessprövning kan anses vara sekretessbelagda.

De uppgifter om enskilda fysiska personer som ska tillgängliggöras enligt artikel 36.6 är följande. För mottagare ska för- och efternamn samt födelsedatum tillgängliggöras, liksom regionen på Nuts 2-nivå där mottagaren befinner sig, om mottagaren har hemvist i unionen. Om mottagaren inte har hemvist i unionen ska i stället uppgift om landet där mottagaren befinner sig tillgängliggöras (artikel 36.6 läst tillsammans med 38.2 b och c). För mottagarens verkliga huvudmän, när mottagaren inte är en fysisk person, ska tillgängliggöras uppgifter om för- och efternamn, födelsedatum samt registreringsnummer för mervärdesskatt eller skatteregistreringsnummer om sådana finns, eller en annan unik identifieringskod på landsnivå. Med det sistnämnda bör kunna avses personnummer.

Artikel 36.6 ställer inte krav på tillgängliggörande av telefonnummer eller e-postadress och när det gäller fysiska personer ställs inte heller krav på postadress. Beträffande fysiska personer som är mottagare av stöd räcker det – när det gäller information om var personen befinner sig – som framgår ovan med uppgift om region på Nuts-2 nivå, om mottagaren har hemvist i unionen. Nuts är den regionala indelning som används inom EU för statistikredovisning. (I Sverige utgörs Nuts-2 av åtta riksområden: Stockholm, Östra Mellansverige, Småland med öarna, Sydsverige, Västsverige, Norra Mellansverige, Mellersta Norrland och Övre Norrland.) Detta, tillsammans med vad som sägs ovan om att det räcker med uppgift om hemvistland om mottagare utanför unionen, innebär att artikel 36.6 inte ställer krav på uppgifter om en fysisk person på ett sådant sätt att det enbart med dessa uppgifter går att lokalisera personen eller ta kontakt med personen.

Det kan i sammanhanget noteras att enligt datafält 7, bilaga XVII i CPR, ska stödmottagarens kontaktuppgifter anges, vilket språkligt synes kunna omfatta adress till fysisk person. Utredningen uppfattar

regelverket så att den begränsning av skyldigheten att tillgängliggöra uppgifter som finns i artikel 36.6 i budgetförordningen får genomslag på ett sådant sätt att endast hemvist på Nuts-2 nivå behöver göras tillgänglig, även om CPR skulle anses kräva mer detaljerad information.

Det kan också noteras att det i användargränssnittet för Arachne beträffande vissa fonder inte finns fält för att lämna adressuppgifter, vilket innebär att det där saknas möjlighet att tillgängliggöra uppgifter om adress (se avsnitt 8.3.2).

Utredningen gör bedömningen att artikel 36.6 inte ställer krav på mer detaljerade uppgifter beträffande hemvist för fysiska personer och att det därför inte bör finnas krav på att tillgängliggöra uppgifter som omfattas av sekretess enligt 21 kap. 3 § första stycket OSL, som handlar om sekretess för uppgift om enskilds bostadsadress eller annan jämförbar uppgift som kan lämna upplysning om var den enskilde bor stadigvarande eller tillfälligt, den enskildes telefonnummer, e-postadress eller annan jämförbar uppgift som kan användas för att komma i kontakt med denne.

Det förefaller också osannolikt att mottagare av stöd och verkliga huvudmän skulle lida sådant men som avses i bestämmelsen genom att deras namn, födelsedatum eller personnummer (för verkliga huvudmän) skulle tillgängliggöras för kommissionen. Som nämns ovan ställer artikel 36.6 i budgetförordningen inte krav på sådana uppgifter om en fysisk person att det enbart med dessa uppgifter går att lokalisera eller ta kontakt med personen.

Sammanfattningsvis bedömer utredningen att de uppgifter som, med anledning av bestämmelsen i artikel 36.6 i budgetförordningen, ska tillgängliggöras i allmänhet kommer att kunna lämnas ut efter en sekretessprövning. I enskilda fall kan det dock inte helt uteslutas att sekretess kan gälla för sådana uppgifter.

När det gäller uppgifter som härrör från ärenden om skyddad folkbokföring borde sådana uppgifter över huvud taget inte behöva tillgängliggöras för kommissionen enligt artikel 36.6.

Sekretess kan komma att gälla även enligt andra bestämmelser

Ovan redogör utredningen för de sekretessbestämmelser vars tillämplighet särskilt har diskuterats när det gäller tillgängliggörande enligt artikel 36.6 i budgetförordningen. Nya sektorsspecifika regler

kommer att tillkomma inför den nya programperioden och därmed kan potentiellt såväl nya uppgifter som nya berörda myndigheter aktualiseras. Det kan därför inte uteslutas att uppgifter kan komma att vara sekretessreglerade enligt andra bestämmelser. Det bör dock erinras om att artikel 36.6 i budgetförordningen utgör en yttersta avgränsning av vilka uppgifter som behöver tillgängliggöras. Även om sektorsspecifika regler i framtiden innehåller krav på att nya uppgifter ska registreras och lagras behöver dessa inte tillgängliggöras för kommissionen, om de inte också omfattas av artikel 36.6.

8.2.4 Det krävs inte författningsändringar på sekretessområdet för tillgängliggörande av obligatoriska uppgifter

Utredningens bedömning: Det behövs inga författningsändringar i sekretesshänseende för att svenska myndigheter ska kunna uppfylla kraven i artikel 36.6 i budgetförordningen om att göra uppgifter tillgängliga för kommissionen. För det fall att uppgifterna i det enskilda fallet är sekretessbelagda är tillgängliggörandet möjligt med stöd av en befintlig bestämmelse i offentlighets- och sekretesslagen om utlämnande till mellanfolkliga organisationer.

Skälen för utredningens bedömning

Det kommer att vara möjligt att tillgängliggöra sekretessbelagda uppgifter med stöd av 8 kap. 3 § 1 OSL

I föregående avsnitt framgår att uppgifter som ska tillgängliggöras för kommissionen som huvudregel inte kommer att omfattas av sekretess. Det kan dock inte helt uteslutas att vissa uppgifter undantagsvis skulle kunna vara sekretessbelagda i det enskilda fallet, exempelvis rörande projektkostnaden. För att uppgifter som annars är sekretessbelagda ska få lämnas ut krävs att det finns en bestämmelse som möjliggör utlämnande.

I detta sammanhang använder utredningen uttrycket annars sekretessbelagda uppgifter för att beskriva uppgifter för vilka sekretess som utgångspunkt gäller enligt offentlighets- och sekretesslagen men som ändå kan lämnas till kommissionen, exempelvis med en tillämpning av bestämmelsen i 8 kap. 3 § OSL. Hade den bestämmelsen inte

varit tillämplig hade uppgiften varit sekretessbelagd enligt definitionen i 3 kap. 1 § OSL (om uttrycket annars sekretessbelagda uppgifter, se SOU 2024:63, s. 31–33). I denna del gör utredningen följande bedömningar.

Utgångspunkten är att en uppgift för vilken sekretess gäller inte heller får röjas för en utländsk myndighet eller en mellanfolklig organisation (8 kap. 3 § OSL). Som undantag från denna huvudregel gäller dock om utlämnande sker i enlighet med särskild föreskrift i lag eller förordning (8 kap. 3 § 1 OSL), eller uppgiften i motsvarande fall skulle få lämnas ut till en svensk myndighet och det enligt den utlämnande myndighetens prövning står klart att det är förenligt med svenska intressen att uppgiften lämnas till den utländska myndigheten eller den mellanfolkliga organisationen (8 kap. 3 § 2 OSL).

Paragrafen medför inte någon förpliktelse att lämna uppgifter utan har bara till funktion att fastställa under vilka förutsättningar som sekretessbelagda uppgifter får lämnas till en utländsk myndighet eller en mellanfolklig organisation.

Kommissionen är, vid en tillämpning av paragrafen, att betrakta som en mellanfolklig organisation, alternativt som en del av en mellanfolklig organisation (EU). Det kan därför konstateras att bestämmelsen kan tillämpas på ett uppgiftsutlämnande till kommissionen. Den första punkten i bestämmelsen avser vidare inte bara svenska författningar, utan även EU-förordningar (se prop. 2023/24:87 s. 66). Artikel 36.6 i budgetförordningen innebär en skyldighet för svenska myndigheter att lämna uppgifter.

Av ovanstående drar utredningen slutsatsen att det kommer att vara möjligt att – för de undantagsfall att uppgifterna annars är sekretessbelagda – göra uppgifter tillgängliga för kommissionen när tillgängliggörandet följer av skyldigheten i artikel 36.6 i budgetförordningen.

En tillämpning av 8 kap. 3 § 1 OSL hindrar inte rutinmässigt uppgiftslämnande

Sekretessregleringen tar inte i sig sikte på sättet för utlämnande, men bestämmelsernas utformning kan påverka på vilket sätt som uppgifter kan lämnas ut. I nu aktuellt sammanhang är det relevant att titta närmare på om en tillämpning av 8 kap. 3 § 1 OSL kan medge den planerade metoden för uppgiftslämnande.

Som framgår av tidigare redovisningar (se t.ex. avsnitt 4.4.5) är uppgiftslämnandet enligt artikel 36.6 i budgetförordningen avsett att kunna ske automatiskt. Av artikel 36.2 d framgår att Arachne ska möjliggöra bland annat elektronisk automatisk hämtning av data och av skäl 30 framgår att aktuell information och uppgifter om mottagare av unionsmedel automatiskt bör hämtas från och överföras till det systemet, i realtid när så är möjligt, bland annat med användning av relevanta nationella databaser. Därmed kommer det inte att göras en manuell inläggning av varje uppgift, utan uppgiftslämnande kommer att ske rutinmässigt.

Det uppgiftslämnande som 8 kap. 3 § 1 OSL möjliggör, utesluter enligt utredningens mening inte ett sådant förfarande. Det krävs dock en bedömning på förhand av utlämnande myndighet av om förutsättningarna för utlämnande är uppfyllda. Det ankommer således på utlämnande myndighet att innan ett sådant automatiskt eller rutinmässigt utlämnande inleds, säkerställa att uppgifterna får lämnas ut.

Arachnes funktionalitet påverkas inte

Utredningen bedömer att rättsligt obligatoriska uppgifter kommer att kunna tillgängliggöras och föras in i Arachne. Därmed har utredningen inte skäl att utreda om Arachnes funktionalitet och användning påverkas om eventuella sekretessbelagda uppgifter på det rättsligt obligatoriska området inte kan registreras.

8.2.5 Skydd motsvarande sekretess när uppgifterna lämnats ut kan inte garanteras

Utredningens bedömning: Uppgifter som svenska myndigheter kommer att tillgängliggöra för kommissionen och som därmed kan komma att föras in i Arachne kan antas ha ett visst skydd när olika aktörer använder Arachne som verktyg men skydd motsvarande sekretess kan inte garanteras. En sådan garanti är inte heller nödvändig.

Skälen för utredningens bedömning

För det fall att annars sekretessbelagda uppgifter lämnas ut kan det inte uteslutas att de efter ett utlämnande får ett svagare skydd

Det ingår i utredningens uppdrag att analysera och bedöma vilket skydd eventuella sekretessbelagda uppgifter skulle ha i samband med andra medlemsstaters och EU-institutioners användning av Arachne. Rättsliga frågor rörande Arachne behandlas i huvudsak i avsnitt 8.5 nedan. I detta avsnitt behandlas frågor om hur uppgifter som kommer att tillgängliggöras av svenska myndigheter enligt artikel 36.6 i budgetförordningen och som skulle kunna omfattas av sekretess i Sverige, kan vara skyddade när de överförts till kommissionen och förts in i Arachne.

Till att börja med kan konstateras, vilket utvecklas i avsnitt 8.2.3, att svenska myndigheter bör ha goda förutsättningar att tillgängliggöra uppgifter på ett sådant sätt att uppgifter som är sekretessbelagda i det enskilda fallet över huvud taget inte behöver lämnas ut. Som utvecklas ovan kan det dock inte helt uteslutas att annars sekretessbelagda uppgifter ändå tillgängliggörs enligt artikel 36.6.

Uppgifter som är sekretessreglerade i Sverige och som tillgängliggörs för kommissionen enligt artikel 36.6 i budgetförordningen kan förenklat sägas inte längre omfattas av någon svensk sekretessreglering. Frågan är då om uppgifterna ändå omfattas av något motsvarande skydd hos de aktörer som använder Arachne som ett verktyg. Dessa aktörer kan vara förvaltande myndigheter i andra medlemsländer eller EU:s institutioner.

När det gäller ett användande av Arachne av myndigheter i andra medlemsländer kommer åtkomstbegränsningar och användningsbegränsningar som framgår av till exempel Arachne-stadgan (Arachne, Charter for the introduction, the application and the integration of the Arachne risk scoring tool) att ge ett visst skydd. Av frågor och svar om Arachne framgår att användare i andra medlemsstater oftast bara har åtkomsträttigheter till egna program eller planer, eller inom medlemsstaten, men att medlemsstater kan välja att medge andra medlemsstater tillgång till uppgifter om egna program eller planer (Arachne, Frequently asked questions, version 2.3, den 19 augusti 2022, fråga 9). Det är således endast i vissa fall som en medlemsstat kan ges direkt tillgång till uppgifter som rör en annan medlemsstat (se mer i avsnitt 4.8.2). Det kan vidare antas att det i EU:s medlems-

länder finns ett visst sekretesskydd för skyddsvärda uppgifter, på liknande sätt som gäller i Sverige. Traditionellt kan Sverige sägas ha i jämförelse med andra länder långtgående krav på öppenhet och transparens. Det kan dock inte uteslutas att uppgifter, som är sekretessreglerade i Sverige, skulle sakna motsvarande skydd hos andra medlemsländer eller hos EU:s institutioner. Arachne-stadgan kan inte anses ställa några krav på skydd motsvarande sekretess för uppgifter som lämnats av en medlemsstat. Inte heller innehåller budgetförordningen några uttryckliga krav på att uppgifter som förts in i Arachne ska omfattas av sekretess. Det så kallade Arachne-teamet vid kommissionen har dock i kontakter med utredningen gett uttryck för att uppgifter i Arachne ska skyddas och inte få spridning.[1] Det bör också beaktas att lagstiftningen på detta område kan ändras i medlemsländerna utan att Sverige kan påverka det.

Även svenska myndigheter kan använda Arachne och då gäller givetvis den svenska sekretessregleringen. Behovet av sekretesskydd vid svenska myndigheters användande av Arachne som ett verktyg behandlas i avsnitt 8.5.

Vilka möjligheter finns det att säkerställa att motsvarande skydd består efter utlämnande till andra aktörer?

För det fall att vissa uppgifter undantagsvis skulle kunna vara sekretessbelagda i det enskilda fallet – exempelvis uppgift om projektkostnad – skulle det kunna vara önskvärt från ett svenskt perspektiv att uppgifter som i Sverige bedöms vara sekretessbelagda inte riskerade att bli offentliga i ett annat medlemsland eller hos kommissionen. Det följer av de intressen som ligger bakom den svenska offentlighets- och sekretessregleringen. I teorin skulle risken endast kunna undvikas antingen genom att Sverige avstår från att lämna ifrån sig den sekretessbelagda information som kan komma att spridas inom EU eller genom att uppgifterna får sekretesskydd hos de andra – utländska – aktörerna.

Mot bakgrund av utredningens bedömning att de uppgifter som ska lämnas i regel inte omfattas av sekretess blir det i allmänhet inte nödvändigt att vidta åtgärder för att skydda sådana uppgifter från att röjas. För fullständighetens skull behandlas ändå i det följande

[1] Komm2025/00388-10.

vilka möjligheter Sverige har att uppnå ett sådant skydd, för det fall sådana uppgifter ändå skulle förekomma.

Den svenska lagstiftaren saknar generellt sett möjlighet att påverka vilka sekretessregler som ska gälla i andra EU-länder eller hos EU:s institutioner. Inom ramen för förhandlingar inom och utanför EU tillämpas dock ibland den så kallade principen om vetorätt för ursprungsinnehavaren. Denna princip innebär att den som har upprättat en handling har rätt att kontrollera till vem handlingen lämnas ut även efter det att den har överlämnats till exempelvis andra myndigheter eller andra länder. I avtalstexter och EU-rättsakter brukar sådana bestämmelser formuleras så att den som tar emot en hemlig handling från ett annat land eller en mellanfolklig organisation inte får lämna handlingen vidare utan ursprungsinnehavarens skriftliga samtycke. Det förekommer också att internationella avtal och EU-rättsakter innehåller bestämmelser om ömsesidigt erkännande av sekretess, det vill säga att uppgifter som Sverige har erhållit från en annan stat ska ges ett sekretesskydd som motsvarar det som uppgiften har hos den utlämnande myndigheten.

Principen om vetorätt för ursprungsinnehavaren förespråkas i många andra länder medan den kan sägas stå i konflikt med en grundläggande princip i Sverige om att det är den myndighet som förvarar en handling som självständigt ska pröva om den kan lämnas ut. I vissa förhandlingar har Sverige försökt – och ibland lyckats – övertyga motparterna om att bestämmelser om vetorätt för ursprungsinnehavaren eller ömsesidigt erkännande av sekretess inte ska tas med i avtalet.

Utredningen gör bedömningen att det vad gäller Arachne är svårt att verka för att ge principen om vetorätt för ursprungsinnehavaren genomslag, ens om det skulle bedömas vara önskvärt för att skydda vissa i Sverige sekretessbelagda uppgifter. Den omarbetade budgetförordningen är redan förhandlad och innehåller inte sådana bestämmelser. Det kan dock vara möjligt för regeringen att inför en ändring av budgetförordningen som innebär att Arachne blir obligatoriskt i den eventuella förhandlingen verka för ett ökat skydd för svenska sekretessbelagda uppgifter. En sådan ordning kan anses avvika något från det traditionella svenska förhållningssättet att verka för större öppenhet (jfr prop. 2012/13:192 s. 11).

Vilka möjligheter finns det för Sverige att avstå från att göra viss information tillgänglig för kommissionen?

Bestämmelserna om krav på tillgängliggörande som finns i artikel 36.6 i budgetförordningen synes inte medge att medlemsstaterna avstår från att göra viss information – som omfattas av kraven i artikeln – tillgänglig. Den närmare informationen som ska göras tillgänglig följer dock av sektorsspecifik reglering. För den kommande programperioden kommer ny reglering att förhandlas fram. Det kan inom ramen för de förhandlingarna finnas möjlighet för regeringen att verka för att särskilt skyddsvärda uppgifter inte måste tillgängliggöras för kommissionen, om ett sådant intresse finns.

Utredningen fördjupar sig mot denna bakgrund inte mer i denna fråga.

Sammanfattande slutsatser

Även om det inte helt kan uteslutas att svenska myndigheter – vid uppfyllandet av skyldigheterna i artikel 36.6 i budgetförordningen – kan komma att tillgängliggöra annars sekretessbelagda uppgifter bedömer utredningen att myndigheterna i regel bör ha goda förutsättningar att tillgängliggöra uppgifter på ett sådant sätt att sådana uppgifter över huvud taget inte lämnas ut. För det fall att annars sekretessbelagda uppgifter ändå lämnas ut bedömer utredningen att ett svagare skydd får anses vara godtagbart, mot bakgrund av syftet med utlämnandet.

8.2.6 Det krävs inte författningsändringar på dataskyddsområdet för tillgängliggörande av obligatoriska uppgifter

Utredningens bedömning: Det behövs inga författningsändringar i dataskyddshänseende för att svenska myndigheter ska kunna uppfylla kraven i artikel 36.6 i budgetförordningen om att göra uppgifter tillgängliga för kommissionen. Befintlig dataskyddsreglering ger ett tillräckligt stöd för behandlingen.

Skälen för utredningens bedömning

Inledning

I avsnitt 7.2 redogör utredningen för gällande rätt på dataskyddsområdet, bland annat för kravet på rättslig grund och de grundläggande principerna för att en personuppgiftsbehandling ska vara laglig.

I detta avsnitt gör utredningen bedömningar av om befintligt dataskyddsregelverk är tillräckligt för den personuppgiftsbehandling som förväntas ske vid det rättsligt obligatoriska tillgängliggörandet av uppgifter enligt artikel 36.6 i budgetförordningen eller om det krävs författningsändringar. Härvid lyfts vissa dataskyddsrättsliga frågor särskilt.

Rättslig grund för behandlingen

Som nämns i avsnitt 7.2.5 är de vanliga rättsliga grunderna för myndigheter dels att fullgöra en rättslig förpliktelse (artikel 6.1 c i dataskyddsförordningen), dels att utföra en uppgift av allmänt intresse (artikel 6.1 e i dataskyddsförordningen). Ett krav är att behandlingen är *nödvändig* för att fullgöra den rättsliga förpliktelsen respektive att utföra uppgiften av allmänt intresse. Vid bedömningen av vad som är nödvändigt bör beaktas att det unionsrättsliga begreppet inte har samma strikta innebörd som det svenska ordet nödvändig: att någonting absolut fordras eller inte kan underlåtas (Svenska Akademiens Ordbok). Nödvändighetsrekvisitet i artikel 7 i föregångaren till dataskyddsförordningen, det tidigare gällande dataskyddsdirektivet, har till exempel inte ansetts utgöra ett krav på att det ska vara omöjligt att utföra en uppgift av allmänt intresse utan att behandlingsåtgärden vidtas (se prop. 2017/18:105 s. 46 och 47). Vilken grad av tydlighet och precision som krävs i fråga om den rättsliga grunden för att en viss behandling av personuppgifter ska anses vara nödvändig måste bedömas från fall till fall, utifrån behandlingens och verksamhetens karaktär (prop. 2017/18:10 s. 51). Utredningen gör dock i detta betänkande generella bedömningar avseende de rättsliga grunderna så långt det är möjligt.

Artikel 36.6 i budgetförordningen innehåller ett uttryckligt krav för myndigheter att tillgängliggöra uppgifter för kommissionen. Den rättsliga grunden att *fullgöra en rättslig förpliktelse* enligt artikel 6.1 c

i dataskyddsförordningen är därmed tillämplig. 2 kap. 1 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning, dataskyddslagen, tydliggör att personuppgifter får behandlas med stöd av artikel 6.1 c i dataskyddsförordningen, 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. Budgetförordningen, som är att jämställa med lag, innehåller uttryckliga krav inte bara på att uppgifter ska tillgängliggöras för kommissionen, utan även på vilka uppgifter som ska tillgänggöras. Att behandlingen är nödvändig står därmed klart.

Även den rättsliga grunden att *utföra en uppgift av allmänt intresse* (artikel 6.1 e) är enligt utredningens mening tillämplig i detta sammanhang. Grunden har förtydligats i svensk rätt genom 2 kap. 2 § dataskyddslagen, enligt vilken personuppgifter får behandlas med stöd av artikel 6.1 e, om behandlingen är nödvändig för att utföra en uppgift av allmänt intresse som följer av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning, eller som ett led i den personuppgiftsansvariges myndighetsutövning enligt lag eller annan författning.

Alla uppgifter som riksdag eller regering har gett i uppdrag åt statliga myndigheter att utföra anses av regeringen vara av allmänt intresse. Den verksamhet som en statlig eller kommunal myndighet bedriver, inom ramen för sin befogenhet, är således av allmänt intresse. I normalfallet utgör en myndighets uppdrag enligt författning, instruktion eller regleringsbrev en rättslig grund för behandling av personuppgifter enligt artikel 6.1 e. Vissa myndigheter har av riksdagen eller regeringen getts befogenhet att bedriva uppdragsverksamhet. Även denna typ av verksamhet är motiverad av ett allmänt intresse (se prop. 2017/18:105 s. 53–57).

Tydliga uppdrag att behandla personuppgifter i författning, exempelvis en myndighets instruktion, kan också utgöra en rättslig förpliktelse enligt artikel 6.1 c. Flera rättsliga grunder kan nämligen vara tillämpliga samtidigt.

Grunderna för nu aktuell behandling är fastställda i unionsrätten och i nationell rätt. Som framgår av tidigare redovisningar ställs höga krav på förvaltande myndigheter och andra aktörer att verka mot oriktigheter gällande hanteringen av EU-medel. Reglering om detta

finns i budgetförordningen, i sektorsspecifik EU-reglering samt i svenska författningar (se kapitel 3).

De krav på registrering och lagring av uppgifter som finns i sektorsspecifik reglering såsom CPR och CAP-förordningen kan också sägas stärka den rättsliga grunden allmänt intresse. Som exempel på svenska författningar som betonar vikten av att verka mot felaktigheter och bistå med information kan nämnas förordningen (2022:1379) om förvaltning av program för vissa EU-fonder och förordningen (2022:1826) om EU:s gemensamma jordbrukspolitik. Det allmänna intresset följer således av författning och behandlingen är enligt utredningens bedömning nödvändig.

Artikel 6.3 i dataskyddsförordningen kräver vidare att unionsrätten eller medlemsstaternas nationella rätt ska vara *proportionell* mot det legitima mål som eftersträvas (se också avsnitt 7.2.5). Regeringen har uttalat att kravet på proportionalitet i detta sammanhang motsvarar det krav som Europakonventionen ställer på lagstiftaren i en rättsstat. Enligt 2 kap. 19 § regeringsformen gäller att lagar och andra föreskrifter inte får meddelas i strid med Sveriges åtaganden enligt Europakonventionen. Enligt regeringen borde det därför vara mycket ovanligt att svensk rätt inte uppfyller Europakonventionens krav. Mot denna bakgrund borde utgångspunkten enligt regeringen vara att även dataskyddsförordningens motsvarande krav är uppfyllt i fråga om de rättsliga förpliktelser, uppgifter av allmänt intresse och den myndighetsutövning som fastställs i enlighet med svensk rätt (prop. 2017/18:105 s. 50). De rättsliga grunderna för behandling i nu aktuellt fall finns både i unionsrätten och i nationell rätt. Utredningen utgår från att även nu berörd unionsrätt är förenlig med Europakonventionen och uppfyller kravet på proportionalitet i artikel 6.3 i dataskyddsförordningen. För en samlad integritetsanalys, se kapitel 9.

Utredningen bedömer vidare att de rättsliga grunderna uppfyller kraven på tydlighet och precision samt på en förutsebar tillämpning för personer som omfattas av grunderna.

Att det finns rättslig grund för utlämnandet av uppgifter innebär att det inte behövs några författningsändringar för att skapa en rättslig grund för behandlingen.

Principerna i artikel 5 i dataskyddsförordningen

I avsnitt 7.2.5 redogör utredningen för principerna i artikel 5.1 i dataskyddsförordningen. Principerna ska tillämpas när en personuppgiftsbehandling planeras och när behandlingen faktiskt sker, till exempel i en viss verksamhet hos en viss myndighet. Det är den personuppgiftsansvarige som ska säkerställa att principerna efterlevs. Utredningen gör dock i detta betänkande så långt det är möjligt bedömningar avseende möjligheten att efterleva principerna.

Den behandling av personuppgifter som kommer att ske har sin grund i budgetförordningen, som är direkt tillämplig för de myndigheter som kommer att behandla uppgifterna. I budgetförordningen anges att behandlingen ska överensstämma med såväl dataskyddsförordningen som dataskyddsförordningen för EU:s institutioner. Utredningen utgår från att de myndigheter som kommer att behandla personuppgifter uppfyller principen om laglighet, korrekthet och öppenhet. Detsamma gäller principen om integritet och konfidentialitet. Flera bestämmelser i budgetförordningen nämner vikten av att uppgifter ska skyddas. Utredningen gör samma bedömning som ovan vad gäller principen om riktighet.

När det gäller principen om ändamålsbegränsning framgår ändamålen med tillgängliggörandet av uppgifter enligt artikel 36.6 i budgetförordningen, både direkt i den bestämmelsen och i andra bestämmelser, till exempel artikel 36.2 d. Vad gäller finalitetsprincipen, som är en del av principen om ändamålsbegränsning, kan följande sägas. Av skäl 50 till dataskyddsförordningen framgår att personuppgifter endast bör få behandlas för andra ändamål än de för vilka personuppgifterna samlades in, om dessa ändamål är förenliga med de ursprungliga ändamålen. I sådana fall krävs inte någon annan rättslig grund än den med stöd av vilken insamlingen av personuppgifter medgavs. Om en prövning enligt finalitetsprincipen i stället innebär att ändamålen är oförenliga, är en ny behandling av insamlade personuppgifter bara tillåten om den har stöd i en bestämmelse i unionsrätten eller den nationella lagstiftningen som utgör ett tillåtet undantag från finalitetsprincipen. Om det i lag eller förordning finns en sekretessbrytande bestämmelse som reglerar att en myndighet ska eller får lämna ut personuppgifter, till exempel en underrättelseskyldighet, har lagstiftaren tagit ställning för att ett sådant utlämnande är

tillåtet. Någon särskild prövning enligt finalitetsprincipen behöver då inte ske vid utlämnandet (se prop. 2024/25:187 s. 91).

De uppgifter som ska tillgängliggöras enligt artikel 36.6 i budgetförordningen gäller uppgifter som det redan finns en skyldighet att lagra och registrera enligt sektorsspecifik reglering. Uppgifterna kommer därmed redan att finnas hos myndigheterna som ska lämna ut dem till kommissionen. Då kan frågor om behandlingen är förenlig med insamlingsändamålet aktualiseras. De aktuella personuppgifterna bör som utgångspunkt ha samlats in som ett led i intresset att se till att medel endast ska gå till den som har rätt till det, vilket är ett ändamål i linje med det för vilka uppgifterna ska lämnas till kommissionen. De samlas också in enligt en skyldighet i ett EU-regelverk, som bland annat syftar till en korrekt förvaltning av EU-medel. Även detta är i linje med syftet med tillgängliggörandet av uppgifter enligt artikel 36.6. Uppgiftslämnandet bör därmed inte anses som oförenligt med insamlingsändamålet. För det fall att uppgiftslämnandet ändå skulle anses som oförenligt med insamlingsändamålet, har utlämnandet ett sådant stöd i unionsrätten att det enligt utredningens mening ska anses som ett tillåtet undantag från finalitetsprincipen och därmed ändå vara tillåtet.

Utredningens bedömning att ändamålen med behandlingen är godtagbara innebär att det inte behövs överväganden om till exempel särskilda ändamålsbestämmelser eller andra bestämmelser för att säkerställa att uppgiftslämnandet är förenligt med principen om ändamålsbegränsning och finalitetsprincipen. Det bör observeras att ändamålen behöver kunna beskrivas när behandlingen sker i det specifika fallet. Detta kan inbegripa ett krav på att beskriva de närmare ändamålen.

När det gäller principen om uppgiftsminimering kan den reglerade omfattningen och utformningen av skyldigheten att tillgängliggöra uppgifter i artikel 36.6 i sig anses vara ett uttryck för den principen. Uppräkningen av uppgifter, vilka situationer som avses, och att skyldigheten gäller endast sådana uppgifter som behöver lagras och registreras enligt sektorsspecifik reglering kan sägas vara resultatet av bedömningar om vilka uppgifter som faktiskt behövs.

När det gäller principen om lagringsminimering finns det ingen reglering i budgetförordningen som direkt anger hur länge personuppgifter som tillgängliggörs enligt artikel 36.6 får behandlas. Uppgifterna avses dock att föras in i Arachne, och beträffande det systemet

finns det en bestämmelse om längsta tid för behandling. Uppgifterna i Arachne ska lagras under den period som är nödvändig och proportionell för att uppfylla det syfte som fastställs i artikel 36.2 d, det vill säga målet att motverka oriktigheter. Den längsta möjliga lagringsperioden får inte överstiga tio år från och med den sista ansökan om utbetalning som lämnats in till kommissionen för den perioden (artikel 36.7 fjärde stycket). Detta innebär att man under lagstiftningsprocessen inom EU har bedömt att det kan vara nödvändigt att behandla personuppgifter i upp till tio år.

Utredningen bedömer att den reglering som finns är tillräcklig och att det inte finns skäl att överväga några författningsändringar som tar sikte på principerna i artikel 5 i dataskyddsförordningen.

Känsliga personuppgifter

Behandling av särskilda kategorier av uppgifter (känsliga personuppgifter) är enligt dataskyddsförordningen som huvudregel förbjudet. Förbudet omfattar 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 (artikel 9.1).

Förbudet kompletteras av ett antal undantag, till exempel om behandlingen 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 förenlig 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). Artikel 9.2 g är direkt tillämplig, men det är möjligt för medlemsstaterna att i nationell rätt införa mer specifika bestämmelser avseende känsliga personuppgifter (se artikel 6.2 och skäl 10). Detta har också skett i nationell rätt, se nedan.

Ytterligare ett undantag från förbudet att behandla känsliga personuppgifter gäller om behandlingen rör personuppgifter som på ett tydligt sätt har offentliggjorts av den registrerade (artikel 9.2 e).

Bestämmelser om behandling av känsliga personuppgifter finns i dataskyddslagen. I 3 kap. 3 § första stycket anges tre undantagssituationer då behandling av känsliga personuppgifter är tillåten. Känsliga personuppgifter får behandlas av en myndighet med stöd av artikel 9.2 g i dataskyddsförordningen 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. Enligt andra stycket är det vid behandling som sker enbart med stöd av första stycket förbjudet att utföra sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter.

Uppgifter som ska tillgängliggöras enligt artikel 36.6 i budgetförordningen är sådana som rör stödmottagare, åtgärden och verkliga huvudmän. Utredningen kan inte se att känsliga personuppgifter i nuläget skulle förekomma bland de uppgifter som ska lämnas.

För det fall att så ändå skulle ske, krävs att något av undantagen från förbudet är tillämpligt. De två första undantagssituationerna i 3 kap. 3 § dataskyddslagen är inte aktuella här, då det inte handlar om att uppgifter har lämnats till myndigheten och det inte heller rör handläggningen av ett ärende. Det är i stället den tredje situationen som kan aktualiseras, det vill säga om behandlingen är nödvändig med hänsyn till ett viktigt allmänt intresse och inte innebär ett otillbörligt intrång i den registrerades personliga integritet.

Vad gäller kravet på att behandlingen ska vara *nödvändig*, är innebörden densamma i artikel 9 som i artikel 6 (prop. 2017/18:105 s. 75 och 76). Kravet ska tolkas i unionsrättslig mening, vilket innebär att det ställs lägre krav än vad som följer av det svenska ordet nödvändig. Åtgärden (behandlingen) måste inte vara oundgänglig (se också ovan under rubriken *Rättslig grund för behandlingen*).

Vad som är ett *allmänt intresse*, det vill säga uttrycket som används i artikel 6.1 e i dataskyddsförordningen, respektive ett *viktigt allmänt intresse* som används i både nu aktuella undantagsbestämmelse i dataskyddslagen och i artikel 9.2 g i dataskyddsförordningen, är inte definierat i dataskyddsförordningen. I förarbetena till dataskyddslagen konstateras att det är svårt att på ett generellt plan definiera vad som skiljer ett allmänt intresse från ett viktigt allmänt intresse. Det måste dock utgöra ett viktigt allmänt intresse att svenska myndigheter, även

utanför området myndighetsutövning, kan bedriva den verksamhet som tydligt faller inom ramen för deras befogenheter på ett korrekt, rättssäkert och effektivt sätt (se prop. 2017/18:105 s. 83).

Budgetförordningen innebär en skyldighet att tillgängliggöra uppgifter och skyldigheten syftar till att motverka oriktigheter och skydda unionens, och därmed också Sveriges, finansiella intressen. Att skydda unionens och Sveriges finansiella intressen får anses vara ett viktigt allmänt intresse. Uppgiftslämnandet får anses vara nödvändigt med hänsyn till det intresset. Behandlingen av känsliga personuppgifter, om sådan skulle förekomma, bör därför som utgångspunkt anses vara nödvändig av hänsyn till ett viktigt allmänt intresse.

Vad gäller nu aktuellt slag av uppgifter bedömer utredningen att behandlingen som utgångspunkt inte bör innebära ett otillbörligt intrång i den registrerades personliga integritet.

Det finns därmed förutsättningar att behandla känsliga personuppgifter, i detta fall genom utlämnande. Det finns därför inte behov av författningsändringar när det gäller behandling av känsliga personuppgifter.

Det är dock alltid utlämnande myndighet som behöver göra bedömningen av om förutsättningarna för att behandla känsliga personuppgifter är uppfyllda.

Uppgifter om personnummer

Personnummer och samordningsnummer utgör inte känsliga personuppgifter i dataskyddsförordningens mening, men har ändå getts en särställning genom att medlemsstaterna har getts möjlighet att införa särskilda villkor för behandling av nationella identifikationsnummer eller annat vedertaget sätt för identifiering. Sådana nummer ska då endast användas med iakttagande av lämpliga skyddsåtgärder för de registrerades rättigheter och friheter enligt dataskyddsförordningen (artikel 87). Enligt 3 kap. 10 § dataskyddslagen får personnummer och samordningsnummer behandlas utan samtycke endast när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl.

Bland uppgifter som ska tillgängliggöras enligt artikel 36.6 i budgetförordningen kan det förekomma personnummer. Identifikations-

uppgifter kan ibland utgöras av endast födelsedatum, även om till exempel Sverige har en utbredd användning av personnummer som identifikationsuppgift. Det har inom ramen för utredningens arbete lyfts tveksamheter kring värdet av att endast födelsedatum används i identifieringssyfte, eftersom födelsedatum inte är ett unikt identifikationsnummer. Ett personnummer kan således ha ett större värde i identifieringssyfte.

Vad gäller nu aktuellt uppgiftslämnande bedömer utredningen att ett utlämnande av uppgifter om personnummer i regel bör anses vara förenligt med kraven i 3 kap. 10 § dataskyddslagen. Det är dock den utlämnande myndigheten som ska kunna motivera behovet.

Det finns inte behov av författningsändringar när det gäller behandling av uppgifter om personnummer och samordningsnummer.

Personuppgiftsansvar

Begreppet personuppgiftsansvarig är centralt i dataskyddsregleringen. Personuppgiftsansvarig definieras som en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter (se artikel 4.7 i dataskyddsförordningen). Definitionen är i allt väsentligt densamma i dataskyddsförordningen för EU:s institutioner.

De svenska myndigheter som tillgängliggör uppgifter eller på annat sätt behandlar uppgifter i samband med tillgängliggörandet enligt skyldigheterna i artikel 36.6 i budgetförordningen är personuppgiftsansvariga för den personuppgiftsbehandling som de utför.

Det finns inte behov av författningsändringar när det gäller personuppgiftsansvaret.

Enskildas rättigheter

I dataskyddsförordningen finns ett antal bestämmelser som rör den registrerades rättigheter, såsom rätten till information, tillgång, rättelse och radering (artiklarna 13–17) rätten att göra invändningar mot behandlingen och att inte bli föremål för visst automatiserat beslutsfattande (artiklarna 21 och 22). Rättigheterna i dataskyddsförordningen kan begränsas under vissa förutsättningar (artikel 23). Detta

har skett i nationell rätt genom bestämmelser i 5 kap. dataskyddslagen, varigenom bland annat rätten att få tillgång till personuppgifter inte alltid gäller, till exempel om sekretess gäller för uppgifterna. Såväl dataskyddsförordningens som dataskyddslagens bestämmelser ska således beaktas av berörda myndigheter när det gäller enskildas rättigheter.

Den befintliga regleringen bedöms vara tillräcklig för att tillgodose enskildas rättigheter. Utredningen har därför inte identifierat något behov av ny reglering eller författningsändringar när det gäller enskildas rättigheter.

Sammanfattning av utredningens slutsatser

Utredningen bedömer att det inte behövs några författningsändringar på dataskyddsområdet för att svenska myndigheter ska kunna tillgängliggöra personuppgifter enligt skyldigheterna i artikel 36.6 i budgetförordningen. Befintlig dataskyddsreglering är tillräcklig. Som en följd av detta ser utredningen inte skäl att föreslå reglering i en ny registerlag eller annan dataskyddslagstiftning för en ändamålsenlig personuppgiftsbehandling. Utredningens bedömning innebär också att det inte behövs ändringar rörande dataskydd i annan reglering för att möjliggöra personuppgiftsbehandlingen.

Det bör observeras att utredningens bedömningar om förenligheten med dataskyddsregelverket inte kan avse behandlingen i det enskilda fallet. Det är den personuppgiftsansvarige som behöver säkerställa att den personuppgiftsbehandling som faktiskt utförs är förenlig med dataskyddsregleringen.

Se också kapitel 9 för en samlad integritetsanalys.

8.3 Lämnande av uppgifter utan att det finns en rättslig skyldighet

8.3.1 Uppdraget i denna del

I avsnitt 8.2 behandlas rättsliga frågor om skyldigheten att göra vissa uppgifter tillgängliga för kommissionen enligt artikel 36.6 i budgetförordningen, som kommer att gälla från och med 2028. I detta avsnitt behandlas rättsliga frågor om följande former av lämnande av

uppgifter som är relevanta i detta betänkande och som inte följer av någon rättslig förpliktelse.

- Lämnande av uppgifter vid ett användande av Arachne:
  - Funktionellt nödvändiga uppgifter (vid ett användande före 2028)
  - Inte funktionellt nödvändiga uppgifter (vid ett användande före 2028)
  - Uppgifter inom ramen för förhandsfunktionen (före och efter 2028)
- Tillgängliggörande av frivilliga uppgifter enligt artikel 36.6 andra stycket i budgetförordningen (efter 2028).

Även situationen att en myndighet lämnar uppgifter inom ett område där det kan finnas en rättslig skyldighet att lämna uppgifter men just den myndigheten inte omfattas av någon sådan skyldighet behandlas i detta avsnitt. Detta tar sikte på ett uppgiftslämnande som ESV kan komma att utföra inom ramen för RRF.

I det följande görs överväganden om ovan nämnda former av uppgiftslämnande kan medföra behov av författningsändringar eller andra åtgärder utifrån regelverken om offentlighet och sekretess respektive personuppgiftsbehandling.

Här behandlas därmed uppdraget att utifrån den gjorda kartläggningen avseende Arachne utreda och analysera om det bland de data som *får* registreras i Arachne finns uppgifter som skulle kunna omfattas av sekretess, och om det finns rättsliga förutsättningar för svenska myndigheter att registrera eller annars utbyta dessa, samt uppdraget att analysera och bedöma vilket skydd eventuella sekretessbelagda uppgifter skulle ha i samband med andra medlemsstaters och EU-institutioners användning av Arachne. Vidare behandlas uppdraget att bedöma om det finns behov av ändrade regler för att svenska myndigheter ska kunna registrera uppgifter i Arachne samt lämna nödvändiga författningsförslag, när det gäller uppgiftslämnande utan rättslig skyldighet. Även uppdraget som rör hur Arachnes funktionalitet och användning påverkas om eventuella sekretessbelagda uppgifter inte kan registreras i fråga om uppgifter som inte är rättsligt obligatoriska att registrera, behandlas.

8.3.2 Om uppgifter som kan komma att lämnas

Utredningen redogör i avsnitt 4.3 för uppgifter som kan komma att lämnas vid ett användande av Arachne före 2028 och inom ramen för den så kallade förhandsfunktionen. I avsnitt 4.5 beskrivs de uppgifter som kan komma att tillgängliggöras enligt artikel 36.6 andra stycket andra meningen i budgetförordningen, det vill säga sådana uppgifter som kan tillgängliggöras trots att de inte omfattas av den skyldighet som börjar gälla 2028.

I stora drag handlar det om samma slags uppgifter i de olika situationerna, nämligen uppgifter om åtgärden, om mottagaren och – eventuellt – om verklig huvudman. Vissa centrala uppgifter om åtgärden och mottagaren är funktionellt nödvändiga vid lämnande av uppgifter om beviljade medel före 2028 och vid användande av förhandsfunktionen och dessa motsvarar i huvudsak de uppgifter som är rättsligt obligatoriska enligt artikel 36.6 i budgetförordningen. Vidare kan generellt sägas att de uppgifter som är valfria att lämna genom förangivna datafält – vid lämnande av uppgifter om beviljade medel före 2028 och vid användande av förhandsfunktionen – i huvudsak motsvarar de uppgifter som kan tillgängliggöras på frivillig basis enligt artikel 36.6 i budgetförordningen.

Det finns dock i dagsläget inte en fullständig överensstämmelse mellan de uppgifter som från och med 2028 kommer att vara rättsligt obligatoriska att tillgängliggöra enligt artikel 36.6 i budgetförordningen och de som i dag är funktionellt nödvändiga att lämna för att Arachne ska kunna fungera. Detta kan bero på skillnader i sektorsspecifik reglering. Det kan erinras om att uppgift om verklig huvudman är nödvändig att registrera och lagra (och därmed att tillgängliggöra enligt artikel 36.6) enligt CPR men inte enligt CAP-förordningen. Det kan också finnas avvikelser som har att göra med utformningen av användargränssnitten i de olika systemen. Det kan också erinras om att en utveckling av Arachne pågår samt om att de sektorsspecifika regelverken kommer att förändras. I avsnitt 4.5.2 berör utredningen flera av de utmaningar som finns när det gäller att bedöma om en uppgift tillhör det nödvändiga/obligatoriska eller valfria området samt att bedöma om det finns ett värde att lämna uppgiften även om den inte är nödvändig/obligatorisk.

Det är mot denna bakgrund inte möjligt för utredningen att klarlägga exakt vilka slags uppgifter som det kan finnas skäl för svenska

myndigheter att lämna utan att det finns en rättslig skyldighet att göra det. Det kan dock konstateras att det generellt kan finnas anledning för svenska myndigheter att lämna samtliga slags uppgifter som är möjliga att lämna utifrån tillgängliga användargränssnitt, oavsett om det finns rättsliga eller funktionella krav för det. Det kan erinras om att kommissionen rekommenderar att alla datafält fylls i när uppgifter laddas upp i Arachne.

Av särskilt intresse för de rättsliga bedömningarna i detta avsnitt är uppgifter som kan beröra fysiska personer. Som framgår ovan kan uppgifter om verklig huvudman vara en valfri uppgift (exempelvis inom ramen för CAP). Datafälten för anknutna personer och nyckelexperter anges som valfria både inom ramen för förhandsfunktionen och i exemplet om vilka uppgifter som kan laddas upp i Arachne i den XML-fil som tillhandahålls avseende fonderna ISF, Amif och BMVI (se avsnitt 4.3).

Det kan noteras att det inte finns fält för att lämna adressuppgifter för någon av dessa tre kategorier – verklig huvudman, anknutna personer och nyckelpersoner – och att uppgifter om adress därmed inte bör bli aktuellt att lämna.

8.3.3 Uppgifter som kan komma att lämnas kommer i regel inte att omfattas av sekretess

Utredningens bedömning: De slags uppgifter som svenska myndigheter kan komma att lämna utan att det finns en rättslig skyldighet kommer i regel inte att omfattas av sekretess. Det kan dock inte uteslutas att vissa uppgifter undantagsvis skulle kunna vara sekretessbelagda i det enskilda fallet.

Skälen för utredningens bedömning: Som framgår i avsnitt 8.2.3 kommer, såvitt utredningen kan bedöma, uppgifter som måste tillgängliggöras enligt artikel 36.6 i budgetförordningen i regel inte att omfattas av sekretess, även om det inte kan uteslutas att vissa uppgifter undantagsvis skulle kunna vara sekretessbelagda i det enskilda fallet. Frågan som utredningen har att bedöma i detta avsnitt är om uppgifter som kan komma att lämnas av svenska myndigheter utan att det finns en rättslig förpliktelse att göra det, kan omfattas av sekretess och vad det kan få för följder.

De uppgifter som i dag är funktionellt nödvändiga att lämna av de myndigheter som använder Arachne får antas huvudsakligen motsvara de uppgifter som kommer att vara rättsligt obligatoriska att tillgängliggöra enligt artikel 36.6 i budgetförordningen, även om det som nämns i avsnitt 8.3.2 inte finns någon fullständig överensstämmelse.

Utredningens bild är att inte heller de slags uppgifter som är funktionellt nödvändiga att lämna som huvudregel omfattas av sekretess. Även sådana slags uppgifter är således som utgångspunkt offentliga. För dessa slags uppgifter gör därför utredningen samma bedömning som för de rättsligt obligatoriska uppgifterna, se avsnitt 8.2.3.

När det gäller de slags uppgifter som inte är funktionellt nödvändiga att lämna, men som ändå skulle kunna vara av värde att lämna, gör utredningen följande överväganden. Även dessa uppgiftsslag motsvarar till stor del uppgifter som redan har offentliggjorts på olika sätt, till exempel av förvaltande myndigheter eller av revisionsmyndigheter, eller på en EU-webbplats. Utredningen bedömer att dessa uppgifter i regel inte omfattas av sekretess. De motsvarar också delvis uppgiftsslag som ska offentliggöras enligt artikel 38 i budgetförordningen.

När det gäller uppgifter om fysiska personer kan följande nämnas. Begreppet *anknutna personer* tar sikte på personer som är anknutna till ett projekt och är viktiga för dess genomförande, till exempel en medlem i urvalskommittén, den som utvärderar projektet eller är projektledare. Det kan också avse personer från programmyndigheten. Det avser inte styrelseledamöter från berört företag. I expertgruppen har särskilt frågan om vad som gäller för uppgifter om anknutna personer lyfts, och i vilken utsträckning det kan omfatta tjänstemän inom berörd myndighet. Av tillgänglig information om Arachne framgår att detta valfria datafält i XML-filen kan användas för att ange information även om en anknuten person inom en myndighet. Det kan till exempel vara en tjänsteman med funktionen att utvärdera ett projekt. Utredningen ser det inte som sannolikt att det i nu aktuell krets av berörda myndigheter skulle finnas uppgifter om medarbetare som skulle vara sekretessbelagda i det enskilda fallet, när det gäller verksamhet med EU-medel. Sekretess för uppgift om medarbetare kan förekomma, till exempel hos brottsbekämpande myndigheter, men sannolikt inte – som utredningen bedömer det – inom ramen för utövande av deras EU-medelsverksamhet. Det kan dock inte helt uteslutas.

En annan sak är att en myndighet av andra skäl än sekretess kan vilja avstå från att föra in uppgifter om enskilda medarbetare i ett EU-gemensamt system. Då det är fråga om uppgiftslämnande som inte omfattas av någon rättslig skyldighet är det upp till respektive myndighet att bedöma vilka uppgifter som bör och kan lämnas.

Begreppet *verklig huvudman* tar sikte på fysiska personer som ytterst äger eller kontrollerar ett företag eller den för vars räkning en transaktion eller en verksamhet utförs. Uppgifter om verkliga huvudmän rör alltså fysiska personer och det kan bland annat handla om uppgifter om namn, födelsedatum samt personnummer eller motsvarande identifieringskod. Av avsnitt 8.2.3 framgår att sådana slags uppgifter normalt inte omfattas av sekretess. Den bedömning som utredningen gör i det avsnittet gör sig gällande även här.

Utredningen bedömer att inte heller uppgifter om *nyckelexperter* (det vill säga personer som är anknutna till ett kontrakt och är viktiga för dess genomförande) i regel omfattas av sekretess, men kan inte utesluta detta, se mer under nästa stycke.

Som framgår av kartläggningen i avsnitt 4.3 och 4.5 är de användargränssnitt som används för att ladda upp uppgifter till Arachne utformade så att det beträffande vissa i och för sig nödvändiga kategorier finns möjlighet att valfritt lämna närmare uppgifter. Utredningen kan inte utesluta att närmare uppgifter om projekt, kontrakt, stödmottagare och anknutna personer och nyckelexperter, i vissa specifika fall, skulle kunna omfattas av sekretess.

Om projektnamnet avslöjar exempelvis geografisk plats för projektet skulle den uppgiften kunna ge kunskap om aktörers marknadsplanering och utbyggnadsplaner, vilket skulle kunna vara uppgifter om enskilds affärs- och driftförhållanden. Ett röjande av en sådan uppgift skulle kunna leda till skada för den enskilde, i vart fall innan ett projekt har påbörjats. Ett utlämnande av uppgifter inom ramen för förhandsfunktionen kan ske innan ett projekt har påbörjats. Det kan inte uteslutas att en sådan uppgift då kan omfattas av sekretess enligt 30 kap. 23 § OSL.

En annan form av frivilligt uppgiftslämnande tar sikte på att det kan bli aktuellt för en myndighet att lämna uppgifter trots att myndigheten i fråga inte har några skyldigheter alls att lämna uppgifter. Som utredningen lyfter i avsnitt 4.5.3 kan det vara ändamålsenligt att ESV inom ramen för RRF-arbetet för in uppgifter i Arachne som myndigheten har fått från de tio rapporterande RRF-myndigheterna.

Utredningen bedömer på samma grunder som ovan och som avseende de rättsligt obligatoriska uppgifterna i avsnitt 8.2.3 att de uppgifter som kan bli relevanta att lämna av ESV i sådana situationer i regel inte kommer att omfattas av sekretess.

8.3.4 Det krävs inte författningsändringar på sekretessområdet för lämnande av uppgifter utan rättslig skyldighet

Utredningens bedömning: Det behövs inga författningsändringar i sekretesshänseende för att svenska myndigheter ska kunna lämna uppgifter i de fall det inte finns någon rättslig skyldighet att lämna uppgifterna, även om uppgifterna omfattas av sekretess.

Skälen för utredningens bedömning

Uppgifter kan lämnas trots eventuell sekretess men kravet på förhandsprövning inför ett eventuellt rutinmässigt uppgiftslämnande bör ställas högt

De uppgifter som svenska myndigheter på frivillig väg kan tillgängliggöra för kommissionen enligt artikel 36.6 i budgetförordningen eller föra in direkt i Arachne kommer som framgår ovan i regel inte att omfattas av sekretess. Det kan dock inte uteslutas att vissa uppgifter undantagsvis skulle kunna vara sekretessbelagda i det enskilda fallet. Frågan är om det då finns en sekretessbrytande bestämmelse som är tillämplig.

Utgångspunkten är att en uppgift för vilken sekretess gäller inte heller får röjas för en utländsk myndighet eller en mellanfolklig organisation (8 kap. 3 § OSL). Undantaget som gäller om utlämnandet sker i enlighet med särskild föreskrift i lag eller förordning (8 kap. 3 § 1 OSL) kan inte tillämpas när det gäller uppgiftslämnande som inte sker i enlighet med någon särskild föreskrift.

Det andra undantaget, 8 kap. 3 § 2 OSL, kan dock möjliggöra att uppgifter lämnas ut till mellanfolkliga organisationer även i fall där tillgängliggörandet inte kan härledas direkt från en särskild föreskrift i lag eller förordning. Det gäller när uppgiften i motsvarande fall skulle få lämnas ut till en svensk myndighet och det enligt den utlämnande myndighetens prövning står klart att det är förenligt med

svenska intressen att uppgiften lämnas till den utländska myndigheten eller den mellanfolkliga organisationen.

Ett utlämnande av annars sekretessbelagda uppgifter med stöd av detta undantag kan aktualiseras gällande uppgiftslämnande utan rättslig skyldighet. Det krävs för det första att uppgiften i motsvarande fall *skulle få lämnas ut till en svensk myndighet*, vilket kräver en bedömning av om det finns en tillämplig sekretessbrytande bestämmelse gentemot svenska myndigheter. Denna bedömning behöver utlämnande myndighet göra. I detta sammanhang kan nämnas att den nya sekretessbrytande bestämmelsen 10 kap. 15 a § OSL, som ska träda i kraft den 1 december 2025, ger en ny grund för utlämnande till andra myndigheter. Enligt bestämmelsen ska sekretess inte hindra att uppgifter under vissa förutsättningar lämnas ut till en annan myndighet om det behövs för bland annat att förebygga, förhindra, upptäcka eller utreda felaktiga utbetalningar, eller för att förebygga, förhindra, upptäcka eller utreda fusk och olika typer av överträdelser (se avsnitt 7.1.2).

För det andra krävs att det står klart att det är *förenligt med svenska intressen* att uppgiften lämnas till, i detta fall, kommissionen. Även denna prövning ska utlämnande myndighet göra. Enligt utredningens mening talar mycket för att ett utlämnande av de slags uppgifter som kan anses som centrala att lämna ut, kan anses vara förenligt med svenska intressen.

När det gäller frågan om *hur uppgifterna får lämnas* bedömer utredningen att förutsättningarna för ett rutinmässigt utlämnande med tillämpning av detta undantag kan vara svårare att uppfylla än vid tillämpning av undantaget i 8 kap. 3 § 1 OSL, med hänsyn till att det krävs en bedömning på förhand av utlämnande myndighet av om förutsättningarna för utlämnande är uppfyllda. Bestämmelsen utesluter inte i sig ett rutinmässigt utlämnande, men det bör enligt utredningens mening ställas än högre krav på att myndigheten gör en gedigen prövning av om förutsättningarna i undantaget är uppfyllda.

Utredningen noterar att det inom ramen för förhandsfunktionen inte bör bli fråga om något rutinmässigt utlämnande.

Vissa uppgifter bör inte lämnas och behöver inte heller lämnas

Detta avsnitt behandlar sådant uppgiftslämnande som inte är rättsligt obligatoriskt. Det innebär att sådana slags uppgifter som behandlas i detta avsnitt inte enligt författningskrav behöver lämnas till kommissionen eller föras in i Arachne. I vissa avseenden kan dock Arachnes funktionalitet påverkas negativt om inte uppgifter utöver de obligatoriska lämnas. Det är också ett av skälen till att utredningen har i uppdrag att utreda frågor som rör frivilligt uppgiftslämnande.

8 kap. 3 § OSL innebär inte någon förpliktelse att lämna uppgifter utan fastställer under vilka förutsättningar som annars sekretessbelagda uppgifter får lämnas till en utländsk myndighet eller en mellanfolklig organisation. Den myndighet som har att pröva utlämnandet behöver därför göra bedömningen av hur stor vikt det är att en uppgift som *får* lämnas ut enligt 8 kap. 3 § 2 också faktiskt *bör* lämnas ut. Prövningen skulle kunna leda till att intresset att inte lämna ut uppgiften väger över intresset att göra ett utlämnande.

I utredningens direktiv anges att uppgifter som omfattas av försvarssekretess inte bör förekomma i Arachne. När det gäller frivilligt uppgiftslämnande bör det inte uppstå några svårigheter att underlåta att lämna uppgifter som omfattas av försvarssekretess. Detta behöver inte betyda att myndigheterna helt avstår från att fylla i uppgiftsfält av värde. Däremot bör myndigheterna kunna avstå från att lämna uppgifter på en sådan detaljeringsnivå att försvarshemligheter röjs. Därmed bör sannolikt Arachnes funktionalitet inte påverkas i någon nämnvärd omfattning. Som framgår av avsnitt 8.2.3 bedömer utredningen att det inte heller inom ramen för det rättsligt obligatoriska uppgiftslämnandet behöver röjas några försvarshemligheter.

Det är utlämnande myndighets ansvar att bedöma om uppgifter kan lämnas ut.

Överväganden kring skydd motsvarande sekretess

Utredningen bedömer att uppgifter som omfattas av sekretess i Sverige och som tillgängliggörs för kommissionen och därmed kan komma att föras in i Arachne – eller som laddas direkt upp i Arachne – kan antas ha ett visst skydd när olika aktörer använder Arachne som verktyg. Fullt skydd kan inte garanteras, men är enligt utred-

ningens mening inte heller nödvändigt. Utredningen gör denna bedömning på samma grunder som framgår av avsnitt 8.2.5.

Vad gäller uppgifter som lämnas inom ramen för förhandsfunktionen uppfattar utredningen det så att uppgifterna inte tillförs Arachne på ett sådant sätt att de utgör underlag för andra riskvärderingar som utförs genom Arachne. Däremot synes de riskvärderingar som görs inom ramen för förhandsfunktionen vara synliga i vart fall för andra användare som har samma behörighet att ta del av information om program i Arachne. Uppgifterna som lämnas inom ramen för förhandsfunktionen kan alltså komma andra till del. På motsvarande sätt som gäller uppgifter som tillgängliggörs och förs in i Arachne kan det beträffande dessa uppgifter inte garanteras fullt skydd motsvarande den sekretess som eventuellt hade gällt enligt svensk rätt. Enligt utredningens mening är detta inte heller nödvändigt.

Sammanfattning av utredningens slutsatser

Utredningen bedömer att det finns förutsättningar för svenska myndigheter att lämna ut uppgifter i de fall det inte finns någon rättslig skyldighet att göra det, det vill säga vid frivilligt tillgängliggörande till kommissionen enligt artikel 36.6 i budgetförordningen och inom ramen för ett användande av Arachne. De flesta uppgifterna kommer inte att omfattas av någon sekretess. Vissa slags uppgifter skulle kunna vara sekretessbelagda i det enskilda fallet, men bör kunna lämnas ut med tillämpning av sekretessbrytande bestämmelser. Utlämnande som av sekretesskäl, eller andra skäl, inte bedöms som lämpligt, kan underlåtas. Det ankommer på myndigheterna att alltid göra en prövning av om sekretessreglerade uppgifter kan lämnas ut.

8.3.5 Det krävs inte författningsändringar på dataskyddsområdet för lämnande av uppgifter utan rättslig skyldighet

Utredningens bedömning: Det behövs inga författningsändringar i dataskyddshänseende för att svenska myndigheter ska kunna lämna uppgifter i de fall det inte finns någon rättslig skyldighet att lämna uppgifterna. Befintlig dataskyddsreglering ger ett tillräckligt stöd för aktuell personuppgiftsbehandling.

Skälen för utredningens bedömning

Inledning

I avsnitt 7.2 redogör utredningen för gällande rätt på dataskyddsområdet, bland annat för kravet på rättslig grund och de grundläggande principerna för att en personuppgiftsbehandling ska vara laglig.

I detta avsnitt gör utredningen bedömningar av om befintligt dataskyddsregelverk är tillräckligt för den personuppgiftsbehandling som kan förväntas ske vid ett sådant uppgiftslämnande som kan komma att ske utan att det finns en rättslig skyldighet, eller om det krävs författningsändringar. Härvid lyfts vissa dataskyddsrättsliga frågor särskilt.

Rättslig grund för behandlingen

Även om det här är fråga om ett frivilligt uppgiftslämnande på så sätt att det inte finns någon rättsligt reglerad skyldighet att lämna uppgifter, kräver budgetförordningen att oriktigheter motverkas och förordningen ställer höga krav på medlemsstaterna att skydda unionens finansiella intressen. Utredningen anser på samma grunder som framförs i avsnitt 8.2.6 att den förväntade personuppgiftsbehandlingen som utgångspunkt uppfyller kraven på allmänt intresse. Intresset är vidare fastställt i unionsrätten och i nationell rätt. Den rättsliga grunden att *utföra en uppgift av allmänt intresse* (artikel 6.1 e i dataskyddsförordningen och 2 kap. 2 § dataskyddslagen) är därmed aktuell avseende nu förväntad personuppgiftsbehandling. Bedömningen utvecklas något i det följande, eftersom uppgiftslämnande

utan att det finns en rättslig skyldighet kan bli aktuellt avseende olika slags uppgifter och situationer.

Vad gäller uppgifter som finns med i *uppräkningen i artikel 36.6* i budgetförordningen men som inte omfattas av krav på tillgängliggörande för en viss myndighet, därför att sektorsspecifik reglering inte kräver detta (frivilliga uppgifter), gör utredningen följande överväganden. Bestämmelsen ger tydligt stöd för medlemsländerna att tillgängliggöra frivilliga uppgifter och även ett sådant uppgiftslämnande får anses vara ett led i att uppfylla syftet i artikel 36.2 d, att motverka oriktigheter. Utredningen anser att det av artikel 36.2 och 36.6 i budgetförordningen framgår att det rör sig om en uppgift av allmänt intresse och att de ger en tydlig rättslig grund för utlämnandet.

Vad gäller uppgifter som kan komma att lämnas inom ramen för ett *användande av Arachne* (före 2028) kan först nämnas uppgifter som är funktionellt nödvändiga. Här gör utredningen bedömningen att det som utgångspunkt är fråga om att utföra en uppgift av allmänt intresse.

Vad gäller det stora antal fält som finns i dagsläget för att lämna uppgifter i Arachne som inte heller är funktionellt nödvändiga att lämna, har kommissionen i relevanta källor rekommenderat att samtliga tillgängliga fält fylls i för att ge bästa utfall och användning av Arachne (se t.ex. Arachne, Frequently asked questions, version 2.3, den 19 augusti 2022, fråga 13). Utgångspunkten är enligt utredningen att även ett lämnande av sådana uppgifter handlar om att utföra en uppgift av allmänt intresse.

Härutöver kan vid ett användande av Arachne uppgifter komma att lämnas inom ramen för förhandsfunktionen (såväl före som efter 2028). Vissa uppgifter måste fyllas i om funktionen används, medan andra inte måste fyllas i. Att begära en riskvärdering av Arachne innan en myndighet fattar beslut om att tilldela EU-medel är ett betydelsefullt sätt att använda verktyget på. Detta kan leda till en närmare utredning av myndigheten, som kan resultera i att det finns skäl att avslå ansökan. Utredningen bedömer även här att det som utgångspunkt är fråga om att utföra en uppgift av allmänt intresse. Det är dock av vikt att den myndighet som väljer att använda funktionen gör en bedömning av om kravet på rättslig grund är uppfyllt i det aktuella fallet.

Som framgår av avsnitt 8.2.6 är kravet på nödvändighet inte så högt ställt som dess ordalydelse kan ge bilden av. Utredningen anser

att kravet på nödvändighet som huvudregel bör anses som uppfyllt i samtliga ovan nämnda situationer.

Då även det frivilliga uppgiftslämnandet behandlas i budgetförordningen och i andra källor avseende personuppgiftsbehandling, bedömer utredningen att den rättsliga grunden bör anses uppfylla kraven på tydlighet och precision samt på en förutsebar tillämpning för personer som omfattas av grunderna. Utredningen utgår också från att unionsrätten är förenlig med Europakonventionen och uppfyller kravet på proportionalitet i artikel 6.3 i dataskyddsförordningen. För en samlad integritetsanalys, se kapitel 9.

Det kan också bli aktuellt för en myndighet, trots att myndigheten inte omfattas av någon skyldighet att lämna uppgifter överhuvudtaget, att ändå lämna ut uppgifter genom att föra in dem i Arachne, det vill säga på helt frivillig basis. När det gäller hanteringen av RRF-medel kan det, som nämns i avsnitt 4.5.3, inom ramen för ett frivilligt uppgiftslämnande vara ändamålsenligt att låta ESV – som redan har samlat in relevanta uppgifter om RRF:s genomförande – ansvara för en eventuell inmatning av uppgifter i Arachne. Ett sådant förfarande skulle medföra att även uppgifter om RRF finns i Arachne, vilket kan bidra till efterkontroller och att förhindra till exempel dubbelfinansiering gentemot andra program. Om detta skulle omfatta även personuppgiftsbehandling, bedömer utredningen att även ett sådant utlämnande som utgångspunkt handlar om att utföra en uppgift av allmänt intresse.

Vad som sägs ovan innebär att utredningen bedömer att den rättsliga grunden att utföra en uppgift av allmänt intresse i regel är tillämplig i ovan nämnda situationer.

Frågan därefter är om det finns ett utrymme att tillämpa även den rättsliga grunden att *fullgöra en rättslig förpliktelse* (artikel 6.1 c i dataskyddsförordningen och 2 kap. 1 § dataskyddslagen) i ovan nämnda fall. För att den grunden ska vara tillämplig måste förpliktelsen vara fastställd i enlighet med gällande rätt, men den behöver inte framgå direkt av en författning. Vid bedömningen av om något följer av exempelvis en lagbestämmelse kan bland annat förarbetsuttalanden, bestämmelsens syfte och den rättsliga kontext som bestämmelsen befinner sig i behöva beaktas. Det är alltså inte bara lagtextens ordalydelse som är av relevans för att avgöra om något följer av lag. I det sammanhanget har regeringen framfört att kravet att behandlingen också måste vara nödvändig för att fullgöra den rätts-

liga förpliktelsen inte innebär ett krav på att behandlingsåtgärden ska vara oundgänglig. Behandlingen kan anses nödvändig och därmed tillåten enligt artikel 6 i dataskyddsförordningen, om behandlingen leder till effektivitetsvinster (prop. 2017/18:105 s. 188 och 189).

Det skulle utifrån dessa förarbetsuttalanden kunna argumenteras för att nu aktuell behandling kan ha en rättslig grund även i artikel 6.1 c i dataskyddsförordningen. Detta är dock förenat med viss osäkerhet och kan bero på hur rutiner avseende uppgiftslämnandet utvecklas. Arachne är under utveckling och det finns därför flera osäkerhetsmoment. Utredningen ser därför inte skäl för myndigheter att i nuläget helt förlita sig på denna grund när det gäller frivilligt uppgiftslämnande. Det gäller särskilt för uppgiftslämnande från en myndighet som inte omfattas av några skyldigheter alls att tillgängliggöra uppgifter, såsom exemplet med ESV ovan.

En ytterligare rättslig grund i dataskyddsförordningen är samtycke, vilken formuleras i artikel 6.1 a så att den registrerade har *lämnat sitt samtycke* till att dennes personuppgifter behandlas för ett eller flera specifika ändamål. Denna rättsliga grund brukar normalt inte tillämpas av svenska myndigheter. Ett samtycke kan återkallas när som helst (artikel 7.3) och därmed kan den rättsliga grunden när som helst upphöra. Vad gäller uppgifter om *anknutna personer* kan de omfatta tjänstemän inom berörd myndighet (se avsnitt 8.3.3). Kommissionen har särskilt gett uttryck för att om en medlemsstat överväger att föra in sådan information i Arachne, måste detta ske i enlighet med nationell dataskyddslagstiftning och den enskilde kan behöva ge sitt samtycke (se Arachne, Frequently asked questions, version 2.3, den 19 augusti 2022, fråga 53). Detta tyder på att en sådan behandling enligt kommissionen skulle kunna vila på samtyckesgrunden. Utredningen anser dock att då ett samtycke när som helst kan återkallas är det att föredra att det finns en annan, mer varaktig rättslig grund för behandlingen av sådana uppgifter.

Det är alltid den utlämnande myndigheten som behöver kunna visa att det finns rättslig grund för den personuppgiftsbehandling som är aktuell. I dessa fall, som gäller utlämnande som inte sker på grund av en uttrycklig uppgiftsskyldighet, kan det sägas ställas högre krav på bedömningen jämfört med när uppgifter lämnas på grund av en sådan skyldighet. Till exempel kan det krävas att behovet av uppgiftslämnandet kan visas tydligare.

Att det kan finnas rättslig grund för uppgiftslämnandet innebär att det inte behövs några författningsändringar för att skapa en rättslig grund för behandlingen.

Principerna i artikel 5 i dataskyddsförordningen

I avsnitt 7.2.5 redogör utredningen för principerna i artikel 5.1 i dataskyddsförordningen och för att det är den personuppgiftsansvarige som ska säkerställa att principerna efterlevs. Utredningen gör så långt det är möjligt bedömningar avseende möjligheten att efterleva principerna.

På samma grunder som anges i avsnitt 8.2.6 utgår utredningen från att de myndigheter som kommer att behandla personuppgifter uppfyller principen om laglighet, korrekthet och öppenhet, principen om integritet och konfidentialitet samt principen om riktighet.

När det gäller principen om ändamålsbegränsning och förenligheten med finalitetsprincipen gör utredningen i stort samma bedömningar som i avsnitt 8.2.6. Det kommer dock att ställas högre krav på myndigheterna vid en fortsatt behandling av personuppgifter när det gäller frivilligt uppgiftslämnande. Om myndigheter överväger att föra in uppgifter i Arachne på frivillig basis, behöver de bedöma om uppgiftslämnandet är förenligt med finalitetsprincipen. Som utgångspunkt bör dock enligt utredningens mening ett utlämnande av uppgifter inte komma i konflikt med finalitetsprincipen, när det gäller uppgifter som myndigheterna har samlat in i syfte att säkerställa att EU-medel går till rätt mottagare eller för att på annat sätt motverka oriktigheter. Ett utlämnade bör i vissa fall kunna vara tillåtet även om det är oförenligt med insamlingsändamålet (se avsnitt 8.2.6). Utredningen bedömer att – även när det inte är fråga om ett uttryckligt krav att lämna uppgifter – ett utlämnande som utgångspunkt bör anses ha ett sådant stöd i unionsrätten att det bör anses som ett tillåtet undantag från finalitetsprincipen.

När det gäller principen om uppgiftsminimering finns det skäl att utgå från att de förangivna fälten för införande av uppgifter i Arachne är en följd av bedömningar som har gjorts på EU-nivå om att fälten motsvarar uppgifter av värde i arbetet med att motverka oriktigheter. En sådan tolkning får också stöd av att kommissionen har rekommenderat att samtliga tillgängliga fält fylls i för att ge bästa

utfall och användning av Arachne. Det är dock myndigheterna som behöver göra egna bedömningar av om principen är uppfylld.

Vad gäller principen om lagringsminimering hänvisar utredningen till vad som sägs i avsnitt 8.2.6 om att den längsta möjliga lagringsperioden i Arachne inte får överstiga tio år.

Ovanstående innebär att den reglering som finns bedöms vara tillräcklig och att det inte finns skäl att överväga några författningsändringar avseende frivilligt uppgiftslämnande som tar sikte på principerna i artikel 5 i dataskyddsförordningen.

Känsliga personuppgifter

Utredningen har svårt att se att känsliga personuppgifter skulle förekomma bland de uppgifter som kan bli aktuella att lämna på frivillig basis. Som framgår av avsnitt 8.2.6 är det som huvudregel förbjudet att behandla känsliga personuppgifter. För det fall det ändå skulle bli aktuellt, kan det undantag från förbudet bli aktuellt att tillämpa som gäller om behandlingen är nödvändig med hänsyn till ett viktigt allmänt intresse, och behandlingen inte innebär ett otillbörligt intrång i den registrerades personliga integritet (3 kap. 3 § första stycket 3 dataskyddslagen).

Uppgifter som motsvaras av sådana uppgifter som räknas upp i artikel 36.6 i budgetförordningen, även om de inte är rättsligt obligatoriska att lämna för att de inte omfattas av gällande sektorsspecifik reglering, bör som utgångspunkt kunna anses vara nödvändiga att lämna med hänsyn till ett viktigt allmänt intresse. Vad gäller övriga slags uppgifter, för det fall det bland dessa skulle kunna finnas känsliga personuppgifter, bör även dessa kunna uppfylla kravet på viktigt allmänt intresse. Det är dock utlämnande myndighet som måste bedöma om behandlingen är nödvändig och inte innebär ett otillbörligt intrång i den registrerades personliga integritet.

Utredningen ser inte behov av författningsändringar när det gäller behandling av känsliga personuppgifter.

Uppgifter om personnummer

Även om det här är fråga om uppgiftslämnande som inte följer av ett krav i budgetförordningen, anser utredningen i likhet med vad som sägs i avsnitt 8.2.6 att ett utlämnande av uppgift om personnummer som utgångspunkt är förenligt med kraven i 3 kap. 10 § dataskyddslagen. Det är dock utlämnande myndighet som har att göra den bedömningen.

Det finns inte behov av författningsändringar när det gäller behandling av uppgifter om personnummer och samordningsnummer.

Personuppgiftsansvar

I likhet med vad som anges i avsnitt 8.2.6 om rättsligt obligatoriskt uppgiftslämnande är de svenska myndigheterna personuppgiftsansvariga för den personuppgiftsbehandling som de utför med anledning av det uppgiftslämnande som kan komma att ske.

Det finns inte behov av författningsändringar när det gäller personuppgiftsansvaret.

Enskildas rättigheter

I avsnitt 8.2.6 behandlas dataskyddsförordningens och dataskyddslagens bestämmelser om enskildas rättigheter och begränsningar av dessa. Dessa bestämmelser är tillämpliga vid den personuppgiftsbehandling som kan aktualiseras vid ett sådant frivilligt uppgiftslämnande som är aktuellt i detta avsnitt.

Utredningen har inte identifierat behov av ny reglering eller författningsändringar när det gäller enskildas rättigheter.

Sammanfattning av utredningens slutsatser

Utredningens bedömningar ovan kan sammanfattas så att det inte finns några hinder i dataskyddshänseende mot den personuppgiftsbehandling som kan förväntas komma att ske utan att det finns en rättslig skyldighet och att det inte behövs några författningsändringar på dataskyddsområdet avseende sådant uppgiftslämnande.

Befintlig dataskyddsreglering är tillräcklig. Utredningen ser därför inte skäl att föreslå reglering i en ny registerlag eller annan dataskyddslagstiftning för en ändamålsenlig personuppgiftsbehandling i denna del. Utredningens bedömning innebär att det inte heller behövs ändringar i någon annan reglering än rörande dataskydd för att möjliggöra personuppgiftsbehandlingen.

Det bör observeras att utredningens bedömningar om förenligheten med dataskyddsregelverket inte kan avse behandlingen i det enskilda fallet. Det är den personuppgiftsansvarige som behöver säkerställa att den personuppgiftsbehandling som faktiskt utförs är förenlig med dataskyddsregleringen.

8.4 Offentliggörande av uppgifter

8.4.1 Betydelsen av att skyldigheten gäller endast vid direkt förvaltning tillsammans med medlemsstaterna

I detta avsnitt behandlas utredningens uppdrag att bedöma om det finns behov av ändrade regler för att svenska myndigheter ska kunna uppfylla de krav som ställs i budgetförordningen, i den del det gäller skyldigheten att offentliggöra uppgifter enligt artikel 38.

Som beskrivs i avsnitt 4.7.3 innebär artikel 38.4 tredje stycket i budgetförordningen en ny skyldighet för medlemsstater att – inom ramen för EU-medel som förvaltas enligt direkt förvaltning tillsammans med medlemsstaterna – se till att viss information offentliggörs på en centraliserad webbplats. Skyldigheten gäller endast program som antas inom ramen för och finansieras genom fleråriga budgetramar efter 2027 (se övergångsbestämmelsen i artikel 277.6 i budgetförordningen).

Den fond som hanteras inom ramen för denna förvaltningsform, RRF, har i praktiken begränsad tillämplighet i tid genom att reformer och investeringar ska ha genomförts till den 31 augusti 2026 och utbetalningar till den 31 december samma år. Mot bakgrund av övergångsbestämmelsen i artikel 277.6 i budgetförordningen ska artikel 38.4 tredje stycket inte tillämpas på RRF och därmed är det inte aktuellt för svenska myndigheter att offentliggöra uppgifter avseende RRF enligt den bestämmelsen.

Det kan inte uteslutas att det under kommande programperioder kommer nya fonder och program som Sverige förvaltar inom ramen

för förvaltningsformen direkt förvaltning tillsammans med medlemsstaterna. Sverige kommer då att vara skyldigt att uppfylla det som sägs i bestämmelsen. Det är dock för närvarande oklart om så blir fallet och vilka fonder och program det då kommer att vara fråga om. Det förhållandet kan i sig innebära utmaningar när det gäller att bedöma behovet av åtgärder. I detta avsnitt behandlas frågan, så långt som det är möjligt, om det finns några hinder för Sverige att uppfylla skyldigheten i artikel 38.4 tredje stycket i budgetförordningen.

8.4.2 Det krävs inte författningsändringar på sekretessområdet för offentliggörande av uppgifter

Utredningens bedömning: Det behövs inga författningsändringar i sekretesshänseende för att svenska myndigheter ska kunna uppfylla kravet i artikel 38.4 tredje stycket i budgetförordningen om att offentliggöra uppgifter.

Skälen för utredningens bedömning: De uppgifter som omfattas av skyldigheten att offentliggöra uppgifter enligt artikel 38.4 tredje stycket i budgetförordningen motsvarar vissa av de uppgifter som svenska myndigheter ska tillgängliggöra för kommissionen enligt artikel 36.6 i budgetförordningen. Som anges i avsnitt 4.7.3 är de uppgifter som ska tillgängliggöras enligt artikel 36.6 beskrivna genom hänvisningar till artikel 38.2. Samtliga slags uppgifter som ska offentliggöras enligt artikel 38.2 (uppgifter om mottagare och om åtgärden) omfattas också av artikel 36.6.

Som utvecklas i avsnitt 8.2.3 bedömer utredningen att de uppgifter som svenska myndigheter ska tillgängliggöra för kommissionen enligt artikel 36.6 i budgetförordningen i regel inte kommer att omfattas av sekretess. Utredningen kan dock inte utesluta att vissa uppgifter undantagsvis skulle kunna vara sekretessbelagda i det enskilda fallet. Det skulle exempelvis kunna handla om uppgifter som kan omfattas av sekretess enligt 30 kap. 23 § OSL, såsom uppgift om total projektkostnad vilket, i kombination med andra uppgifter, skulle kunna avslöja information om stödmottagares ekonomiska planer.

För det fall att uppgifter skulle bedömas vara sekretessbelagda anser utredningen, när det gäller tillgängliggörande enligt artikel 36.6, att uppgifterna kommer att kunna lämnas ut till kommissionen med

stöd av 8 kap. 3 § OSL, se avsnitt 8.2.4. Bestämmelsen möjliggör att uppgifter som annars är sekretessbelagda lämnas till en utländsk myndighet eller en mellanfolklig organisation om utlämnande sker i enlighet med särskild föreskrift i lag eller förordning eller om uppgiften i motsvarande fall skulle få lämnas ut till en svensk myndighet och det enligt den utlämnande myndighetens prövning står klart att det är förenligt med svenska intressen att uppgiften lämnas till den utländska myndigheten eller den mellanfolkliga organisationen. Det kan möjligtvis argumenteras för att bestämmelsen kan tillämpas i detta fall till den del offentliggörandet kan ses som ett utlämnande till kommissionen, som äger den centraliserade webbplatsen. Det framstår dock som osäkert om den bestämmelsen kan tillämpas här. Visserligen är det fråga om ett utlämnande men det är inte endast fråga om ett utlämnande till kommissionen utan om ett offentliggörande på en webbplats som når en stor och okänd mängd mottagare.

Det kan dock ifrågasättas om det alls kommer att finnas hinder inom ramen för sekretessregelverket att offentliggöra uppgifterna. Det handlar delvis om sådana uppgifter som svenska myndigheter redan i dag offentliggör enligt andra regelverk (jfr avsnitt 4.2). Vissa av de uppgifter som ska tillgängliggöras enligt artikel 36.6 ingår vidare inte i skyldigheten att offentliggöra uppgifter enligt 38.4 tredje stycket (uppgifter om verklig huvudman). Den här aktuella skyldigheten är alltså mer begränsad. Dessutom finns det undantag i artikel 38.3 som innebär att uppgifterna inte ska offentliggöras i vissa fall. Dessa undantag innebär att uppgifterna inte ska offentliggöras i vissa situationer där det finns ett behov av att skydda uppgifterna från spridning. Det handlar bland annat om situationer då ett offentliggörande innebär en risk för berörda personers eller enheters fri- och rättigheter enligt EU:s rättighetsstadga eller kan skada mottagarnas affärsintressen.

Mot denna bakgrund gör utredningen bedömningen att det inte finns behov av några ändringar av regelverket på sekretessområdet för att möjliggöra ett offentliggörande enligt artikel 38.4 tredje stycket i budgetförordningen. För det fall att nya förvaltningsformer skulle inrättas och förutsättningarna för offentliggörande skulle ändras i framtiden kan det dock finnas skäl att ompröva utredningens ställningstagande.

8.4.3 Det krävs inte författningsändringar på dataskyddsområdet för offentliggörande av uppgifter

Utredningens bedömning: Det behövs inga författningsändringar i dataskyddshänseende för att svenska myndigheter ska kunna uppfylla kravet i artikel 38.4 tredje stycket i budgetförordningen om att offentliggöra uppgifter. Befintlig dataskyddsreglering ger ett tillräckligt stöd för behandlingen.

Skälen för utredningens bedömning

Inledning

I avsnitt 7.2 redogör utredningen för gällande rätt på dataskyddsområdet, bland annat för kravet på rättslig grund och de grundläggande principerna för att en personuppgiftsbehandling ska vara laglig.

I detta avsnitt gör utredningen bedömningar av om befintligt dataskyddsregelverk är tillräckligt för den personuppgiftsbehandling som kan förväntas ske vid offentliggörande av uppgifter enligt 38.4 tredje stycket i budgetförordningen eller om det krävs författningsändringar. Härvid lyfts vissa dataskyddsrättsliga frågor särskilt.

Rättslig grund för behandlingen

Om eller när skyldigheten att offentliggöra uppgifter enligt artikel 38.4 tredje stycket i budgetförordningen kommer att inträda för en svensk myndighet kommer det att finnas rättslig grund för den personuppgiftsbehandling som offentliggörandet kan medföra. Budgetförordningen är nämligen direkt tillämplig och därmed gäller de skyldigheter som följer av den. Den rättsliga grunden att *fullgöra en rättslig förpliktelse* (artikel 6.1 c i dataskyddsförordningen och 2 kap. 1 § dataskyddslagen) såväl som grunden att *utföra en uppgift av allmänt intresse* (artikel 6.1 e i dataskyddsförordningen och 2 kap. 2 § dataskyddslagen) bedöms då vara tillämpliga. Utredningen bedömer på samma grunder som framgår av avsnitt 8.2.6 att det rör sig om ett allmänt intresse och att behandlingen är att anse som nödvändig. De rättsliga grunderna bör också anses uppfylla kraven på tydlighet och precision samt på en förutsebar tillämpning för personer som

omfattas av grunderna. Utredningen utgår också från att unionsrätten är förenlig med Europakonventionen och uppfyller kravet på proportionalitet i artikel 6.3 i dataskyddsförordningen. För en samlad integritetsanalys, se kapitel 9.

Principerna i artikel 5 i dataskyddsförordningen

I avsnitt 7.2.5 redogör utredningen för principerna i artikel 5.1 i dataskyddsförordningen och för att det är den personuppgiftsansvarige som ska säkerställa att principerna efterlevs. Utredningen gör så långt det är möjligt bedömningar avseende möjligheten att efterleva principerna.

På samma grunder som anges i avsnitt 8.2.6 utgår utredningen från att de myndigheter som kan komma att behandla personuppgifter vid ett eventuellt offentliggörande av uppgifter uppfyller principen om laglighet, korrekthet och öppenhet, principen om integritet och konfidentialitet samt principen om riktighet. Detsamma gäller principen om ändamålsbegränsning och förenligheten med finalitetsprincipen. Det är dock berörda myndigheter som behöver göra egna bedömningar av om principerna är uppfyllda.

Det anges uttryckligen i artikel 38.2 i budgetförordningen att vederbörlig hänsyn ska tas till kraven på konfidentialitet och säkerhet, i synnerhet skyddet av personuppgifter. I skälen till budgetförordningen tas skyddet för personuppgifter i relation till offentliggörande av uppgifter upp. Största möjliga transparens i fråga om uppgifter om mottagare bör eftersträvas, utan att det påverkar tillämpningen av reglerna om skydd av personuppgifter. Informationen om mottagare av unionsmedel som bör offentliggöras på en centraliserad och särskild webbplats för unionsinstitutionerna bör vara lätt tillgänglig via lämpliga och säkra tekniska lösningar (skäl 34).

När det gäller principen om uppgiftsminimering är det av relevans att det finns flera situationer då offentliggörande inte ska ske. Undantagen, som finns i artikel 38.3 i budgetförordningen, gäller bland annat då ett offentliggörande innebär en risk för berörda personers eller enheters fri- och rättigheter enligt EU:s rättighetsstadga eller kan skada mottagarnas affärsintressen. Dessa begränsningar utgör ett uttryck för principen om uppgiftsminimering.

Vad gäller principen om lagringsminimering framgår direkt av artikel 38.7 att om personuppgifter offentliggörs ska informationen tas bort två år efter utgången av det budgetår då rättsliga åtaganden gjordes för medlen.

Det ovanstående innebär att utredningen bedömer att den reglering som finns är tillräcklig och att det inte finns skäl att överväga några författningsändringar avseende offentliggörande som tar sikte på principerna i artikel 5 i dataskyddsförordningen.

Andra relevanta dataskyddsrättsliga krav

Utredningen har svårt att se att känsliga personuppgifter skulle förekomma bland de uppgifter som kan bli aktuella att offentliggöra, särskilt då det finns ett utrymme att underlåta offentliggörande av uppgifter när det innebär en risk för berörda personers eller enheters fri- och rättigheter enligt EU:s rättighetsstadga. Som framgår av avsnitt 8.2.6 är det som huvudregel förbjudet att behandla känsliga personuppgifter. För det fall det ändå skulle bli aktuellt i något fall, kan eventuellt undantaget att behandlingen är nödvändig med hänsyn till ett viktigt allmänt intresse, och det inte innebär ett otillbörligt intrång i den registrerades personliga integritet, vara tillämpligt (3 kap. 3 § första stycket 3 dataskyddslagen).

Om det skulle bli aktuellt att behandla uppgifter om personnummer, anser utredningen – i enlighet med vad som sägs i avsnitt 8.2.6 – att en sådan behandling i samband med ett offentliggörande bör anses vara förenligt med kraven i 3 kap. 10 § dataskyddslagen. Det är utlämnande myndighet som har att göra den bedömningen.

I likhet med vad som anges i avsnitt 8.2.6 är de svenska myndigheterna personuppgiftsansvariga för den personuppgiftsbehandling som de utför med anledning av ett eventuellt offentliggörande av uppgifter. Vad gäller enskildas rättigheter gäller dataskyddsförordningens och dataskyddslagens bestämmelser om detta. Utredningen har inte identifierat behov av ny reglering eller författningsändringar i dessa avseenden.

Sammanfattning av utredningens slutsatser

Utredningens bedömningar ovan kan sammanfattas så att det inte finns hinder i dataskyddshänseende att offentliggöra nödvändiga uppgifter och att det inte behövs några författningsändringar på dataskyddsområdet avseende ett sådant uppgiftslämnande.

Befintlig dataskyddsreglering är tillräcklig. Utredningen ser därför inte skäl att föreslå reglering i en ny registerlag eller annan dataskyddslagstiftning för en ändamålsenlig personuppgiftsbehandling i denna del. Utredningens bedömning innebär att det inte heller behövs ändringar i någon annan reglering än rörande dataskydd för att möjliggöra personuppgiftsbehandlingen.

Det bör observeras att utredningens bedömningar om förenligheten med dataskyddsregelverket inte kan avse behandlingen i det enskilda fallet. Det är den personuppgiftsansvarige som behöver säkerställa att den personuppgiftsbehandling som faktiskt utförs är förenlig med dataskyddsregleringen.

8.5 Användande av Arachne som verktyg

8.5.1 Uppdraget i denna del

Det är frivilligt att använda Arachne – även enligt den omarbetade budgetförordningen – men det kan bli obligatoriskt för medlemsländerna att använda Arachne i sin handläggning och kontroll av EU-medel i framtiden. Även om det inte blir obligatoriskt att använda Arachne kan det finnas starka skäl för svenska myndigheter att göra det, något som framhållits av Utredningen om hantering av EU-medel (se avsnitt 3.4.5 och SOU 2024:22, s. 23 och 448–452).

Nu aktuell utredning har också som uttryckligt uppdrag att utreda frågor som syftar till att säkerställa att svenska myndigheter har förutsättningar att använda Arachne. Det handlar i denna del om uppdragen att bedöma om mottagna eller tillgängliga uppgifter inom ramen för Arachne kommer att utgöra allmänna handlingar i Sverige och i vilken mån uppgifterna omfattas av befintliga sekretessbestämmelser eller om det finns behov av nya sekretessbestämmelser för att säkerställa att uppgifterna får ett tillfredsställande skydd. Det handlar också om uppdraget att kartlägga det skydd för personuppgifter som finns i Arachne och utreda om det finns behov av

nya eller ändrade bestämmelser för att möjliggöra den personuppgiftsbehandling som en användning av Arachne medför samt att lämna nödvändiga författningsförslag. En kartläggning av skyddet för personuppgifter finns också i den samlade integritetsanalysen i kapitel 9.

Med användande av Arachne som verktyg avses alltså här att svenska myndigheter bereder sig tillgång till uppgifter i databasen och använder systemet som ett datautvinnings- och riskvärderingsverktyg. Det kan ske dels i samband med överväganden inför beviljandet av stöd (ex ante), dels vid efterföljande kontroller eller urval av vad som ska kontrolleras (ex post). Det är således fråga om något annat än att svenska myndigheter tillgängliggör uppgifter för kommissionen enligt artikel 36.6, som läggs in i Arachne, eller för in uppgifter direkt i Arachne, något som behandlas i kapitel 4 och avsnitt 8.2 och 8.3.

8.5.2 Blir uppgifterna i Arachne allmänna handlingar hos svenska myndigheter?

Utredningens bedömning: Uppgifter i Arachne kan bli allmänna handlingar hos de svenska myndigheter som använder systemet.

Skälen för utredningens bedömning

När blir det fråga om allmänna handlingar?

Vad som utgör en handling och när en handling är en allmän handling enligt nationell rätt regleras i 2 kap. tryckfrihetsförordningen, TF. Med en *handling* avses en framställning i skrift eller bild samt en upptagning som endast med tekniska hjälpmedel kan läsas eller avlyssnas eller uppfattas på annat sätt (2 kap. 3 §). För att vara en *allmän handling* krävs att den förvaras hos en myndighet och enligt 2 kap. 9 eller 10 § är att anse som inkommen till eller upprättad hos en myndighet (2 kap. 4 §).

En upptagning som avses i 2 kap. 3 § TF anses *förvarad* hos en myndighet om upptagningen är tillgänglig för myndigheten med tekniskt hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas eller avlyssnas eller uppfattas på annat

sätt (2 kap. 6 § första stycket). En sammanställning av uppgifter ur en upptagning för automatiserad behandling anses dock förvarad hos myndigheten endast om myndigheten kan göra sammanställningen tillgänglig med rutinbetonade åtgärder och inte annat följer av 2 kap. 7 § (2 kap. 6 § andra stycket). Enligt 2 kap. 7 § TF anses en sammanställning enligt 2 kap. 6 § andra stycket TF inte förvarad hos myndigheten om sammanställningen innehåller personuppgifter och myndigheten enligt lag eller förordning saknar befogenhet att göra sammanställningen tillgänglig. Med personuppgift avses all slags information som direkt eller indirekt kan hänföras till en fysisk person.

En handling anses *inkommen* till en myndighet, när den har anlänt till myndigheten eller kommit behörig befattningshavare till handa (2 kap. 9 § första stycket). I fråga om en upptagning som avses i 2 kap. 3 § gäller i stället att den anses ha kommit in till myndigheten när någon annan har gjort den tillgänglig för myndigheten på det sätt som anges i 6 §. I fråga om en upptagning som endast kan uppfattas med tekniska hjälpmedel gäller därmed i stället att den anses ha kommit in till myndigheten när någon annan för myndigheten har gjort upptagningen tillgänglig med tekniskt hjälpmedel som myndigheten själv utnyttjar.

Slutligen kan sägas att en handling anses ha *upprättats* hos en myndighet, när den har expedierats. En handling som inte har expedierats anses upprättad när det ärende som den hänför sig till har slutbehandlats hos myndigheten eller, om handlingen inte hänför sig till ett visst ärende, när den har justerats av myndigheten eller färdigställts på annat sätt (2 kap. 10 § TF).

Arachne – ett system med flera olika delar där alla uppgifter inte är tillgängliga för alla

Enligt utredningen bör Arachne ses som en databas som i sig innehåller olika delar, vilka kan vara att bedöma olika i rättsligt hänseende. Uppgifter som medlemsstaternas myndigheter (t.ex. projektdata) och kommissionen (från FTS) har fört in i systemet är en del (så kallade interna data).

En annan del – i rättsligt hänseende – skulle kunna vara uppgifter som hämtas in från externa databaser, såsom i dagsläget Orbis och World Compliance. Uppgifter från dessa databaser lagras i Arachne och används för att berika uppgifter avseende interna data, varigenom

systemets interna data får ett högre informationsvärde. Vid en användning av Arachne söker inte användaren i de externa databaserna utan tar del av uppgifter som härrör från dessa sedan de har blivit en del av innehållet i Arachne. Kommissionen ansvarar för att var tredje månad uppdatera uppgifterna från databaserna Orbis och World Compliance (se Arachne, Frequently asked questions, version 2.3, den 19 augusti 2022, fråga 31). Vad gäller uppgifter i databasen World Compliance bör nämnas att det inte går att söka på enskilda personer eller företag, men om en person eller ett företag är involverat i ett projekt som en myndighet hanterar framgår det av sådana riskvärderingar som görs genom Arachne (se mer i avsnitt 5.4.2).

En särskild del av Arachne utgörs av tidigare gjorda riskvärderingar. Sådana riskvärderingar lagras i Arachne. Arachne-användare kan hämta dessa riskvärderingar med hjälp av gränssnittet i Arachne-applikationen och har möjlighet att bedöma riskerna relaterade till de stödprogram beträffande vilka de har rätt till åtkomst. Eftersom användare endast får tillgång till riskvärderingar avseende projekt som de själva har någon roll i, är vissa delar av innehållet i Arachne över huvud taget inte tillgängliga för en användande myndighet (Arachne, Frequently asked questions, version 2.3, den 19 augusti 2022, fråga 24, jfr Arachne-stadgan, punkt 10). Det bör noteras att detta gäller *gjorda* riskvärderingar och inte riskvärderingar som skulle kunna göras, men inte har gjorts. Som framgår av avsnitt 5.2.1 har Arachne en förhandsfunktion där en riskvärdering utförs på användarens begäran.

Det finns olika former av elektroniskt uppgiftslämnande

I Sverige skiljer lagstiftningen ofta mellan två former av elektroniskt utlämnande: direktåtkomst och annat elektroniskt utlämnande (även kallat utlämnande på medium för automatiserad behandling). Det finns inte någon legaldefinition av begreppet direktåtkomst. Den grundläggande innebörden anses vara att någon har tillgång till information hos någon annan, och på egen hand kan söka i den, dock utan att själv kunna påverka innehållet. Direktåtkomst kan ge användaren möjlighet att även hämta in information till sitt eget system och bearbeta den där (se t.ex. prop. 2016/17:58 s. 112). Vid direktåtkomst uppkommer i regel så kallad överskottsinformation, eftersom den

mottagande myndigheten ofta rent tekniskt måste ha tillgång till fler uppgifter än de som faktiskt kommer att utnyttjas. Sammanställningar av uppgifter hos en myndighet, som i samband med direktåtkomst görs tekniskt tillgängliga för en annan myndighet, anses vara förvarade även hos den andra myndigheten, och därmed också utgöra allmänna handlingar hos den myndigheten om sammanställningarna kan göras tillgängliga via rutinbetonade åtgärder (jfr 2 kap. 3, 4 och 6 §§ TF och prop. 2007/08:160 s. 67–70).

Direktåtkomst kan generellt sägas öka riskerna för intrång i den personliga integriteten, eftersom den typiskt sett innebär att uppgifterna blir tillgängliga för fler personer och att den utlämnande myndighetens möjlighet att kontrollera utlämnandet minskar.

Uttrycken ”annat elektroniskt utlämnande” och ”utlämnande på medium för automatiserad behandling” har samma innebörd. Det förra uttrycket förekommer i nyare registerförfattningar. Vad som avses med uttrycken har förändrats i takt med teknikutvecklingen, men de förhåller sig alltid på något sätt till utlämnande genom direktåtkomst. Med dagens teknik kan utlämnande av information ske genom annat elektroniskt utlämnande, exempelvis genom e-post, på ett usb-minne eller genom direkt överföring från ett datorsystem till ett annat. Vid ett mer omfattande informationsutbyte mellan myndigheter är det oftast den senare metoden, direkt överföring från ett datorsystem till ett annat, som används.

De praktiska skillnaderna mellan direktåtkomst och annat elektroniskt utlämnande har med tiden kommit att minska. Högsta förvaltningsdomstolen har i avgörandet HFD 2015 ref. 61 uttalat att avgörande för gränsdragningen mellan vad som utgör direktåtkomst respektive utlämnande på medium för automatiserad behandling är om den aktuella upptagningen kan anses förvarad hos den mottagande myndigheten enligt nuvarande 2 kap. 6 § TF, det vill säga om den är tillgänglig för myndigheten med tekniska hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas, avlyssnas eller på annat sätt uppfattas. Uttalandet kan tolkas så att den tekniska utformningen av en myndighets system för utlämnande av uppgifter kan bli avgörande för om ett utlämnande ska anses ske genom direktåtkomst eller annat elektroniskt utlämnande.

Blir uppgifter i Arachne att betrakta som inkomna och förvarade hos svenska myndigheter genom direktåtkomst?

Om svenska myndigheter anses ha direktåtkomst till uppgifter i Arachne – det vill säga, något förenklat, om uppgifterna är tillgängliga för myndigheterna med tekniska hjälpmedel som myndigheterna själva utnyttjar – anses uppgifterna förvarade hos myndigheterna och är därmed allmänna handlingar, som ska lämnas ut om inte sekretess hindrar ett utlämnande. Det skulle också innebära att även viss överskottsinformation som finns i Arachne men som en myndighet inte eftersökt, skulle anses utgöra allmänna handlingar hos myndigheten. Om åtkomsten inte anses utgöra direktåtkomst utan utlämnandet anses ske genom annat elektroniskt utlämnande och enbart de uppgifter som härrör från en viss sökning eller annan åtgärd hos myndigheten blir tillgängliga skulle bedömningen om vad som blir allmänna handlingar kunna bli en annan.

För bedömningen om svenska myndigheter har tillgång till uppgifter i Arachne genom direktåtkomst är det avgörande hur systemet tekniskt sett är utformat. Utredningen konstaterar att det i detta avseende finns flera osäkerhetsmoment, som bland annat hänger samman med att en utveckling av systemet pågår och det är oklart hur det kommer att vara konstruerat i framtiden.

Bedömningen av om en teknisk lösning innebär en direktåtkomst är inte heller helt okomplicerad. I det nämnda målet HFD 2015 ref. 61 prövades om socialnämnders åtkomst till uppgifter ur socialförsäkringsdatabasen via ett visst system var att betrakta som direktåtkomst. Såväl förvaltningsrätten som kammarrätten fann att så var fallet, men Högsta förvaltningsrätten gjorde en annan bedömning. Det avgörande var enligt domstolen om informationen var tillgänglig med tekniska hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas, avlyssnas eller på annat sätt uppfattas på det sätt som avses i numera 2 kap. 6 § TF. Domstolen fäste vikt vid att socialnämnderna inte på egen hand kunde söka information i socialförsäkringsdatabasen, utan ett utlämnande förutsatte att Försäkringskassan reagerade på en begäran om att de efterfrågade uppgifterna ska lämnas ut. Försäkringskassan fick därigenom anses förfoga över frågan om och i så fall vilka uppgifter som ska lämnas ut. Socialnämnderna ansågs därför inte ha sådan teknisk

tillgång till upptagningar som avses i numera 2 kap. 6 § TF och det var därför inte fråga om direktåtkomst.

Även tillgång till uppgifter via Arachne kan sägas – liksom avseende många databaser – delvis bygga på ett förfarande med frågor och svar efter automatisk bearbetning. Det framstår inte som helt klart hur detta kriterium kan användas för att särskilja direktåtkomst från annat elektroniskt utlämnande (jfr Sören Öman, Direktåtkomst till databaser, Blendow Lexnova Expertkommentar – Offentlig rätt, december 2015).

Det kan också noteras att ett kriterium som brukar ställas upp för direktåtkomst är att mottagaren saknar möjlighet att själv kunna påverka innehållet. När det gäller Arachne kommer mottagaren av uppgifter ofta vara en myndighet som inte bara använder Arachne som ett verktyg för riskvärderingar utan som också bidrar till att tillgängliggöra uppgifter som tillförs Arachne och därmed faktiskt påverkar databasens innehåll. Data som laddats upp i Arachne kan i princip inte ändras. Medlemsstatens enda möjlighet att ändra eller korrigera data är att ladda upp en ny datafil (Arachne, Frequently asked questions, version 2.3, den 19 augusti 2022, fråga 10).

Som nämns ovan är inte heller alla delar av Arachne tillgängliga för alla användare.

Enligt utredningen talar dock mycket för att den tekniska utformningen av Arachne kan innebära att svenska myndigheter anses få direktåtkomst till uppgifter genom systemet. Systemet synes nämligen vara utformat så att informationen kommer att vara tillgänglig för användaren för att på egen hand söka eller få svar på frågor. Vidare synes åtkomsten ge användaren en möjlighet att också hämta hem informationen till sitt eget system och bearbeta den där. Åtkomsten innebär också att uppgifter kan hämtas utan att kommissionen har kontroll över vilka uppgifter som hämtas.

Det förhållandet att vissa nationella myndigheter som använder Arachne också bidrar med uppgifter till systemet bedöms inte i sig innebära att det inte är fråga om direktåtkomst. Myndigheternas möjligheter att påverka innehållet är begränsade och inte en följd av åtkomsten till systemet i sig.

Det finns skäl att lyfta riskvärderingar särskilt. Mycket talar enligt utredningens mening för att svenska myndigheter anses få direktåtkomst till gjorda riskvärderingar som finns lagrade i Arachne. Det mesta talar vidare för att svenska myndigheter inte kan sägas få direkt-

åtkomst till riskvärderingar som ännu inte har begärts av myndigheten inom ramen för den så kallade förhandsfunktionen. Så som Arachne fungerar i dag genereras inom ramen för förhandsfunktionen en riskvärdering först på en användares begäran. Enligt utredningen talar mycket för att svenska myndigheter anses få direktåtkomst även till sådana riskvärderingar som har gjorts genom förhandsfunktionen. Sådana riskvärderingar som ännu inte har utförts, bör däremot inte anses vara tillgängliga för användare på det sätt som avses i 2 kap. 6 § TF.

Om svenska myndigheter anses få tillgång till uppgifter genom direktåtkomst till en utländsk myndighets databas innebär det att uppgifterna skulle kunna anses vara förvarade hos den svenska myndigheten i tryckfrihetsförordningens mening. Den omständigheten att utländska myndigheter inte omfattas av offentlighetsprincipen påverkar inte i sig bedömningen. Uppgifter i utländska databaser som en svensk myndighet har direktåtkomst till utgör enligt regeringen som utgångspunkt allmänna handlingar hos myndigheten, om uppgifterna ingår i en så kallad färdig elektronisk handling eller om de kan sammanställas med rutinbetonade åtgärder och utan användning av förbjudna sökbegrepp (jfr prop. 2011/12:157 s. 8 och 17).

Det kan dock inte uteslutas att tillgången till uppgifter i Arachne kan bedömas på annat sätt. Det pågår en teknisk utveckling av Arachne och det är oklart hur konstruktionen kommer att se ut i framtiden. Arachne innehåller flera funktioner och uppgifter från olika källor och det kan inte uteslutas att olika funktioner och olika typer av uppgifter bör bedömas på olika sätt.

Det kan inte heller uteslutas att konstruktionen av Arachne anses innebära att användaren får tillgång till information först efter att ha ställt frågor på ett sådant sätt att det inte är fråga om direktåtkomst. Det kan då diskuteras i vilken utsträckning som uppgifter i Arachne anses vara förvarade hos myndigheten på ett sådant sätt att de anses som allmänna handlingar där.

Sammanfattningsvis bedömer utredningen att mycket talar för att det kan bli fråga om direktåtkomst – i vart fall beträffande vissa slags uppgifter. Bedömningarna i detta betänkande behöver mot denna bakgrund ta höjd för att uppgifter i Arachne kan anses vara allmänna handlingar utifrån 2 kap. 6 § TF. Det är den myndighet som får en begäran om utlämnande av allmän handling som har att ta ställning i frågan.

Begränsningsregeln i 2 kap. 7 § TF kan innebära att sammanställningar inte anses förvarade hos en myndighet

Från huvudregeln som beskrivs ovan om när upptagningar för automatiserad behandling ska anses förvarade hos en myndighet finns undantag, bland annat i 2 kap. 7 § TF, som ibland kallas begränsningsregeln. Av bestämmelsen framgår att en sammanställning enligt 2 kap. 6 § andra stycket TF inte är förvarad hos myndigheten om sammanställningen innehåller personuppgifter och myndigheten enligt lag eller förordning saknar befogenhet att göra sammanställningen tillgänglig. Paragrafen innebär att om en myndighet av hänsyn till integritetsskyddsintresset är förhindrad att i sin verksamhet ta fram en viss sammanställning, så är den inte heller tillgänglig för allmänheten. Den bestämmelsen kan bli aktuell om någon av en myndighet begär ut en sammanställning av uppgifter ur Arachne som innebär att myndigheten måste söka efter ett urval av personer som exempelvis har en viss politisk åsikt (se Kammarrätten i Stockholms dom den 18 april 2023 i mål nr 1330-23). Det är då upp till myndigheten att bedöma om bestämmelsen är tillämplig.

Den så kallade biblioteksregeln innebär att vissa handlingar inte anses vara allmänna handlingar

I 2 kap. 13–14 §§ TF finns bestämmelser om handlingar som inte anses som allmänna, trots att de anses förvarade hos en myndighet. Som allmän handling anses inte – trots att en handling förvaras hos en myndighet och är inkommen dit – en tryckt skrift, en ljud- eller bildupptagning eller någon annan handling som ingår i ett bibliotek eller som från en enskild har tillförts ett allmänt arkiv uteslutande för förvaring och vård eller forsknings- och studieändamål eller privata brev, skrifter eller upptagningar som annars har överlämnats till en myndighet uteslutande för något av de angivna ändamålen. Inte heller en upptagning av innehållet i en sådan handling anses som en allmän handling, om upptagningen förvaras hos en myndighet där den ursprungliga handlingen inte skulle vara att anse som allmän. Detta framgår av 2 kap. 14 § första stycket 3 och 4 TF. Av bestämmelsens andra stycke framgår att det som föreskrivs i första stycket 3 om handlingar som ingår i bibliotek inte tillämpas på en upptagning i en databas som en myndighet har tillgång till enligt ett avtal med

en annan myndighet, om upptagningen är allmän handling hos den myndigheten.

Är biblioteksregeln tillämplig på uppgifterna i Arachne?

Biblioteksregeln omfattar handlingar som en myndighet använder på motsvarande sätt som böcker i ett bibliotek, det vill säga för att söka faktaunderlag i allmänhet, rättsfallsreferenser eller tidskriftsartiklar och liknande (jfr prop. 1990/91:60 s. 31). När det gäller referensdatabaser som producerats av enskilda organ, med vilka utländska myndigheter jämställs, har det inte ansetts rimligt att dessa skulle vara fria för insyn enligt offentlighetsprincipen (prop. 2001/02:70 s. 26). Det har alltså betydelse vilka slags uppgifter det är fråga om och hur uppgifterna används av myndigheterna.

Som anges under rubriken *Arachne – ett system med flera olika delar* bör Arachne ses som en databas som i sig innehåller olika delar, vilka kan vara att bedöma olika i rättsligt hänseende. Arachne kan vidare inte sägas endast vara en traditionell databas eftersom det också sker en bearbetning av uppgifterna i systemet.

Beträffande de delar av Arachne som består av uppgifter som härrör från databasen *Orbis* är det enligt utredningen möjligt att bedöma dessa som uppgifter i en referensdatabas som biblioteksregeln kan vara tillämplig på. Uppgifterna i Orbis utgör då inte allmänna handlingar, även om de kan anses förvarade hos en användande myndighet. Detta kan dock komma att ändras, eftersom avsikten synes vara att uppgifter i Orbis endast ska vara tillgängliga för användare beträffande sådana program som användaren hanterar. När det gäller databasen *World Compliance* är uppgifter i databasen, som det fungerar i dag, tillgängliga enbart genom riskvärderingar i Arachne (se mer i avsnitt 5.4.2). Biblioteksregeln bör därför inte bli tillämplig för sådana uppgifter.

Resultaten av gjorda riskvärderingar som finns i Arachne bör anses vara upptagningar för automatiserad behandling. Sådana riskvärderingar är inte jämförbara med innehållet i ett bibliotek och biblioteksregeln bör enligt utredningens mening inte vara tillämplig på dessa.

Sammanfattande slutsatser

Många faktorer har betydelse för frågan om uppgifter i Arachne ska anses som allmänna handlingar hos en svensk myndighet, och centrala faktorer är hur Arachne är uppbyggt och hur åtkomsten rent tekniskt fungerar. I dagsläget finns det flera osäkerhetsfaktorer i det avseendet. Utgångspunkten bör enligt utredningens mening vara att uppgifter i Arachne kan anses förvarade hos och därmed bli allmänna handlingar hos de svenska myndigheter som använder Arachne. Det är dock möjligt att vissa uppgifter som finns i Arachne kan komma att omfattas av biblioteksregeln och därmed inte anses utgöra allmänna handlingar. Det är utlämnande myndighet som har att göra bedömningen i en utlämnandesituation.

8.5.3 Finns det behov av sekretesskydd för uppgifter som finns i Arachne?

Utredningens bedömning: Det kan finnas behov av sekretesskydd för uppgifter som svenska myndigheter får tillgång till vid ett användande av Arachne. Det handlar främst om följande behov.

- Behov att kunna hemlighålla uppgifter
  - för att samarbetet inom EU inte ska försämras, och
  - för att myndigheternas arbete med kontroller och granskning inte ska motverkas
- Behov att kunna hemlighålla uppgift om en enskilds affärs- eller driftförhållanden med mera i tillsynsverksamhet och liknande
- Behov att kunna hemlighålla uppgifter om personliga förhållanden, särskilt för förföljda personer.

Skälen för utredningens bedömning

Inledning

Som konstateras ovan kan uppgifter i Arachne komma att bli allmänna handlingar hos de myndigheter som använder systemet. Om det inte finns någon tillämplig sekretessbestämmelse kommer därför svenska myndigheter vara skyldiga att på begäran lämna ut uppgifterna. I detta avsnitt behandlas frågan om huruvida det finns behov av sekretessskydd för uppgifter i Arachne. Ett led i den bedömningen är om EU-rätten ställer krav på skydd motsvarande sekretess för uppgifter i Arachne.

Allmänt om öppenhet och sekretessreglering inom EU

Den fria rörligheten och det omfattande samarbetet inom EU kräver ett betydande informationsutbyte mellan medlemsstaterna. I takt med att det internationella samarbetet tätnar, är det naturligt och i grunden positivt att uppgiftsutbytet mellan staterna ökar. Information kan på så sätt återanvändas och erfarenheter spridas, vilket bidrar till en effektivare förvaltning. Sverige har inom det internationella samarbetet arbetat aktivt för en ökad öppenhet. I förhandlingar om bland annat EU-rättsakter har Sverige konsekvent drivit en linje som innebär att rättsakten eller avtalet ska ges en utformning som i största möjliga mån tillgodoser allmänhetens intresse av insyn i berörda myndigheters verksamhet. Arbetet har i flera avseenden varit framgångsrikt, även om utvecklingen – eftersom de flesta medlemsstater har en annan tradition än Sverige när det gäller handlingsoffentlighet – dock gått relativt långsamt (prop. 2012/13:192 s. 23).

Vissa allmänna bestämmelser om öppenhet finns i artikel 15 i EUF-fördraget, där det anges att unionens institutioner, organ och byråer ska utföra sitt arbete så öppet som möjligt, för att främja en god förvaltning och se till att det civila samhället kan delta. Vidare anges att varje unionsmedborgare och varje fysisk eller juridisk person som är bosatt eller har sitt stadgeenliga säte i en medlemsstat ska ha rätt till tillgång till unionens institutioners, organs och byråers handlingar, oberoende av medium, enligt de principer och villkor som ska bestämmas i enlighet med vad som närmare anges i artikeln.

Ett uttryck för ökad öppenhet inom EU är vidare den så kallade öppenhetsförordningen från 2001. Den innebär i huvudsak att medborgare har rätt att ta del av alla handlingar som dessa institutioner innehar, med undantag för sådan information som omfattas av de särskilda sekretessundantag som finns uppräknade i förordningen. Förordningen ger uttryck för att det är nödvändigt att göra arbetet vid unionens institutioner öppnare (se skäl 3). Syftet med förordningen är att ge allmänhetens rätt till tillgång till handlingar största möjliga effekt (se skäl 4).

Det förekommer sekretessbestämmelser i internationella avtal och EU-rättsakter. Bland annat på grund av det arbete som Sverige har bedrivit för ökad öppenhet inom EU, förekommer det numera även att sådana sekretessbestämmelser är försedda med skaderekvisit, i likhet med flertalet svenska sekretessbestämmelser (prop. 2012/13:192 s. 11 och 12).

Budgetförordningen och Arachne-stadgan ger ingen tydlig ledning

Budgetförordningen ger på flera ställen uttryck för nödvändigheten av transparens i arbetet med att genomföra EU:s budget. Exempelvis ska enligt artikel 6 budgeten upprättas och genomföras bland annat i enlighet med principen om transparens, något som särskilt behandlas i kapitel 8 i budgetförordningen. Av artikel 63 framgår att – när budgeten genomförs inom ramen för delad förvaltning – även medlemsstaterna ska iaktta principen om transparens. Vidare anges att – utan att det påverkar tillämpningen av reglerna om skydd av personuppgifter – största möjliga transparens i fråga om uppgifter om mottagare bör eftersträvas (skäl 34).

Frågan är om budgetförordningen medför att uppgifter i Arachne ändå ska skyddas genom sekretess. Arachne-teamet vid kommissionen har under arbetet med denna utredning gett uttryck för synen att ingen information som finns i Arachne ska offentliggöras (be published) och har därvid bland annat hänvisat till artikel 36.7 i budgetförordningen.[2] Budgetförordningen innehåller dock – som utredningen uppfattar det – inte några bestämmelser som tar direkt sikte på offentlighet och sekretess avseende uppgifter som finns i Arachne. Artikel 36.7 innehåller bestämmelser om åtkomstbegränsning och

[2] Komm2025/00388-10.

anger bland annat att kommissionen som personuppgiftsansvarig ska ansvara för utveckling, förvaltning och övervakning av Arachne, för att bland annat säkerställa uppgifternas säkerhet och konfidentialitet. Även om uttrycket konfidentialiet kan åsyfta sekretess synes detta inte vara vad som avses med begreppet i detta sammanhang, då bestämmelsen tar sikte på den personuppgiftsansvariges skyldigheter vid personuppgiftsbehandling. Budgetförordningen ger därmed enligt utredningens mening inget tydligt svar på frågan om uppgifter i Arachne generellt sett ska vara offentliga eller sekretessbelagda.

I *Arachne-stadgan* anges bland annat att den externa informationen i Arachne till fullo redan är offentliggjord och tillgänglig för allmänheten (på engelska ”officially published and publicly available”), se punkt 6.2. Det talar för att det beträffande sådana uppgifter inte krävs något sekretesskydd och att det inte heller bör finnas något sådant. Här kan också påminnas om att en del av uppgifterna som kommer att finnas i Arachne också kommer att offentliggöras av kommissionen och i vissa fall av medlemsstaterna med stöd av artikel 38, se mer om detta i avsnitt 4.7.1.

Vad gäller resultat av riskberäkningar finns dock i Arachne-stadgan skrivningar som kan tyda på att dessa bör behandlas på särskilt sätt. Av punkt 3 framgår att programmyndigheterna som får tillgång till resultaten av Arachnes riskvärderingar bara ska använda dessa för förvaltningskontroller (management verifications), kontroller (controls) och revisioner (audits). Resultaten ska inte användas för personliga intressen eller några andra ändamål. Av punkt 6.2 framgår att resultat av riskvärderingar utgör interna data som ska användas för skyddet av EU:s finansiella intressen och för förvaltningskontroller. Vidare framgår av punkten att sådana riskvärderingar omfattas av dataskydd (subject to data protection conditions) och att de inte ska publiceras (should not be published), varken av kommissionen eller av programmyndigheterna.

Det kan alltså konstateras att Arachne-stadgan i vart fall när det gäller resultatet av riskvärderingar ställer krav av något slag. Stadgan är dock inte helt tydlig. Det kan diskuteras om det med skrivningen ”should not be published” avses att resultatet inte ska offentliggöras, till exempel på en särskild hemsida, eller att resultatet ska vara sekretessbelagt och inte lämnas ut på begäran från allmänheten.

Enligt ett svar till utredningen från Arachne-teamet vid kommissionen ställer budgetförordningen inte något krav på särskilda åt-

gärder för att uppnå konfidentialitet när det gäller resultat av riskberäkningar. De har också uppgett att resultaten inte är avsedda för den breda allmänheten utan enbart för vissa personer, varför det behöver säkerställas att de inte sprids fritt. Arachne-teamet uppmanar därför till nödvändiga åtgärder på nationell nivå för att se till att riskvärderingarna inte blir tillgängliga för allmänheten, utan att det kommer i strid med de nationella regelverken.[3]

Sammanfattningsvis ger inte budgetförordningen och Arachnestadgan någon tydlig vägledning när det gäller eventuella krav på hemlighållande av uppgifter i Arachne och de besked som utredningen har fått från Arachne-teamet vid kommission i frågan får anses vara något motstridiga.

Uppgifterna i Arachne kommer i regel inte att omfattas av sekretess

Utöver ovan nämnda oklarheter är en grundläggande utmaning att det är svårt för utredningen att tillfullo veta vilka uppgifter Arachne innehåller och kommer att innehålla. Uppgifterna härrör från flera olika källor och det kan också ske förändringar som Sverige saknar möjlighet att påverka, exempelvis när det gäller vilka uppgifter som finns i olika sanktionslistor och liknande. Vidare kan kommande programperiod medföra nya fonder och därmed nya uppgifter.

Som utgångspunkt gör dock utredningen bedömningen att i vart fall en betydande del av uppgifterna i Arachne inte kräver något särskilt sekretesskydd. Som utvecklas i avsnitt 5.4.2 innehåller Arachne interna och externa data. De externa uppgifterna är redan huvudsakligen offentliggjorda (notera att uppgifter i databasen World Compliance endast är tillgängliga via riskvärderingar i Arachne, se avsnitt 5.4.2). De interna uppgifterna härrör bland annat från medlemsstaterna, inklusive Sverige (i vart fall från och med 2028). I avsnitt 8.2 framgår att de uppgifter som svenska myndigheter kommer att vara skyldiga att göra tillgängliga för bruk i Arachne från och med 2028 i regel inte kommer att omfattas av sekretess men att det inte kan uteslutas att sådana uppgifter undantagsvis kan förekomma. Motsvarande bedömning gör utredningen avseende de uppgifter som svenska myndigheter kan komma att lämna på frivillig basis (avsnitt 8.3).

[3] Komm2025/00388-6.

Särskilt om uppgifter som härrör från medlemsstater

Kraven avseende de uppgifter som medlemsstaterna ska tillgängliggöra enligt artikel 36.6 är utformade på ett tämligen övergripande sätt. I allmänhet behöver inte skyddsvärd information tillgängliggöras för att fullgöra skyldigheterna enligt bestämmelsen (se avsnitt 8.2.3) eller lämnas för att Arachne ska fungera på ett ändamålsenligt sätt (se avsnitt 8.3.3). På samma sätt som när det gäller svenska myndigheter utgår utredningen från att utländska myndigheter i allmänhet inte kommer att lämna uppgifter på ett sådant sätt att information som är särskilt skyddsvärd i den medlemsstaten röjs. Det kan dock inte uteslutas att sådan information kan finnas i Arachne som härrör från svenska eller utländska myndigheter.

Särskilt om uppgifter i databasen World Compliance

Vad särskilt gäller uppgifter om PEP (politiskt utsatta personer), som finns i databasen World Compliance, bör det ofta handla om oproblematiska uppgifter, såsom att en viss person innehar eller har innehaft ett visst uppdrag. Sådana uppgifter bör ofta redan vara allmänt kända. Likaså uppgiften att en person är närstående till en person som har innehaft ett visst uppdrag bör i sig vara oproblematisk.

Det skulle kunna förekomma att politiskt utsatta personer har skyddade personuppgifter eller liknande. Det bör kunna förväntas att sådana skyddsvärda uppgifter inte förekommer i databasen. Det är dock inte möjligt för utredningen att överblicka exakt vilka uppgifter, exempelvis om adresser, som PEP-listor i dag och i framtiden innehåller.

Vad gäller sanktionslistor kommer dessa bland annat från EU och FN. Generellt bör det vara fråga om redan offentliga uppgifter om fattade beslut om sanktioner. Detta får också stöd i vad som sägs i Arachne-stadgan om att externa data redan är offentliggjorda.

Databasen World Compliance innehåller också uppgifter om negativ publicitet, vilket kan ta sikte på rena misstankar om överträdelser.

Utredningens överväganden och slutsatser

Arachne kommer att innehålla en stor mängd uppgifter från olika källor. Det är rimligt att anta att den stora majoriteten av uppgifterna inte kommer att vara av sådan karaktär att det finns behov av skydd i form av sekretess i Sverige. Det kan dock inte uteslutas att sådana behov, avseende vissa uppgifter, skulle kunna förekomma. Enligt utredningen kan det främst finnas ett behov av sekretess i följande avseenden, vilka kort utvecklas nedan.

- Behov att kunna hemlighålla uppgifter
  - för att samarbetet inom EU inte ska försämras, och
  - för att myndigheternas arbete med kontroller och granskning inte ska motverkas
- Behov att kunna hemlighålla uppgift om en enskilds affärs- eller driftförhållanden med mera i tillsynsverksamhet och liknande
- Behov att kunna hemlighålla uppgifter om personliga förhållanden, särskilt för förföljda personer.

Det kan finnas behov av sekretess för uppgifter i Arachne till skydd för *allmänna intressen*. Enligt utredningen är uppgifter om gjorda riskvärderingar särskilt centrala när det gäller behovet av sekretessreglering. Behovet av sekretess kan dock även handla om andra uppgifter, exempelvis uppgifter som tar sikte på projekt som har betydelse för Sveriges tillgång till livsmedel under kris- och krigstider och annat som rör Sveriges försvarsförmåga.

Arachne-teamet vid kommissionen har gett uttryck för ett önskemål om att uppgifter i Arachne inte ska spridas fritt.[4] När det gäller gjorda riskvärderingar har detta önskemål även kommit till skriftligt uttryck i Arachne-stadgan. Detta kan tala för att ett hemlighållande kan behövas för att *Sveriges möjlighet att delta i samarbetet inom EU* inte ska försämras. Hur starkt det behovet ska anses vara kan delvis beskrivas som en utrikespolitisk fråga som berör en intresseavvägning mellan den svenska offentlighetsprincipen och relationen med EU.

Om EU och andra medlemsstater känner tveksamhet inför Sveriges möjligheter att förhindra spridning av skyddsvärda uppgifter som svenska myndigheter får tillgång till genom Arachne kan

[4] Komm2025/00388-10.

det vidare finnas en risk att det samarbete som är en förutsättning för ett effektivt motverkande av felaktigheter med EU-medel fungerar mindre effektivt. Detta skulle också kunna få negativa effekter för Sveriges möjligheter att bedriva tillsyn. Det kan därmed också finnas behov att sekretessbelägga uppgifter i Arachne för att *myndigheternas arbete med kontroller och granskning* inte ska motverkas.

Det kan också finnas behov av sekretess till skydd för *uppgift om enskildas ekonomiska förhållanden*. Uppgifter om enskildas *affärs- eller driftförhållanden* kan ingå bland de uppgifter som svenska myndigheter får tillgång till genom Arachne, vilka kan behöva skyddas. Det kan handla exempelvis om upphandlingsunderlag, avtal och affärshemligheter. Det kan inte heller uteslutas att det i vissa fall kan finnas behov av sekretess för uppgift om total projektkostnad vilken, i kombination med andra uppgifter, skulle kunna avslöja information om stödmottagares ekonomiska planer.

Det kan inte heller uteslutas att det kan finnas behov av sekretessskydd för *enskildas personliga förhållanden*. Arachne innehåller uppgifter om personliga förhållanden beträffande bland andra stödmottagare, personer i ledningen för ett företag, aktieägare, leverantörer, underleverantörer och anknutna personer. Det kan handla om exempelvis namn, adress och identifikationsnummer.

Risken för att svenska myndigheter får tillgång till skyddsvärd information genom Arachne bedöms dock som begränsad. Tillgången till uppgifterna är, eller kommer att vara, begränsad till de program som förvaltande myndighet hanterar. Som framgår av Arachne-stadgan är utgångspunkten att uppgifter som erhålls från externa databaser redan är offentliga och publicerade. De uppgifter som måste tillgängliggöras av medlemsstaterna avser uppgifter som i regel är harmlösa. Behov av sekretesskydd kan dock finnas även för sådana i regel harmlösa uppgifter för *förföljda personer*. Det kan vara så att – även om uppgifterna som finns i Arachne generellt var för sig får anses som relativt harmlösa – en användare genom Arachne kan få tillgång till mycket information, vilket kan vara mer problematiskt.

Det kan vidare inte uteslutas att det kan finnas behov av skydd för uppgifter även om andra personliga förhållanden, exempelvis om det finns en risk att personuppgifter *behandlas i strid mot personuppgiftsregelverket* efter ett eventuellt utlämnande. I detta sammanhang kan särskilt nämnas uppgifter från databasen World Compliance, som kan innehålla uppgifter om tidigare regelöverträdelser, liksom rena

misstankar om överträdelser. Innehållet i negativ publicitet behöver inte alltid vara korrekt. Det bör beaktas att tillgången till uppgifter från World Compliance är starkt begränsad, dels då det krävs särskild behörighet, dels då det endast är genom riskvärderingar avseende egna projekt som sådana uppgifter kan nås (se avsnitt 5.4.2).

När det gäller så kallade *anknutna personer* (related persons) kan det uppkomma särskilda frågor som rör behovet av och möjligheten att sekretessbelägga uppgifter om personer som arbetar vid myndigheter. Uppgifter om anknutna personer är dock frivilliga att lämna. Det framgår i dokumentation från kommissionen att om medlemsländerna överväger att föra in uppgifter om personer som arbetar vid nationella myndigheter, bör man följa nationella dataskyddsregler vilket kan innebära att det krävs samtycke (Arachne, Frequently asked questions, version 2.3, den 19 augusti 2022, fråga 53). För närmare om behandling av uppgifter om anknutna personer och samtycke, se avsnitt 8.3.5.

Det kan slutligen konstateras att det – bland annat eftersom systemet är under utveckling – kan vara svårt att förutse vilka uppgifter som kommer att finnas i Arachne och därmed vilka ytterligare behov av sekretesskydd som kan uppstå.

8.5.4 Vilket skydd ger gällande sekretessreglering för allmänna intressen?

Utredningens bedömning: När det gäller sekretess till skydd för allmänna intressen kommer gällande sekretessreglering att ge ett betydande skydd för de uppgifter som eventuellt skulle kunna behöva ett sådant skydd. Det kan dock inte uteslutas att uppgifter i Arachne, inklusive gjorda riskvärderingar, i vissa fall inte kan sekretessbeläggas med stöd av gällande sekretessreglering.

Skälen för utredningens bedömning

Inledning

De behov av sekretesskydd som utredningen har identifierat för allmänna intressen rör bland annat möjligheten att kunna hemlighålla de riskvärderingar som Arachne genererar. De intressen som därvid

aktualiseras är dels att Sveriges förhållande till EU och andra medlemsländer fungerar väl så att Sverige kan delta i samarbetet på ett effektivt sätt, dels att myndigheternas kontroll- och granskningsverksamhet ska kunna fungera effektivt. Därutöver skulle vissa andra allmänna intressen kunna aktualiseras vid ett användande av Arachne, vilket också berörs i detta avsnitt. I det följande analyseras vilket skydd gällande sekretessbestämmelser ger när det gäller sekretess till skydd för allmänna intressen.

Utrikessekretess – 15 kap. 1 § OSL

Utrikessekretessen regleras i 15 kap. 1 § OSL, som anger att det gäller sekretess för uppgift som rör Sveriges förbindelser med en annan stat eller i övrigt rör annan stat, mellanfolklig organisation, myndighet, medborgare eller juridisk person i annan stat eller statslös, om det kan antas att det stör Sveriges mellanfolkliga förbindelser eller på annat sätt skadar landet om uppgiften röjs.

När den tidigare gällande sekretesslagen (1980:100) trädde i kraft 1981 gällde utrikessekretess med olika skaderekvisit beroende på var en uppgift fanns. För uppgifter hos regeringen och inom utrikesrepresentationen föreskrevs sekretess med ett omvänt skaderekvisit. Hos andra myndigheter gällde däremot sekretess med ett rakt skaderekvisit för samma uppgifter. För dessa myndigheter gällde alltså sekretess för en uppgift om det kunde antas att det störde Sveriges mellanfolkliga förbindelser eller på annat sätt skadade landet om uppgiften röjdes. I förarbetena (prop. 1979/80:2 Del A s. 131) konstaterades att skade- och störningsbegreppen i bestämmelsen om utrikessekretess inte bör ges en alltför vid innebörd. Det måste röra sig om någon olägenhet för landet för att en uppgift ska sekretessbeläggas. Att mindre och tillfälliga störningar eller irritationer inom ett lands ledning inte kan uteslutas ska med andra ord inte alltid leda till sekretess.

I och med att Sverige blev medlem i EU ändrades bestämmelsen i 2 kap. 1 § sekretesslagen och fick den lydelse den nu har i offentlighets- och sekretesslagen, med ett enhetligt rakt skaderekvisit. Det råder således numera en presumtion för offentlighet hos alla svenska myndigheter. I fråga om tillämpningen av ett enhetligt rakt skaderekvisit för utrikessekretessen anförde regeringen att det inte i sig bör medföra några risker för att Sverige inte ska ha möjlighet att till-

godose sådana berättigade krav på sekretess som gemenskapsrätten ställer. Vid bedömningen av om en uppgift som erhållits från en annan stat eller från en mellanfolklig organisation kan lämnas ut eller inte ansågs avsändarens uppfattning i frågan i och för sig inte kunna avgöra om uppgiften ska hållas hemlig, men avsändarens intresse av sekretess kan ha betydelse för skadeprövningen i det enskilda fallet. Om den främmande staten eller den mellanfolkliga organisationen anser att en överlämnad uppgift är hemlig, kan det givetvis vara ett skäl för att anse att ett utlämnande skulle störa Sveriges mellanfolkliga förbindelser (prop. 1994/95:112 s. 29).

Riksdagen beslutade i enlighet med regeringens förslag efter att konstitutionsutskottet uttalat att möjligheterna till insyn i den nationella beredningsprocessen inom EU-samarbetet bör vara desamma som om det slutliga beslutet skulle fattas på nationell nivå. Enligt utskottet framstod det därmed som helt nödvändigt att låta en presumtion för offentlighet gälla för alla uppgifter inom utrikessekretessens tillämpningsområde (bet. 1994/95:KU18, rskr. 1994/95:128).

Det gäller inte någon begränsning av bestämmelsens räckvidd. Bestämmelsen är tillämplig i all offentlig verksamhet, oberoende av vilken myndighet eller vilket annat offentligt organ som förfogar över de aktuella uppgifterna.

Bestämmelsen om utrikessekretess har enligt sin ordalydelse inte heller någon begränsning i fråga om uppgiftens innehåll. Högsta förvaltningsdomstolen (tidigare Regeringsrätten) har dock i ett par avgöranden (RÅ 1998 ref. 42 och RÅ 2000 ref. 22) anfört att det måste vara det konkreta informationsinnehållet i en uppgift – eller i vissa fall uppgiftens art och anknytning till internationell verksamhet – som medför att ett röjande av uppgiften kan skada landet eller förorsaka störningar i de mellanfolkliga förbindelserna för att bestämmelsen ska vara tillämplig.

Utredningen gör bedömningen att det är oklart i vilken utsträckning som uppgifter i Arachne kommer att omfattas av 15 kap. 1 §, det vill säga i vilken utsträckning det kommer att handla om uppgifter som till sitt innehåll och sin art rör Sveriges förbindelser med en annan stat eller i övrigt rör annan stat, mellanfolklig organisation, myndighet, medborgare eller juridisk person i annan stat eller statslös. Det får anses tveksamt om exempelvis en gjord riskvärdering kan anses vara av sådant innehåll. En sådan bedömning kan dock

inte heller uteslutas, eftersom riskvärderingen är ett led i ett samarbete mellan kommissionen och de olika medlemsländerna.

För att en riskvärdering som Arachne genererar ska kunna sekretessbeläggas enligt bestämmelsen krävs vidare att ett röjande kan antas störa Sveriges mellanfolkliga förbindelser eller på annat sätt skada landet. Det är här av betydelse hur negativt EU och andra medlemsländer skulle uppleva att uppgifterna röjdes och hur detta skulle påverka de mellanfolkliga förbindelserna. Som nämns har det i förarbetena till bestämmelsen angetts att avsändarens uppfattning i frågan i och för sig inte ska kunna avgöra om uppgiften ska hållas hemlig, men avsändarens intresse av sekretess kan ha betydelse för skadeprövningen i det enskilda fallet. Om avsändaren anser att en överlämnad uppgift är hemlig, kan det vara ett skäl för att anse att ett utlämnande skulle störa Sveriges mellanfolkliga förbindelser.

Utredningen konstaterar att det inte finns någon uttrycklig sekretessbestämmelse i budgetförordningen som rör Arachne. Arachneteamet vid kommissionen har gett uttryck för ett önskemål att uppgifter i Arachne inte ska spridas.[5] När det gäller gjorda riskvärderingar har detta tagit sig skriftligt uttryck i Arachne-stadgan. Det får dock anses oklart hur långt detta önskemål sträcker sig. Det finns också skäl att påminna om vad som sades i de ursprungliga förarbetena från 1979 om att skade- och störningsbegreppen inte bör ges en alltför vid innebörd och att mindre och tillfälliga störningar eller irritationer inom ett lands ledning inte alltid ska leda till sekretess. Det bör också här beaktas det intresse för ökad öppenhet även inom EU som exempelvis öppenhetsförordningen ger uttryck för.

Sammanfattningsvis bedömer utredningen att det får anses vara tveksamt om uppgifter i Arachne, inklusive gjorda riskvärderingar, kan sekretessbeläggas med stöd av 15 kap. 1 § OSL, även om en sådan tillämpning inte kan anses utesluten i vissa fall.

Sekretess i det internationella samarbetet – 15 kap. 1 a § OSL

Enligt 15 kap. 1 a § OSL gäller sekretess 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

[5] Komm2025/00388-10.

kan antas att Sveriges möjlighet att delta i det internationella samarbete som avses i rättsakten eller avtalet försämras om uppgiften röjs.

Som nämns ovan innehåller inte budgetförordningen någon bestämmelse om sekretess för uppgifter i Arachne. Arachne-stadgan innehåller villkor för användningen. Arachne-stadgan kan dock inte anses vara en bindande EU-rättsakt eller ett av EU ingånget eller av riksdagen godkänt avtal med en annan stat eller med en mellanfolklig organisation.

Ett användande av Arachne är enligt gällande reglering inte heller nödvändigt och någon skyldighet att använda systemet följer inte heller i nuläget av någon sådan rättsakt eller sådant avtal som avses i 15 kap. 1 a § OSL.

Det kan dock noteras att det enligt ordalydelsen av 15 kap. 1 a § OSL inte krävs att någon sekretessreglering finns i en sådan rättsakt eller ett sådant avtal. Det räcker att en myndighet har fått uppgiften från ett utländskt organ på grund av en bindande EU-rättsakt. Med uttrycket ”bindande EU-rättsakt” avses förordningar, direktiv och beslut (prop. 2012/13:192 s. 31). Det skulle möjligen kunna argumenteras för att – för det fall en svensk myndighet väljer att använda Arachne – myndigheten anses ha fått uppgiften från ett utländskt organ, nämligen kommissionen som tillhandahåller systemet, och att det sker på grund av en bindande EU-rättsakt, nämligen budgetförordningen. Möjligheten att använda Arachne är reglerad i artikel 36.2 d i budgetförordningen och därmed kan det möjligen sägas att tillgängliggörandet av uppgifterna i systemet sker på grund av budgetförordningen. Som nämns krävs det inte heller enligt ordalydelsen någon uttrycklig sekretessbestämmelse i rättsakten eller avtalet. För att sekretess ska gälla räcker det med att det kan antas att Sveriges möjlighet att delta i det internationella samarbete som avses i rättsakten eller avtalet försämras om uppgiften röjs. Det kan sägas att det i budgetförordningen förutsätts ett internationellt samarbete mellan medlemsländerna och kommissionen när det gäller att tillgängliggöra och använda sig av uppgifter. När det gäller bedömningen av om Sveriges möjlighet att delta i samarbetet skulle försämras bör man enligt utredningens mening kunna beakta innehållet i Arachne-stadgan. Även om den inte i sig är bindande får det antas att kommissionen, liksom medlemsländer som använder systemet, förväntar sig att det som står där tillämpas lojalt av de länder och myndigheter som väljer att använda systemet. I samarbetet mellan

länderna och i förhållande till EU:s institutioner är det viktigt att förtroendet mellan aktörerna värnas. Informationsutbyte mellan aktörerna är centralt i många avseenden och det kan riskera att försvåras om aktörerna inte har förtroende för att samtliga inblandade avser att behandla uppgifter som härrör från andra medlemsländer eller från kommissionen med tillbörlig aktsamhet. Av Arachne-stadgan framgår också att kommissionen har rätt att dra tillbaka tillgången för programmyndigheter till Arachne om användarvillkoren inte följs (punkt 13).

Enligt utredningen kan det därmed argumenteras för att i vart fall gjorda riskvärderingar i Arachne ska vara belagda med sekretess och att detta följer av 15 kap. 1 a § OSL. Det bör enligt utredningens mening vara möjligt att sekretessbelägga även andra uppgifter som en svensk myndighet får tillgång till genom ett användande av Arachne, under förutsättning att det kan antas att Sveriges möjlighet att delta i det internationella samarbete som avses i rättsakten eller avtalet försämras om uppgiften röjs.

Det är dock också möjligt att göra en annan bedömning i denna fråga. Det kan argumenteras för att en myndighets tillgång till uppgifterna vid ett frivilligt användande av Arachne inte kan sägas ske ”på grund av” en bindande EU-rättsakt. Möjligen är kopplingen mellan den tillgången och budgetförordningen för svag. I förarbetena till bestämmelsen framgår att det förutsätts att uppgiftsinnehavet är ”en direkt följd” av en bindande EU-rättsakt eller avtal (prop. 2012/13:192 s. 30). Vidare anges i förarbetena att – även om det inte utesluts av dess ordalydelse – bestämmelsen normalt inte aktualiseras i situationer då avtalet eller EU-rättsakten inte innehåller någon tydlig sekretessbestämmelse. I sådana fall bör det främst vara uppgiftens art och anknytning till det internationella samarbetet som medför att skaderekvisitet anses uppfyllt. Enligt förarbetena ligger det då närmare till hands att tillämpa bestämmelsen om utrikessekretess i 15 kap. 1 § OSL (prop. 2012/13:192 s. 35). Som anförs ovan finns det tveksamheter när det gäller i vilken utsträckning som den bestämmelsen kan användas för att sekretessbelägga uppgifter i Arachne.

Det är alltså inte säkert att några uppgifter – inte ens gjorda riskvärderingar – kan sekretessbeläggas enligt 15 kap. 1 a § OSL. Under alla förhållanden måste det göras en bedömning i det enskilda fallet om det kan antas att Sveriges möjlighet att delta i det internationella samarbete som avses i rättsakten försämras om uppgiften röjs.

Det kan här nämnas att bedömningen skulle bli annorlunda om ett användande av Arachne skulle bli obligatoriskt i framtiden. Det ligger då närmare till hands att bedöma 15 kap. 1 a § OSL som tillämplig. Det bör nämligen då kunna argumenteras för att den svenska myndigheten har fått uppgifterna från ett utländskt organ på grund av en bindande EU-rättsakt. För att sekretess ska gälla krävs då en bedömning i det enskilda fallet om det kan antas att Sveriges möjlighet att delta i det internationella samarbete som avses i rättsakten försämras om uppgiften röjs.

Utrikessekretess vid direktåtkomst – 15 kap. 1 b § OSL

Det gäller absolut sekretess för uppgift som en myndighet har elektronisk tillgång till i en upptagning för automatiserad behandling hos en annan stat eller mellanfolklig organisation, om myndigheten inte får behandla uppgiften enligt en bindande EU-rättsakt eller ett av Sverige eller EU ingånget avtal med en annan stat eller mellanfolklig organisation. Det följer av 15 kap. 1 b § OSL.

Bestämmelsen är föranledd av att uppgifter i utländska databaser som en svensk myndighet har direktåtkomst till som utgångspunkt utgör allmänna handlingar hos myndigheten, om uppgifterna ingår i en så kallad färdig elektronisk handling eller om de kan sammanställas med rutinbetonade åtgärder och utan användning av förbjudna sökbegrepp. I förarbetena anges att syftet med bestämmelsen är att en myndighet inte i strid med ändamålsbegränsningar eller villkorade sökbegränsningar ska behöva söka fram uppgifter som inte omfattas av överenskommelsen om informationsutbyte endast för att kunna avgöra sekretessfrågan om uppgifterna begärs ut. För sådana uppgifter som myndigheten får behandla enligt överenskommelsen om informationsutbyte är bestämmelsen inte tillämplig och innebär således inte någon begränsning av rätten att ta del av allmänna handlingar (prop. 2011/12:157 s. 17).

Som utvecklas i avsnitt 8.5.2 talar mycket för att svenska myndigheter får anses ha direktåtkomst i vart fall till vissa uppgifter i Arachne, även om den bedömningen är förenad med viss osäkerhet.

För att 15 kap. 1 b § OSL ska vara tillämplig på uppgifter i Arachne krävs att det bedöms finnas ändamålsbegränsningar, sökbegräns-

ningar eller liknande i en bindande EU-rättsakt eller ett av Sverige eller EU ingånget avtal.

I Arachne-stadgan sägs att resultaten av riskvärderingar inte ska offentliggöras (should not be published) och att de inte ska användas för personliga intressen eller några andra syften (not be used for personal interests or any other purposes, se vidare Arachne-stadgan punkterna 3 och 6.2 samt avsnitt 8.5.3). Det kan diskuteras om detta kan anses innebära en sådan begränsning. Dessutom kan det ifrågasättas om stadgan utgör en sådan rättsakt eller ett sådant avtal.

Budgetförordningen är en bindande rättsakt. Det följer vissa begränsningar av artikel 36.7 där det framgår att åtkomsten till uppgifter i Arachne ska överensstämma med tillämpliga dataskyddsregler och begränsas till unionsinstitutioner och organ som genomför budgeten. Det ligger enligt utredningen nära till hands att betrakta dessa som åtkomstbegränsningar enligt 15 kap. 1 b § OSL. Utredningen uppfattar det så att avsikten är att förvaltande myndigheter endast ska ha tillgång till uppgifter som de faktiskt har användning för i sin verksamhet. Detta tar sig bland annat uttryck i att myndigheterna endast ska ha tillgång till uppgifter avseende de projekt som myndigheten hanterar. I kommande versioner av Arachne är också – som utredningen har uppfattat det – avsikten att myndigheterna endast ska få tillgång till uppgifter i databasen Orbis som rör personer och företag som är relevanta för dessa projekt. Avsikten synes vara att den närmare fördelningen av behörighet ska skötas av en nationell administratör. Även om detta inte i detalj uttryckligen framgår av budgetförordningen kan det enligt utredningen ändå sägas ha sin grund där. Det kan sägas följa av budgetförordningen att det ska finnas vissa användarbegränsningar, även om den närmare fördelningen och utformningen av dessa bestäms på annat sätt. Det framgår bland annat av artikel 36.7 andra stycket, enligt vilket åtkomsten till uppgifter i Arachne ska överensstämma med tillämpliga dataskyddsregler, respektera principerna om nödvändighet och proportionalitet och begränsas till aktörer som på olika sätt har roller när det gäller att genomföra budgeten.

Denna bedömning får dock anses vara förenad med viss osäkerhet, eftersom de exakta användarbegränsningarna inte uttryckligen fastställs i någon bindande EU-rättsakt eller något ingånget avtal.

Det är något oklart för utredningen om den tekniska utformningen av Arachne kommer att innebära att svenska myndigheter

kommer att kunna få tillgång till fler uppgifter än de har rätt att behandla. Om svenska myndigheter genom Arachne får faktisk tillgång till fler uppgifter än vad de på grund av användarbegränsningar får behandla skulle 15 kap. 1 b § OSL möjligen kunna tillämpas på de uppgifter som omfattas av nämnda åtkomstbegränsningar.

Försvarssekretess – 15 kap. 2 § OSL

Bland de uppgifter som medlemsländerna från och med 2028 ska tillgängliggöra enligt 36.6 i budgetförordningen finns en beskrivning av åtgärdens art och ändamål (se artikel 38.2 e läst tillsammans med artikel 36.6 första stycket b). Som utvecklas i avsnitt 8.2.3 kan det inte uteslutas att det i förhållandena bakom ett stödprojekt kan finnas information som omfattas av försvarssekretess enligt 15 kap. 2 § OSL. Enligt den bestämmelsen gäller sekretess för uppgift som rör verksamhet för att försvara landet eller planläggning eller annan förberedelse av sådan verksamhet eller som i övrigt rör totalförsvaret, om det kan antas att det skadar landets försvar eller på annat sätt vållar fara för rikets säkerhet om uppgiften röjs.

Utredningen bedömer att i allmänhet bör åtgärdens art och ändamål kunna beskrivas på ett sådant sätt att skyddsvärd information inte röjs. Det framstår mot den bakgrunden inte som sannolikt att det i Arachne kommer att finnas uppgifter som omfattas av bestämmelsen. Skulle sådana uppgifter ändå finnas i Arachne kan de sekretessbeläggas enligt 15 kap. 2 § OSL, om skaderekvisitet anses vara uppfyllt i det enskilda fallet.

Förberedelser för inspektion, revision eller annan granskning – 17 kap. 1 § OSL

Uppgifter som svenska myndigheter får tillgång till genom Arachne, bland annat gjorda riskvärderingar, kan vara av intresse för och vara en del av myndighetens planläggning eller andra förberedelser för inspektioner, revisioner eller annan granskning. Om så är fallet och om syftet med granskningsverksamheten motverkas om uppgiften röjs kan uppgiften beläggas med sekretess enligt 17 kap. 1 § OSL.

Utredningen gör bedömningen att 17 kap. 1 § OSL kan få betydelse för vissa uppgifter som myndigheter tar del av genom Arachne

som ett led i förberedelser för granskningar. En betydande del av det arbete som myndigheterna ska göra inom ramen för sådan kontroll och revision som är en del av genomförandet av EU:s budget bör kunna rymmas inom begreppet granskning enligt bestämmelsen. Vidare bör flera av de typer av uppgifter som därvid kan komma i fråga kunna omfattas av bestämmelsen.

Det framstår dock som tveksamt om bestämmelsen kan användas för att sekretessbelägga samtliga gjorda riskvärderingar som en myndighet har tillgång till genom Arachne. Som utvecklas i avsnitt 5.4.2 sparas samtliga historiska riskvärderingar för projekt i Arachne. Det kan ifrågasättas om sådana historiska uppgifter kan anses avse planläggning eller andra förberedelser för granskningar. (Jfr Kammarrätten i Stockholms dom den 24 maj 2000 i mål nr 2303-2000, där kammarrätten fann att paragrafen – dåvarande 4 kap. 1 § sekretesslagen – inte kunde tillämpas generellt på allt material i ett granskningsärende utan endast på uppgifter som angick förberedelser inför en förestående granskning.) Utredningens bedömning är ändå att paragrafen bör kunna användas i vissa fall för att sekretessbelägga uppgifter i Arachne, inklusive gjorda riskvärderingar, i vart fall när uppgifterna mer konkret tar sikte på planläggning eller förberedelser för granskning. Det bör noteras att detta gäller gjorda riskvärderingar och inte riskvärderingar som inte har gjorts men skulle kunna göras.

Dataanalyser och urval för att förebygga, förhindra och upptäcka felaktiga utbetalningar – 17 kap. 1 b § OSL

En fråga är om 17 kap. 1 b § OSL skulle kunna användas för att sekretessbelägga uppgifter som en myndighet får tillgång till genom Arachne, till exempel gjorda riskvärderingar. Enligt bestämmelsen gäller sekretess för uppgift om metoder, modeller och riskfaktorer som hänför sig till dataanalyser och urval för att förebygga, förhindra och upptäcka felaktiga utbetalningar, om det kan antas att det allmännas syfte med verksamheten motverkas om uppgiften röjs. Paragrafen tillkom i samband med framtagandet av rättslig reglering för den nya Utbetalningsmyndighetens verksamhet. Bestämmelsen omfattar exempelvis uppgifter om vilka riskfaktorer som en myndighet har tagit fram för att identifiera misstänkt felaktiga utbetalningar, men även uppgifter om hur dataanalyser eller urvalsmodeller har utformats eller utvecklats kan sekretessbeläggas med stöd av bestäm-

melsen (prop. 2022/23:34 s. 215). Sekretessen gäller för dessa uppgifter oavsett i vilken verksamhet som de förekommer.

Utredningen bedömer att det här *kan vara fråga om felaktiga utbetalningar* i den mening som avses i bestämmelsen. Det kan också här påminnas om den sekretessbrytande bestämmelse, 10 kap. 15 a § OSL, som ska träda i kraft den 1 december 2025 (se avsnitt 7.1.2). Den avser också felaktiga utbetalningar. I propositionen anges att bestämmelsen avser att motverka alla typer av felaktiga utbetalningar, och den tar alltså inte enbart sikte på felaktiga utbetalningar från välfärdssystemen utan också på utbetalningar som till exempel avser stöd till företag, civilsamhällesorganisationer och andra juridiska personer (prop. 2024/25:180 s. 28).

Det bör enligt utredningens mening kunna finnas utrymme för svenska myndigheter att tillämpa 17 kap. 1 b § OSL vid en användning av Arachne i vissa fall. Det bör till exempel finnas utrymme att sekretessbelägga uppgifter i Arachne, såsom gjorda riskvärderingar – trots att riskfaktorerna inte tagits fram av en svensk myndighet – med stöd av bestämmelsen. I vilken utsträckning detta kan ske får dock betraktas som något osäkert.

Enligt utredningen bör flera av de uppgifter som ingår i Arachne kunna anses avse metoder, modeller och riskfaktorer som hänför sig till dataanalyser och urval för att upptäcka felaktiga utbetalningar. Det får dock bedömas som oklart i vilken utsträckning bestämmelsen kan tillämpas på exempelvis gjorda riskvärderingar och andra mer konkreta uppgifter som hänför sig till kontroller eller granskningar. Det bör dock enligt utredningen inte uteslutas att bestämmelsen kan tillämpas också på gjorda riskvärderingar, i vart fall i vissa situationer.

Det framgår inte direkt av 17 kap. 1 b § OSL *hur länge sekretessen gäller*. Det anses dock följa av skaderekvisitet – att sekretess gäller endast om det kan antas att det allmännas syfte med verksamheten motverkas om uppgiften röjs – att sekretessen gäller endast så länge som uppgiften används i verksamheten. När uppgifterna inte längre används upphör sekretessen (se prop. 2022/23:34 s. 216). När det gäller uppgifter i Arachne, bland annat gjorda riskvärderingar, är det inte helt enkelt att ange tiden under vilken de används. Arachne är ett datautvinnings- och riskvärderingsverktyg som kopplar ihop data från medlemsstaterna om projekt och kontrakt med uppgifter i kommersiella databaser. Det görs automatiskt löpande riskvärderingar av

pågående projekt, vilka sparas i Arachne och kan tas fram för senare efterhandskontroller (se avsnitt 5.4.2). Det framgår av artikel 36.7 i budgetförordningen att uppgifterna i Arachne endast ska lagras under den period som är nödvändig och proportionell för att uppfylla det syfte som fastställs i punkt 2 d, det vill säga att motverka oriktigheter. Den längsta möjliga lagringsperioden får inte överstiga tio år från och med den sista ansökan om utbetalning som lämnats in till kommissionen för den perioden. Enligt utredningens mening ligger det nära till hands att anse att uppgifterna kan sägas användas i den meningen att sekretess enligt 17 kap. 1 b § kan föreligga, om övriga kriterier är uppfyllda, under hela den tid som uppgifterna lagras i Arachne.

Vidare bör det kunna argumenteras för att *syftet med granskningsverksamheten i stort skulle motverkas* om vissa sådana riskvärderingar skulle röjas, eftersom det skulle kunna ge aktörer inblick i hur sådana riskvärderingar och urval görs. Det får också antas att svenska myndigheter som använder Arachne inte kommer att få tillgång till allt innehåll i Arachne, utan endast sådant som har betydelse för att motverka felaktigheter rörande de projekt som de hanterar. Som utredningen uppfattat det kommer från och med 2028 inte heller databasen Orbis att vara sökbar beträffande personer och företag som saknar koppling till sådana projekt. Vad gäller databasen World Compliance är det redan i dag så att det inte är möjligt att söka på individer och att information om förekomst på de listor som ingår i databasen endast erhålls rörande individer och företag som förekommer i sådana projekt, via riskvärderingar. Detta talar med styrka för att de uppgifter som svenska myndigheter kommer att ha tillgång till genom Arachne huvudsakligen är sådana som kan sägas användas i arbetet med att förebygga, förhindra och upptäcka felaktiga utbetalningar.

Det skyddsintresse som skaderekvisitet avser tar sikte på *det allmännas syfte* med verksamheten. Frågan kan ställas om detta täcker de syften som ligger bakom budgetförordningen. Enligt utredningen bör den frågan besvaras jakande. När svenska myndigheter hanterar EU-stöd sker det i allmänhet inom ramen för delad förvaltning (och ibland genom direkt förvaltning tillsammans med medlemsstaterna). Sverige har då ett ansvar som medlemsland att säkerställa att felaktiga utbetalningar motverkas. Att använda Arachne som ett verktyg i den verksamheten bidrar till att svenska myndigheter kan uppfylla det ansvaret. Om ett röjande av uppgifter försvårar ett effektivt an-

vändande av Arachne bör det anses motverka svenska myndigheters och därmed det allmännas syfte med verksamheten.

Det är som framkommit dock inte säkert att bestämmelsen kan användas i samtliga situationer för att sekretessbelägga gjorda riskvärderingar. Som nämns är det oklart om sådana uppgifter över huvud taget kan anses utgöra metoder, modeller och riskfaktorer på det sätt som krävs enligt bestämmelsen. Även om så skulle vara fallet är det inte säkert att en prövning av bestämmelsens skaderekvisit skulle leda till att uppgifterna kan sekretessbeläggas i samtliga fall. Bestämmelsen är utformad med ett rakt skaderekvisit vilket innebär att det föreligger en presumtion för offentlighet. Vidare framgår i förarbetena att behovet av att sekretessbelägga en riskfaktor kan minska om det blir känt att en viss faktor uppfattas som en riskfaktor. Där anges att kända riskfaktorer, som därför antagligen inte behöver sekretessbeläggas, skulle exempelvis kunna vara att företrädaren för ett assistansbolag har stora skulder, saknar branschkunskap eller tidigare har varit involverad i bolag som har försatts i konkurs. Exakt vilka riskfaktorer som kan komma att sekretessbeläggas måste vara upp till respektive myndighet att bedöma. Det bör också kunna ändras över tid, eftersom nya riskfaktorer tillkommer (prop. 2022/23:34 s. 81 och 82).

Sammanfattningsvis bedömer utredningen att 17 kap. 1 b § OSL i viss utsträckning bör kunna användas för att sekretessbelägga uppgifter i Arachne, bland annat gjorda riskvärderingar. Det får dock betraktas som oklart i vilken utsträckning detta kommer att vara möjligt.

Sammanfattande slutsatser

Utredningen bedömer att de uppgifter beträffande vilka det kan finnas behov av sekretesskydd för det allmännas intresse i betydande grad kommer att kunna beläggas med sekretess enligt gällande sekretessbestämmelser. Det kan dock inte uteslutas att uppgifter i Arachne, inklusive gjorda riskvärderingar, i vissa fall inte kan sekretessbeläggas med stöd av gällande sekretessreglering i 15 kap. OSL – till skydd för rikets säkerhet eller dess förhållande till andra stater eller mellanfolkliga organisationer – samt i 17 kap. – till skydd främst för myndigheters verksamhet för inspektion, kontroll eller annan tillsyn.

8.5.5 Vilket skydd ger gällande sekretessreglering för enskildas personliga och ekonomiska förhållanden?

Utredningens bedömning: De behov som utredningen har identifierat när det gäller sekretess till skydd för enskildas personliga och ekonomiska intressen kan tillgodoses genom gällande sekretessbestämmelser.

Uppgifter om enskildas affärs- eller driftförhållanden vid tillsyn, stödverksamhet och liknande har ett tillräckligt skydd genom 30 kap. 23 § OSL.

Skyddet för förföljda personer har ett tillräckligt skydd genom 21 kap. 3 § OSL. Därtill ger 21 kap. 7 § OSL ett skydd i de fall det kan antas att en uppgift efter ett utlämnande kommer att behandlas i strid med dataskyddsregelverket.

Skälen för utredningens bedömning

Inledning

Genom Arachne kommer svenska myndigheter att få tillgång till en stor mängd uppgifter om enskildas personliga och ekonomiska förhållanden. Det kommer att finnas sådana uppgifter i underlag från medlemsländerna och från kommissionen samt från databaserna Orbis och World Compliance. Det kan handla om normalt sett harmlösa uppgifter som namn och kontaktuppgifter. Även om uppgifterna var för sig framstår som mindre integritetskänsliga kan de dock tillsammans ge en myndighet tillgång till en mer omfattande bild av den enskildes personliga och ekonomiska förhållanden. För personer som är förföljda kan givetvis även uppgifter om adress och liknande vara problematiska om de får spridning.

Genom databasen World Compliance kan myndigheter också få tillgång till information av känslig karaktär, såsom uppgifter om att en individ eller ett företag har begått vissa regelöverträdelser eller fått vissa sanktioner. Uppgifterna kan avse överträdelser som har fastställts av domstol men också exempelvis medieuppgifter om misstankar om oegentligheter, som senare visar sig vara grundlösa. Det kan också handla om uppgifter om affärs- eller driftförhållanden, såsom upphandlingsunderlag, avtal och affärshemligheter.

Som utvecklas i avsnitt 5.4.2 gör utredningen bedömningen att uppgifter i databaserna, såsom World Compliance, är en del av den information som kan anses ingå i en riskvärdering. Det är dock inte möjligt för en användare att söka direkt på enskilda personer eller företag i World Compliance.

Uppgift om enskilds affärs- eller driftförhållanden vid tillsyn, stödverksamhet och liknande – 30 kap. 23 § OSL

Det kan finnas behov av att hemlighålla uppgifter om affärs- eller driftförhållanden. Som nämns kan det inte uteslutas att uppgifter om affärs- eller driftförhållanden kan ingå bland de uppgifter som svenska myndigheter får tillgång till genom Arachne. Det kan handla exempelvis om upphandlingsunderlag, avtal, affärshemligheter och uppgifter om total projektkostnad.

I dessa fall kan 30 kap. 23 § OSL vara tillämplig. Med stöd av bestämmelsen kan sekretess gälla för uppgift om en enskilds affärs- eller driftförhållanden, uppfinningar eller forskningsresultat, om det kan antas att den enskilde lider skada om uppgiften röjs, och för uppgift om andra ekonomiska eller personliga förhållanden för den som har trätt i affärsförbindelse eller liknande förbindelse med den som är föremål för myndighetens verksamhet.

Som utvecklas i avsnitt 7.1.7 krävs det, för att sekretess ska gälla enligt 30 kap. 23 § OSL, att regeringen har meddelat föreskrifter om det, vilket skett inom aktuellt område. Relevanta bestämmelser finns i 9 § offentlighets- och sekretessförordningen (2009:641), OSF, som i sin tur hänvisar till förordningens bilaga där det närmare anges i vilka fall sådan sekretess gäller. EU-förordningarna på området gäller ofta endast för en viss programperiod. Om det utfärdas nya förordningar som reglerar stödformerna för den kommande programperioden får det antas att bilagan till offentlighets- och sekretessförordningen ändras så att dessa inkluderas.

De verksamheter som avses i 30 kap. 23 § OSL beskrivs som utredning, planering, prisreglering, tillståndsgivning, tillsyn eller stödverksamhet. 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. Med stödverksamhet avses bland annat sådan verksamhet som åsyftas i de olika stödförfattningarna på jordbruksområdet (Lenberg m.fl., Offentlig-

hets- och sekretesslagen, Norstedts Juridik, JUNO Version 31, Publicerad digitalt den 17 juni 2025, kommentaren till 30 kap. 23 § OSL). Dessa verksamheter bör enligt utredningens mening fånga in myndigheternas arbete med att motverka felaktigheter i de projekt som omfattas av denna utredning.

Verksamheten ska vidare avse näringslivet, vilket beskrivs som produktion, handel, transportverksamhet eller näringslivet i övrigt. Många av de stöd som behandlas i detta betänkande tar sikte på näringslivet. I vissa fall kan det dock vara mera tveksamt om en sådan koppling till näringslivet finns som gör att bestämmelsen är tillämplig. I de fallen bör det inte heller finnas något behov av sekretess, till exempel därför att mottagaren av stöd är en myndighet.

Mot denna bakgrund bedömer utredningen att det kommer att finnas ett betydande skydd för uppgifter om enskilds affärs- eller driftförhållanden vid kontroller som utförs beträffande de stödformer som är aktuella i detta betänkande.

Sekretess till skydd för förföljda personer

Som utvecklas i avsnitt 8.2.3 följer det inte av krav i artikel 36.6 i budgetförordningen att medlemsstaterna eller deras myndigheter behöver tillgängliggöra adress till fysiska personer. Det synes inte heller finnas någon möjlighet att frivilligt lämna adressuppgifter i användargränssnittet för Arachne beträffande vissa fonder (se avsnitt 8.3.2). Sådana uppgifter kan dock bli tillgängliga för svenska myndigheter i vart fall genom databaserna Orbis och World Compliance.

Enligt 21 kap. 3 § första stycket OSL gäller sekretess för uppgift om enskilds bostadsadress eller annan jämförbar uppgift som kan lämna upplysning om var den enskilde bor stadigvarande eller tillfälligt, den enskildes telefonnummer, e-postadress eller annan jämförbar uppgift som kan användas för att komma i kontakt med denne. Skaderekvisitet innebär att det krävs att det av särskild anledning kan antas att den enskilde eller någon närstående till denne kan komma att utsättas för hot eller våld eller lida annat allvarligt men om uppgiften röjs. Utredningen anser att 21 kap. 3 § första stycket OSL innebär ett tillräckligt skydd för förföljda personer för uppgifter om adress och liknande.

Behandling i strid med dataskyddsregleringen

Sekretess enligt 21 kap. 7 § skulle kunna aktualiseras om det kan antas att uppgifter i Arachne efter ett utlämnande kommer att behandlas i strid med dataskyddsregelverket. Bestämmelsen innebär att även om en uppgift inte omfattas av sekretess enligt någon annan bestämmelse i offentlighets- och sekretesslagen, omfattas den av sekretess om det kan antas att den efter ett utlämnande kommer att behandlas i strid med till exempel dataskyddsförordningen eller dataskyddslagen. Som framgår av avsnitt 7.1.7 tar bedömningen som ska göras inte sikte på om myndighetens eget utlämnande av uppgifter skulle strida mot dataskyddsregleringen, utan det är den efterföljande behandlingen som ska bedömas.

Om det kan antas att de krav som gäller för att personuppgifter i Arachne ska få behandlas inte följs efter att personuppgiften lämnats ut, till exempel avseende för vilka ändamål som uppgifterna får behandlas, omfattas uppgiften av sekretess och ska inte lämnas ut. Om det blir aktuellt med en begäran att lämna ut en gjord riskvärdering, skulle en sådan begäran eventuellt kunna nekas efter en sådan prövning. Denna bestämmelse skulle således enligt utredningen kunna aktualiseras i vissa fall.

Utredningens överväganden om behov av åtgärder på dataskyddsområdet för ett användande av Arachne behandlas i avsnitt 8.5.8.

Sammanfattande överväganden och slutsatser

De behov som utredningen har identifierat när det gäller sekretess till skydd för enskildas personliga och ekonomiska intressen bedöms kunna uppfyllas genom gällande sekretessbestämmelser. Uppgifter om enskildas affärs- eller driftförhållanden vid tillsyn, stödverksamhet och liknande bedöms ha ett tillräckligt skydd genom 30 kap. 23 § OSL. Skyddet för förföljda personer bedöms ha ett tillräckligt skydd genom 21 kap. 3 § OSL. Därtill ger 21 kap. 7 § OSL ett skydd i de fall det kan antas att en uppgift efter ett utlämnande kommer att behandlas i strid med dataskyddsregelverket.

8.5.6 Det kan finnas skäl för ny sekretessreglering

Utredningens bedömning: Gällande sekretessreglering ger ett betydande skydd när det gäller uppgifter som finns i Arachne. Om ett mer omfattande skydd är önskvärt, kan det finnas skäl för en ny sekretessreglering, både för att samarbetet inom EU inte ska försämras och för att svenska myndigheters arbete med kontroller och granskning inte ska motverkas.

Skälen för utredningens bedömning

Inledning

Som framkommer av föregående avsnitt bedömer utredningen behovet av sekretesskydd för uppgifter i Arachne som utgångspunkt vara begränsat, bland annat eftersom det huvudsakligen rör sig om offentliga uppgifter och det i vissa fall är tveksamt om uppgifterna ens utgör allmänna handlingar.

Trots detta kan det finnas behov av sekretesskydd för vissa uppgifter i Arachne, vilket också utvecklas ovan. De behov som utredningen har identifierat när det gäller sekretess till skydd för enskildas personliga och ekonomiska intressen bedöms kunna tillgodoses genom gällande sekretessbestämmelser. Även när det gäller sekretess till skydd för det allmännas intressen bedöms gällande sekretessreglering ge ett betydande skydd. Det kan dock inte uteslutas att uppgifter i Arachne, inklusive gjorda riskvärderingar, i vissa fall inte kan sekretessbeläggas med stöd av ovan nämnda bestämmelser i 15 kap. OSL – till skydd för rikets säkerhet eller dess förhållande till andra stater eller mellanfolkliga organisationer – samt i 17 kap. – till skydd främst för myndigheters verksamhet för inspektion, kontroll eller annan tillsyn.

En intresseavvägning mellan sekretessintresset och det motstående insynsintresset görs nedan. Dessförinnan behandlas möjligheten att även ytterligare sekretessbestämmelser kan komma att aktualiseras, att sekretessen ibland kan ge vika till förmån för partsinsyn samt att det finns en viss osäkerhet om vilka uppgifter som kan komma att finnas i Arachne och därmed vilka behov av sekretess som kan uppstå i framtiden.

Ytterligare sekretessbestämmelser kan komma att aktualiseras

Det är svårt att helt överblicka vilka uppgifter som svenska myndigheter kan få tillgång till genom Arachne. Det kan därför inte uteslutas att ytterligare sekretessbestämmelser än de som utredningen behandlar i det föregående kan komma att bli tillämpliga. För det fall uppgifter i Arachne används under pågående granskning skulle uppgifterna eventuellt kunna omfattas av sekretess enligt 17 kap. 2 § OSL. Vidare kan uppgifter som härrör från Arachne komma att lämnas från en förvaltande myndighet till en annan myndighet. Uppgifterna kan då komma att användas i ett annat syfte än de som kommer till uttryck i budgetförordningen. (Givetvis behöver myndigheterna i detta skede beakta dataskyddsregleringens krav, inte minst finalitetsprincipen, se vidare avsnitt 8.5.8.) Hos en mottagande myndighet kan ytterligare sekretessbestämmelser vara tillämpliga. Det får anses ligga utanför utredningens uppdrag att uttömmande redogöra för de olika situationer och sekretessbestämmelser som då kan vara aktuella. Följande exempel kan dock nämnas. För det fall uppgifter lämnas av en förvaltande myndighet för att användas i den brottsbekämpande verksamheten vid Polismyndigheten eller Ekobrottsmyndigheten skulle uppgifterna då, beroende på omständigheterna, kunna komma att omfattas av förundersökningssekretess enligt 18 kap. 1 § OSL.

Bestämmelser om partsinsyn kan innebära att sekretessen bryts

Vid bedömningen av om gällande sekretessbestämmelser är tillräckliga bör man också beakta att bestämmelserna om partsinsyn ibland innebär att uppgifter ska lämnas ut till vissa personer trots sekretess. I 10 § förvaltningslagen anges i fråga om partsinsyn att den som är part i ett ärende har rätt att ta del av allt material som har tillförts ärendet. Bestämmelsen i förvaltningslagen innehåller också en hänvisning till offentlighets- och sekretesslagen. Det är nämligen så, att även om uppgifter skyddas av sekretess – exempelvis det skydd som uppgifter i stödärenden åtnjuter enligt 30 kap. 23 § OSL som behandlas ovan – har en part i ärendet omfattande rätt till insyn i ärendet. 10 kap. 3 § OSL innehåller en sekretessbrytande bestämmelse som innebär att sekretess inte hindrar att en enskild eller en myndighet som är part i ett mål eller ärende hos domstol eller annan myndig-

het och som på grund av sin partsställning har rätt till insyn i handläggningen, tar del av en handling eller annat material i målet eller ärendet. För att partens möjlighet till insyn enligt paragrafen ska gälla ska det vara fråga om uppgifter *i* målet eller ärendet. Allmän bakgrundsinformation som en myndighet har tillgång till och som inte har särskild relevans i målet eller ärendet omfattas däremot inte. Detta innebär att bestämmelserna om partsinsyn inte ger rätt att ta del av samtliga uppgifter i Arachne utan endast sådant som har tillförts ett ärende där en person är part. Om en riskvärdering har tillförts ett ärende, till exempel i ett ärende om återkrav av ett utbetalat stöd, omfattas denna som utgångspunkt av rätten till partsinsyn (se nedan om att rätten inte är oinskränkt). Utredningen antar dock att det i regel inte finns skäl att tillföra gjorda riskvärderingar ärenden, då de inte utgör något bevis på att en oriktighet föreligger, utan endast ger indikationer på risker (se mer i avsnitt 3.4.3 och 5.2.2).

Den kategori av personer som av förvaltningslagen tillerkänns rätt till aktinsyn betecknas som part. Uttrycket part avser sökande, klagande och 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 bland annat den som är föremål för ett tillsynsärende och därmed intar ställning som så kallad förklarande part (Lenberg m.fl., Offentlighets- och sekretesslagen, Norstedts Juridik, JUNO Version 31, Publicerad digitalt den 17 juni 2025, kommentaren till 10 kap. 3 § OSL).

Partsinsynen i ärenden är inte oinskränkt. En sådan handling eller ett sådant material får nämligen inte lämnas ut till parten i den utsträckning det av hänsyn till ett allmänt eller enskilt intresse är av synnerlig vikt att en sekretessbelagd uppgift i materialet inte röjs. I sådana fall ska myndigheten på annat sätt lämna parten upplysning om vad materialet innehåller i den utsträckning det behövs för att parten ska kunna ta till vara sin rätt och det kan ske utan allvarlig skada för det intresse som sekretessen ska skydda (10 kap. 3 § OSL).

Den bedömning som utredningen gör ovan om det skydd som gällande sekretessregler ger ändras inte av det faktum att skyddet i vissa fall ger vika till förmån för partsinsynen. Denna intresseavvägning har lagstiftaren redan gjort och det saknas anledning i detta

lagstiftningsärende att göra någon annan bedömning. Dessutom är partsinsynen inte oinskränkt.

En viss osäkerhet om vilka skyddsbehov som kan uppstå kvarstår

Det är svårt att helt överblicka vilka uppgifter som svenska myndigheter kan få tillgång till genom Arachne. Sverige och svenska myndigheter har inte någon kontroll över vilka uppgifter som tillförs Arachne från andra medlemsländer eller de databaser som är kopplade till systemet. Vidare är Arachne under utveckling vilket kan komma att förändra vilken tillgång till uppgifter som svenska myndigheter får på ett ännu oförutsebart sätt. Det kan inte uteslutas att det i Arachne kan komma att finnas uppgifter som har ett skyddsintresse vilka utredningen inte har identifierat.

Intresseavvägning

Som framgår ovan kan det finnas sekretessbehov som inte täcks av befintliga sekretessbestämmelser. Det följer av förarbetena till sekretessregleringen att en avvägning mellan sekretessintresset och insynsintresset ska göras i sådana fall. Behovet av sekretess för en uppgift är oftast detsamma oavsett i vilket sammanhang uppgiften förekommer. Allmänintresset av insyn kan dock variera beroende på vilken verksamhet som det är fråga om. En avvägning mellan sekretessrespektive insynsintresset i fråga om en och samma uppgift kan därför utfalla olika hos olika myndigheter respektive i olika verksamheter hos en och samma myndighet (prop. 1979/80:2 Del A s. 75 och 76).

Rätten att ta del av allmänna handlingar är en medborgerlig rättighet som utgör en viktig del av vårt demokratiska statsskick. Syftet med denna rätt är, så som det kommer till uttryck i 2 kap. 1 § TF, att främja ett fritt meningsutbyte och en fri och allsidig upplysning. Genom tillgången till allmänna handlingar underlättas en fri åsiktsbildning, en fri och på fakta grundad debatt i skilda samhällsfrågor liksom den medborgerliga kontrollen av den offentliga maktutövningen.

De situationer som omfattas av detta betänkande rör på ett övergripande plan svenska myndigheters hantering av EU-stöd. Det finns ett betydande insynsintresse när det gäller att kunna ta del av hand-

lingar för att säkerställa att myndigheternas hantering är korrekt. Detta insynsintresse måste dock vägas mot behovet av att sekretessbelägga uppgifter, bland annat i det allmännas intresse för att säkerställa en effektiv granskning av ansökningar och utbetalade stöd.

Inledningsvis kan det konstateras att det finns en risk att det uppstår behov av sekretesskydd som inte har kunnat förutses, bland annat på grund av att det är oklart exakt vilka uppgifter som kommer att finnas i Arachne. Förhållandena kan också komma att ändras i framtiden eftersom Arachne är under utveckling. Dessa förhållanden kan dock enligt utredningens mening inte åberopas för att införa ny sekretessreglering för uppgifter i Arachne, så att säga för säkerhets skull. För att det ska vara motiverat att göra undantag från det grundlagsskyddade insynsintresset bör det krävas mer konkreta risker för olägenheter om uppgifter röjs.

Enligt utredningen är det möjligt att argumentera för att gällande sekretessregler ska anses som tillräckliga. Gällande bestämmelser kommer i många situationer att kunna ge ett sekretesskydd för uppgifter i Arachne, inklusive gjorda riskvärderingar. Det kan visserligen inte uteslutas att uppgifter i Arachne, inklusive gjorda riskvärderingar, i vissa fall inte kommer att kunna sekretessbeläggas. Det beror delvis på intresseavvägningar som lagstiftaren redan har gjort mellan behovet av sekretess och insynsintresset, både när det gäller gällande sekretessbestämmelsers tillämpningsområde och valda skaderekvisit. Exempelvis aktualiseras sekretess enligt 15 kap. 1 a § OSL enligt förarbetena normalt bara om det finns en tydlig sekretessbestämmelse i en bindande EU-rättsakt (prop. 2012/13:192 s. 35), något som inte gäller för Arachne. Det är också tveksamt i vilken utsträckning gjorda riskvärderingar – om de ens omfattas av tillämpningsområdet för 17 kap. 1 b § OSL – kan beläggas med sekretess enligt bestämmelsen mot bakgrund av utformningen av dess skaderekvisit. Det är dock alltså möjligt att argumentera för att en sådan ordning är i linje med de avvägningar som redan gjorts inom den svenska sekretessregleringen.

I sammanhanget kan det erinras om att Arachne-teamet vid kommissionen har framfört ett önskemål om att uppgifter i Arachne inte ska spridas fritt[6] och detta har vidare – beträffande gjorda riskvärderingar – kommit till uttryck i Arachne-stadgan. Utredningen konstaterar dock att detta inte har kommit till uttryck i en tydlig sekretess-

[6] Komm2025/00388-10.

reglering i en bindande rättsakt. Det talar för att insynsintresset bör ha företräde. Det är enligt utredningens mening alltså ett fullt möjligt alternativ för regeringen att välja att inte gå vidare med något förslag på en ny sekretessbestämmelse. Ställningstagandet berör delvis utrikespolitiska frågor om intresseavvägningen mellan den svenska offentlighetsprincipen och relationen med EU.

Det kan samtidigt argumenteras för att risken att uppgifter i Arachne i vissa fall inte kan sekretessbeläggas enligt gällande sekretessbestämmelser kan leda till att viktiga allmänna intressen inte får genomslag. Det skulle kunna innebära att möjligheterna för Sverige att delta i samarbetet med EU och övriga medlemsländer i genomförandet av EU:s budget försämras. Det kan leda till att Sveriges möjligheter att uppfylla skyldigheterna enligt budgetförordningen minskar. En ökad möjlighet att sekretessbelägga uppgifter i Arachne skulle tydliggöra Sveriges ambition att delta i samarbetet med kommissionen och övriga medlemsländer för att motverka felaktigheter i utbetalningen av EU-stöd. Detta talar för att en ny sekretessreglering införs.

Begränsade möjligheter att avstå från att lämna ut uppgifter som finns i Arachne, inklusive gjorda riskvärderingar, skulle också kunna innebära att syftet med den granskning- och kontrollverksamhet som svenska myndigheter bedriver för att motverka felaktigheter med EU-stöd motverkas.

Enligt utredningens mening kan det mot denna bakgrund argumenteras för att det finns skäl för en utökad möjlighet att sekretessbelägga uppgifter i Arachne, särskilt kopplat till riskvärderingsdelen av verktyget, både för att samarbetet inom EU inte ska försämras och för att myndigheternas arbete med kontroller och granskning inte ska motverkas. Ett sådant undantag från det grundlagsskyddade insynsintresset bör därmed anses som godtagbart. I det följande lämnas ett förslag på hur en ny sekretessbestämmelse skulle kunna utformas.

8.5.7 Hur en ny sekretessreglering skulle kunna utformas

Utredningens förslag: Sekretess ska gälla för uppgift som härrör från en riskvärdering som har gjorts genom ett sådant system som avses i artikel 36.2 d i budgetförordningen, om det kan antas att syftet med den förvaltning, övervakning, kontroll och revision som ska ske i enlighet med budgetförordningen motverkas om uppgiften röjs.

Rätten att meddela och offentliggöra uppgifter ska ha företräde framför den tystnadsplikt som följer av den nya bestämmelsen.

Utredningens bedömning: I skaderekvisitet ingår vilken effekt ett offentliggörande av uppgiften skulle kunna antas få på samarbetet inom EU.

Det behövs inte någon ny sekretessbrytande bestämmelse.

Skälen för utredningens förslag och bedömning

En ny sekretessreglering har stöd i 2 kap. 2 § TF

En förutsättning för att kunna införa en ny reglering för skydd för uppgifter i Arachne är att det är möjligt med hänsyn till någon av de sekretessgrunder som räknas upp i 2 kap. 2 § TF. I paragrafen anges bland annat att rätten att få del av allmänna handlingar får begränsas om det krävs med hänsyn till rikets säkerhet eller dess förhållande till en annan stat eller en mellanfolklig organisation, myndigheters verksamhet för inspektion, kontroll eller annan tillsyn, intresset av att förebygga eller beivra brott, det allmännas ekonomiska intresse eller skyddet för enskildas personliga eller ekonomiska förhållanden.

Flera av de sekretessgrunder som anges i 2 kap. 2 § TF kan aktualiseras i nuvarande fall. När det gäller gjorda riskvärderingar finns det grund för hemlighållande med hänsyn till Sveriges förhållande till en annan stat eller en mellanfolklig organisation. Om uppgifterna röjs kan det motverka myndigheternas arbete med att motverka felaktigheter med EU-stöd. Uppgifterna bör därför också kunna hemlighållas med hänsyn till myndigheters verksamhet för inspektion, kontroll eller annan tillsyn. Som utvecklas i avsnitt 5.4.2 kan uppgifter om enskilda som finns i databaserna Orbis och World Compliance anses vara en del av den information som omfattas av en

riskvärdering. En bestämmelse som ger utökad möjlighet att sekretessbelägga sådana skulle alltså också kunna motiveras med hänsyn till behovet av skyddet för enskildas personliga eller ekonomiska förhållanden.

Räckvidd – i vilken verksamhet bör sekretess gälla?

En sekretessbestämmelses räckvidd bestäms i allmänhet genom att det i bestämmelsen anges att sekretessen för vissa typer av uppgifter bara gäller i viss typ av verksamhet eller hos en viss myndighet. I detta fall bör sekretessen ha en vid räckvidd. Den bör i vart fall motsvara budgetförordningens definition av budgetgenomförande (artikel 2.7). Sekretessbestämmelsen bör nämligen minst gälla i all verksamhet där svenska myndigheter deltar i genomförande av EU:s budget, såväl vid delad förvaltning som vid direkt förvaltning tillsammans med medlemsstaterna (den förvaltningsform som i dag gäller för RRF).

Ett alternativ är mot den bakgrunden att begränsa räckvidden på så sätt att sekretessen ska gälla i verksamhet som rör förvaltning, övervakning, kontroll och revision som ska ske i enlighet med budgetförordningen. Insynsintresset talar för att inte låta räckvidden bli mer omfattande än vad som är nödvändigt.

Enligt utredningens mening är det dock lämpligare att sekretessen ska gälla hos alla myndigheter. Detta motsvarar regleringen i flera andra bestämmelser i 15 och 17 kap. OSL, exempelvis 15 kap. 1 och 2 §§ samt 17 kap. 1 a och 1 b §§ OSL. Det kan vara ändamålsenligt att myndigheter delar uppgifter mellan varandra för att mer effektivt motverka oriktigheter med allmänna medel. Om myndigheter delar uppgifter mellan varandra kommer bestämmelsen att vara en primär sekretessbestämmelse vid såväl den överlämnande som den mottagande myndigheten (jfr prop. 2022/23:34 s. 215).

Föremål – för vilka uppgifter ska sekretessen gälla?

Sekretessens föremål tar sikte på de uppgifter som kan hemlighållas med stöd av bestämmelsen. Enligt utredningen kan det övervägas två olika sätt att utforma en ny bestämmelse: ett vidare eller ett mer begränsat föremål. Ett *vidare angreppssätt* skulle kunna ta sikte på alla

uppgifter som härrör från Arachne. Det skulle omfatta både uppgifter som en svensk myndighet tar del av när Arachne används som ett riskvärderingsverktyg och uppgifter som erhålls när systemet används som ett datautvinningsverktyg. Detta skulle lagtekniskt kunna uppnås på så sätt att sekretessen avser *uppgift som härrör från ett sådant system* som avses i artikel 36.2 d i budgetförordningen. Bestämmelsen skulle då täcka samtliga uppgifter som härrör från Arachne, inklusive uppgifter som erhålls inom ramen för gjorda riskvärderingar. För en sådan ordning talar bland annat att det finns oklarheter när det gäller exakt vilka uppgifter som kommer att finnas i Arachne, vilka skyddsbehov som kan uppstå och hur långt gällande sekretessbestämmelser räcker för att tillgodose dessa skyddsbehov. För en sådan ordning talar också att Arachne-teamet vid kommissionen kan sägas ha gett uttryck för ett önskemål att uppgifter i Arachne över huvud taget inte ska offentliggöras.[7]

Insynsintresset talar för att inte ange sekretessens föremål vidare än vad som är nödvändigt utifrån de konkreta risker som har identifierats. Enligt utredningen talar därför det mesta för ett mer *begränsat angreppssätt*. Det är när det gäller just uppgifter som myndigheter tar del av när verktyget används för att göra riskvärderingar som ett sekretessbehov har kommit tydligare till uttryck i relevanta dokument. Det kan erinras om att Arachne-stadgan särskilt berör behovet av att riskvärderingar inte sprids. Det kan vidare erinras om att användare av Arachne inte kan söka fritt i den databas som kan antas innehålla de mest skyddsvärda uppgifterna, World Compliance, utan kan endast ta del av sådana uppgifter om de förekommer som en del av gjorda riskvärderingar avseende egna projekt (se mer i avsnitt 5.4.2). Liknande är tänkt att gälla för uppgifterna i Orbis.

Utredningen föreslår mot denna bakgrund att sekretessens föremål bestäms till *uppgift som härrör från en riskvärdering som har gjorts genom Arachne*. Med detta avser utredningen att fånga in i princip alla de uppgifter som en myndighet kan få del av när Arachne används som ett riskvärderingsverktyg. Inte bara sådana uppgifter som en myndighet därvid faktiskt tar del av bör omfattas, utan alla uppgifter som myndigheten *kan* få del av. Det är nämligen så att användargränssnittets utformning innebär att användaren i viss mån kan välja hur mycket och hur detaljerade uppgifter användaren ska ta del av inom ramen för en riskvärdering.

[7] Komm2025/00388-10.

Inom ramen för detta bör många olika typer av information kunna omfattas. Till att börja med bör information om vilka värden en viss aktör får beträffande de olika riskindikatorerna omfattas. Även information som en användare kan få del av om kopplingar till andra bolag samt om de bolag och personer som berörs bör ingå. Dessutom bör den information som nås via länkar till externa källor ingå i sekretessens föremål.

Riskvärderingar i Arachne kan göras på olika sätt. Vissa riskvärderingar genereras automatiskt i Arachne. När det gäller förhandsfunktionen krävs det dock att en användare begär att en sådan riskvärdering ska göras. Alla dessa former av riskvärderingar kan sägas göras *genom* Arachne och bör omfattas av en eventuell ny bestämmelse.

Som utvecklas i avsnitt 8.5.2 bedömer utredningen vidare att endast uppgifter som härrör från *gjorda riskvärderingar* bör kunna utgöra allmänna handlingar. En begäran om att få ut de uppgifter som härrör från en riskvärdering inom ramen för förhandsfunktionen bör – i en situation där någon sådan riskvärdering inte redan har gjorts – kunna avslås redan på den grunden att någon sådan handling över huvud taget inte förvaras hos myndigheten.

Exakt vilka uppgifter som kan anses härröra från en riskvärdering som har gjorts genom Arachne är till viss del beroende på den tekniska utformningen av systemets användargränssnitt, något som kan komma att förändras under det pågående utvecklingsarbetet. Det kan alltså inom ramen för denna utredning inte helt fastställas vilken information som kommer att omfattas av bestämmelsen. Det är den myndighet som får en begäran om utlämnande som ska ta ställning till om den begärda uppgiften i det enskilda fallet omfattas av bestämmelsen.

För det fall ytterligare skyddsbehov identifieras i framtiden kan vid behov kompletterande reglering införas.

Styrka – under vilka förutsättningar ska sekretessen gälla?

Sekretessens styrka – det vill säga bestämmelsens skaderekvisit – bör beskrivas på så sätt att sekretess gäller om det kan antas att syftet med viss verksamhet motverkas om uppgiften röjs. Verksamheten bör beskrivas som den förvaltning, övervakning, kontroll och revision som ska ske i enlighet med budgetförordningen. Om bedöm-

ningen görs att syftet med den verksamheten i stort motverkas om uppgifter i Arachne röjs – exempelvis därför att det underlättar för aktörer som felaktigt vill utnyttja stöd att ta fram strategier för ett sådant missbruk – bör sekretess kunna gälla även efter det att ett enskilt granskningsärende är avslutat.

Även fall då det kan antas att möjligheten för svenska myndigheter att delta i samarbetet som kommer till uttryck i budgetförordningen försämras om uppgiften röjs bör omfattas. Om EU och andra medlemsstater känner tveksamhet inför Sveriges möjligheter att förhindra spridning av skyddsvärda uppgifter som svenska myndigheter får tillgång till genom Arachne finns det en risk att det samarbete som är en förutsättning för ett effektivt motverkande av felaktigheter med EU-medel fungerar mindre effektivt. Liknande resonemang har förts i tidigare lagstiftningsärenden, bland annat när det gäller sekretess inom ramen för internationellt samarbete avseende tillsyn av civil luftfart (17 kap. 6 § OSL) och sekretess inom ramen för samarbetet inom EU avseende tillsyn av marknaderna för el och naturgas (17 kap. 7 b § OSL). Om Sverige inte skulle anses ha ett adekvat sekretesskydd skulle andra medlemsstater kunna bli mindre benägna att tillgängliggöra uppgifter som svenska myndigheter kan ha nytta av. Det skulle kunna leda till att informationsutbytet blir mindre omfattande och av sämre kvalitet än vad som annars skulle ha blivit fallet. Om så skulle ske skulle effektiviteten minska inte bara i Sveriges utan också i andra medlemsstaters arbete med att motverka felaktigheter med EU-medel och då skulle syftet med budgetförordningen motverkas (jfr prop. 2006/07:110 s. 45–48 och prop. 2012/13:7 s. 15–18).

Vid bedömningen av om skaderekvisitet är uppfyllt bör alltså bland annat vägas in vilken effekt ett offentliggörande av uppgiften skulle kunna antas få på det framtida samarbetet inom EU (jfr prop. 2012/13:7 s. 17).

Sekretesstiden

När en ny sekretessbestämmelse ska införas behöver man ta ställning till hur länge sekretessen enligt den nya bestämmelsen högst ska få gälla. Sekretesstiden i olika sekretessbestämmelser varierar beroende på vilken typ av uppgift det är fråga om. När det gäller

sekretess till skydd för allmänna intressen förekommer sekretesstider om 40 år (se t.ex. utrikes- respektive försvarssekretessen i 15 kap. 1 och 2 §§ OSL). I vissa fall anges inte någon sekretesstid alls. Så är fallet bland annat när det gäller 17 kap. 1–4 §§ OSL. Någon tidsbegränsning behövs där inte eftersom skaderekvisitet klart anger den tidpunkt då sekretessen upphör.

Som framgår ovan föreslår utredningen att skaderekvisitet ska utformas på liknande sätt som i nämnda bestämmelser i 17 kap. OSL, det vill säga att sekretess gäller om det kan antas att syftet med viss verksamhet motverkas om uppgiften röjs. Motsvarande skaderekvisit har ansetts innebära att behovet av att sekretessbelägga uppgifterna finns under den tid som de används i myndighetens arbete. När uppgifterna inte längre används upphör sekretessen, och uppgifterna ska lämnas ut om de efterfrågas. Utredningen gör i avsnitt 8.5.4 vissa överväganden rörande tillämpningen av skaderekvisitet i 17 kap. 1 b § OSL på uppgifter i Arachne. Motsvarande överväganden gör sig gällande här. Det framgår av artikel 36.7 i budgetförordningen att uppgifterna i Arachne endast ska lagras under den period som är nödvändig och proportionell för att uppfylla det syfte som fastställs i punkt 2 d, det vill säga att motverka oriktigheter. Den längsta möjliga lagringsperioden får inte överstiga tio år från och med den sista ansökan om utbetalning som lämnats in till kommissionen för den perioden. Enligt utredningens mening bör uppgifterna som utgångspunkt anses användas i den meningen att skaderekvisitet är uppfyllt under hela den tid som uppgifterna lagras i Arachne. En prövning i det enskilda fallet behöver dock göras av den myndighet som hanterar frågan om utlämnande.

Hänvisning till budgetförordningen

Det finns två sätt att hänvisa till unionslagstiftning i nationell rätt, antingen genom statiska hänvisningar eller genom dynamiska hänvisningar. En statisk hänvisning innebär att hänvisningen avser EU-rättsakten i en viss angiven 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. För att eventuella ändringar i förordningen ska

få omedelbart genomslag i Sverige är det lämpligt att hänvisningar i den nya lagen är dynamiska.

Den nya bestämmelsens placering

Var en ny sekretessbestämmelse ska placeras beror på vilket intresse sekretessen är avsedd att skydda. Om en ny sekretessbestämmelse gäller till skydd för ett allmänt intresse bör den alltså placeras i relevant kapitel i lagens fjärde avdelning (15–20 kap.).

I aktuellt fall kan grunden för sekretess sägas främst vara dels skyddet för myndighets verksamhet för inspektion, kontroll eller tillsyn, dels skyddet för rikets förhållande till andra stater eller mellanfolkliga organisationer. I 17 kap. OSL finns bestämmelser om sekretess till skydd främst för myndigheters verksamhet för inspektion, kontroll eller annan tillsyn. I detta kapitel finns dock även bestämmelser som också baseras på behovet av att skydda rikets förhållande till andra stater eller mellanfolkliga organisationer. Som exempel kan nämnas 17 kap. 7 § andra stycket, 17 kap. 7 a § och 17 kap. 7 b § OSL. I samband med införandet av den förstnämnda bestämmelsen ändrades rubriken till 17 kap. till att lyda ”Sekretess till skydd främst för myndigheters verksamhet för inspektion, kontroll eller annan tillsyn” (prop. 2009/10:231 s. 35 och 36). Utredningen bedömer mot denna bakgrund att en placering i 17 kap. är väl förenlig med lagens systematik.

Rätten att meddela och offentliggöra uppgifter

Enligt 3 kap. 1 § OSL innebär sekretess ett förbud att röja uppgift, vare sig det sker muntligen, genom utlämnande av allmän handling eller på något annat sätt. Sekretess innebär således såväl tystnadsplikt som handlingssekretess. När en ny bestämmelse om sekretess införs måste man ta ställning till om den tystnadsplikt som följer av den föreslagna sekretessbestämmelsen ska ha företräde framför rätten att meddela och offentliggöra uppgifter som följer av 1 kap. 1 och 7 §§ TF och 1 kap. 1 och 10 §§ yttrandefrihetsgrundlagen. Enligt förarbetena till sekretesslagen bör som grundprincip alltid gälla att stor återhållsamhet ska iakttas vid prövningen av om undantag från rätten att meddela och offentliggöra uppgifter ska göras i ett särskilt

fall. Där anges vidare att den enskilda sekretessbestämmelsens konstruktion kan ge viss vägledning – när det är fråga om bestämmelser om absolut sekretess kan det finnas större anledning att överväga undantag från rätten att meddela och offentliggöra uppgifter än i andra fall (prop. 1979/80:2 Del A s. 110 och 111).

När det gäller exempelvis sekretessbestämmelserna i 17 kap. 1–2 §§ OSL – som rör förberedelser för inspektion, dataanalyser och urval i syfte att motverka felaktigheter i folkbokföringsverksamheten och felaktiga utbetalningar samt viss pågående granskning – har rätten att meddela och offentliggöra uppgifter företräde framför tystnadsplikten.

Den föreslagna nya bestämmelsen innebär inte absolut sekretess. Den avser att skydda uppgifter om riskvärderingar som har genererats av Arachne i fall då det kan antas att syftet med den förvaltning, övervakning, kontroll och revision som ska ske i enlighet med budgetförordningen motverkas om uppgiften röjs. Utredningen anser att rätten att meddela och offentliggöra uppgifter ska ha företräde framför den tystnadsplikt som följer av den föreslagna bestämmelsen. Det bör därför inte göras någon ändring av 17 kap. 8 § OSL, den bestämmelse som anger i vilka fall tystnadsplikten inskränker rätten att meddela och offentliggöra uppgifter när det gäller bestämmelserna i 17 kap. OSL.

Inte något behov av nya sekretessbrytande bestämmelser

Införande av en ny sekretessbestämmelse innebär att sekretess kommer att gälla mellan olika myndigheter. När en ny sekretessbestämmelse införs bör det därför övervägas om det behöver införas några sekretessbrytande bestämmelser. Enligt utredningen innebär inte införandet av den föreslagna bestämmelsen något sådant behov. De befintliga sekretessbrytande bestämmelserna bedöms vara tillräckliga. Utredningen beaktar också den nya sekretessbrytande bestämmelsen som behandlas i regeringens proposition Ökat informationsutbyte mellan myndigheter – en ny sekretessbrytande bestämmelse (se prop. 2024/25:180 och avsnitt 7.1.2).

8.5.8 Det krävs inte författningsändringar på dataskyddsområdet för användande av Arachne

Utredningens bedömning: Svenska myndigheters användning av Arachne kräver inga författningsändringar på dataskyddsområdet.

Skälen för utredningens bedömning

Inledning

I avsnitt 7.2 redogör utredningen för gällande rätt på dataskyddsområdet, bland annat för kravet på rättslig grund och de grundläggande principerna för att en personuppgiftsbehandling ska vara laglig.

I detta avsnitt gör utredningen bedömningar av om befintligt dataskyddsregelverk är tillräckligt för den personuppgiftsbehandling som förväntas ske vid en användning av Arachne eller om det krävs författningsändringar. Härvid lyfts vissa dataskyddsrättsliga frågor särskilt. Vidare ingår i detta delvis en kartläggning av skyddet för personuppgifter i Arachne. Sådana frågor behandlas också i den samlade integritetsanalysen i kapitel 9.

Budgetförordningens reglering om dataskydd som rör Arachne och andra relevanta källor

Artikel 36.7 i budgetförordningen är central för den personuppgiftsbehandling som kan förväntas ske vid en användning av Arachne. Artikeln är omfattande och innehåller bestämmelser om syftet med och användningen av Arachne. Systemet ska vara utformat för att användas i enlighet med de allmänna dataskyddsprinciper, inbegripet uppgiftsminimering och lagringsbegränsning, som är tillämpliga på behandling av personuppgifter. Artikeln innehåller också bestämmelser om åtkomst till systemet, personuppgiftsansvar och längsta tid för behandling.

Arachne-stadgan innehåller ett antal principer men också information. Den tar upp ändamål som systemet kan användas för, vilka som är avsedda användare, skyldigheter för användare och för kommissionen samt frågor om åtkomststyrning. Längsta tid för behandling och enskildas rättigheter tas också upp. Det framgår också av stadgan

att en konsekvensbedömning enligt dataskyddsförordningen för EU:s institutioner har gjorts. För mer om denna, se den samlade integritetsanalysen i kapitel 9.

Enligt artikel 31 i dataskyddsförordningen för EU:s institutioner ska varje personuppgiftsansvarig föra ett register över behandling som utförs under dess ansvar, under vissa närmare förutsättningar. Ett centralt register kan föras. EU:s dataskyddsombud för ett register över personuppgiftsbehandling som utförs av kommissionen. En beskrivning av personuppgiftsbehandlingen för Arachne[8] finns i registret. Där beskrivs ändamålen med behandlingen, vilka personuppgifter som behandlas, hur behandlingen ska gå till, längsta tid för behandling, vilka som får tillgång till uppgifter, säkerhetsåtgärder samt information till enskilda om deras rättigheter. Det kan nämnas att en motsvarande skyldighet att förteckna personuppgiftsbehandling finns i dataskyddsförordningen, och gäller därmed även för svenska myndigheter.

Den vars personuppgifter behandlas ska i regel informeras om detta. Därför finns ofta information riktad till enskilda om hur deras personuppgifter behandlas. Det finns en sådan personuppgiftspolicy för Arachne[9] som kommissionen har tagit fram. Personuppgiftspolicyn innehåller en beskrivning av varför och hur kommissionen behandlar personuppgifter, vilken rättslig grund som behandlingen vilar på, vilka personuppgifter som kommissionen samlar in och behandlar vidare, hur länge kommissionen behandlar personuppgifter och hur de skyddas samt vem som har tillgång till uppgifterna. Det finns också en beskrivning av den enskildes rättigheter och hur de kan utövas samt hänvisningar till var mer information kan hittas.

Tidigare nämnda frågor och svar avseende Arachne innehåller information som riktar sig till dem som behandlar personuppgifter, däribland myndigheter (Arachne, Frequently asked questions, version 2.3, den 19 augusti 2022 och Arachne, FAQ on data protection

[8] Record for processing of personal data, Title: Risk analysis for fraud prevention and detection in the management of EU funds (ARACHNE SYSTEM). Reference: DPR-EC-00598.4, publicerad den 27 november 2023. https://ec.europa.eu/dpo-register/detail/DPR-EC-00598. Hämtat 2025-10-29.

[9] Protection of your personal data, Processing operation: Risk analysis for fraud prevention and detection in the management of European Structural Funds (ARACHNE), Data Controller: DAC, Record reference: DPR-EC-00598. Personuppgiftspolicyn är inte daterad och utredningen har inte kunnat identifiera ett entydigt datum för dess framtagande. En uppgift tyder på att den publicerades den 1 januari 2024. https://employment-social-affairs.ec.europa.eu/policies-and-activities/funding/european-social-fund-plus-esf/what-arachne_en. Hämtat 2025-10-23.

and related issues, Status as of 10th July 2024). I den senare behandlas flera frågor som rör risker för integritetsintrång.

Kommissionen har också en webbsida dedikerad för Arachne, med information riktad bland annat till enskilda.[10]

Det bör observeras att då Arachne är under utveckling och regleringen i budgetförordningen i stora delar ännu inte ska tillämpas, tar ovan nämnda källor sikte på Arachne som det fungerar i dag, och inte nödvändigtvis på en framtida användning av Arachne.

Rättslig grund för behandlingen

Användningen av Arachne som verktyg är frivillig, även om det finns reglerade skyldigheter för myndigheter att aktivt motverka oriktigheter i såväl unionsrätten som nationell reglering. Särskilt artikel 36.2 i budgetförordningen betonar vikten av intern kontroll på alla förvaltningsnivåer – därmed inom såväl delad som direkt förvaltning – och av att oriktigheter motverkas bland annat genom (den frivilliga) användningen av Arachne. Artikel 36.7 beskriver också syftet med och vikten av att använda Arachne för att uppnå målen i artikel 36.2.

Av avsnitt 8.2.6 framgår att den verksamhet som en statlig myndighet bedriver, inom ramen för sin befogenhet, är av allmänt intresse. Ett användande av Arachne faller inom berörda myndigheternas befogenheter. Vidare är enligt utredningen behandlingen att anse som nödvändig (jfr utredningens bedömning i avsnitt 8.3.5). Den personuppgiftsbehandling som kan förväntas bli aktuell genom ett användande av Arachne faller därmed enligt utredningen tydligt inom grunden *utförande av en uppgift av allmänt intresse* (artikel 6.1 e i dataskyddsförordningen och 2 kap. 2 § dataskyddslagen).

Om det framöver blir en rättslig skyldighet att använda Arachne, kommer även den rättsliga grunden att *fullgöra en rättslig förpliktelse* (artikel 6.1 c i dataskyddsförordningen och 2 kap. 1 § dataskyddslagen) att aktualiseras. Det kan, på samma grunder som utredningen framför i avsnitt 8.3.5 avseende uppgiftslämnande som sker utan att det finns en rättslig skyldighet till det, vara möjligt att argumentera för att denna rättsliga grund kan vara tillämplig även utan en uttryck-

[10] https://employment-social-affairs.ec.europa.eu/policies-and-activities/funding/european-social-fund-plus-esf/what-arachne_en. Hämtat 2025-10-25.

lig skyldighet att använda Arachne, men detta kan inte konstateras med säkerhet.

I likhet med bedömningen i avsnitt 8.2.6 anser utredningen att den rättsliga grunden kan uppfylla kraven på tydlighet och precision samt på en förutsebar tillämpning för personer som omfattas av den. Den reglering och det offentligt tillgängliga stöd- och informationsmaterialet om Arachne ger omfattande upplysningar om behandlingen och grunden för den.

Utredningen utgår vidare från att unionsrätten är förenlig med Europakonventionen och uppfyller kravet på proportionalitet i artikel 6.3 i dataskyddsförordningen. För en samlad integritetsanalys, se kapitel 9.

Att det finns rättslig grund för personuppgiftsbehandlingen innebär att det inte genom författning behöver skapas några nya rättsliga grunder.

Principerna i artikel 5 i dataskyddsförordningen

I avsnitt 7.2.5 redogör utredningen för principerna i artikel 5.1 i dataskyddsförordningen och för att det är den personuppgiftsansvarige som ska säkerställa att principerna efterlevs. Utredningen gör så långt det är möjligt bedömningar avseende möjligheten att efterleva principerna.

Arachne innehåller en stor mängd uppgifter och är ett kraftfullt verktyg. Det är av yttersta vikt att verktyget endast används på avsett sätt. På samma grunder som anges i avsnitt 8.2.6 utgår utredningen från att de myndigheter som kommer att behandla personuppgifter uppfyller principen om laglighet, korrekthet och öppenhet, principen om integritet och konfidentialitet samt principen om riktighet. Även om det nu är fråga om svenska myndigheters ansvar att efterleva principerna i artikel 5 i dataskyddsförordningen och budgetförordningen och andra relevanta källor i flera delar avser kommissionens ansvar, kan källorna ändå ge svenska myndigheter viss vägledning i fråga om principerna. Vad gäller ovan nämnda princip om konfidentialitet hänvisar budgetförordningen uttryckligen till den principen när det gäller Arachne, med sikte på kommissionens ansvar (artikel 36.7 tredje stycket). Såväl artikel 36.7 i budgetförordningen som Arachne-stadgan (punkt 11) lyfter vidare kommissio-

nens ansvar att säkerställa att personuppgifter skyddas. I Arachne-stadgan anges också att kommissionen säkerställer transparens genom att informera enskilda om behandlingen (punkt 6.1).

När det gäller rättelser av fel gör ett förfarande benämnt ”Feedback loop” det möjligt för användare – och därmed svenska myndigheter – att anmäla fel eller inkonsekvenser och begära rättelse hos kommissionen av felaktiga matchningar mellan interna och externa data (punkt 6.2). Det finns således ett system för myndigheter att anmäla vissa felaktigheter, vilket kan underlätta möjligheten att efterleva ovan nämnda princip om riktighet.

Det syfte med Arachne som framgår av budgetförordningen påverkar också för vilka ändamål som personuppgifter får behandlas – även av svenska myndigheter – och ger därmed uttryck för principen om ändamålsbegränsning. Motverkandet av oriktigheter kan ske genom användningen av Arachne och systemet ska utformas för att underlätta riskbedömningar för urval, tilldelning, ekonomisk förvaltning, övervakning, utredning, kontroll och revision och bidra till att effektivt förebygga, upptäcka, korrigera och följa upp oriktigheter såsom bedrägerier, korruption, intressekonflikter och dubbelfinansiering. Systemet ska endast använda riskindikatorer som är objektiva, proportionella, nödvändiga för riskbedömning och baserade på tillförlitliga uppgifts- och informationskällor (artikel 36.2 d och 36.7 första stycket).

Även Arachne-stadgan innehåller ändamålsangivelser. Av punkt 3 framgår vad programmyndigheterna kan använda systemet till och att programmyndigheterna som får tillgång till resultaten av Arachnes riskvärderingar bara ska använda dessa för förvaltningskontroller (management verifications), kontroller (controls) och revisioner (audits). Resultaten ska inte användas för personliga intressen eller några andra ändamål. Denna punkt riktar sig således till myndigheter.

Punkt 6.2 i Arachne-stadgan behandlar insamling av uppgifter. När det gäller externa data ska sådana uppgifter behandlas enbart för att identifiera risker för bedrägerier och oriktigheter när det gäller bland annat slutliga mottagare, stödmottagare, leverantörer, verklig huvudman och kontrakt, både vid godkännande- och genomförandefasen. Detta ger också ett visst uttryck för en ändamålsbegränsning, som dock enligt utredningens bedömning tar sikte på kommissionens behandling av sådana uppgifter inom ramen för riskvärderings-

verktyget, eftersom det är kommissionen (och inte medlemsländernas myndigheter) som samlar in externa data.

Vad gäller principen om uppgiftsminimering nämns den uttryckligen i artikel 36.7 första stycket b och skäl 31 till budgetförordningen i fråga om utformningen av Arachne, så även principen om lagringsminimering. Uppgifterna ska lagras under den period som är nödvändig och proportionell för att uppfylla syftet att motverka oriktigheter. Den längsta möjliga lagringsperioden får inte överstiga tio år från och med den sista ansökan om utbetalning som lämnats in till kommissionen för den perioden (artikel 36.7 fjärde stycket). Även Arachne-stadgan tar upp frågor om längsta tid för behandling. Enligt stadgan lagras interna data och resultaten av riskberäkningar under tio år efter myndighetens betalningsanspråk till kommissionen. När det gäller RRF är lagringstiden fem år efter sista betalning (punkt 6.2 i Arachne-stadgan). Principen om lagringsminimering får därmed anses vara beaktad. Det bör noteras att då det är kommissionen som driver Arachne och myndigheterna inte kan ta bort uppgifter i Arachne är det främst kommissionen som råder över frågan om lagringstiden.

En användning av Arachne bedöms av utredningen kunna vara förenlig med ovan nämnda principer, men det är den myndighet som behandlar personuppgifter som behöver följa dem även i praktiken.

Vad gäller finalitetsprincipen kan det finnas skäl att lyfta följande. För att riskvärderingsverktyget ska ha god funktionalitet används uppgifter som finns i Arachne för att ta fram riskindikatorer. Detta kan innebära att uppgifter i Arachne också används som så kallade träningsdata. Det är enligt utredningens mening logiskt att ett tekniskt verktyg som innehåller data använder dessa data för att träna verktyget så att det blir så effektivt och träffsäkert som möjligt. Utredningen ser en sådan användning, och därmed sådan personuppgiftsbehandling som följer av detta, som en så naturlig del av ändamålet med behandlingen att den som utgångspunkt inte kommer i konflikt med finalitetsprincipen (se också punkt 6.2 i Arachne-stadgan om att enskilda ska informeras om att deras uppgifter kan komma att användas för ändamålet att identifiera riskindikatorer).

Även om utredningens uppdrag avser myndigheters användning av Arachne kan det finnas skäl att lyfta att information som finns i Arachne kan vara av stort intresse för berörda myndigheter att använda även i annan verksamhet hos dessa myndigheter. Om en myndighet har ett sådant intresse behöver den bedöma om en sådan

personuppgiftsbehandling är förenlig med finalitetsprincipen. Det ankommer alltså på myndigheterna att bedöma förutsättningarna för en sådan fortsatt användning av uppgifterna.

Det ovanstående innebär att den reglering som finns bedöms vara tillräcklig och att det inte finns skäl att överväga några författningsändringar som tar sikte på att uppfylla principerna i artikel 5 i dataskyddsförordningen.

Känsliga personuppgifter

I avsnitt 5.4 beskriver utredningen vilka slags uppgifter som Arachne kan innehålla. Det gäller bland annat uppgifter om personer i politiskt utsatt ställning, från den så kallade PEP-listan. Denna information kan innehålla uppgifter som avslöjar politiska åsikter, vilket utgör känsliga personuppgifter (artikel 9.1 i dataskyddsförordningen). Detta är också den kategori av känsliga personuppgifter som kommissionen har angett som förekommande i beskrivningen av personuppgiftsbehandlingen för Arachne. Arachne innehåller därmed känsliga personuppgifter. Svenska myndigheter skulle därmed vid en användning av Arachne kunna få tillgång till känsliga personuppgifter. Läsning är exempel på behandling som då skulle kunna aktualiseras.

Behandling av känsliga personuppgifter är som huvudregel förbjudet, men det finns undantag från förbudet i dataskyddsförordningen (se mer i avsnitt 8.2.6). Dataskyddsförordningen för EU:s institutioner innehåller i princip motsvarande förbud och undantag. I beskrivningen av personuppgiftsbehandlingen för Arachne anges de grunder på vilka den behandling av känsliga personuppgifter som förekommer är tillåten enligt artikel 10.2 i dataskyddsförordningen för EU:s institutioner, som är tillämplig vid kommissionens personuppgiftsbehandling. En av dessa grunder är att behandlingen är nödvändig av hänsyn till ett *viktigt allmänt intresse*, på grundval av unionsrätten som ska stå i proportion till det eftersträvade syftet (artikel 10.2 g).

För svenska myndigheters behandling av känsliga personuppgifter är motsvarigheten i dataskyddsförordningen – artikel 9.2 g – och undantagen i 3 kap. 3 § första stycket dataskyddslagen tillämpliga. En första fråga är om undantagssituationen i 3 kap. 3 § första stycket 1 dataskyddslagen – att uppgiften har lämnats till myndigheten och

behandlingen krävs enligt lag – kan bli aktuell här. Utredningen bedömer att så inte blir fallet, så länge användningen av Arachne inte är obligatorisk.

Undantaget i 3 kap. 3 § första stycket 2 dataskyddslagen – att behandlingen är nödvändig för handläggningen av ett ärende – skulle kunna aktualiseras i vissa fall. Begreppen handläggning och ärende ska tolkas på samma sätt som enligt 1 § förvaltningslagen. Begreppet handläggning innefattar alla åtgärder som en myndighet vidtar från det att ett ärende inleds till dess att det avslutas. Vad gäller kravet att behandlingen är *nödvändig* för handläggningen av ärendet, innebär det bland annat att bara sådana uppgifter som behövs i ärendet får behandlas. Som framgår tidigare (avsnitt 8.2.6) innebär begreppet nödvändig inte ett krav på att behandlingsåtgärden ska vara oundgänglig (jfr också prop. 2017/18:105 s. 194). Då Arachne kan komma att användas inom ramen för ett ärende är det inte uteslutet att denna undantagssituation kan aktualiseras.

Undantaget i 3 kap. 3 § första stycket 3 dataskyddslagen – att behandlingen är nödvändig med hänsyn till ett viktigt allmänt intresse – behandlas närmare i avsnitt 8.2.6. Bestämmelsen möjliggör under vissa omständigheter behandling av känsliga personuppgifter hos myndigheter då behandlingen varken sker med koppling till ett visst ärende eller krävs enligt annan lag. Den är således tillämplig i så kallad faktisk verksamhet hos myndigheter, det vill säga i sådan förvaltningsverksamhet som inte utgör ärendehandläggning. Det krävs att den personuppgiftsansvarige gör en bedömning av om behandlingen innebär ett otillbörligt intrång i den registrerades personliga integritet (se mer i prop. 2017/18:105 s. 194).

Behandling av känsliga personuppgifter med stöd av denna punkt förväntas kunna bli aktuell vid användning av Arachne. En stor del av myndigheternas kontrollverksamhet kan ske utan att det är en del i ärendehandläggning. Det är också ett viktigt allmänt intresse att svenska myndigheter kan bedriva den verksamhet som tydligt faller inom ramen för deras befogenheter på ett korrekt, rättssäkert och effektivt sätt (jfr avsnitt 8.2.6).

Ovanstående kan sammanfattas så att utredningen bedömer att känsliga personuppgifter kan få behandlas med stöd av 3 kap. 3 § dataskyddslagen. Bedömningen av om det är möjligt i det enskilda fallet behöver göras av den berörda myndigheten som ställs inför behandlingen.

En annan fråga är om det kan finnas ytterligare grunder på vilka känsliga personuppgifter kan få behandlas. Utöver grunden viktigt allmänt intresse, som behandlas ovan, anges i beskrivningen av personuppgiftsbehandlingen för Arachne också den grund som motsvarar artikel 9.2 e i dataskyddsförordningen, nämligen att behandlingen rör personuppgifter som på ett tydligt sätt har *offentliggjorts av den registrerade* (artikel 10.2 e i dataskyddsförordningen för EU:s institutioner). Vidare nämns grunden att behandlingen är nödvändig för att fastställa, göra gällande eller försvara *rättsliga anspråk* eller som en del av en domstols dömande verksamhet (artikel 10.2 f i dataskyddsförordningen för EU:s institutioner). Denna grund har sin motsvarighet i artikel 9.2 f i dataskyddsförordningen. Dessa undantagsbestämmelser skulle eventuellt kunna bli aktuella att tillämpa för svenska myndigheter till exempel när det gäller känsliga personuppgifter som rör politiskt utsatta personer. Även i sådana fall är det dock berörd myndighet som måste göra bedömningen om det är möjligt att behandla personuppgifterna i fråga.

Bland funktionerna i Arachne finns sökfunktioner. Vad gäller sökförbudet i 3 kap. 3 § andra stycket dataskyddslagen, att det vid behandling som sker enbart med stöd av första stycket är förbjudet att utföra sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter, kan följande nämnas. Sökbegränsningen omfattar alla tekniska åtgärder som innebär att uppgifter används för att strukturera eller systematisera information i syfte att få fram ett urval av personer grundat på känsliga personuppgifter. Därmed förbjuds sökningar som görs för att få fram ett urval av personer som till exempel har en viss politisk åsikt, religiös åskådning eller sexuell läggning. Däremot hindrar bestämmelsen inte sökningar som görs i ett annat syfte än att identifiera ett urval av individer, till exempel för att utöva tillsyn, för att ta fram verksamhetsstatistik eller för registervård (se prop. 2017/18:105 s. 195).

Myndigheterna borde inte ha något sakligt intresse av att få fram ett urval av personer grundat på känsliga personuppgifter vid en användning av Arachne. Förutsättningarna för att behandla känsliga personuppgifter behöver bedömas av den myndighet som vid en användning av Arachne har för avsikt att utföra till exempel den aktuella sökningen.

Det finns inte behov av författningsändringar när det gäller behandling av känsliga personuppgifter.

Uppgifter om domar och lagöverträdelser

Arachne kan komma att innehålla uppgifter om lagöverträdelser, exempelvis om domar. Det framgår också av beskrivningen av personuppgiftsbehandlingen för Arachne att så är fallet i dagsläget.

Enligt artikel 10 i dataskyddsförordningen får behandling av personuppgifter som rör fällande domar i brottmål och lagöverträdelser som innefattar brott eller därmed sammanhängande säkerhetsåtgärder endast utföras under kontroll av en myndighet eller då behandlingen är tillåten enligt unionsrätten eller medlemsstaternas nationella rätt, där lämpliga skyddsåtgärder för de registrerades rättigheter och friheter fastställs. Ett fullständigt register över fällande domar i brottmål får dock endast föras under kontroll av en myndighet.

3 kap. 8 § dataskyddslagen ger ett tydligt stöd i nationell rätt att personuppgifter som avses i artikel 10 i dataskyddsförordningen får behandlas av myndigheter. Svenska myndigheter får alltså behandla sådana uppgifter. Det finns därför inte behov av författningsändringar när det gäller behandling av uppgifter om domar och lagöverträdelser.

Uppgifter om personnummer

Som framgår av avsnitt 8.2.6 har personnummer och samordningsnummer en särställning genom att medlemsstaterna har getts möjlighet att införa särskilda villkor för behandlingen (artikel 87 i dataskyddsförordningen), vilket också har skett genom 3 kap. 10 § dataskyddslagen. Behandling av sådana uppgifter får ske utan samtycke om det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl.

Det kommer sannolikt att förekomma personnummer i Arachne, även om födelsedatum kan förväntas vara den vanligaste formen av identifikationsuppgift inom EU. Utredningen bedömer att svenska myndigheters behandling av uppgifter om personnummer och samordningsnummer i regel ska anses som förenlig med kraven i 3 kap. 10 § dataskyddslagen. Det är dock den berörda myndigheten som har att bedöma behovet.

Det finns inte behov av författningsändringar när det gäller behandling av uppgifter om personnummer och samordningsnummer.

Personuppgiftsansvar

Begreppet personuppgiftsansvarig är centralt i dataskyddsregleringen och definieras som en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter (se också avsnitt 8.2.6).

Kommissionen är personuppgiftsansvarig för Arachne i den mening som avses i artikel 3.8 i dataskyddsförordningen för EU:s institutioner. Detta följer direkt av artikel 36.7 tredje stycket i budgetförordningen. Kommissionen pekas också ut som ansvarig för utveckling, förvaltning och övervakning av Arachne, för att säkerställa uppgifternas säkerhet och konfidentialitet samt autentisering av användarna och för att skydda it-systemet mot felaktig förvaltning och missbruk.

I beskrivningen av personuppgiftsbehandlingen för Arachne anges det inte vara aktuellt med ett gemensamt personuppgiftsansvar. Detta talar starkt för att endast kommissionen bestämmer ändamålen och medlen för behandlingen av personuppgifter i Arachne.

I frågor och svar om Arachne finns dock uttalanden som skapar viss osäkerhet i frågan. I en uppsättning frågor och svar besvaras frågan om kommissionen kommer att vara personuppgiftsansvarig för Arachne – eftersom kommissionen bestämmer ändamålen och medlen för RRF – med att kommissionen vid direkt förvaltning är ensamt personuppgiftsansvarig för uppgifter som avser RRF. Vidare anges att detta betyder att kommissionen bestämmer ändamålen och medlen för behandlingen av personuppgifter inom Arachne-ramverket. Det anges dock i samma svar att vid delad förvaltning kan – till skillnad från ovan – *både* kommissionen och medlemsstaterna agera som personuppgiftsansvariga, och dela på ansvaret att bestämma ändamålen och medlen för behandlingen (Arachne, FAQ on data protection and related issues, Status as of 10th July 2024, fråga 16).

Det kan också nämnas att en fråga huruvida kommissionen kommer att bli ägare av uppgifter som en nationell myndighet för in i Arachne besvaras nekande. Kommissionen anger i svaret att de nationella myndigheterna kommer att fortsätta vara ägare av sina uppgifter och att kommissionens ansvar inte går längre än till fördjupade analyser och berikning av uppgifter (Arachne, Frequently asked questions, version 2.3, den 19 augusti 2022, fråga 69). Som svar på

en efterföljande fråga uppger kommissionen att medlemsstaterna behåller ägandet av uppgifter som de har fört in i Arachne, och att det därför är upp till de nationella myndigheterna att ha rutiner för att hantera begäranden från enskilda gällande tillgång till och rättelse av uppgifter som delas i Arachne. Det anges dock därefter att på kommissionsnivå behandlas alla personuppgifter i enlighet med dataskyddsförordningen för EU:s institutioner och att alla begäranden från enskilda att få tillgång till och rättelse av personuppgifter hanteras i enlighet med den regleringen (fråga 70).

Frågan kan därför ställas om svenska myndigheter – trots vad som anges i budgetförordningen – kan anses som personuppgiftsansvariga avseende uppgifter som de kan komma att föra in i Arachne. Ovan nämnda något tvetydiga uttalanden förhåller sig inte till den gällande budgetförordningen. Europeiska datatillsynsmannen (EDPS, på engelska European Data Protection Supervisor) lämnade ett yttrande under förhandlingarna av den nu gällande budgetförordningen. EDPS välkomnade då att artikel 36.7 utsåg kommissionen som personuppgiftsansvarig för systemet. EDPS noterade dock att andra enheter kommer att använda och få tillgång till uppgifter inom ramen för sina uppdrag och bedömde det som sannolikt att dessa också skulle komma att agera som personuppgiftsansvariga. EDPS föreslog därför att rollerna för dem som ska använda och få tillgång till personuppgifter som behandlas av systemet skulle klargöras i förslaget (Opinion 14/2022, den 7 juli 2022).[11]

Utredningen har inte identifierat några bestämmelser i budgetförordningen i fråga om personuppgiftsansvar för andra än kommissionen. Några sådana klargöranden som EDPS efterfrågade verkar inte ha gjorts.

Utredningen anser att utgångspunkten i nuläget måste vara att kommissionen ska anses som personuppgiftsansvarig för uppgifter i Arachne, oavsett vem som har fört in uppgifterna i systemet. Det är kommissionen som närmast råder över ändamålen och medlen för Arachne. Då Arachne är under utveckling och stödjande dokumentation och rutiner behöver tas fram som gäller kommande versioner av Arachne, kan dock frågor om personuppgiftsansvar komma att klargöras framöver.

[11] https://www.edps.europa.eu/system/files/2022-07/22-07-07_financial-rules-applicable-to-general-budget-union_en.pdf. Hämtat 2025-10-29.

Oavsett om man är personuppgiftsansvarig eller inte ligger alltid ett ansvar hos den som behandlar personuppgifter att säkerställa behandlingens förenlighet med dataskyddsregelverket. Eftersom bland annat sökning och läsning utgör behandling av personuppgifter ansvarar de svenska myndigheter som bereds tillgång till uppgifter i databasen för sådan behandling som de utför.

Det finns inte behov av författningsändringar när det gäller personuppgiftsansvaret.

Enskildas rättigheter

Genom att dataskyddsförordningen och dataskyddsförordningen för EU:s institutioner gäller vid den personuppgiftsbehandling som sker i Arachne, gäller dessa författningars bestämmelser om enskildas rättigheter. Rätten till information är en av rättigheterna (artikel 13 och 14 i dataskyddsförordningen). Som framgår av avsnitt 8.2.6 har begränsningar av rättigheterna i dataskyddsförordningen införts i nationell rätt genom bestämmelser i 5 kap. dataskyddslagen, varigenom bland annat rätten att få tillgång till personuppgifter inte alltid gäller, till exempel om sekretess gäller för uppgifterna.

I Arachne-stadgan anges att kommissionen säkerställer transparens genom att följa villkoren om tillhandahållande av information och om enskildas rättigheter enligt artiklarna 15–24 i dataskyddsförordningen för EU:s institutioner. Det hänvisas också till att personuppgiftspolicyn för Arachne är publicerad på Arachnes hemsida (punkt 6.1). I Arachne-stadgan finns vidare uttalanden som riktar sig direkt till användare av Arachne. Myndigheterna måste informera mottagare om att deras uppgifter kommer att behandlas för att identifiera riskindikatorer. Informationen bör lämpligen lämnas som dataskyddsklausuler i tilldelningsbeslutet eller kontraktet. Det anges också att kommissionen har en webbsida som förklarar förfarandet och syftet med dataanalyser. Myndigheterna ska ha en länk till denna sida på sin egen webbsida (punkt 6.2).

Som nämns ovan riktar sig personuppgiftspolicyn för Arachne till dem vars personuppgifter behandlas och den ger information till enskilda om hur personuppgifter behandlas och hur deras rättigheter kan tillgodoses. Kommissionens webbsida om Arachne ger också information om den personuppgiftsbehandling som sker i Arachne.

Även om detta främst tar sikte på kommissionens personuppgiftsbehandling ger dokumentationen samtidigt upplysningar om den behandling som en användning av Arachne medför även när Arachne används av andra, till exempel av medlemsstaters myndigheter.

En annan rättighet är rätten till rättelse (artikel 16 i dataskyddsförordningen). Enligt beskrivningen av personuppgiftsbehandlingen för Arachne är medlemsstaterna huvudsakligen ansvariga för de data som medlemsstaterna själva tillhandahåller (punkt 7). Som framgår under föregående rubrik anser utredningen att det finns vissa oklarheter när det gäller hur långt ansvaret för svenska myndigheter sträcker sig när det gäller uppgifter som de för in i systemet. Svenska myndigheters ansvar kan enligt utredningens mening inte sträcka sig längre än vad som är möjligt att utöva utifrån att det är kommissionen som driver systemet. Enligt nämnda punkt i beskrivningen av personuppgiftsbehandlingen ska en registrerad som begär ändringar rörande sina uppgifter rikta sin begäran till medlemsstatens myndighet. Medlemsstaters myndigheter kan dock inte göra ändringar i Arachne, varken avseende uppgifter som de har fört in i systemet eller avseende riskvärderingar. Ändring av uppgifter kan dock ske genom att en myndighet sänder in uppgifter på nytt, vilka bearbetas av kommissionen en gång i veckan varefter ändringarna beaktas vid kommande riskvärderingar.

I avsnitt 8.5.2 beskrivs hur uppgifter från vissa databaser används för att berika uppgifter avseende interna data från medlemsstaterna. Dessa uppgifter från databaserna baseras enligt beskrivningen av personuppgiftsbehandlingen för Arachne på bland annat mottagares årsredovisningar. En begäran av rättelse av sådana uppgifter bör av den registrerade sändas till den organisation som ansvarar för mottagande av årsredovisningar. Sådan information uppdateras i Arachne-databasen var tredje månad och beaktas därefter i kommande riskvärderingar. Inte heller beträffande sådana uppgifter kan medlemsstater göra ändringar. Den registrerade kan också kontakta medlemsstatens myndigheter för att få rättelse av sådana uppgifter som har gjorts offentligt tillgängliga (punkt 7).

Ovan beskrivna rättelseförfaranden, även om det avser nu gällande Arachne-system och dess framtida funktion är oklar, påvisar enligt utredningen att svenska myndigheter kan utöva sitt ansvar i viss utsträckning, nämligen genom att verka för att uppgifter rättas – i nuläget genom att sända in korrekta uppgifter.

Utredningen har inte identifierat behov av ny reglering eller författningsändringar när det gäller enskildas rättigheter. Utredningen bedömer att befintlig EU-rättslig och nationell reglering är tillräcklig när det gäller enskildas rättigheter och möjligheterna att begränsa dessa.

Utlämnande till tredjeland

Enligt beskrivningen av personuppgiftsbehandlingen för Arachne – som avser den tidigare budgetförordningen – kan personuppgifter komma att överföras till tredjeland, då uppgifter kan överföras till Storbritannien (punkt 6). Denna överföring utförs inte av medlemsstaternas myndigheter utan av kommissionen, varför ansvaret för att överföringen är förenlig med dataskyddsregleringen ligger på kommissionen. Det kan dock nämnas att i beskrivningen av personuppgiftsbehandlingen anges också enligt vilka bestämmelser i dataskyddsförordningen för EU:s institutioner som överföringen är laglig.

Om en svensk myndighet avser att överföra uppgifter som den hämtar från Arachne till tredjeland ankommer det på myndigheten att bedöma om förutsättningarna enligt dataskyddsförordningen är uppfyllda, både när det gäller själva överföringen och den fortsatta behandling som överföringen innebär.

Särskilt om åtkomst, tillgång och behörigheter

Såväl budgetförordningen som Arachne-stadgan och andra relevanta källor anger villkor för åtkomsten till uppgifter.

Enligt artikel 36.7 andra stycket i budgetförordningen ska åtkomsten till de uppgifter som behandlas av Arachne överensstämma med tillämpliga dataskyddsregler, respektera principerna om nödvändighet och proportionalitet och begränsas till vissa aktörer. Det handlar bland annat om de unionsinstitutioner och organ som genomför budgeten, de medlemsstater som genomför budgeten inom ramen för delad förvaltning eller inom ramen för direkt förvaltning tillsammans med medlemsstaterna samt de personer eller enheter som genomför budgeten inom ramen för indirekt förvaltning. Vidare kan åtkomst ges till unionens utrednings-, kontroll- och revisionsorgan,

däribland Olaf, ECA och Eppo, inom ramen för utövandet av deras respektive befogenheter.

Uppgifter som är tillgängliga via Arachne ska enligt samma stycke göras tillgängliga för Europaparlamentet och rådet från fall till fall i den utsträckning som är nödvändig och står i proportion till utövandet av deras respektive befogenheter, i samband med förfarandet för beviljande av ansvarsfrihet för kommissionen.

Även Arachne-stadgan innehåller upplysningar om tillgången för EU-organ såsom Olaf, ECA och Eppo samt om uppgifter som kommissionen kan komma att ta del av. Kommissionen har tillgång till både gjorda riskvärderingar och företagens databaser. När det gäller myndigheter får rätt till åtkomst ges till den som är en del av förvaltnings- eller kontrollsystemet avseende ett program. Det är den lokala administratören som ska säkerställa att den som begär tillgång till systemet verkligen är en del av förvaltningen och kontrollen av det aktuella programmet. Av stadgan framgår också att kommissionen har rätt att dra tillbaka tillgången till Arachne för myndigheter om användarvillkoren inte följs (punkterna 5, 8, 10 och 13).

Av beskrivningen av personuppgiftsbehandlingen för Arachne framgår att varje användare av Arachne i medlemsländerna ska ha tillgång till uppgifter som rör företag och personer beträffande de program som de har fått tillgång till. Det framgår också att tillgång till personuppgifter ska ske på ”need-to-know basis” (punkt 5).

Enligt frågor och svar om Arachne har användare i andra medlemsstater i de flesta fall bara åtkomsträttigheter till program eller planer inom medlemsstaten. Viss information från andra medlemsstater är tillgänglig, till exempel när ett företag är involverat i flera projekt som genomförs i olika medlemsstater. En medlemsstat kan också välja att medge andra medlemsstater tillgång till uppgifter om egna program, vilket kan vara relevant till exempel gällande Interregprogrammen (Arachne, Frequently asked questions, version 2.3, den 19 augusti 2022, fråga 9).

Begränsningarna av ovan nämnda slag kan sägas tillgodose flera olika krav i dataskyddsförordningen, såsom principerna om ändamålsbegränsning och uppgiftsminimering (artikel 5), kraven på inbyggt dataskydd och dataskydd som standard (artikel 25) samt kravet på rättslig grund för de olika aktörer som behandlar personuppgifter vid en användning av Arachne (artikel 6). De har också betydelse

för de bedömningar som görs i den samlade integritetsanalysen, se kapitel 9.

Sammanfattning av utredningens slutsatser

Utredningens bedömningar ovan kan sammanfattas så att det inte finns hinder i dataskyddshänseende mot att berörda myndigheter utför en sådan personuppgiftsbehandling som en användning av Arachne förväntas innebära, samt att det inte finns skäl att föreslå några författningsändringar på dataskyddsområdet avseende sådan behandling.

Befintlig dataskyddsreglering är tillräcklig. Som en följd av detta ser inte utredningen skäl att föreslå reglering i en ny registerlag eller annan dataskyddslagstiftning för en ändamålsenlig personuppgiftsbehandling i denna del. Utredningens bedömning innebär också att det inte behövs ändringar i annan reglering än rörande dataskydd för att möjliggöra personuppgiftsbehandlingen.

Det bör observeras att utredningens bedömningar om förenligheten med dataskyddsregelverket inte kan avse behandlingen i det enskilda fallet. Det är den personuppgiftsansvarige som behöver säkerställa att den personuppgiftsbehandling som faktiskt utförs är förenlig med dataskyddsregleringen.

8.6 Användande av Edes som verktyg

8.6.1 Uppdraget i denna del

Den 1 januari 2028 blir det obligatoriskt att tillämpa Edes vid hantering av samtliga EU-stöd, förutom avseende RRF (se artikel 144.5 och 277 i budgetförordningen, se också avsnitt 6.2.8).

Utredningen har i uppdrag att utreda frågor som syftar till att säkerställa att svenska myndigheter har förutsättningar att använda Edes-databasen. Det handlar om att bedöma om mottagna eller tillgängliga uppgifter inom ramen för Edes kommer att utgöra allmänna handlingar i Sverige och i vilken mån uppgifterna omfattas av befintliga sekretessbestämmelser eller om det finns behov av nya sekretessbestämmelser för att säkerställa att uppgifterna får ett tillfredsställande skydd. Det handlar också om uppdraget att kartlägga det skydd

för personuppgifter som finns i Edes-databasen och utreda om det finns behov av nya eller ändrade bestämmelser för att möjliggöra den personuppgiftsbehandling som krävs för att uppfylla kraven inom ramen för Edes och att lämna nödvändiga författningsförslag. En kartläggning av skyddet för personuppgifter finns också i den samlade integritetsanalysen i kapitel 9.

Som framgår i avsnitt 6.2.9 bedömer utredningen att de skyldigheter och krav som hänför sig till utanordnare inte riktar sig mot medlemsländerna och därför saknar betydelse i detta betänkande. Inte heller bedömer utredningen att budgetförordningen medför några nya krav på att tillgängliggöra eller registrera uppgifter som ska användas i Edes. Att svenska myndigheter inte kommer att föra in uppgifter direkt i Edes innebär att det inte finns skäl att behandla utredningens uppdrag som gäller sekretesskydd för uppgifter som svenska myndigheter registrerar inom ramen för Edes, rättsliga förutsättningar för registrering av uppgifter eller behov av författningsändringar i dessa avseenden.

Det som är nytt och som blir obligatoriskt för svenska myndigheter är en skyldighet att kontrollera Edes-databasen innan stöd betalas ut, och att stöd inte ska betalas ut om det vid en sådan kontroll framkommer att det finns ett beslut om uteslutning beträffande den som söker medel. En sådan användning av Edes-databasen innebär en åtkomst till uppgifter, vilket i sig leder till vissa rättsliga frågor. Myndigheter kan också använda Edes-databasen på frivillig väg, vilket också medför åtkomst till uppgifter.

8.6.2 Blir uppgifterna i Edes allmänna handlingar hos svenska myndigheter?

Utredningens bedömning: Uppgifter i Edes kan bli allmänna handlingar hos de svenska myndigheter som använder systemet.

Skälen för utredningens bedömning

Blir uppgifter i Edes att betrakta som inkomna och förvarade hos svenska myndigheter genom direktåtkomst?

I avsnitt 8.5.2 redogörs för gällande rätt när det gäller allmänna handlingar och direktåtkomst. Enligt domstolspraxis är det avgörande vid bedömningen av om en teknisk lösning innebär en direktåtkomst om informationen är tillgänglig med tekniska hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas, avlyssnas eller på annat sätt uppfattas på det sätt som avses i 2 kap. 6 § TF. Om svenska myndigheter anses få tillgång till uppgifter genom direktåtkomst till en utländsk myndighets databas innebär det att uppgifterna skulle kunna anses vara förvarade hos den svenska myndigheten i tryckfrihetsförordningens mening.

Enligt utredningen talar mycket för att den tekniska utformningen av Edes kan innebära att svenska myndigheter anses få direktåtkomst till information genom systemet. Systemet synes nämligen vara utformat så – och det får antas gälla även framtida versioner – att informationen kommer vara tillgänglig för användaren för att på egen hand söka eller få svar på frågor. Vidare synes åtkomsten ge användaren en möjlighet att också hämta hem informationen till sitt eget system och bearbeta den där. Åtkomsten innebär också att uppgifter kan hämtas utan att kommissionen har kontroll över vilka uppgifter som hämtas. Ett kriterium som brukar anföras för att beskriva direktåtkomst är att mottagaren saknar möjlighet att själv kunna påverka innehållet, något som får anses gälla svenska myndigheters tillgång till Edes.

Det kan dock inte uteslutas att tillgången till uppgifter i Edes kan bedömas på annat sätt. Det finns vissa oklarheter när det gäller Edes som inte har kunnat klargöras under arbetet med denna utredning (se avsnitt 6.2.2). Utformningen av och funktionerna i Edes kan dessutom komma att förändras i framtiden.

Sammanfattningsvis bedömer utredningen att mycket talar för att det kan bli fråga om direktåtkomst till uppgifter i Edes. Bedömningarna i detta betänkande behöver därför ta höjd för att uppgifter i Edes kan anses vara allmänna handlingar utifrån 2 kap. 6 § TF.

Är biblioteksregeln tillämplig på uppgifterna i Edes?

Biblioteksregeln – som behandlas närmare i avsnitt 8.5.2 – omfattar handlingar som en myndighet använder på motsvarande sätt som böcker i ett bibliotek, det vill säga för att söka faktaunderlag i allmänhet, rättsfallsreferenser eller tidskriftsartiklar och liknande (jfr prop. 1990/91:60 s. 31). När det gäller referensdatabaser som producerats av enskilda organ, med vilka utländska myndigheter jämställs, har det inte ansetts rimligt att dessa skulle vara fria för insyn enligt offentlighetsprincipen (prop. 2001/02:70 s. 26). Det har alltså betydelse vilka slags uppgifter det är fråga om och hur uppgifterna används av myndigheterna.

Enligt utredningen är det tveksamt om uppgifterna i Edes är sådana att biblioteksregeln är tillämplig, även om det inte kan uteslutas.

Begränsningsregeln i 2 kap. 7 § TF kan innebära att sammanställningar inte anses förvarade hos en myndighet

Den så kallade begränsningsregeln i 2 kap. 7 § TF – som behandlas närmare i avsnitt 8.5.2 – innebär att en sammanställning inte anses vara förvarad hos en myndighet om sammanställningen innehåller personuppgifter och myndigheten enligt lag eller förordning saknar befogenhet att göra sammanställningen tillgänglig. Den bestämmelsen skulle kunna bli aktuell om någon av en myndighet begär ut en sammanställning av uppgifter ur Edes som innebär att myndigheten måste söka efter ett urval av personer som exempelvis har en viss politisk åsikt. Om sådana sökningar är möjliga och en dylik begäran inkommer är det upp till myndigheten att bedöma om bestämmelsen är tillämplig.

Sammanfattande slutsatser

Utgångspunkten bör enligt utredningens mening vara att uppgifter i Edes kan anses förvarade hos och därmed bli allmänna handlingar hos de svenska myndigheter som använder Edes. Det bedöms inte vara troligt men kan inte uteslutas att uppgifter som finns i Edes kan komma att omfattas av biblioteksregeln och därmed inte anses utgöra allmänna handlingar. Den så kallade begränsningsregeln kan

också bli aktuell när det gäller sammanställningar som myndigheten saknar befogenhet att göra tillgängliga, med följden att sådana sammanställningar inte anses vara förvarade hos myndigheten. Det är utlämnande myndighet som har att göra bedömningen i en utlämnandesituation.

8.6.3 Finns det behov av sekretesskydd för uppgifter som finns i Edes?

Utredningens bedömning: Det kan finnas behov av sekretesskydd för uppgifter som svenska myndigheter får tillgång till vid ett användande av Edes. Det kommer inte i någon större utsträckning finnas behov av sekretess till skydd för rikets säkerhet eller dess förhållande till andra stater eller mellanfolkliga organisationer. De behov som har identifierats är främst följande.

- Behov att kunna hemlighålla uppgifter för att myndigheternas arbete med kontroller och granskning inte ska motverkas
- Behov att kunna hemlighålla uppgift om en enskilds affärs- eller driftförhållanden med mera i tillsynsverksamhet och liknande
- Behov att kunna hemlighålla uppgifter om personliga förhållanden, särskilt för förföljda personer.

Skälen för utredningens bedömning

Inledning

Som framgår ovan bedömer utredningen att skyldigheten för svenska myndigheter att använda Edes enligt budgetförordningen inte omfattar någon skyldighet att lämna uppgifter som ska tillföras Edesdatabasen. Det ligger därför utanför utredningens uppdrag att bedöma behovet av sekretess när det gäller den skyldighet som svenska myndigheter kan ha enligt sektorsspecifika regler att lämna uppgifter som eventuellt tillförs Edes (jfr avsnitt 4.6 och 6.2.6).

Behovet av sekretess behöver dock bedömas när det gäller svenska myndigheters tillgång till uppgifter i Edes. Som konstateras i föregå-

ende avsnitt kan uppgifter i Edes komma att bli allmänna handlingar hos de myndigheter som använder systemet. Om det inte finns någon tillämplig sekretessbestämmelse kommer därför svenska myndigheter vara skyldiga att på begäran lämna ut uppgifterna. I detta avsnitt behandlas frågan om huruvida det finns behov av sekretessskydd för dessa uppgifter.

Vilken ledning kan dras av budgetförordningen och andra relevanta källor?

Budgetförordningen innehåller inte några bestämmelser som tar direkt sikte på frågor om offentlighet och sekretess vid enheter som deltar i genomförandet av budgeten för uppgifter som finns i Edes. Vissa bestämmelser finns som kan sägas ge uttryck för att uppgifter som rör Edes bör behandlas med försiktighet, men det synes då främst ta sikte på kommissionens åtgärder att tillhandahålla information som en del av sin årsrapport till Europaparlamentet (artikel 144.6 andra stycket) och på publicering av uppgifter på kommissionens webbplats (artikel 142.2). Dessa bestämmelser bedöms alltså inte rikta sig till medlemsstaterna eller deras myndigheter.

Som utvecklas i avsnitt 8.5.3 ger budgetförordningen i stället på flera ställen uttryck för nödvändigheten av transparens i arbetet med att genomföra EU:s budget. Budgetförordningen innehåller regler som tar sikte på dataskydd och vem som ska få åtkomst till uppgifterna. Att uppgifter i Edes ska behandlas i enlighet med rätten till integritet och övriga rättigheter som fastställs i dataskyddsförordningen för EU:s institutioner framgår av artikel 144.1 första stycket i budgetförordningen.

Enligt artikel 144.5 första stycket ska alla personer och enheter som deltar i genomförandet av budgeten i enlighet med artikel 62 av kommissionen beviljas tillgång till uppgifterna om beslut om uteslutning enligt artikel 138. Som utvecklas i avsnitt 6.2.7 bedömer utredningen att svenska myndigheters tillgång till uppgifter i Edesdatabasen kan vara begränsad till uppgifter om uteslutning på vissa grunder.

I *personuppgiftspolicyn för Edes* (som nämns i avsnitt 6.2.6) finns det skrivningar om krav på konfidentialitet som träffar bland andra externa experter knutna till kommissionen som deltar i utveckling och underhåll av Edes. Av skrivningarna framgår att sådana aktörer

är bundna av skyldigheter som rör konfidentialitet med mera. Några liknande skrivningar om att mottagare av uppgifter från Edes är bundna av skyldigheter som rör konfidentialitet finns inte beträffande den tillgång till uppgifter som medlemsstater har.

Personuppgiftspolicyn för Edes innehåller också information om till vilka aktörer och under vilka förutsättningar som kommissionen överför personuppgifter till vissa mottagare i tredjeländer eller till internationella organisationer. Det anges att uppgifter överförs baserat på särskilda bestämmelser i överenskommelser med mera. Det anges också att informationen som kommissionen samlar in inte ska lämnas till någon tredje part, om det inte finns någon rättslig skyldighet att göra detta. Denna sistnämnda skrivning nämns särskilt i utredningens direktiv i samband med uppdraget att utreda om det finns behov av skydd för uppgifter vid användning av Edes. Utredningen uppfattar att denna skrivning i personuppgiftspolicyn för Edes tar sikte på att kommissionen beskriver att de inte lämnar ifrån sig uppgifter i Edes annat än när det finns en rättslig skyldighet att göra det, och att skrivningen inte i sig innebär några skyldigheter för eller förväntningar på nationella myndigheter i medlemsstaterna att hantera uppgifter på ett särskilt sätt eller att säkerställa något särskilt skydd för uppgifterna.

Utredningen har frågat Edes-teamet vid kommissionen om medlemsstater eller deras myndigheter får eller kommer att få tillgång till uppgifter genom Edes som behöver hållas hemliga, men inte fått några klargörande svar.[12]

Sammantaget konstaterar utredningen att såväl budgetförordningen som personuppgiftspolicyn för Edes innehåller skrivningar som kan sägas ge uttryck för att uppgifter i Edes bör behandlas med försiktighet, men att de inte utgör några konkreta bestämmelser eller skrivningar om att vissa uppgifter ska kunna beläggas med sekretess.

Utredningens överväganden och slutsatser

Svenska myndigheter kommer genom Edes-databasen att få tillgång till uppgifter om fall som avser uteslutning. Se avsnitt 6.2.6 för en närmare beskrivning av vilka uppgifter som kan finnas i Edes. Det kan inte uteslutas att det i Edes kan förekomma uppgifter där det

[12] Komm2025/00388-7 och Komm2025/00388-8.

finns ett behov av sekretess. Enligt utredningen kan det främst finnas behov av sekretesskydd i följande avseenden, vilka kort utvecklas nedan.

- Behov att kunna hemlighålla uppgifter för att myndigheternas arbete med kontroller och granskning inte ska motverkas
- Behov att kunna hemlighålla uppgift om en enskilds affärs- eller driftförhållanden med mera i tillsynsverksamhet och liknande
- Behov att kunna hemlighålla uppgifter om personliga förhållanden, särskilt för förföljda personer.

Det kan finnas behov av sekretess för uppgifter i Edes till skydd för *allmänna intressen*. Beträffande Edes har utredningen inte identifierat något tydligt behov av sekretess för att Sveriges möjlighet att delta i samarbetet inom EU inte ska försämras. Även om det i budgetförordningen och personuppgiftspolicyn för Edes förekommer generella skrivningar om att uppgifter i Edes ska hanteras med omsorg har det inte getts uttryck för något tydligt önskemål om sekretess hos medlemsstater som genomför budgeten beträffande några uppgifter i Edes. Ett sådant behov av sekretess kan dock inte helt uteslutas, eftersom det från EU:s sida ändå på olika sätt har getts uttryck för att uppgifter i Edes bör hanteras på ett omsorgsfullt sätt.

Ett behov av sekretesskydd i det allmännas intresse skulle kunna ta sikte på exempelvis uppgifter om projekt som har betydelse för Sveriges tillgång till livsmedel under kris- och krigstider och annat som rör Sveriges försvarsförmåga.

Det kan också finnas behov att sekretessbelägga uppgifter för att *myndigheternas arbete med kontroller och granskning* inte ska motverkas. I sammanhanget kan erinras om att information ska undantas från offentliggörande på kommissionens webbsida om det är nödvändigt att bevara konfidentialiteten i en utredning eller i nationella rättsliga förfaranden (artikel 142.2 i budgetförordningen).

Det kan också finnas behov av sekretess till skydd för uppgift om *enskildas ekonomiska förhållanden*. Det kan inte uteslutas att uppgifter om enskildas *affärs- eller driftförhållanden* kan ingå bland de uppgifter som svenska myndigheter får tillgång till genom Edes. Det kan handla exempelvis om avtal och affärshemligheter. Det skulle även kunna förekomma uppgifter om total projektkostnad, vilka skulle kunna vara skyddsvärda för näringsidkare i vissa fall. I vilken

utsträckning sådana uppgifter kan förekomma i Edes bedöms vara oklart. I allmänhet bör uppgifterna där – till exempel om grunderna för beslut om uteslutning – kunna utformas på ett sätt så att sådana uppgifter inte röjs.

Det kan inte heller uteslutas att det kan finnas behov av sekretessskydd för *enskildas personliga förhållanden*. Edes kan innehålla uppgifter om bland andra stödmottagare och personer i ledningen för ett företag. Uppgifterna i Edes kan röra exempelvis namn, adress och identifikationsnummer. Risken för att svenska myndigheter får tillgång till skyddsvärd information av detta slag genom Edes bedöms vara begränsad. Behov av sekretess kan dock finnas även för sådana i regel harmlösa uppgifter för *förföljda personer*.

Det kan inte uteslutas att det kan finnas behov av skydd för uppgifter även om andra personliga förhållanden, exempelvis om det finns en risk att personuppgifter *behandlas i strid mot personuppgiftsregelverket* efter ett eventuellt utlämnande. I detta sammanhang kan särskilt nämnas uppgifter om brott och överträdelser (jfr artikel 10 i dataskyddsförordningen).

Det kan slutligen konstateras att det – bland annat eftersom systemet kan komma att förändras – kan vara svårt att förutse vilka uppgifter som kommer att finnas i Edes och därmed vilka ytterligare behov av sekretesskydd som kan uppstå.

8.6.4 Vilket skydd ger gällande sekretessreglering för allmänna intressen?

Utredningens bedömning: För det fall att uppgifter i Edes skulle aktualisera behov av sekretess till skydd för rikets säkerhet eller dess förhållande till andra stater eller mellanfolkliga organisationer är gällande sekretessbestämmelser tillräckliga.

När det gäller behov av sekretess till skydd främst för myndigheters verksamhet för inspektion, kontroll eller annan tillsyn är gällande sekretessbestämmelser tillräckliga.

Skälen för utredningens bedömning

Utrikessekretess – 15 kap. 1 § OSL

Utredningen har inte identifierat något behov av att sekretessbelägga uppgifter för att Sveriges förbindelser med annan stat eller mellanfolklig organisation inte ska störas. Om ett sådant behov skulle uppstå kan det finnas utrymme att sekretessbelägga uppgiften enligt 15 kap. 1 § OSL om utrikessekretess.

Sekretess i det internationella samarbetet – 15 kap. 1 a § OSL

Utredningen har inte identifierat något tydligt behov av sekretess för att Sveriges möjlighet att delta i samarbetet kring Edes inte ska försämras om uppgifter röjs. Om ett sådant behov skulle uppstå kan det finnas utrymme att använda 15 kap. 1 a § OSL.

Enligt 15 kap. 1 a § OSL gäller sekretess 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.

Från och med den 1 januari 2028 blir det obligatoriskt att använda Edes inom ramen för samtliga förvaltningsformer. Svenska myndigheters tillgång till uppgifterna i Edes kommer då att ske på grund av budgetförordningen, som är en bindande EU-rättsakt. Det kriteriet i paragrafen är alltså uppfyllt.

Budgetförordningen innehåller inte någon bestämmelse om sekretess för uppgifter i Edes, något som inte heller krävs enligt ordalydelsen i 15 kap. 1 a § OSL. På motsvarande sätt som beskrivs beträffande Arachne (se avsnitt 8.5.4) kan det argumenteras för att 15 kap. 1 a § är tillämplig, trots att det inte finns någon bestämmelse om sekretess. Det skulle då vara möjligt att belägga uppgifter i Edes med sekretess om det skulle kunna antas att Sveriges möjlighet att delta i det internationella samarbetet kring Edes försämras om uppgiften röjs. Det kan sägas att det i budgetförordningen förutsätts ett internationellt samarbete mellan medlemsländerna och kommissionen när det gäller Edes.

Det är dock också möjligt att göra en annan bedömning i denna fråga. Det anges i förarbetena att – även om det inte utesluts av dess ordalydelse – bestämmelsen normalt aktualiseras bara i situationer då avtalet eller EU-rättsakten innehåller en tydlig sekretessbestämmelse (prop. 2012/13:192 s. 35).

Det är alltså inte säkert att några uppgifter kan beläggas med sekretess enligt 15 kap. 1 a § OSL. Under alla förhållanden måste det göras en bedömning i det enskilda fallet om det kan antas att Sveriges möjlighet att delta i det internationella samarbete som avses i rättsakten försämras om uppgiften röjs. Som nämns har dock utredningen inte heller identifierat något tydligt behov av att sekretessbelägga uppgifter i det syftet.

Utrikessekretess vid direktåtkomst – 15 kap. 1 b § OSL

Det gäller absolut sekretess för uppgifter som en myndighet har elektronisk tillgång till i en upptagning för automatiserad behandling hos en annan stat eller mellanfolklig organisation, om myndigheten inte får behandla uppgiften enligt en bindande EU-rättsakt eller ett av Sverige eller EU ingånget avtal med en annan stat eller mellanfolklig organisation. Det följer av 15 kap. 1 b § OSL, som behandlas närmare i avsnitt 8.5.4.

För att bestämmelsen ska vara tillämplig på Edes krävs att det finns ändamålsbegränsningar, sökbegränsningar eller liknande i en bindande EU-rättsakt eller ett av Sverige eller EU ingånget avtal. Budgetförordningen är en bindande rättsakt. Svenska myndigheters tillgång till uppgifter bedöms vara begränsad till beslut om uteslutning på vissa grunder (se vidare avsnitt 6.2.7). Även om det framstår som naturligt att Edes kommer att innehålla tekniska sökbegränsningar som innebär att användare inte får tillgång till annat än vad de har rätt att få del av är det oklart exakt hur sökbegränsningarna ser ut och kommer att se ut i Edes och i vilken mån det kommer att vara möjligt för svenska myndigheter att få tillgång till uppgifter som de inte har rätt att behandla. Om så skulle vara fallet skulle 15 kap. 1 b § OSL möjligen kunna tillämpas på de uppgifter som omfattas av gällande åtkomstbegränsningar.

Försvarssekretess – 15 kap. 2 § OSL

En särskild fråga är om svenska myndigheter genom Edes skulle få tillgång till uppgifter som det finns anledning att hemlighålla för att skydda försvarsintressen. I 15 kap. 2 § OSL regleras försvarssekretessen, som behandlas i avsnitt 8.5.4.

Bland de uppgifter som kan finnas i Edes finns grunderna för beslut om uteslutning. Det är oklart för utredningen exakt vilka uppgifter som därvid kommer att vara tillgängliga för svenska myndigheter. I förhållandena bakom ett stödprojekt kan det finnas information som omfattas av försvarssekretess enligt 15 kap. 2 § OSL. Utredningen bedömer att grunderna för en uteslutning i allmänhet bör kunna anges på ett sådant sätt att försvarshemligheter inte röjs. Det framstår mot den bakgrunden inte som sannolikt att det i Edes kommer att finnas uppgifter som omfattas av bestämmelsen. Skulle sådana uppgifter ändå finnas i Edes kan de sekretessbeläggas enligt 15 kap. 2 § OSL, om skaderekvisitet anses vara uppfyllt i det enskilda fallet.

Förberedelser för inspektion, revision eller annan granskning – 17 kap. 1 § OSL

De uppgifter som en svensk myndighet tar del av genom Edes skulle kunna vara av betydelse exempelvis inom ramen för förberedelser inför en granskning som tar sikte på återbetalning av felaktigt utbetalat stöd. Det bör i sådana situationer kunna finnas utrymme att sekretessbelägga uppgifterna enligt 17 kap. 1 § OSL (som behandlas närmare i avsnitt 8.5.4), om syftet med granskningsverksamheten motverkas om uppgiften röjs.

Dataanalyser och urval för att förebygga, förhindra och upptäcka felaktiga utbetalningar – 17 kap. 1 b § OSL

Enligt sekretessbestämmelsen i 17 kap. 1 b § OSL gäller sekretess för uppgift om metoder, modeller och riskfaktorer som hänför sig till dataanalyser och urval för att förebygga, förhindra och upptäcka felaktiga utbetalningar, om det kan antas att det allmännas syfte med verksamheten motverkas om uppgiften röjs. Den behandlas närmare i avsnitt 8.5.4. Enligt utredningen kommer de uppgifter som erhålls

genom Edes i allmänhet inte att avse sådana metoder, modeller och riskfaktorer som avses i bestämmelsen och den bedöms därför inte vara relevant när det gäller Edes.

Sammanfattande överväganden och slutsatser

Som utvecklas ovan bedömer utredningen att det inte i någon större utsträckning kommer att finnas uppgifter som behöver sekretessbeläggas med anledning av intresset av skydd för rikets säkerhet eller dess förhållande till andra stater eller mellanfolkliga organisationer. I den mån sådana uppgifter förekommer i Edes bedöms gällande sekretessbestämmelser vara tillräckliga.

När det gäller behov av sekretess till skydd främst för myndigheters verksamhet för inspektion, kontroll eller annan tillsyn bedömer utredningen att gällande sekretessbestämmelser är tillräckliga.

8.6.5 Vilket skydd ger gällande sekretessreglering för enskildas personliga och ekonomiska förhållanden?

Utredningens bedömning: De behov som utredningen har identifierat när det gäller sekretess till skydd för enskildas personliga och ekonomiska intressen kan tillgodoses genom gällande sekretessbestämmelser.

Uppgifter om enskildas affärs- eller driftförhållanden vid tillsyn, stödverksamhet och liknande har ett tillräckligt skydd genom 30 kap. 23 § OSL.

Skyddet för förföljda personer har ett tillräckligt skydd genom 21 kap. 3 § OSL. Därtill ger 21 kap. 7 § OSL ett skydd i de fall det kan antas att en uppgift efter ett utlämnande kommer att behandlas i strid med dataskyddsregelverket.

Skälen för utredningens bedömning

Uppgift om enskilds affärs- eller driftförhållanden vid tillsyn, stödverksamhet och liknande – 30 kap. 23 § OSL

Det kan inte uteslutas att uppgifter om enskildas affärs- eller driftförhållanden kan ingå bland de uppgifter som svenska myndigheter får tillgång till genom Edes. Det kan handla exempelvis om avtal och affärshemligheter. För det fall att sådana uppgifter i undantagsfall skulle förekomma omfattas de av tillämpningsområdet för 30 kap. 23 § OSL (se vidare avsnitt 8.5.5).

För att en uppgift ska kunna beläggas med sekretess krävs vidare att skaderekvisitet är uppfyllt, vilket är fallet om det kan antas att den enskilde lider skada om uppgiften röjs.

Behovet av sekretess till skydd för enskild i verksamhet som avser tillsyn med mera i fråga om näringslivet bedöms vara tillräckligt tillgodosett genom 30 kap. 23 § OSL.

Sekretess till skydd för förföljda personer

I Edes kan det förekomma uppgifter om adress och andra kontaktuppgifter rörande fysiska personer. Enligt 21 kap. 3 § första stycket OSL gäller sekretess för uppgift om enskilds bostadsadress eller annan jämförbar uppgift som kan lämna upplysning om var den enskilde bor stadigvarande eller tillfälligt, den enskildes telefonnummer, e-postadress eller annan jämförbar uppgift som kan användas för att komma i kontakt med denne. Enligt bestämmelsens skaderekvisit krävs att det av särskild anledning kan antas att den enskilde eller någon närstående till denne kan komma att utsättas för hot eller våld eller lida annat allvarligt men om uppgiften röjs. Utredningen anser att 21 kap. 3 § första stycket OSL innebär ett tillräckligt skydd för förföljda personer för uppgifter om adress och liknande.

Behovet av sekretess till skydd för uppgift om enskilds personliga förhållanden när det gäller förföljda personer bedöms vara tillgodosett genom gällande reglering.

Behandling i strid med dataskyddsregleringen

Sekretess enligt 21 kap. 7 § OSL skulle kunna aktualiseras om det kan antas att uppgifter i Edes efter ett utlämnande kommer att behandlas i strid med dataskyddsregelverket. Bestämmelsen innebär att även om en uppgift inte omfattas av sekretess enligt någon annan bestämmelse i offentlighets- och sekretesslagen, omfattas den av sekretess om det kan antas att den efter ett utlämnande kommer att behandlas i strid med till exempel dataskyddsförordningen eller dataskyddslagen. Bestämmelsen behandlas närmare i avsnitt 7.1.7 och 8.5.5.

Om det kan antas att de krav som gäller för att personuppgifter i Edes ska få behandlas inte följs efter det att personuppgiften har lämnats ut, till exempel avseende för vilka ändamål som uppgifterna får behandlas, omfattas uppgiften av sekretess och ska inte lämnas ut. Denna bestämmelse skulle således enligt utredningen kunna aktualiseras i vissa fall.

Utredningens överväganden om behov av åtgärder på dataskyddsområdet för ett användande av Edes behandlas i avsnitt 8.6.7.

Sammanfattande överväganden och slutsatser

De behov som utredningen har identifierat när det gäller sekretess till skydd för enskildas personliga och ekonomiska intressen bedöms kunna tillgodoses genom gällande sekretessbestämmelser. Uppgifter om enskildas affärs- eller driftförhållanden vid tillsyn, stödverksamhet och liknande bedöms ha ett tillräckligt skydd genom 30 kap. 23 § OSL. Skyddet för förföljda personer bedöms vara tillräckligt genom 21 kap. 3 § OSL. Därtill ger 21 kap. 7 § OSL ett skydd i de fall det kan antas att en uppgift efter ett utlämnande kommer att behandlas i strid med dataskyddsregelverket. Gällande sekretessbestämmelser bedöms ge ett tillräckligt skydd för uppgifter som svenska myndigheter kan få tillgång till genom Edes.

8.6.6 Det krävs inte författningsändringar på sekretessområdet för användande av Edes

Utredningens bedömning: Det finns inte behov av någon ny sekretessreglering med anledning av svenska myndigheters användande av Edes.

Skälen för utredningens bedömning: Som framgår ovan bedömer utredningen att befintlig sekretessreglering är tillräcklig för att tillgodose identifierade sekretessbehov när det gäller uppgifter som svenska myndigheter kan komma att få tillgång till genom Edes. Det kan inte uteslutas att det i Edes kan förekomma uppgifter som inte skyddas av sekretess. Det kan handla om uppgifter som omfattas av befintliga sekretessbestämmelsers tillämpningsområde men där en prövning av tillämplig bestämmelses skaderekvisit i det enskilda fallet inte leder till att en uppgift kan hemlighållas. Att sådana uppgifter ska lämnas ut beror då på intresseavvägningar som lagstiftaren redan har gjort mellan behovet av sekretess och insynsintresset. Inte heller det förhållandet att det kan finnas en risk för att det kommer att uppstå behov av sekretesskydd som inte har kunnat förutses kan enligt utredningen motivera att ny sekretessreglering införs. För att det ska vara motiverat att göra undantag från det grundlagsskyddade insynsintresset bör det krävas mer konkreta risker för olägenheter om uppgifter röjs.

Sammanfattningsvis gör utredningen bedömningen att det inte krävs någon ny sekretessreglering för att svenska myndigheter ska kunna använda Edes.

8.6.7 Det krävs inte författningsändringar på dataskyddsområdet för användande av Edes

Utredningens bedömning: Svenska myndigheters användning av Edes-databasen kräver inga författningsändringar på dataskyddsområdet.

Skälen för utredningens bedömning

Inledning

I avsnitt 7.2 redogör utredningen för gällande rätt på dataskyddsområdet, bland annat för kravet på rättslig grund och de grundläggande principerna för att en personuppgiftsbehandling ska vara laglig.

I detta avsnitt gör utredningen bedömningar av om befintligt dataskyddsregelverk är tillräckligt för den personuppgiftsbehandling som kommer att aktualiseras vid en användning av Edes eller om det krävs författningsändringar. Härvid lyfts vissa dataskyddsrättsliga frågor särskilt. Vidare görs i detta avsnitt delvis en kartläggning av skyddet för personuppgifter i Edes-databasen. Skyddet för personuppgifter behandlas också i den samlade integritetsanalysen i kapitel 9.

Budgetförordningens reglering om dataskydd som rör Edes och andra relevanta källor

Det finns flera bestämmelser i budgetförordningen om Edes som avser skyddet för personuppgifter. Dessa tar inte sikte på medlemsstaters eller deras myndigheters behandling av personuppgifter, då det är kommissionen som för in uppgifter i Edes-databasen och driver systemet. Enligt artikel 144.1 första stycket ska uppgifter som utbyts inom ramen för Edes och som centraliseras i databasen som inrättats av kommissionen behandlas i enlighet med rätten till integritet och övriga rättigheter som fastställs i dataskyddsförordningen för EU:s institutioner.

I det register över personuppgiftsbehandling som EU:s dataskyddsombud för finns en beskrivning av personuppgiftsbehand-

lingen för Edes[13]. I denna beskrivs ändamålen med behandlingen, hur och vilka personuppgifter som behandlas, längsta tid för behandling, vilka som får tillgång till uppgifter, säkerhetsåtgärder och information till enskilda om deras rättigheter.

Personuppgiftspolicyn för Edes innehåller beskrivningar av varför och hur kommissionen behandlar personuppgifter, vilken rättslig grund som behandlingen vilar på, vilka personuppgifter som kommissionen samlar in och behandlar vidare, hur länge kommissionen lagrar personuppgifterna och skyddar dem samt vilka som har tillgång till uppgifterna. Det finns också beskrivningar av den enskildes rättigheter och hur dessa kan utövas, samt hänvisningar till var mer information kan hittas.

Kommissionen har också en webbsida för Edes.[14]

Rättslig grund för behandlingen

Den 1 januari 2028 blir det obligatoriskt att tillämpa Edes vid hantering av samtliga EU-stöd, förutom avseende RRF. Utredningen bedömer att det för de myndigheter som omfattas av skyldigheten att verkställa beslut om uteslutning kommer att finnas rättslig grund för nu aktuell personuppgiftsbehandling enligt grunden *fullgöra en rättslig förpliktelse* (artikel 6.1 c i dataskyddsförordningen och 2 kap. 1 § dataskyddslagen). För att kunna kontrollera om det finns beslut om uteslutning behöver berörda myndigheter konsultera databasen. En sökning på till exempel den stödsökande kan ge en träff som innehåller personuppgifter. Den stödsökande kan också vara en enskild firma. Enligt utredningens mening innebär detta att det är nödvändigt att behandla personuppgifter.

Även den rättsliga grunden att *utföra en uppgift av allmänt intresse* (artikel 6.1 e i dataskyddsförordningen och 2 kap. 2 § dataskyddslagen) kommer enligt utredningens mening att vara tillämplig. Edesdatabasen kan komma att användas av svenska myndigheter både enligt skyldigheter och på frivillig väg, men i båda fallen med grund i budgetförordningen. Utredningen bedömer på samma grunder som

[13] Record for processing of personal data, Title: Entry of a Data Subject in the Early Detection and Exclusion System (EDES-DB), Reference DPR-EC-04410.2, publicerad den 8 februari 2022. https://ec.europa.eu/dpo-register/detail/DPR-EC-04410. Hämtat 2025-10-29.
[14] https://commission.europa.eu/strategy-and-policy/eu-budget/how-it-works/annual-lifecycle/implementation/anti-fraud-measures/edes_sv. Hämtat 2025-11-02.

framgår av avsnitt 8.2.6 och 8.5.8 att berörda myndigheters användning av Edes-databasen rör sig om ett allmänt intresse och att den personuppgiftsbehandling som den kan medföra som utgångspunkt är att anse som nödvändig.

Utredningen bedömer att de rättsliga grunderna kan uppfylla kraven på tydlighet och precision samt på en förutsebar tillämpning för de personer som omfattas av dem. Utredningen utgår också från att unionsrätten är förenlig med Europakonventionen och uppfyller kravet på proportionalitet i artikel 6.3 i dataskyddsförordningen. För en samlad integritetsanalys, se kapitel 9.

Att det finns rättslig grund för den förväntade personuppgiftsbehandlingen innebär att det inte genom författning behöver skapas några nya rättsliga grunder.

Principerna i artikel 5 i dataskyddsförordningen

I avsnitt 7.2.5 redogör utredningen för principerna i artikel 5.1 i dataskyddsförordningen och för att det är den personuppgiftsansvarige som ska säkerställa att principerna efterlevs. Utredningen gör så långt det är möjligt bedömningar avseende möjligheten att efterleva principerna.

På samma grunder som anges i avsnitt 8.2.6 utgår utredningen från att de myndigheter som kommer att behandla personuppgifter uppfyller principen om laglighet, korrekthet och öppenhet, principen om integritet och konfidentialitet samt principen om riktighet. Även om det här är fråga om svenska myndigheters ansvar att efterleva principerna i artikel 5 i dataskyddsförordningen och budgetförordningen och andra relevanta källor i flera delar avser kommissionens ansvar, kan källorna ändå ge svenska myndigheter viss vägledning i fråga om principerna. Vad gäller sistnämnda princip anges i budgetförordningen att om några uppgifter har rättats, utplånats eller ändrats ska uppgifterna i Edes-databasen uppdateras, där så är lämpligt (artikel 144.1 fjärde stycket).

Vad gäller principen om ändamålsbegränsning framgår ändamålet med en användning av Edes av till exempel artikel 137.1 i budgetförordningen. Detta är en generell beskrivning och avser inte specifikt personuppgiftsbehandling eller användningen av databasen. Syftet med systemet är att göra det lättare att

- tidigt upptäcka personer eller enheter som är ett hot mot unionens ekonomiska intressen,
- utesluta personer eller enheter som befinner sig i en uteslutningssituation från att ta del av EU-medel,
- ålägga ekonomiska sanktioner mot mottagare av EU-medel.

När det gäller ändamålet med Edes-databasen finns en beskrivning i skäl 132: Information om tidig upptäckt av risker och om beslut om uteslutning och åläggande av ekonomiska sanktioner för en person eller enhet bör sammanföras centralt och för detta ändamål bör tillhörande uppgifter lagras i en databas som inrättas och drivs av kommissionen som ägare av det centraliserade systemet.

Även personuppgiftspolicyn för Edes och beskrivningen av personuppgiftsbehandlingen beskriver ändamålen med behandlingen av personuppgifter i Edes.

När det gäller principerna om uppgifts- och lagringsminimering framgår av budgetförordningen i stor utsträckning vilka uppgifter som Edes ska innehålla och i viss mån också hur länge som uppgifter ska behandlas. Då det är kommissionen som driver Edes-databasen och svenska myndigheter inte för in uppgifter direkt i databasen, råder inte svenska myndigheter över dess innehåll. Utgångspunkten bör dock enligt utredningens mening vara att de uppgifter som finns i Edes-databasen motsvaras av vad som behövs för att Edes ska kunna fungera på ett ändamålsenligt sätt.

När det gäller längsta tid för behandling finns i artikel 144.4 tredje stycket reglerade lagringstider för uppgifter avseende vissa situationer. När det gäller uppgifter om tidig upptäckt som lämnas i enlighet med artikel 144.3 får lagringstiden inte överstiga ett år. Om den behöriga utanordnaren under den perioden begär att panelen ska utfärda en rekommendation i ett fall som avser uteslutning eller ekonomiska sanktioner får lagringstiden förlängas fram till dess att den behöriga utanordnaren har fattat ett beslut. Även i beskrivningen av personuppgiftsbehandlingen och personuppgiftspolicyn för Edes finns närmare angivelser om längsta tid för behandling av uppgifter. Det finns således anvisningar som rör lagringsminimering.

Det ovanstående innebär att den reglering som finns bedöms vara tillräcklig och att det inte finns skäl att överväga några författnings-

ändringar som tar sikte på att uppfylla principerna i artikel 5 i dataskyddsförordningen.

Känsliga personuppgifter

I avsnitt 6.2.6 beskrivs vilka slags uppgifter som Edes-databasen kan innehålla och som svenska myndigheter kan förväntas få del av. Av beskrivningen framkommer inte något som kan anses som känsliga personuppgifter. I beskrivningen av personuppgiftsbehandlingen för Edes, som utgår från regleringen om Edes enligt den tidigare budgetförordningen, anges det inte vara aktuellt med känsliga personuppgifter.

För det fall det ändå skulle bli aktuellt att behandla känsliga personuppgifter inom ramen för Edes kan det erinras om att det finns undantag från förbudet mot behandling av sådana uppgifter. I avsnitt 8.2.6 beskriver utredningen närmare de tre undantagssituationerna i 3 kap. 3 § första stycket dataskyddslagen, som tar sikte på behandling som är nödvändig med hänsyn till ett *viktigt allmänt intresse*.

En första fråga är om undantagssituationen som avser att uppgifterna har lämnats till myndigheten och behandlingen krävs enligt lag kan bli aktuell vid ett användande av Edes. I aktuella fall kommer berörd myndighet att ta del av uppgifter genom att konsultera en databas som ägs av kommissionen. Utredningen gör bedömningen att detta bör likställas med att uppgifter lämnas till myndigheten. Detta ligger i linje med de bedömningar som utvecklas i avsnitt 8.6.2 om att mycket talar för att det kan bli fråga om direktåtkomst till uppgifter i Edes. Frågan, om uppgifterna kan anses ha lämnats till myndigheten, behöver dock bedömas av myndigheten som har att behandla personuppgifterna.

Härutöver ska behandlingen krävas enligt lag. Enligt förarbetena klargör bestämmelsen att det är tillåtet att utföra sådan behandling som krävs i myndigheternas verksamhet som en direkt följd av framför allt offentlighets- och sekretesslagens och förvaltningslagens bestämmelser om hur allmänna handlingar ska hanteras (prop. 2017/18:105 s. 194). Den behandling som här är i fråga kan inte sägas vara en direkt följd av sådana bestämmelser. Behandlingen är i stället en följd av budgetförordningen. Det kommer att vara nödvändigt att konsul-

tera Edes-databasen, och om en myndighet därvid behöver kontrollera en uteslutningsgrund, som ger information som innehåller känsliga personuppgifter, bör detta innebära att behandlingen krävs enligt budgetförordningen. EU-förordningar jämställs med lag vid tillämpningen av offentlighets- och sekretesslagen (prop. 2017/18:105 s. 130). Behandlingen bör därför enligt utredningen bedömas omfattas av undantagsregelns ordalydelse och det kan konstateras att förarbetsuttalandet inte anger att uppräkningen av lagbestämmelser är uttömmande. Enligt utredningen talar mycket för att undantaget bör kunna vara tillämpligt vid ett användande av Edes. Det är den berörda myndigheten som har att bedöma om förutsättningar för behandling av känsliga uppgifter föreligger.

Den andra undantagssituationen, behandling som är nödvändig för handläggningen av ett ärende, skulle kunna aktualiseras i vissa fall. Den behandlas närmare i avsnitt 8.5.8. På samma grunder som anges i det avsnittet är det inte uteslutet att denna undantagsbestämmelse kan bli tillämplig. Det är den berörda myndigheten som har att bedöma om myndigheten har stöd för att ta del av känsliga personuppgifter.

Den tredje undantagssituationen, att behandlingen är nödvändig med hänsyn till ett viktigt allmänt intresse och inte innebär ett otillbörligt intrång i den registrerades personliga integritet, behandlas närmare i avsnitt 8.2.6 och 8.5.8. Behandling av känsliga personuppgifter med stöd av denna undantagsbestämmelse skulle kunna bli aktuell vid användningen av Edes, då en stor del av myndigheternas kontrollverksamhet kan ske utan att det är en del i ärendehandläggning. Utredningen anser att behandlingen bör kunna anses som nödvändig med hänsyn till ett viktigt allmänt intresse. Om ovan nämnda undantagsbestämmelser inte är tillämpliga, kan därmed denna i flera fall förväntas kunna ge stöd för behandling av känsliga personuppgifter.

En grundläggande användning av Edes-databasen är att myndigheter ska söka i den. Sökförbudet i 3 kap. 3 § andra stycket dataskyddslagen, att det vid behandling som sker enbart med stöd av första stycket är förbjudet att utföra sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter, behandlas närmare i avsnitt 8.5.8. Myndigheterna borde inte ha något sakligt intresse av att få fram ett urval av personer grundat på känsliga personuppgifter vid en behandling av uppgifter i Edes-databasen. Förutsättningarna för att behandla känsliga personuppgifter behöver be-

dömas av den myndighet som vid en användning av Edes har för avsikt att utföra en viss sökning.

Det finns inte behov av författningsändringar när det gäller behandling av känsliga personuppgifter.

Uppgifter om domar och lagöverträdelser

Edes-databasen kommer att innehålla uppgifter som rör domar och överträdelser och svenska myndigheter kommer vid sin användning av databasen att få tillgång till sådana uppgifter och behandla dem, till exempel genom läsning. Det framgår också av beskrivningen av personuppgiftsbehandlingen för Edes att sådana uppgifter kan förekomma i dag. Som framgår av artikel 10 i dataskyddsförordningen får personuppgifter som rör fällande domar i brottmål bara behandlas under kontroll av en myndighet eller när behandlingen är tillåten enligt unionsrätten eller medlemsstaternas nationella rätt, där lämpliga skyddsåtgärder för de registrerades rättigheter och friheter fastställs (se mer i avsnitt 8.5.8). Genom 3 kap. 8 § dataskyddslagen finns också stöd i nationell rätt för myndigheter att behandla personuppgifter enligt artikel 10. Svenska myndigheter får därmed behandla sådana uppgifter.

Det finns därför inte behov av författningsändringar när det gäller behandling av uppgifter om domar och lagöverträdelser.

Uppgifter om personnummer

Som framgår av avsnitt 8.2.6 har personnummer och samordningsnummer en särställning genom att medlemsstaterna har getts möjlighet att införa särskilda villkor för behandlingen (artikel 87 i dataskyddsförordningen), vilket också har skett genom 3 kap. 10 § dataskyddslagen. Behandling av sådana uppgifter får ske utan samtycke om det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl.

Det kommer sannolikt att förekomma personnummer i Edes-databasen, även om födelsedatum kan förväntas vara den vanligaste formen av identifikationsuppgift inom EU. Utredningen bedömer att svenska myndigheters behandling av uppgifter om personnummer

och samordningsnummer i regel ska anses som förenlig med kraven i 3 kap. 10 § dataskyddslagen. Det är dock den berörda myndigheten som har att bedöma behovet.

Det finns inte behov av författningsändringar när det gäller behandling av uppgifter om personnummer och samordningsnummer.

Personuppgiftsansvar

Det anges visserligen inte uttryckligen i budgetförordningen att kommissionen är personuppgiftsansvarig för den personuppgiftsbehandling som sker i Edes-databasen, men att så är fallet framgår av flera förhållanden. Det är kommissionen som inrättat och driver databasen. I budgetförordningen hänvisas såvitt gäller Edes till dataskyddsförordningen för EU:s institutioner. I personuppgiftspolicyn för Edes beskrivs kommissionen som den som samlar in och behandlar personuppgifter vidare. Som kontaktuppgift till den personuppgiftsansvarige anges vidare en funktionsbrevlåda hos kommissionen. Något gemensamt personuppgiftsansvar anges i beskrivningen av personuppgiftsbehandlingen för Edes inte vara aktuellt.

Eftersom sökning och läsning är behandling av personuppgifter ansvarar dock de myndigheter som bereds tillgång till uppgifter i databasen för den behandlingen. Svenska myndigheter är personuppgiftsansvariga för den behandling som de utför.

Det finns inte behov av författningsändringar när det gäller personuppgiftsansvaret.

Enskildas rättigheter

Som framgår ovan är det kommissionen som för in uppgifter i Edes-databasen och som driver databasen. Dataskyddsförordningen för EU:s institutioner gäller vid personuppgiftsbehandling som sker i Edes och därmed gäller den förordningens bestämmelser om enskildas rättigheter. Det finns också bestämmelser om enskildas rättigheter direkt i budgetförordningen.

Det finns flera bestämmelser som tar sikte på enskildas rätt till information. Uppgifter om fall som avser tidig upptäckt, uteslutning eller ekonomiska sanktioner ska föras in i databasen av den behöriga utanordnaren, dock först efter att ha underrättat den berörda perso-

nen eller enheten. En sådan underrättelse kan skjutas upp under exceptionella omständigheter (artikel 144.1 andra stycket i budgetförordningen). Kommissionen ska i vissa fall på begäran informera personer eller enheter om vilka uppgifter som lagrats i databasen med avseende på den personen eller enheten (artikel 144.1 tredje stycket).

När det gäller offentliggörande av uteslutning och ekonomiska sanktioner ska den behöriga utanordnaren i enlighet med dataskyddsförordningen för EU:s institutioner informera den berörda personen eller enheten om dennes rättigheter enligt bestämmelserna om uppgiftsskydd och om vilka förfaranden som gäller för att utöva rättigheterna (artikel 142.1 femte stycket).

Dessa skyldigheter att informera är därmed inte lagda på medlemsstaterna eller deras myndigheter.

I personuppgiftspolicyn för Edes finns information som tar sikte på bland annat rätten till rättelse (punkt 8). Den registrerade har rätt till rättelse om personuppgifterna inte är korrekta eller ofullständiga, och begäran om rättelse ska lämnas till den ansvariga utanordnaren. Rättigheterna rörande uppgifter i Edes-databasen kan också utövas genom att den registrerade kontaktar den personuppgiftsansvarige, dataskyddsombudet eller EDPS, vars kontaktuppgifter lämnas i samma dokument.

När svenska myndigheter behandlar personuppgifter i Edes-databasen (söker och läser) gäller dataskyddsförordningens och dataskyddslagens bestämmelser om enskildas rättigheter (se närmare i avsnitt 8.2.6). Möjligheten för svenska myndigheter att tillgodose enskildas rättigheter när det gäller Edes är dock begränsad, då det är kommissionen som råder över systemets innehåll.

Utredningen har inte identifierat behov av ny reglering eller författningsändringar när det gäller enskildas rättigheter.

Utlämnande till tredjeland

Enligt beskrivningen av personuppgiftsbehandlingen för Edes – som avser den tidigare budgetförordningen – kan personuppgifter komma att överföras till tredjeland. Denna överföring utförs inte av medlemsstaternas myndigheter varför ansvaret för att överföringen är förenlig med dataskyddsregleringen ligger på kommissionen. I beskrivningen av personuppgiftsbehandlingen anges enligt vilka bestämmelser i

dataskyddsförordningen för EU:s institutioner som en överföring kan bedömas vara laglig.

Om en svensk myndighet avser att överföra uppgifter som den hämtar från Edes-databasen till tredjeland ankommer det på myndigheten att bedöma om förutsättningarna enligt dataskyddsförordningen är uppfyllda, både när det gäller själva överföringen och den fortsatta behandling som överföringen innebär.

Sammanfattning av utredningens slutsatser

Utredningens bedömningar ovan kan sammanfattas så att det inte finns hinder i dataskyddshänseende mot att berörda myndigheter ska kunna utföra den personuppgiftsbehandling som en användning av Edes-databasen förväntas medföra och att det inte behövs några författningsändringar på dataskyddsområdet med anledning av en sådan behandling.

Befintlig dataskyddsreglering är tillräcklig. Som en följd av detta ser utredningen inte skäl att föreslå reglering i en ny registerlag eller annan dataskyddslagstiftning för att möjliggöra en ändamålsenlig personuppgiftsbehandling i denna del. Utredningens bedömning innebär också att det inte behövs ändringar rörande dataskydd i annan reglering för att möjliggöra personuppgiftsbehandlingen.

Det bör observeras att utredningens bedömningar om förenligheten med dataskyddsregelverket inte kan avse behandlingen i det enskilda fallet. Det är den personuppgiftsansvarige som behöver säkerställa att den personuppgiftsbehandling som faktiskt utförs är förenlig med dataskyddsregleringen.

8.7 Finns det behov av ytterligare åtgärder?

Utredningens bedömning: Det krävs inte några ändringar i berörda myndigheters instruktioner eller annan författning som reglerar myndigheternas uppdrag med anledning av de skyldigheter som behandlas i detta betänkande. Några sådana ändringar krävs inte heller med anledning av det uppgiftslämnande som svenska myndigheter kan komma att göra på frivillig basis eller med anledning av ett användande av Arachne eller Edes på frivillig basis.

Skälen för utredningens bedömning

Inte något behov av ändringar i myndighetsinstruktioner eller andra författningar

Budgetförordningen är direkt tillämplig och därmed är också de skyldigheter som följer av den direkt tillämpliga. Det krävs därmed inte någon åtgärd på nationell nivå för att dessa skyldigheter ska gälla för svenska myndigheter. Det handlar här om skyldigheterna att tillgängliggöra uppgifter enligt artikel 36.6 i budgetförordningen, att säkerställa ett visst offentliggörande av uppgifter samt att använda Edes. Dessa skyldigheter börjar gälla från och med 2028.

Av myndigheternas instruktioner framgår i dag vilka uppdrag och uppgifter som myndigheterna har beträffande de olika EU-fonderna, se exempelvis 9 § förordningen (2009:1464) med instruktion för Statens jordbruksverk och 1 § förordningen (2007:907) med instruktion för Rådet för Europeiska socialfonden i Sverige. Enligt utredningens bedömning kommer det att åligga myndigheterna att uppfylla skyldigheterna i budgetförordningen inom ramen för de uppdrag de har enligt bland annat sina instruktioner. Det krävs därmed inte någon författningsändring för att myndigheterna ska ha de skyldigheter som är reglerade i budgetförordningen inom sina respektive områden.

När det gäller de situationer då myndigheterna har anledning att lämna uppgifter utan att det finns en rättslig skyldighet att göra det, kommer det inte att ske till följd av uttryckliga krav i någon EU-förordning eller svensk författning. På liknande sätt som utredningen anför i avsnitt 8.3.5 har myndigheterna dock en rättslig grund för

att lämna uppgifter som en del i sin uppgift att ha fungerande kontrollsystem och säkerställa att EU-medel endast går till den som har rätt till det. Det krävs inte att en myndighets instruktion föreskriver ett uppgiftslämnande för att detta ska vara möjligt. Utredningen bedömer att det inte finns behov av ändringar i berörda myndigheters instruktioner eller annan författning som reglerar myndigheternas uppgifter för att möjliggöra det frivilliga uppgiftslämnande som berörs i detta betänkande.

Utredningen bedömer att det inte heller finns behov av ändringar i berörda myndigheters instruktioner eller annan författning som reglerar myndigheternas uppgifter för att möjliggöra en användning av Arachne som verktyg. Inte heller krävs några sådana ändringar för att det ska vara möjligt för myndigheterna att – i förekommande fall – använda Edes på frivillig basis.

I sammanhanget kan också konstateras att det kan förväntas ske förändringar när det gäller organisationen av fonder på EU-nivå, som också medför ändringar av organisationen av förvaltningen av EU-medel på nationell nivå, exempelvis med nya svenska förordningar som gäller den kommande programperioden. Även om det skulle krävas ändringar i myndighetsinstruktioner för att peka ut de uppgifter som berörs i detta betänkande saknas det därför för närvarande förutsättningar att lämna förslag i dessa delar.

Utredningen bedömer att det inte heller finns andra skäl för ändringar i berörda myndigheters instruktioner eller annan författning som reglerar myndigheternas uppgifter utifrån de frågor som behandlas i detta betänkande.

Interna myndighetsrutiner eller liknande kan dock behövas, vilket inte omfattas av denna utrednings uppdrag att utreda närmare.

Nationell administratör för Edes

En nationell administratör kan behöva utses för att Edes ska kunna användas i Sverige (se SOU 2024:22 s. 439). Den frågan ligger dock utanför utredningens uppdrag.

9 Samlad integritetsanalys

9.1 Inledning

Som framgår av kapitel 8 lämnar utredningen inte några författningsförslag när det gäller dataskydd och personuppgiftsbehandling, eftersom befintlig reglering bedöms vara tillräcklig. Det uppgiftslämnande till kommissionen och den användning av Arachne och Edes som budgetförordningen kräver eller möjliggör medför dock en utökad och ändrad personuppgiftsbehandling hos de berörda svenska myndigheterna och innebär också att uppgifter som lämnas av svenska myndigheter kommer att få en större spridning än i dag. Motsvarande kan ske om offentliggörande av uppgifter skulle bli aktuellt enligt artikel 38.4 tredje stycket i budgetförordningen.

I detta kapitel finns en integritetsanalys, som innefattar en samlad bedömning av integritets- och proportionalitetsaspekter av den förväntade personuppgiftsbehandlingen. Detta kapitel kan därmed sägas också delvis behandla utredningens uppdrag att kartlägga skyddet för personuppgifter, utöver vad som redan följer av kapitel 7 och 8.

9.2 Vad är personlig integritet och hur görs bedömningar om skyddet för den personliga integriteten?

Respekten för individens självbestämmande och integritet är grundläggande i en demokrati. Någon enhetlig definition av begreppet personlig integritet finns inte. Regeringen uttalade dock i samband med den senaste utvidgningen av integritetsskyddet i regeringsformen att en rimlig utgångspunkt för bedömningen av behovet av ett utökat skydd för den personliga integriteten var att den skulle ske utifrån den enskildes intresse av att skydda information om sina

personliga förhållanden (se prop. 2009/10:80 s. 175). Vissa faktorer har ansetts särskilt viktiga att ta hänsyn till när det gäller att bedöma integritetskänsligheten vid helt eller delvis automatiserad behandling av personuppgifter. Det gäller arten av personuppgifter som samlas in och registreras, varför detta görs, hur och av vem uppgifterna används samt mängden av uppgifter som samlas på ett och samma ställe eller som på något annat sätt är tillgängliga för bearbetningar och sammanställningar. Även rådande samhällsvärderingar kan ha påverkan på vilken reglering och begränsning av behandlingen av personuppgifter som är nödvändig för att skydda den personliga integriteten (prop. 2005/06:173 s. 15).

Enligt artikel 35.1 i dataskyddsförordningen ska den personuppgiftsansvarige i vissa fall göra en konsekvensbedömning avseende dataskydd före behandlingen av personuppgifter. En konsekvensbedömning behöver dock inte göras om en sådan redan har gjorts i lagstiftningsarbetet (se närmare artikel 35.10).

I nu aktuellt fall måste det antas att integritetsanalyser och motsvarande konsekvensbedömningar av den personuppgiftsbehandling som kommer att ske med anledning av budgetförordningen har utförts på EU-nivå (se också avsnitt 4.4). Det finns dock utrymme att göra vissa bedömningar avseende den förväntade påverkan på integriteten genom en integritetsanalys även inom ramen för denna utredning uppdrag. En del i detta är att göra en värdering av eventuella risker som har identifierats på EU-nivå, vilket utredningen också har som uttryckligt uppdrag att göra. Härvid beaktas även annan integritetsreglering, som EU:s rättighetsstadga.

9.3 Den aktuella personuppgiftsbehandlingen och gällande dataskyddsreglering

Den personuppgiftsbehandling som väntas bli aktuell beskrivs i flera avsnitt ovan. Förenklat rör det sig om att personuppgifter kan komma att behandlas vid svenska myndigheters uppgiftslämnande till kommissionen – såväl enligt rättsliga krav som på frivillig basis – och vid myndigheters eventuella offentliggörande av uppgifter samt att personuppgifter kan komma att behandlas när svenska myndigheter använder sig av Arachne och Edes, då främst genom läsning och sökning. Beskrivningarna omfattar personuppgiftsbehandling

som väntas ske av svenska myndigheter, men också vilka andra aktörer som kan förväntas behandla personuppgifter som svenska myndigheter kommer att lämna, såsom kommissionen, andra EU-institutioner och andra medlemsstaters myndigheter med motsvarande uppdrag som berörda svenska myndigheter.

Vidare beskrivs syftena med den förväntade personuppgiftsbehandlingen, vilket rör motverkandet av oriktigheter gällande EU-medel. Det redogörs också för att dataskyddsförordningen är tillämpligt regelverk när det gäller svenska myndigheters personuppgiftsbehandling.

Det framgår också av beskrivningen att en stor del av de uppgifter som kommer att behandlas med anledning av budgetförordningen inte utgör personuppgifter.

9.4 Kartläggning och bedömning av integritetsriskerna

9.4.1 Vilka typer av personuppgifter behandlas och är de skyddsvärda?

Utredningen beskriver i tidigare avsnitt när känsliga personuppgifter liksom personuppgifter som rör domar och lagöverträdelser samt personnummer kan komma att behandlas. Dessa slags uppgifter är mer skyddsvärda och kringgärdas av särskilda krav. Utredningen redogör också för i vilken utsträckning en sådan behandling kan vara tillåten.

Även behandling av andra slags uppgifter än ovan nämnda slag kan medföra särskilda integritetsrisker. Det kan till exempel vara uppgifter om enskildas ekonomi, uppgifter om personer med skyddade personuppgifter eller uppgifter som rör negativa omdömen om personer, utan att det behöver gälla domar eller lagöverträdelser. Sådana slags uppgifter kan förekomma bland de uppgifter som svenska myndigheter kommer att lämna ut eller få tillgång till.

Av relevans vid bedömningen av integritetsrisker kan vara om uppgifter omfattas av sekretess. De flesta personuppgifter som förväntas behandlas kommer inte att vara sekretessbelagda och kommer dessutom i stor omfattning redan att vara offentliggjorda. Samtidigt bedömer utredningen också att bland det mindre antal uppgifter som kan vara skyddsvärda finns det ett gott sekretesskydd utifrån ett svenskt perspektiv. Vidare finns användnings- och åtkomstbe-

gränsningar som begränsar möjligheten för andra aktörer att få del av uppgifter. Utredningen föreslår vidare en ändring av sekretessregleringen i syfte att ge ett ytterligare skydd för uppgifter.

9.4.2 Hur omfattande är personuppgiftsbehandlingen?

De uppgifter som förväntas behandlas rör uppgifter om mottagare av EU-stöd, stödåtgärder och verkliga huvudmän. Andelen personuppgifter bedöms i förhållande till det totala antalet uppgifter komma att vara liten. Svenska myndigheter bedöms inte komma att lämna detaljerad information om enskilda. Arachne och Edes skulle kunna innehålla detaljerad information, men det är då i allmänhet inte fråga om uppgifter som svenska myndigheter har lämnat.

Som helhet är det fråga om mycket stora uppgiftsmängder som förväntas tillgängliggöras för kommissionen av svenska myndigheter samt behandlas i systemen, och då främst i Arachne. Arachne är ett riskvärderings- och datautvinningsverktyg som syftar till att bearbeta stora datamängder. Detta i sig kan medföra integritetsrisker. Uppgifterna kan också komma att behandlas under lång tid. En stor del av uppgifterna som svenska myndigheter kommer att tillgängliggöra är dock sådana som redan tillgängliggörs för kommissionen eller som är offentliggjorda eller kommer att offentliggöras.

9.4.3 Vilka andra omständigheter kan vara relevanta vid bedömningen av integritetsriskerna?

Flera andra omständigheter kan vara relevanta vid bedömningen av integritetsriskerna. Utredningen beskriver i tidigare avsnitt ingående vilka aktörer som förväntas behandla uppgifter och i vilka roller. Personuppgiftsansvariga är såväl kommissionen som, för svenskt vidkommande, svenska myndigheter som kommer att utföra behandlingen. Vad gäller systemen Arachne och Edes är kommissionen personuppgiftsansvarig. I den utsträckning som kommissionen är personuppgiftsansvarig, ligger det större ansvaret att beakta integritetsaspekter på kommissionen.

De registrerades inflytande över och kännedom om den förväntade personuppgiftsbehandlingen kan också ha betydelse. I många fall rör det sig om personuppgifter som den enskilde har lämnat till

myndigheter, till exempel inom ramen för en ansökan om EU-medel, eller för registrering till exempel hos Bolagsverket. Vad gäller personuppgiftsbehandling som kan komma att ske i Arachne gäller informationsskyldigheter både för kommissionen och svenska myndigheter.

De övergripande ändamålen med behandlingen är också relevanta. Utredningen har kartlagt dessa – det övergripande syftet är att motverka oriktig hantering av EU-medel – samt bedömer ändamålen som godtagbara.

Den spridning som personuppgifterna kommer att få har också betydelse, då spridning normalt ökar integritetsriskerna. De uppgifter som svenska myndigheter förväntas lämna till kommissionen förväntas få en bred spridning, då uppgiftslämnandet syftar till att uppgifterna ska komma till användning, främst som underlag för riskvärderingar. Samtidigt kommer tillgången till uppgifter i Arachne för andra aktörer att vara begränsad. Kommissionen kommer att offentliggöra vissa av de uppgifter som kommer att lämnas av svenska myndigheter, med stöd av artikel 38 i budgetförordningen. Svenska myndigheter kan också komma att offentliggöra uppgifter med stöd av artikeln, i de fall det rör direkt förvaltning tillsammans med medlemsstaterna. I båda dessa fall finns det möjlighet att avstå från offentliggörande av hänsyn till integritetsrisker.

Den teknik som kringgärdar personuppgiftsbehandlingen kan också ha betydelse. Det finns därför flera bestämmelser i dataskyddsförordningen som tar sikte på säkerhetsaspekter och skyddsåtgärder vid behandlingen.

En särskild risk handlar om automatiserat individuellt beslutsfattande. Den enskilde har rätt att inte bli föremål för ett beslut som enbart grundas på automatiserad behandling, inbegripet profilering, vilket har rättsliga följder för honom eller henne eller på liknande sätt i betydande grad påverkar honom eller henne. Ett sådant beslutsfattande får dock ske under vissa förutsättningar (artikel 22 i dataskyddsförordningen).

9.4.4 Vilka risker finns och hur tas de om hand?

Då Arachne och Edes har inrättats och drivs av kommissionen och den behandling som aktualiseras följer främst av EU-reglering och inte av nationell rätt, är en naturlig utgångspunkt för utredningens överväganden av integritetsaspekterna det som följer av den reglering som finns och de överväganden som har gjorts på EU-nivå. Som anges i avsnitt 9.2 förväntas kommissionen ha utfört integritetsanalyser och konsekvensbedömningar i den utsträckning som det är nödvändigt.

Enligt Arachne-stadgan (Arachne, Charter for the introduction, the application and the integration of the Arachne risk scoring tool) har en konsekvensbedömning gjorts enligt dataskyddsförordningen för EU:s institutioner för att analysera, identifiera och minimera de risker för dataskyddet som följer av kommissionens behandling. Personuppgiftsbehandlingen bedömdes genom befintliga skyddsåtgärder, säkerhetsåtgärder och mekanismer för att minska riskerna inte innebära någon hög risk för fysiska personers rättigheter och friheter. Konsekvensbedömningen har validerats av dataskyddsombudet (punkt 6.1). Här bör påminnas om att stadgan avser nu gällande förhållanden och därmed inte tar sikte på en framtida version av Arachne.

Vidare finns det skäl att lyfta vissa synpunkter som EDPS lämnade under förhandlingarna av den nu gällande budgetförordningen. EDPS välkomnade att artikel 36.7 på ett tydligt sätt angav mottagare av uppgifter och användare av systemet samt att kommissionen pekades ut som personuppgiftsansvarig för systemet. EDPS påpekade vidare bland annat att lagring och behandling av flera olika kategorier av uppgifter samlat i ett it-system skapar risker och att kraven på uppgiftsminimering, inbyggt dataskydd och säkerhetsaspekter måste beaktas för att minska dessa risker (Opinion 14/2022, den 7 juli 2022).

Risker som utredningen har identifierat när det gäller myndigheters uppgiftslämnande till kommissionen och till Arachne är att en rutinmässig överföring kan medföra en risk att fler uppgifter än de som ska eller får lämnas ut, ändå lämnas ut. Vidare kan själva överföringsmomentet innebära risker ur säkerhetssynpunkt, såsom obehörig åtkomst till uppgifter. Dessa risker omhändertas enligt utredningens mening genom att överföring av uppgifter till Arachne sker genom ifyllande av förvalda fält, vilket i nuläget sker manuellt i vart fall första gången som en överföring ska ske, samt genom att kom-

missionen ska säkerställa säkra kanaler för överföring av uppgifter (jfr punkt 11 i Arachne-stadgan). Vidare ankommer det på berörd myndighet att inför ett rutinmässigt utlämnande göra en gedigen prövning av om uppgifterna kan lämnas ut.

När det gäller det eventuella offentliggörandet av uppgifter på EU:s webbplats kan det finnas risk att uppgifter som inte ska offentliggöras enligt artikel 38.4 tredje stycket i budgetförordningen, ändå publiceras. Det ankommer på berörd myndighet att göra bedömningar av vilka uppgifter som ska offentliggöras. Härvid behöver särskilt beaktas att offentliggörande ska underlåtas i vissa situationer.

När det gäller den behandling av personuppgifter som kommer att ske i Arachne utgör den sambearbetning av uppgifter som Arachne utför i sig en risk, eftersom den kan möjliggöra en omotiverad kartläggning av enskilda. Samlingen av ett stort antal uppgifter i en enda databas kan också medföra risk för en omfattande obehörig intern och extern åtkomst till uppgifter. Utredningen bedömer att omhändertagande av dessa risker kan antas ske av kommissionen genom regler om och rutiner för åtkomstbegränsningar samt säkra it-lösningar. Ett stort ansvar vilar också på den lokala administratören att endast tilldela behörigheter till den som har rätt till det. Åtkomst ska, som utgångspunkt, dessutom ges endast till uppgifter som rör det egna programmet eller planen. Därmed får risken för en omotiverad kartläggning av enskilda anses som liten.

Risker ur säkerhetssynpunkt, såsom för obehörig åtkomst, kan finnas även för uppgifter i Edes. Liknande åtgärder för att omhänderta riskerna som nämns ovan avseende Arachne, kan förväntas avseende Edes. Här kan dock påminnas om att svenska myndigheter inte kommer att föra in uppgifter direkt i det systemet, och att ansvaret för säkerheten och omhändertagande av integritetsrisker ligger på kommissionen.

Det följer krav på inbyggt dataskydd och dataskydd som standard samt krav på att vidta lämpliga tekniska och organisatoriska skyddsåtgärder direkt av såväl dataskyddsförordningen som dataskyddsförordningen för EU:s institutioner. Denna reglering är i sig att anse som skyddsåtgärder. Kraven gäller generellt, och är därmed tillämpliga gällande personuppgiftsbehandling som sker såväl i Edes som i Arachne. Regleringen kan också sägas kompletteras av bland annat Arachne-stadgan, där exempelvis punkt 11 anger att kommissionen genomför alla tekniska och organisatoriska säkerhetsåtgärder för

att skydda personuppgifterna mot oavsiktlig eller avsiktlig förstöring eller förlust av uppgifter eller mot obehörig tillgång.

Även viss reglering i budgetförordningen kan sägas ta sikte på skyddsåtgärder, såsom följande. Vid genomförandet av budgeten ska medlemsstaterna och kommissionen säkerställa överensstämmelse med EU:s rättighetsstadga, i enlighet med artikel 51 i stadgan, och respektera unionens värden enligt artikel 2 i Fördraget om Europeiska unionen som är relevanta vid genomförandet av budgeten (artikel 6.3). När det gäller Arachne anges i artikel 36.7 i budgetförordningen att kommissionen är ansvarig för utveckling, förvaltning och övervakning av Arachne, för att säkerställa uppgifternas säkerhet och konfidentialitet, autentisering av användarna samt för att skydda it-systemet mot felaktig förvaltning och missbruk.

Även reglering på nationell nivå kan utgöra skyddsåtgärder. Lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning, dataskyddslagen, innehåller sådan reglering. Krav på skyddsåtgärder har i svensk rätt ofta ansetts tillgodosett genom att uppgifter omfattas av bestämmelser om sekretess (se prop. 2017/18:105 s. 85). Som framgår av tidigare avsnitt bedömer utredningen att sekretess kan komma att gälla för flera av de uppgifter som kan förekomma i Arachne och Edes. Utredningen föreslår även en ändring i sekretessregleringen i syfte att ge ett ytterligare skydd för uppgifter.

Vad gäller automatiserat beslutsfattande, inklusive profilering, förekommer inte detta enligt nu gällande dokumentation för behandling i Arachne och Edes. Riskvärderingar som Arachne producerar ska inte heller direkt leda till beslut utan syftar till att ge en indikation på vad berörd myndighet kan ha skäl att utreda närmare. Det sker därmed inget automatiserat beslutsfattande till följd av gjorda riskvärderingar. Om sådant beslutsfattande skulle bli aktuellt framöver, finns det i såväl dataskyddsförordningen som dataskyddsförordningen för EU:s institutioner regelverk som anger förutsättningarna för sådant beslutsfattande.

Sammanfattningsvis bedömer utredningen att de integritetsrisker som har identifierats kan omhändertas.

9.5 AI-förordningen behöver beaktas

Arachne är under utveckling, och bland insatser och åtgärder som bör genomföras för att säkerställa att Arachnes funktioner förblir av hög standard nämns i budgetförordningen användning av artificiell intelligens för analys och tolkning av data (skäl 32 till budgetförordningen).

Användningen av artificiell intelligens (AI) kan medföra stor påverkan på enskildas integritet. Även om det är kommissionen som driver och ansvarar för Arachne och därmed ansvarar för att det finns stöd för att använda AI-system finns det skäl att nämna EU:s allmänna reglering av artificiell intelligens, AI-förordningen[1]. Den syftar till att förbättra den inre marknadens funktion och främja användningen av människocentrerad och tillförlitlig AI, samtidigt som en hög skyddsnivå säkerställs för hälsa, säkerhet och grundläggande rättigheter som fastställs i stadgan, inbegripet demokrati, rättsstatens principer och miljöskydd, mot de skadliga effekterna av AI-system i unionen, och att stödja innovation (artikel 1.1). AI-förordningen trädde i kraft den 1 augusti 2024 och den 2 augusti 2026 blir de flesta delar av förordningen tillämpliga.

I AI-förordningen klassificeras AI-system baserat på deras potentiella risk för samhället och individers rättigheter i olika risknivåer. Viss användning ska förbjudas och annan tillåtas med restriktioner och krav i form av bland annat tillsyn och registrering. AI-förordningen gäller för den som utvecklar, tillhandahåller eller använder AI-system, både inom privat och offentlig verksamhet.

AI-förordningen och dataskyddsförordningen gäller parallellt. Detta betyder bland annat att dataskyddsförordningen gäller när personuppgifter behandlas i samband med utveckling eller användning av AI. Som framgår av avsnitt 8.5.8 kan uppgifter som finns i Arachne användas som så kallade träningsdata vid framtagande och förbättring av riskindikatorer. Detta är ett exempel på när det kan bli fråga om att använda personuppgifter vid träning av AI-modeller. Utredningen utgår från att kommissionen beaktar såväl dataskyddsregelverkets som AI-förordningens reglering vid användningen av

[1] 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).

AI. När det gäller svenska myndigheters användning av AI-system har även de att förhålla sig till AI-förordningen. AI-förordningen är i sig en skyddsåtgärd för att ta om hand möjliga integritetsrisker (jfr avsnitt 9.4.4).

Det förväntas ske förändringar av svensk rätt med anledning av AI-förordningen. Utredningen om AI-förordningen lämnade i oktober 2025 betänkandet Anpassningar till AI-förordningen – Säker användning, effektiv kontroll och stöd för innovation (SOU 2025:101).

9.6 Samlad nödvändighets- och proportionalitetsbedömning

Såväl lämnandet och offentliggörandet av uppgifter som användningen av Arachne och Edes kommer att ske som en följd av reglering på EU-nivå. Den författningsändring som utredningen föreslår avser en ändring i sekretessregleringen i syfte att ge ett ytterligare skydd för uppgifter. EU är vid sin lagstiftning bunden av – i nu aktuella delar – motsvarande regelverk som Sverige, vilket innebär att den lagstiftning som EU tar fram ska vara förenlig med dataskyddsregelverket och EU:s rättighetsstadga. Begränsningar i utövandet av de rättigheter och friheter som erkänns i stadgan, bland annat rätten till skydd för personuppgifter, får med beaktande av proportionalitetsprincipen endast göras om de är nödvändiga och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av unionen eller behovet av skydd för andra människors rättigheter och friheter (artikel 52.1 i EU:s rättighetsstadga). Krav på proportionalitet genomsyrar också EU-lagstiftningen generellt. Utgångspunkten är därför att den förväntade behandlingen är såväl nödvändig som proportionerlig i förhållande till det integritetsintrång som den kan medföra.

I det följande gör utredningen vissa överväganden om behovet av behandlingen och proportionaliteten av den i förhållande till syftena ur ett svenskt perspektiv.

Svenska myndigheter har flera roller när det gäller att hantera EU-medel. De kan sägas vara en kanal för att förmedla EU-medel, men de har också ett ansvar att säkerställa att medlen bara går till den som har rätt till det, och att ha välfungerande rutiner för att säkerställa detta. Både Arachne och Edes är verktyg för att säkerställa en korrekt hantering av EU-medel och att därmed motverka oriktig-

heter på det området. Skyldigheten att tillgängliggöra uppgifter för kommissionen har samma syfte. Det är fråga om att uppfylla mål av allmänt samhällsintresse, och gemensamma verktyg förbättrar möjligheterna att uppnå målen. Att det finns behov av ett sådant tillgängliggörande och en sådan användning av Arachne och Edes har bedömts på EU-nivå. Av ett sådant tillgängliggörande och en sådan användning följer att det också krävs viss personuppgiftsbehandling. Utredningen ifrågasätter inte det behovet. Regleringen i budgetförordningen ger också utrymme för att inte fler personuppgifter behöver lämnas än de som redan behandlas enligt sektorsspecifik reglering.

Utredningen bedömer vidare att den behandling som svenska myndigheter förväntas utföra medför ett begränsat intrång i den grundläggande rätten till privatliv och dataskydd. Utredningen bedömer också att de risker som har identifierats kan tas om hand (se avsnitt 9.4.4). Utöver detta finns skäl att påminna om att en stor del av personuppgifterna som kommer att behandlas är sådana som redan är offentliggjorda, inte sällan av den enskilde själv. Åtgärderna och det integritetsintrång som åtgärderna innebär för de registrerade är enligt utredningens bedömning proportionerliga i förhållande till målet att motverka oriktigheter avseende EU-medel, vilket är av allmänt samhällsintresse.

Utredningen bedömer sammanfattningsvis den personuppgiftsbehandling som svenska myndigheter förväntas utföra som såväl nödvändig som proportionerlig. Utredningen har också bedömt att den personuppgiftsbehandling som svenska myndigheter förväntas utföra även i övrigt kan ske i enlighet med gällande dataskyddsreglering.

10 Ikraftträdande och övergångsbestämmelser

Utredningens förslag: Den nya bestämmelsen i offentlighets- och sekretesslagen ska träda i kraft den 1 januari 2027.

Utredningens bedömning: Några övergångsbestämmelser behövs inte.

Skälen för utredningens förslag och bedömning: Om regeringen väljer att gå på linjen att det bör införas en ny sekretessbestämmelse för att säkerställa att svenska myndigheter har rättsliga förutsättningar att använda Arachne bör författningsändringen träda i kraft så snart som möjligt, för att möjliggöra ett frivilligt användande av Arachne. Utredningen bedömer att den nya bestämmelsen i offentlighets- och sekretesslagen (2009:400) bör kunna träda i kraft den 1 januari 2027. Det finns inte behov av övergångsbestämmelser.

11 Konsekvenser

11.1 Inledning

I detta kapitel redovisas konsekvenserna av utredningens förslag. Konsekvenserna redovisas i enlighet med förordningen (2024:183) om konsekvensutredningar. Konsekvensbeskrivningen innehåller också en redovisning av vilka konsekvenser förslaget innebär för skyddet av EU:s finansiella intressen, spridningen av personuppgifter inom och mellan myndigheter samt skyddet av den personliga integriteten, vilket särskilt tas upp i kommittédirektiven.

11.2 Utredningens uppdrag

Utredningen har i uppdrag att undersöka de rättsliga förutsättningarna för svenska myndigheter att använda det av kommissionen administrerade riskvärderingsverktyget Arachne och uppfylla kraven enligt den omarbetade budgetförordningen, bland annat skyldigheterna inom ramen för systemet för tidig upptäckt och uteslutning (Edes), för att motverka felaktiga utbetalningar och bedrägerier i samband med hantering av EU-medel. I uppdraget ingår att bedöma om det finns behov av ändrade regler för att svenska myndigheter ska kunna använda Arachne och uppfylla sina skyldigheter inom ramen för Edes samt lämna nödvändiga författningsförslag. Utredningen har kommit fram till att det finns anledning att lämna ett författningsförslag.

11.3 Utgångspunkter för bedömningen av konsekvenserna

Utredningen lämnar ett författningsförslag, nämligen en ny bestämmelse i offentlighets- och sekretesslagen (2009:400), OSL, som innebär att sekretess under vissa förhållanden ska gälla för uppgifter som härrör från en riskvärdering som har gjorts genom Arachne. Enligt utredningens bedömning är det också möjligt att argumentera för att Arachne kan användas även utan en sådan ny bestämmelse, det vill säga att befintliga sekretessbestämmelser är tillräckliga.

Det är konsekvenserna av detta förslag som beskrivs i detta avsnitt. Syftet med förslaget är att säkerställa att det finns rättsliga förutsättningar för ett användande av Arachne.

De övergripande intressen som ligger bakom utredningens uppdrag och därmed också det lämnade förslaget handlar om att EU:s finansiella intressen ska skyddas. Sverige deltar i genomförandet av EU:s budget. För att Sverige ska kunna uppfylla det ansvar som följer av detta krävs det att svenska myndigheter har tillgång till information och verktyg för att kunna motverka oriktigheter med EU-medel. Ett användande av Arachne är för närvarande frivilligt men det kan vara ett viktigt led i att Sverige effektivt ska kunna motverka oriktigheter med EU-medel. Om det inte finns förutsättningar för Sverige att uppfylla de krav som ställs kan det försvåra för svenska myndigheter att delta i det samarbete som EU och medlemsländerna har kring informationsutbyte med mera och som bland annat manifesteras i användandet av nämnda verktyg.

Rent generellt kan sägas att Arachne är ett datautvinnings- och riskvärderingsverktyg som kommissionen har tagit fram för att hjälpa medlemsstaternas myndigheter att kontrollera hur EU-stöd används och förvaltas. Verktyget kan leda till att svenska myndigheter får information om fler risker för missbruk av EU-medel. Det kan minska förekomsten av sådant missbruk. Denna information kan också – under vissa förutsättningar – komma de brottsbekämpande myndigheterna till del. På så sätt skulle ett användande av Arache möjligen också kunna leda till ett mer effektivt brottsbekämpande arbete.

Utredningen ser dock inte som sin uppgift att analysera konsekvenserna av ett användande av Arachne i sig. Inför ett beslut att ansluta svenska myndigheter till Arachne behöver vissa överväganden göras beträffande kostnader som en sådan anslutning innebär

å ena sidan och de vinster som en sådan anslutning innebär å andra sidan. Det ligger utanför utredningens uppdrag att göra sådana överväganden. Utredningens uppgift är att utreda de rättsliga förutsättningarna för bland annat ett användande av Arachne. Konsekvensbeskrivningen är därför utformad med fokus på förslaget om en ny sekretessbestämmelse.

11.4 Problembeskrivning och målsättning

Det är viktigt att det finns rättsliga förutsättningar för svenska myndigheter att använda Arachne och att uppfylla sina skyldigheter enligt Edes. Edes kommer att bli obligatoriskt att använda även för svenska myndigheter och det kan även vara ändamålsenligt att svenska myndigheter använder Arachne i arbetet med att motverka felaktigheter med EU-medel. Sverige har ett ansvar i förhållande till EU att uppfylla sin del i att skydda EU:s finansiella intressen. Om kommissionen anser att Sverige inte lever upp till detta riskerar Sverige finansiella sanktioner. Sverige har också ett eget intresse av att motverka felaktiga utbetalningar.

När det gäller Edes anser utredningen att det står klart att det inte krävs några författningsåtgärder. Även när det gäller Arachne är det enligt utredningen möjligt att argumentera för att svensk rätt redan uppfyller dessa förutsättningar. Det finns dock också utrymme för en annan bedömning. Det bör därför lämnas förslag på utformning av en bestämmelse som säkerställer att det finns rättsliga förutsättningar för att använda Arachne.

11.5 Utredningens förslag

Utredningen lämnar ett förslag på utformning av en ny bestämmelse i offentlighets- och sekretesslagen. Förslaget innebär att sekretess ska gälla för uppgift som härrör från en riskvärdering som har gjorts genom Arachne, om det kan antas att syftet med den förvaltning, övervakning, kontroll och revision som ska ske i enlighet budgetförordningen motverkas om uppgiften röjs. Bestämmelsen syftar både till att samarbetet inom EU inte ska försämras och till att myndigheternas arbete med kontroller och granskning inte ska motverkas.

11.6 Nollalternativ

Nollalternativet innebär att förslaget inte genomförs. Det är enligt utredningen möjligt att argumentera för att förslaget inte behövs och att gällande sekretessregler är tillräckliga. Gällande bestämmelser kommer i många situationer att kunna ge ett sekretesskydd för uppgifter i Arachne, inklusive gjorda riskvärderingar. Det kan visserligen inte uteslutas att uppgifter i Arachne, inklusive riskvärderingar, i vissa fall inte kommer att kunna sekretessbeläggas. Det beror delvis på intresseavvägningar som lagstiftaren redan har gjort mellan behovet av sekretess och insynsintresset, både när det gäller gällande sekretessbestämmelsers tillämpningsområde och valda skaderekvisit.

Även om det från kommissionens sida har framförts ett önskemål om att uppgifter i Arachne – och särskilt gjorda riskvärderingar – inte ska spridas har detta inte kommit till uttryck i en tydlig sekretessreglering i en bindande rättsakt. Det är möjligt att argumentera för att insynsintresset därmed bör väga över. Ställningstagandet i denna del berör delvis utrikespolitiska frågor om intresseavvägningen mellan den svenska offentlighetsprincipen och relationen med EU.

Om det inte införs någon ny bestämmelse i offentlighets- och sekretesslagen kan det dock finnas en risk att svenska myndigheter inte kommer att kunna sekretessbelägga uppgifter som härrör från riskvärderingar i den utsträckning som vore önskvärt och att det därmed kan anses finnas rättsliga hinder mot att använda Arachne.

11.7 Alternativa lösningar

11.7.1 En mer begränsad räckvidd

Förslaget innebär att den nya sekretessbestämmelsens räckvidd är obegränsad. Ett alternativ är att begränsa räckvidden på så sätt att sekretessen ska gälla endast i viss verksamhet, nämligen i verksamhet som rör sådan förvaltning, övervakning, kontroll och revision som ska ske i enlighet budgetförordningen. Insynsintresset talar för att inte låta räckvidden bli mer omfattande än vad som är nödvändigt.

11.7.2 Ett vidare föremål

Enligt förslaget bestäms sekretessens föremål till uppgifter som härrör från en riskvärdering som har gjorts genom Arachne.

Ett alternativ skulle kunna vara att ange föremålet på ett vidare sätt och låta det ta sikte på alla uppgifter som härrör från Arachne, inklusive riskvärderingar. För en sådan ordning talar bland annat att det finns oklarheter när det gäller exakt vilka uppgifter som kommer att finnas i Arachne, vilka skyddsbehov som kan uppstå och hur långt gällande sekretessbestämmelser räcker för att tillgodose dessa skyddsbehov. För en sådan ordning talar också att Arachne-teamet vid kommissionen kan sägas ha gett uttryck för ett önskemål att uppgifter i Arachne över huvud taget inte ska offentliggöras.[1] Ett vidare föremål skulle alltså kunna bidra till att främja relationen till EU.

11.8 Motivering till och syftet med förslaget

Gällande sekretessregler bedöms kunna ge ett betydande skydd för de uppgifter som eventuellt skulle kunna behöva ett sådant skydd. Det kan dock inte uteslutas att uppgifter i Arachne, inklusive gjorda riskvärderingar, i vissa fall inte kan sekretessbeläggas med stöd av gällande sekretessreglering. Genom förslaget säkerställs det därmed att det finns möjlighet för svenska myndigheter att, under vissa förutsättningar, sekretessbelägga uppgifter som härrör från riskvärderingar som har gjorts genom Arachne.

En obegränsad räckvidd är att föredra framför en sådan mer begränsad räckvidd som skisseras ovan. Enligt utredningens mening är det lämpligare att sekretessen ska gälla hos alla myndigheter för uppgifter av ett visst slag. Detta motsvarar regleringen i flera andra bestämmelser i 15 och 17 kap. OSL, exempelvis 15 kap. 1 och 2 §§ samt 17 kap. 1 a och 1 b §§ OSL. Det kan vara ändamålsenligt att myndigheter delar uppgifter mellan varandra för att mer effektivt motverka oriktigheter med allmänna medel.

Det är vidare lämpligast att ange föremålet på ett mer begränsat sätt än att – som beskrivs ovan – låta det omfatta alla uppgifter som härrör från Arachne. Det är när det gäller just gjorda riskvärderingar som ett sekretessbehov har framkommit tydligare. Insynsintresset

[1] Komm2025/00388-10.

talar för att inte ange sekretessens föremål vidare än vad som är nödvändigt utifrån de konkreta risker som har identifierats. För det fall ytterligare skyddsbehov identifieras i framtiden kan det vid behov införas kompletterande reglering.

Utredningen har vidtagit åtgärder för att förslaget inte ska medföra mer långtgående begränsningar än vad som bedöms vara nödvändigt. Till dessa hör att föremålet är begränsat till just uppgifter som härrör från riskvärderingar. Vidare har bestämmelsen försetts med ett rakt skaderekvisit, vilket innebär att en skadebedömning ska göras i varje enskilt fall. Detta säkerställer att uppgifter inte sekretessbeläggs slentrianmässigt.

11.9 Påverkan på offentlighetsprincipen och insynsintresset

Utredningens bedömning: Förslaget har en godtagbar påverkan på offentlighetsprincipen och insynsintresset.

Skälen för utredningens bedömning: Eftersom utredningens förslag är en ny sekretessbestämmelse analyseras först förslagets påverkan på offentlighetsprincipen och insynsintresset. Rätten att ta del av allmänna handlingar är en medborgerlig rättighet som utgör en viktig del av vårt demokratiska statsskick. För att det ska vara motiverat att göra undantag från det grundlagsskyddade insynsintresset bör det krävas mer konkreta risker för olägenheter om uppgifter röjs. En avvägning mellan sekretessintresset och insynsintresset presenteras i en intresseanalys i avsnitt 8.5.6. Utredningen bedömer där att det kan finnas skäl för en utökad möjlighet att sekretessbelägga riskvärderingar, både för att samarbetet inom EU inte ska försämras och för att myndigheternas arbete med kontroller och granskning inte ska motverkas. Det föreslagna undantaget från det grundlagsskyddade insynsintresset bedöms alltså vara motiverat.

11.10 Konsekvenser för skyddet av EU:s finansiella intressen

Det övergripande syfte som ligger bakom utredningens uppdrag och därmed dess förslag handlar om att EU:s finansiella intressen ska skyddas. För att Sverige ska kunna uppfylla sin del i att skydda EU:s finansiella intressen krävs det att svenska myndigheter har tillgång till information och verktyg för att kunna motverka oriktigheter med EU-medel.

I stor utsträckning bedöms gällande sekretessregler vara tillräckliga för att svenska myndigheter ska kunna använda Arachne. Det kan dock finnas skäl för ny sekretessreglering när det gäller möjligheten att hemlighålla riskvärderingar, både för att samarbetet inom EU inte ska försämras och för att myndigheternas arbete med kontroller och granskning inte ska motverkas. Genom förslaget säkerställs det därmed att det finns rättsliga förutsättningar för svenska myndigheter att använda Arachne. Förslaget bedöms alltså ge positiva konsekvenser för skyddet av EU:s finansiella intressen.

11.11 Konsekvenser för staten, kommuner och regioner

Utredningens bedömning: Förslaget innebär inte några kostnader för staten, kommuner och regioner.

Skälen för utredningens bedömning

Konsekvenser för myndigheterna

Genom förslaget säkerställs att myndigheterna som hanterar EU-stöd har rättsliga förutsättningar att använda Arachne. Det är möjligt att en anslutning till och ett användande av Arachne leder till både kostnader och besparingar för myndigheterna som ansluter sig till Arachne. Dessa konsekvenser ligger dock utanför utredningens uppdrag att analysera.

Den föreslagna sekretessbestämmelsen har en obegränsad räckvidd, vilket innebär att den ska tillämpas av alla myndigheter och andra som omfattas av offentlighets- och sekretesslagen om de förvarar uppgifter som härrör från riskvärderingar som har gjorts genom

Arachne och sådana begärs ut. Det får antas att så sker i begränsad omfattning, särskilt när det gäller andra myndigheter än de som använder Arachne. Det är inte möjligt att uppskatta i vilken utsträckning sådana begäranden om utlämnande skulle ske eller vilka kostnader de skulle orsaka. Under alla förhållanden bedömer utredningen att sådana eventuella kostnader får antas rymmas inom ordinarie ramar.

Konsekvenser för de brottsbekämpande myndigheterna och domstolarna

Det är möjligt att de brottsbekämpande myndigheterna får tillgång till information från myndigheter som kan komma att använda Arachne och att denna information kan leda till att fler misstankar om brottslighet med EU-medel uppkommer. Det skulle i sin tur kunna leda till en ökning av antalet åtal och brottmålsrättegångar rörande missbruk av EU-medel. Det är inte möjligt att uppskatta hur stor en sådan ökning skulle vara. I sammanhanget kan det ha betydelse att Eppo som EU:s oberoende åklagarmyndighet väcker talan när det gäller brott som skadar EU:s ekonomiska intressen, och att brottsanmälningar kan göras direkt till Eppo (se avsnitt 5.3.5).

De eventuella konsekvenserna av ett användande av Arachne för de svenska brottsbekämpande myndigheterna och domstolarna är vidare inte en direkt konsekvens av utredningens förslag i sig, som syftar till att säkerställa rättsliga förutsättningar för svenska myndigheter att använda Arachne men inte angår själva användandet av verktyget.

Övriga konsekvenser för staten

Det övergripande syfte som ligger bakom utredningens uppdrag och därmed förslag handlar som nämns ovan om att EU:s finansiella intressen ska skyddas. Betydande belopp betalas ut genom EU-fonderna. Utredningen har inte tillgång till någon uppskattning av vad missbruket av de EU-stöd som omfattas av denna utredning uppgår till. Generellt kan dock antas att missbruk med EU-stöden kan uppgå till stora belopp. Olaf har i ett pressmeddelande från juni 2025 uppgett att myndigheten under 2024 avslöjat missbruk av EU-medel

på över 870 miljoner euro.[2] Om myndigheterna får bättre möjligheter att förebygga, förhindra, upptäcka, utreda och korrigera oriktigheter med EU-medel kan det leda till samhällsekonomiska vinster inom de områden där EU-stöd betalas ut. Utredningen har inte något underlag för att uppskatta hur stora de ekonomiska effekterna av ett användande av Arachne skulle vara. Denna konsekvensbeskrivning tar inte heller sikte på konsekvenserna av ett användande av Arachne i sig.

Ekonomiska konsekvenser för staten kan också uppkomma om kommissionen anser att skyddet av EU-medel inte är tillräckligt starkt i Sverige och beslutar om finansiella sanktioner. Detta skulle kunna medföra att kommissionen beslutar att inte finansiera vissa stöd med medel från EU:s budget. Sverige skulle då kunna bli tvunget att finansiera stöden med uteslutande nationella medel. Uppmärksammade brister kan även påverka tilldelningen av medel vid nästkommande programperiod (SOU 2024:22, s. 511). Förslaget innebär att det säkerställs att det finns rättsliga förutsättningar för svenska myndigheter att använda Arachne. Därmed undviks enligt utredningen risken att Sverige drabbas av finansiella sanktioner från EU på den grunden att Sverige inte uppfyller kraven på kontroll av EU-medel med avseende på ett användande av Arachne.

Konsekvenser för kommuner och regioner

Utredningen bedömer att förslaget inte har några särskilda konsekvenser för kommuner och regioner. De berörs inte av förslaget på annat sätt än att sekretessbestämmelsen gäller i all verksamhet som omfattas av offentlighets- och sekretesslagen, se ovan. Förslaget bedöms inte heller ha någon påverkan på den kommunala självstyrelsen.

[2] https://anti-fraud.ec.europa.eu/document/download/2faf8402-7723-4d69-a4c8-5568acd1e27e_en?filename=pr-16062025-OLAF-exposes-fraud-involving-over-eur870-million_en.pdf. Hämtat 2025-11-01.

11.12 Konsekvenser för företag och andra enskilda

Utredningens bedömning: Förslaget innebär inte några administrativa krav eller kostnader för företag.

Förslaget kan innebära ett stärkt sekretesskydd för uppgifter som rör enskilda.

Skälen för utredningens bedömning: Förslaget innebär inte några administrativa krav eller kostnader för företag. Generellt kan sägas att åtgärder som kan bidra till att arbetet med att motverka felaktigheter med EU-stöd blir mer effektivt snarare kan leda till positiva effekter för företag genom att utrymmet minskar för de aktörer som missbrukar stöden. Det i sin tur kan bidra positivt till andra företags verksamhet på så sätt att den osunda konkurrensen minskar. Dessa följder är dock inte konsekvenser av förslaget till ny sekretessbestämmelse och behandlas inte vidare här.

Både företag och andra enskilda kan påverkas av förslaget till ny sekretessbestämmelse på så sätt att bestämmelsen kan möjliggöra ett sekretessbeläggande av uppgifter vars röjande kan skada enskilda. Det kan handla om uppgifter om en enskilds affärs- eller driftförhållanden eller om uppgifter om personliga förhållanden, exempelvis rörande förföljda personer. För att den föreslagna bestämmelsen ska kunna tillämpas på sådana uppgifter krävs att uppgifterna härrör från en riskvärdering som har gjorts genom Arachne och att det kan antas att syftet med viss förvaltning, övervakning, kontroll och revision motverkas om uppgiften röjs. Det bör dock noteras att den föreslagna bestämmelsen inte ger utrymme för sekretess enbart i den enskildes intresse.

11.13 EU-rätten och Sveriges internationella åtaganden

Utredningens bedömning: Förslaget är förenligt med EU-rätten och Sveriges internationella åtaganden.

Skälen för utredningens bedömning: Förslaget syftar till att svenska myndigheter ska ha rättsliga förutsättningar att använda Arachne. Genom förslaget säkerställs att sådana rättsliga förutsättningar finns.

Förslaget överensstämmer därmed med de skyldigheter som följer av Sveriges anslutning till EU.

Några andra internationella åtaganden bedöms inte påverkas.

11.14 Konsekvenser för spridningen av personuppgifter inom och mellan myndigheter

I avsnitt 9.4.3 behandlas den spridning som personuppgifter kan få vid ett användande av Arachne och Edes samt vid uppfyllande av Sveriges skyldigheter enligt budgetförordningen. När det gäller förslaget till ny bestämmelse i offentlighets- och sekretesslagen gör utredningen bedömningen att den i sig inte skulle leda till någon ökad spridning av personuppgifter inom eller mellan myndigheter. Bestämmelsen innebär en möjlighet att sekretessbelägga uppgifter som härrör från riskvärderingar som Arachne genererar. Inom ramen för sådana riskvärderingar kan det förekomma personuppgifter och förslaget kan således innebära att spridningen av dessa uppgifter blir mindre omfattande.

11.15 Konsekvenser för skyddet av den personliga integriteten

I kapitel 9 gör utredningen en samlad integritetsanalys av den förväntade personuppgiftsbehandling som följer av ett användande av Arachne och Edes samt av ett uppfyllande av Sveriges skyldigheter enligt budgetförordningen. Som där utvecklas kan det vid bedömningen av integritetsrisker vara av relevans om uppgifter omfattas av sekretess. Utredningen gör bedömningen att förslaget om en ny sekretessbestämmelse inte har några negativa konsekvenser för skyddet av den personliga integriteten. Det är möjligt att sekretessbestämmelsen kan bidra till att ytterligare minska integritetsriskerna vid användandet av Arachne genom att möjligheten att sekretessbelägga uppgifter ökar. Inom ramen för riskvärderingar kan det förekomma personuppgifter. Det bör dock noteras att den föreslagna bestämmelsens skaderekvisit tar sikte på situationen att syftet med viss förvaltning, övervakning, kontroll och revision motverkas om uppgiften

röjs. Bestämmelsen ger alltså inte utrymme för sekretess enbart i den enskildes intresse.

11.16 Ikraftträdande, informationsinsatser och utvärdering

Om regeringen väljer att gå på linjen att det bör införas en ny sekretessbestämmelse bör den nya bestämmelsen – för att möjliggöra ett frivilligt användande av Arachne och säkerställa ett sekretesskydd för uppgifter – träda i kraft så fort som möjligt. Något behov av särskilda informationsinsatser bedöms inte föreligga.

Den föreslagna sekretessbestämmelsen bör utvärderas två år efter ikraftträdandet. Denna tidsperiod bedöms ge ett tillräckligt underlag för att kunna bedöma bestämmelsens effekter samtidigt som eventuella brister kan åtgärdas inom rimlig tid. Regeringen bör ta ställning till om utvärderingen ska göras inom Regeringskansliet eller av en extern aktör, exempelvis ESV. Det framstår som lämpligt med en statistisk sammanställning av antalet ärenden där bestämmelsen har tillämpats och en stickprovsgranskning av eventuella beslut för att bedöma enhetligheten i tillämpningen. Detta skulle kunna kompletteras med intervjuer med handläggare som tillämpar bestämmelsen och eventuellt en enkät till berörda externa parter för att fånga upp eventuella oförutsedda konsekvenser.

Utvärderingen kan lämpligen ta sikte på i vart fall bestämmelsens ändamålsenlighet att uppfylla sitt syfte, dess tillämpbarhet – om bestämmelsens utformning ger tydlig vägledning för handläggare – samt dess proportionalitet – om inskränkningen i offentlighetsprincipen står i proportion till skyddsintresset. Det kan särskilt noteras att förslagets föremål är begränsat till uppgifter som härrör från riskvärderingar som har gjorts genom Arachne. För det fall ytterligare skyddsbehov identifieras i framtiden kan vid behov kompletterande reglering införas där föremålet tar sikte på alla uppgifter som härrör från Arachne (se vidare avsnitt 8.5.7).

12 Författningskommentar

12.1 Förslaget till lag om ändring i offentlighets- och sekretesslagen (2009:400)

17 kap.

Riskvärderingar vid genomförande av EU:s budget

7 d §

Sekretess gäller för uppgift som härrör från en riskvärdering som har gjorts genom ett sådant system som avses i artikel 36.2 d i Europaparlamentets och rådets förordning (EU, Euratom) 2024/2509 av den 23 september 2024 om finansiella regler för unionens allmänna budget (omarbetning), om det kan antas att syftet med den förvaltning, övervakning, kontroll och revision som ska ske i enlighet med Europaparlamentets och rådets förordning (EU, Euratom) 2024/2509 motverkas om uppgiften röjs.

Paragrafen är ny. Övervägandena finns i avsnitt 8.5.6 och 8.5.7.

De uppgifter som omfattas av sekretess är uppgifter som härrör från en riskvärdering som har gjorts genom ett visst system som behandlas i artikel 36.2 d i budgetförordningen. Verktyget har namnet Arachne.

Endast uppgifter som härrör från riskvärderingar som *redan har gjorts* omfattas. I den mån den tekniska utformningen av Arachne innebär att en riskvärdering genereras först på begäran av en myndighet och någon sådan begäran inte har gjorts förvaras över huvud taget inte några uppgifter som härrör från en sådan riskvärdering hos myndigheten.

I begreppet *uppgifter som härrör från riskvärderingar* ingår till att börja med information om vilka värden som en viss aktör har beträffande olika riskindikatorer. Även den information som en användare

får del av om kopplingar till andra bolag samt om de bolag och personer som berörs kan ingå. Dessutom kan den information som nås via länkar till externa källor ingå i sekretessens föremål. Exakt vilken information som ingår får bedömas i det enskilda fallet, bland annat utifrån den tekniska utformningen av användargränssnittet.

Sekretess gäller för uppgifterna *oavsett i vilken verksamhet som de förekommer*. Om myndigheter delar uppgifter som härrör från riskvärderingar mellan varandra kommer bestämmelsen att vara en primär sekretessbestämmelse vid såväl den överlämnande som den mottagande myndigheten. Om sekretess gäller vid den mottagande myndigheten kan det inte antas att syftet med sådan verksamhet som avses i bestämmelsen motverkas om uppgiften lämnas till myndigheten.

Sekretessens styrka beskrivs på så sätt att sekretess gäller om det kan antas att syftet med viss verksamhet motverkas om uppgiften röjs. Regelns utformning med ett rakt skaderekvisit innebär en presumtion för offentlighet. Vid bedömningen av om skaderekvisitet är uppfyllt bör bland annat vägas in vilken effekt ett offentliggörande av uppgiften skulle kunna antas få på det framtida samarbetet inom EU som förutsätts i budgetförordningen (jfr prop. 2012/13:7 s. 20).

Den verksamhet som avses är den förvaltning, övervakning, kontroll och revision som ska ske i enlighet med budgetförordningen. Det handlar alltså om den kontroll- och granskningsverksamhet som ska bedrivas av de svenska myndigheter som deltar i genomförandet av EU:s budget. Formuleringen anknyter till definitionen i artikel 2.7 i budgetförordningen, enligt vilken budgetgenomförande betyder utförande av verksamheter som rör förvaltning, övervakning, kontroll och revision av budgetanslag i enlighet med de metoder som föreskrivs i artikel 62.

Bestämmelsen innebär att sekretess kan hindra ett utlämnande så länge som uppgiften har betydelse i verksamheten. När uppgifterna inte längre har betydelse i verksamheten upphör sekretessen och uppgifterna får lämnas ut. Det förhållandet att det framgår av artikel 36.7 i budgetförordningen att uppgifterna i Arachne endast ska lagras under den period som är nödvändig och proportionell för att uppfylla det syfte som fastställs i punkt 2 d – det vill säga att motverka oriktigheter – kan tala för att uppgifterna har betydelse för verksamheten så länge som de lagras. En prövning i det enskilda fallet behöver göras av den myndighet som hanterar frågan om utlämnande.

Kommittédirektiv 2024:125

Användning av vissa verktyg för att skydda EU:s finansiella intressen

Beslut vid regeringssammanträde den 12 december 2024

Sammanfattning

En särskild utredare ska undersöka de rättsliga förutsättningarna för svenska myndigheter att använda riskbedömningsverktyget Arachne och uppfylla kraven enligt den omarbetade budgetförordningen, bl.a. skyldigheterna inom ramen för systemet för tidig upptäckt och uteslutning (Edes), för att motverka felaktiga utbetalningar och bedrägerier i samband med hantering av EU-medel.

Utredaren ska bl.a.

- kartlägga vilka uppgifter myndigheterna skulle få tillgång till, registrera eller annars utbyta vid en användning av Arachne och inom ramen för Edes, samt vilken tillgång andra aktörer skulle få till uppgifterna,
- kartlägga och bedöma vilka skyldigheter som svenska myndigheter skulle ha vid en användning av Arachne och inom ramen för Edes,
- utifrån kartläggningen bedöma om det finns behov av ändrade regler för att svenska myndigheter ska kunna använda Arachne och uppfylla sina skyldigheter inom ramen för Edes,
- lämna nödvändiga författningsförslag.

Uppdraget ska redovisas senast den 19 november 2025.

Att motverka felaktiga utbetalningar, dubbelfinansiering och andra oegentligheter är centralt för skyddet av EU:s finansiella intressen

Det är viktigt att de svenska myndigheter som deltar i genomförandet av EU:s budget har ändamålsenliga system för att säkerställa tillgång till den information som behövs för att göra riskbedömningar av stödsökande och slutliga stödmottagare, och för att i efterhand kontrollera dessa. Bristfälliga kontroller av de stödsökande riskerar att leda till felaktiga utbetalningar av EU-medel.

I dagsläget saknar myndigheterna tillräckliga möjligheter att strukturerat och regelmässigt utbyta och samköra uppgifter om utbetalda medel och stödsökande respektive slutliga stödmottagare. Detta medför svårigheter att kontrollera riktigheten i vissa ingivna underlag som ligger till grund för beslut om stöd. Ett förbättrat informationsutbyte mellan myndigheterna kan därför bidra till att förebygga och motverka otillåten dubbelfinansiering och andra typer av bedrägerier.

Riskbedömningsverktyget Arachne och systemet för tidig upptäckt och uteslutning (Edes)

Arachne är ett verktyg för riskbedömning som Europeiska kommissionen har utvecklat för att hjälpa medlemsstaternas myndigheter att kontrollera och följa upp användningen och förvaltningen av EU-medel. För närvarande är användningen av Arachne frivillig, och tjänsten tillhandahålls kostnadsfritt av kommissionen.

Systemet för tidig upptäckt och uteslutning (Edes) inrättades 2016 och syftar till att göra det lättare att tidigt upptäcka personer eller aktörer som konstaterats utgöra en risk för EU:s ekonomiska intressen, och utesluta dem från att ta del av EU-medel. En uteslutning kan gälla i upp till fem år. Systemet omfattar i dag hantering av EU-medel inom s.k. direkt och indirekt förvaltning, dvs. medel som EU-institutioner eller deras partnerorganisationer förvaltar. Reglerna om Edes finns i Europaparlamentets och rådets förordning (EU, Euratom) 2024/2509 av den 23 september 2024 om finansiella regler för unionens allmänna budget (budgetförordningen).

Den omarbetade budgetförordningen innebär skärpta krav på rapportering av uppgifter och ett utökat tillämpningsområde för Edes

Hösten 2024 trädde den omarbetade budgetförordningen i kraft. Enligt den ska Arachne i möjligaste mån kunna använda automatiskt registrerade uppgifter från relevanta nationella och europeiska databaser. Av artikel 36 i budgetförordningen framgår också att de organ som deltar i genomförandet av EU:s budget fr.o.m. nästa programperiod ska göra viss information tillgänglig för kommissionen i ett maskinläsbart format. Kommissionen ska därefter registrera uppgifterna i Arachne. Det finns också möjlighet att registrera ytterligare uppgifter i Arachne, utöver de obligatoriska, för en mer komplett riskvärdering.

Av artikel 36 i budgetförordningen framgår också att kommissionen senast under 2027 ska presentera en utvärdering av Arachne. Kommissionen, ministerrådet och Europaparlamentet har gemensamt uttalat en avsikt att efter denna utvärdering överväga om det ska bli obligatoriskt för medlemsländerna att använda Arachne i sin handläggning och kontroll av EU-medel. Av budgetförordningen framgår vidare att Edes ska omfatta samtliga stöd som utbetalas under den nya programperioden. Edes ska därmed fr.o.m. 2028 omfatta även de EU-medel som hanteras inom ramen för delad förvaltning, dvs. medel som EU och medlemsstaterna förvaltar gemensamt. Det innebär bl.a. att förvaltande myndigheter och utbetalande organ ska kontrollera i Edes-databasen om en stödsökande är utesluten från att ta del av EU-medel, innan de beslutar om tilldelning eller utbetalning av sådana medel.

Enligt artiklarna 36 och 38 i budgetförordningen ska medlemsstaterna tillhandahålla vissa uppgifter om stödmottagare och underleverantörer till kommissionen, som sedan ska publicera uppgifterna på en central webbplats på europeisk nivå. Även denna skyldighet gäller fr.o.m. nästa programperiod.

Systemen har ansetts ändamålsenliga i en svensk kontext

Regeringen gav den 3 november 2021 en särskild utredare i uppdrag att utreda hanteringen av EU-medel i Sverige (dir. 2021:109). I uppdraget ingick att analysera om det finns behov av en gemensam plattform för hantering av information om sådana medel. I betänkandet

En ny organisation för förvaltning av EU-medel, som överlämnades till regeringen den 15 mars 2024, bedömer utredningen att myndigheter mer systematiskt än i dag behöver kunna dela information om EU-medel i syfte att uppfylla högt ställda krav på granskning och kontroll (SOU 2024:22 s. 23). Enligt utredningen skulle en svensk anslutning till Arachne kunna öka myndigheternas förmåga att på ett ändamålsenligt, effektivt och rättssäkert sätt dela information med varandra i syfte att motverka felaktiga utbetalningar och bedrägerier. Vidare bedömer utredningen att Edes är ändamålsenligt för att säkerställa att EU-medel inte utbetalas till uppenbart olämpliga aktörer. Utredningen anser dock att de rättsliga förutsättningarna behöver utredas närmare (SOU 2024:22 s. 448 och 455–457).

Uppdraget att säkerställa att svenska myndigheter uppfyller kraven i den omarbetade budgetförordningen och har förutsättningar att använda Arachne

Efter det att den omarbetade budgetförordningen har trätt i kraft behöver svenska myndigheter kunna uppfylla kraven i förordningen, bl.a. skyldigheterna inom ramen för Edes. Det finns därför behov av att utreda om det behövs ändrade regler för att uppfylla kraven. Även de rättsliga förutsättningarna för svenska myndigheter att registrera data i Arachne och använda verktyget för riskbedömning behöver utredas närmare.

Kartlägga tillgången till uppgifter och skyldigheter vid användning av Arachne och Edes

Arachne sammanställer information om aktörer i projekt från deltagande medlemsstaters nationella projektdatabaser med uppgifter i två kommersiella databaser som bl.a. innehåller information om cirka 400 miljoner företag och 200 miljoner företagsägare från hela världen samt företag och individer som tilldömts sanktioner eller andra påföljder. Med hjälp av denna sammanställning genererar Arachne en riskbedömning som syftar till att hjälpa förvaltningsmyndigheter att identifiera de projekt, stödmottagare, leverantörer och avtal där det finns risk för bedrägerier, intressekonflikter eller andra oegentligheter.

Uppgifter som utbyts inom ramen för Edes förvaras i en databas som inrättats och tillhandahålls av kommissionen (se artikel 144 i budgetförordningen). Edes-databasen innehåller uppgifter om personer och enheter som är uteslutna från möjligheten att motta EU-medel och som har ålagts ekonomiska sanktioner. Databasen är tillgänglig för personer och enheter som deltar i genomförandet av EU-budgeten, för att de ska kunna kontrollera dess uppgifter när de tilldelar kontrakt eller beslutar om stöd.

Det behövs en kartläggning av vilken tillgång svenska myndigheter skulle ha till uppgifter i Arachne och vilka skyldigheter de skulle få vid hanteringen av sådana uppgifter. Motsvarande kartläggning bör göras för uppgifter som mottas eller annars hanteras inom ramen för Edes och vid användning av Edes-databasen.

De svenska myndigheter som främst bedöms vara aktuella för att använda systemen är förvaltande och attesterande myndigheter i delad förvaltning, dvs. myndigheter som förvaltar medel tillsammans med kommissionen. Det kan innefatta utbetalande organ och myndigheter som deltar i genomförandet av Sveriges återhämtningsplan. Det behöver dock klarläggas om även andra myndigheter som deltar i genomförandet av EU:s budget kan komma att omfattas av de krav som gäller för Arachne respektive Edes-databasen enligt budgetförordningen.

Utredaren ska därför

- beskriva vilka myndigheter som kan komma att använda Arachne eller Edes-databasen,
- kartlägga och beskriva vilken typ av åtkomst de aktuella myndigheterna, vid användning av Arachne eller inom ramen för Edes, skulle få till uppgifter i Arachne eller i Edes-databasen när dessa används som ett led i handläggningen av ärenden eller vid kontrollåtgärder, med beaktande av eventuella begränsningar avseende vilka sökningar som får göras i systemet eller för vilka ändamål personuppgiftsbehandling får ske,
- kartlägga och beskriva vilka uppgifter som ska eller får registreras eller annars utbytas i Arachne och inom ramen för Edes, samt i vilken utsträckning som aktörer utanför den egna myndigheten skulle få tillgång till uppgifterna,

- kartlägga vilka regler som styr användningen av Arachne och bedöma vilka skyldigheter som berörda myndigheter skulle få vid en användning av verktyget, och
- kartlägga och bedöma vilka skyldigheter berörda myndigheter skulle få inom ramen för Edes, särskilt vid användning av Edes-databasen.

Finns det behov av skydd för uppgifter vid användning av Arachne eller Edes?

Enligt offentlighetsprincipen har allmänheten rätt att få insyn i statens och kommunens verksamhet, bl.a. genom rätten att ta del av allmänna handlingar hos myndigheter (se 2 kap. tryckfrihetsförordningen). Begränsningar av rätten att ta del av allmänna handlingar regleras i offentlighets- och sekretesslagen (2009:400), i det följande förkortad OSL, eller i lag som OSL hänvisar till.

I betänkandet En ny organisation för förvaltning av EU-medel framhålls att uppgifter som finns tillgängliga i Arachne kan komma att klassificeras som allmänna handlingar hos myndigheter som använder riskbedömningsverktyget. Uppgifterna skulle därmed kunna begäras ut av externa aktörer, under förutsättning att de inte omfattas av sekretess. Utredningen noterar samtidigt att det av kommissionens stadga för införandet och tillämpningen av Arachnes riskbedömningsverktyg vid förvaltningskontroller, den s.k. Arachnestadgan, framgår att resultaten av riskberäkningar som görs i systemet omfattas av villkoren för skydd av personuppgifter och inte får offentliggöras (SOU 2024:22 s. 453).

I betänkandet anges att liknande frågor kan uppstå i fråga om myndigheters hantering av uppgifter inom ramen för Edes. Förutsättningarna för offentliggörande av uppgifter ur Edes-databasen regleras i artikel 142 i budgetförordningen. Enligt denna reglering ska kommissionen som huvudregel offentliggöra viss information om uteslutningen och i tillämpliga fall om de ekonomiska sanktionerna, om det behövs för att förstärka uteslutningsbeslutets och de ekonomiska sanktionernas avskräckande verkan. Vidare framgår det av beskrivningen av integritetsskyddet inom Edes att uppgifter inte ska lämnas till en tredje part, om det inte finns någon rättslig skyldighet att göra

detta (Privacy Statement for the database of the Early Detection and Exclusion System [EDES], DPR-EC-04410).

Utredaren ska därför

- utifrån sin kartläggning bedöma i vilken utsträckning mottagna eller tillgängliga uppgifter inom ramen för Arachne och Edes kommer att utgöra allmänna handlingar i Sverige, och i vilken mån uppgifterna i sådana fall omfattas av befintliga sekretessbestämmelser eller om det finns behov av nya sekretessbestämmelser för att säkerställa att uppgifterna får ett tillfredsställande skydd, och
- lämna nödvändiga författningsförslag.

Finns det förutsättningar för att registrera eller annars utbyta uppgifter i Arachne eller inom ramen för Edes?

För att myndigheter ska kunna utbyta sekretessbelagda uppgifter krävs att en sekretessbrytande bestämmelse är tillämplig. I 10 kap. OSL finns ett antal sekretessbrytande bestämmelser och undantag från sekretess som gäller till förmån för såväl enskilda som myndigheter. Av 10 kap. 28 § OSL följer att sekretess inte hindrar att en uppgift lämnas till en annan myndighet, om uppgiftsskyldigheten följer av lag eller förordning. I 8 kap. 3 § OSL finns en motsvarande reglering för uppgifter som lämnas till en utländsk myndighet.

Av betänkandet En ny organisation för förvaltning av EU-medel framgår att vissa myndigheter är osäkra på om de skulle kunna registrera uppgifter i Arachne som omfattas av sekretess (SOU 2024:22 s. 456). I betänkandet anges att liknande frågor kan uppstå i fråga om myndigheters hantering av uppgifter som utbyts inom ramen för Edes.

Det kan inte uteslutas att uppgifter om stödsökande eller stödmottagares projekt omfattas av försvarssekretess enligt 15 kap. 2 § OSL. Den typen av uppgifter bör inte förekomma i systemen.

Utredaren ska därför

- utifrån sin kartläggning utreda och analysera om det, bland den data som får eller ska registreras eller annars utbytas i Arachne eller inom ramen för Edes, finns uppgifter som skulle kunna omfattas av sekretess, och om det finns rättsliga förutsättningar för svenska myndigheter att registrera eller annars utbyta dessa,

- analysera och bedöma vilket skydd eventuella sekretessbelagda uppgifter skulle ha i samband med andra medlemsstaters och EU-institutioners användning av Arachne och inom ramen för Edes,
- utreda hur Arachnes funktionalitet och användning påverkas om eventuella sekretessbelagda uppgifter inte kan registreras, särskilt i fråga om uppgifter som inte är obligatoriska att registrera,
- bedöma om det finns behov av ändrade regler för att svenska myndigheter ska kunna registrera uppgifter i Arachne eller uppfylla kraven inom ramen för Edes, och
- lämna nödvändiga författningsförslag.

Kan svenska myndigheter uppfylla kraven i den omarbetade budgetförordningen?

Enligt artikel 36.6 i budgetförordningen ska medlemsstaterna för program som beslutas under programperioden som löper fr.o.m. 2028 och framåt göra vissa uppgifter tillgängliga för kommissionen, som i sin tur ska registrera uppgifterna i Arachne. Enligt artikel 38 ska medlemsstaterna också göra vissa uppgifter tillgängliga för publicering på en av kommissionen tillhandahållen webbplats. Det behöver därför klarläggas om det finns några hinder för myndigheterna att uppfylla dessa skyldigheter.

Utredaren ska därför

- bedöma om det finns behov av ändrade regler för att svenska myndigheter ska kunna uppfylla de krav som ställs i den omarbetade budgetförordningen, särskilt i fråga om rapportering av uppgifter för registrering i Arachne, och
- lämna nödvändiga författningsförslag.

Behovet av ytterligare regler om skydd för den personliga integriteten och personuppgiftsbehandling

Ett utökat informationsutbyte kan innebära ett intrång i den enskildes personliga integritet. Regler om skydd för den personliga integriteten finns bl.a. i regeringsformen (2 kap. 6 § andra stycket), den europeiska konventionen angående skydd för de mänskliga rättigheterna och de

grundläggande friheterna (artikel 8) och Europeiska unionens stadga om de grundläggande rättigheterna (artiklarna 7 och 8). Ett allmänt skydd för den personliga integriteten finns även i 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), i det följande förkortad EU:s dataskyddsförordning.

Den information som svenska myndigheter skulle kunna behöva behandla vid användning av Arachne eller inom ramen för Edes kan innehålla personuppgifter. För personuppgiftsbehandling i allmänhet gäller EU:s dataskyddsförordning. Denna förordning kompletteras i olika avseenden av nationella författningar, t.ex. lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen). Förutom dataskyddslagen finns även registerförfattningar som reglerar hur personuppgifter får behandlas i vissa offentliga verksamheter. Vidare finns ett dataskyddsombud på EU-nivå, som bl.a. ansvarar för att tillhandahålla information om de register som finns och validera de konsekvensbedömningar av uppgiftsskydd som görs av kommissionen.

När vissa myndigheter behandlar personuppgifter i syfte att t.ex. förebygga, förhindra eller upptäcka brottslig verksamhet gäller i stället brottsdatalagen (2018:1177). Om det för en myndighet som bedriver verksamhet inom brottsdatalagens tillämpningsområde finns en författning med bestämmelser som avviker från brottsdatalagen, ska dock den författningen tillämpas.

Den 1 januari 2025 träder lagen (2024:488) om personuppgiftsbehandling i vissa ärenden om stöd till civilsamhället i kraft. Lagen gäller för myndigheter och enskilda organ som handlägger ärenden om statligt reglerat stöd till civilsamhället, och syftar till att ge dessa möjlighet att behandla personuppgifter på ett ändamålsenligt sätt och skydda människor mot att deras personliga integritet kränks vid sådan behandling. I förarbetena till lagen anför regeringen att den föreslagna, gemensamma regleringen av behandling av personuppgifter i ärenden om stöd syftar till att säkerställa ett enhetligt och tillräckligt säkert skydd för personuppgifter, oberoende av vilket organ som handlägger ärendet (prop. 2023/24:119 s. 138).

När det gäller registerförfattningar har det också framhållits att bredare ändamålsbestämmelser kan skapa flexibilitet och förutsätt-

ningar att hålla jämna steg med samhällsutvecklingen (SOU 2023:100 s. 514). Om det finns behov av nya eller ändrade bestämmelser för att möjliggöra den personuppgiftsbehandling som en användning av Arachne medför eller som krävs för att uppfylla kraven inom ramen för Edes, finns det mot den bakgrunden skäl att överväga om regleringen bör samlas i en särskild lag och om den kan vara brett formulerad för att ge myndigheterna möjlighet att behandla personuppgifter på ett ändamålsenligt sätt.

Utredaren ska därför

- kartlägga vilken personuppgiftsbehandling som en anslutning till Arachne och Edes skulle medföra,
- kartlägga det skydd för personuppgifter som finns i Arachne och Edes-databasen, samt värdera eventuella risker som kommissionens dataskyddsombud har identifierat,
- utreda om det finns behov av nya eller ändrade bestämmelser för att möjliggöra den personuppgiftsbehandling som en användning av Arachne medför eller som krävs för att uppfylla kraven inom ramen för Edes,
- lämna nödvändiga författningsförslag.

Konsekvensbeskrivningar

Utredaren ska, i enlighet med förordningen (2024:183) om konsekvensutredningar, redovisa en konsekvensutredning. Utredaren ska särskilt redovisa vilka konsekvenser utredarens förslag innebär för skyddet av EU:s finansiella intressen, spridningen av personuppgifter inom och mellan myndigheter samt skyddet av den personliga integriteten.

Kontakter och redovisning av uppdraget

Utredaren ska hålla sig informerad om och beakta relevant arbete på området som pågår inom Regeringskansliet och EU.

Vid genomförandet av uppdraget ska utredaren samråda med de delar av Regeringskansliet som ansvarar för hantering av EU-medel, samt övriga berörda myndigheter och organisationer.

De myndigheter som deltar i genomförandet av Sveriges återhämtningsplan inom ramen för faciliteten för återhämtning och resiliens har fått i uppdrag att analysera sina respektive förutsättningar att använda Arachne (se t.ex. KN2024/01135). Utredaren ska beakta återrapporteringen från dessa uppdrag.

Uppdraget ska redovisas senast den 19 november 2025.

(Finansdepartementet)

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.

Statens offentliga utredningar 2025

Systematisk förteckning

Klimat- och näringslivsdepartementet

Kulturdepartementet

Landsbygds- och infrastrukturdepartementet

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]

Utrikesdepartementet

Skydd för biologisk mångfald i havsområden utanför nationell jurisdiktion. [36]

En säkrare utrikesförvaltning. [94]