



Försvarsdepartementet

103 33 Stockholm

Er referens
Anneli HagdahlVår referens
Linda Eriksson

Remissvar gällande Europaparlamentets och rådets förordning om dataförvaltning (dataförvaltningsakten), (Fö2020/01225)

I expedieringen av remissen hänvisades till "Europaparlamentets och rådets förordning om europeisk datastyrning (datastyrningsförordningen) KOM (2020) 762". FOI misstänker felskrivning och har därför lämnat synpunkter på COM (2020) 767 och det namn som förordningen fått i förslaget till förordning.

Totalförsvarets forskningsinstitut (FOI) har – från de utgångspunkter myndigheten har att beakta – följande synpunkter på dataförvaltningsakten, COM (2020) 767.

Sammanfattning

FOI föreslår att myndigheten tillsammans med övriga försvarsmyndigheter i ges rätt till undantag från förordningen för data som innehas av försvarsmyndigheter. I annat fall riskeras att uppgifter som är till men för rikets säkerhet röjs. Undantaget som rör data som är skyddade av skäl som rör nationell säkerhet, försvar eller allmän säkerhet är inte tillräckligt utan behöver utökas för att ge FOI stöd i förordningen för att skydda all sådana data och information som inte omfattas av sekretess enligt offentlighets- och sekretesslagen.

I likhet med FOI:s remissvar avseende betänkandet Innovation genom information (SOU 2020:55, 12020/02346) kan FOI i detta svar konstatera att Sverige i ett internationellt sammanhang torde ha en speciell situation när förordning om dataförvaltning blir direkt gällande i Sverige. Detta mot bakgrund av att landet sedan tidigare har en offentlighetsprincip med utgångspunkten att all information i en myndighet som inte är sekretessbelagd är offentlig och ska lämnas ut på begäran. Den utgångspunkten medför att mer information kommer att lämnas ut för vidareutnyttjning av data i Sverige än i många andra länder. Öppenheten innebär en önskad insyn i förvaltningen som inte är helt enkel eller försvarbar när det gäller skyddet för Sveriges säkerhet. Detta gör sig särskilt gällande när det gäller just försvarsforskning.

FOI:s uppfattning är vidare att förordningen måste ge FOI:s verksamhet åtminstone samma undantag som för verksamheten vid utbildnings- och kulturinstitut. I likhet med

FOI
Totalförsvarets forskningsinstitut

Postadress
FOI
164 90 STOCKHOLM

Besöksadress
Gullfossgatan 6, Kista

Leveransadress
Gullfossgatan 12, Kista

Telefon
08-55 50 30 00

Org.nr
202100-5182

registrator.@foi.se
www.foi.se

utbildnings- och kulturinstitut är myndighetens immateriella tillgångar av avgörande betydelse för FOI:s verksamhet.

FOI ser behov av förtydligande vad gäller användande av begreppen personuppgifter och icke-personuppgifter i de villkor som beskriver att åtgärder ska vidtas av datadelningsleverantörer vid lagring och överföring. FOI anser att det bör förtydligas att villkoren även omfattar skydd av personuppgifter vid lagring och överföring. Det är även oklart vilken rättslig grund myndigheter ska använda enligt förordning (EU) 2016/679 (GDPR) när den tillåter vidareutnyttjande av personuppgifter (jfr artikel 5.6). En annan fråga är på vilket sätt det är förenligt med finalitetsprincipen i GDPR att tillåta det vidareutnyttjande av personuppgifter som av allt att döma beskrivs i den aktuella förordningen.

FOI ser stora risker med de möjligheter som förordningen ger avseende etablering utanför unionen med tanke på aktuell utveckling inom EU vad gäller tredjelandsöverföringar och personuppgifter (EU-domen Schrems II). Leverantörer som är verksamma i EU kan omfattas av tredjeländers lagstiftning, vilka potentiellt inte är förenliga med EU-lagstiftning på området. Data med ursprung i unionens medlemsländer, som anges vara en dyrbar resurs, riskerar alltså bli åtkomliga för tredjeländers jurisdiktioner som inte följer EU:s dataskyddsram.

FOI befarar också att arbetet med utlämnande enligt den föreslagna förordningen kan komma att bli mycket kostsamt, kräva stora resurser i form av personalinsatser och behov av avancerad teknisk infrastruktur, som inte finns tillgänglig på myndigheten.

Allmänt om lagens tillämpningsområde och skyddet för olika rättigheter

Kommissionens avsikt med förordning om europeisk dataförvaltning COM (2020) 767 är att främja tillgängligheten och användbarheten för data genom att öka förtroendet mellan aktörer som hanterar data samt att stärka mekanismer för datadelning inom EU. Förordningen ska tillämpas på data som innehas av offentliga myndigheter och som är skyddad på grund av affärshemlighet, insynsskydd för statistiska uppgifter, skydd av tredje parts immateriella rättigheter, och skydd av personuppgifter (artikel 3.1).

FOI ifrågasätter hur det är tänkt att myndigheters verksamhet ska kunna fortgå om myndigheterna i sin verksamhet inte ska beakta skydd för affärshemligheter, skydd för tredje parts immateriella rättigheter och personuppgifter. Enligt FOI:s mening främjar det inte förtroendet för en myndighets uppdragsgivare och leverantörer om dessa inte kan lita på att en myndighet t.ex. kommer att skydda deras affärshemligheter (enligt offentlighets- och sekretesslagen), immateriella rättigheter eller personuppgifter.

FOI uppfattar att förordningens tillämpning möjligen bygger på en missuppfattning om att myndigheters information inte omfattas av rättigheter som behöver skyddas, utan fritt kan delas. Överlag kan förordningen uppfattas så att den innebär att flera i rättsordningar erkända regler och principer om rättigheter för enskilda inte respekteras. FOI befarar även när det gäller nationell lagstiftning som offentlighets- och sekretesslagen att den på sikt kommer att förlora i betydelse (t.ex. bestämmelser om företagshemligheter och utlämnande av personuppgifter).

FOI och immateriella rättigheter

I artikel 3.2c och skäl 8 till förordningen anges att data som innehas av kultur- och utbildningsanstalter, för vilka immateriella rättigheter i verk och andra handlingar är av betydelse, inte omfattas av förordningen. FOI:s uppfattning är att förordningen ska ge FOI:s verksamhet samma undantag som ges för verksamheten vid utbildnings- och kulturinstitut. I likhet med utbildnings- och kulturinstitut är myndighetens immateriella tillgångar av avgörande betydelse för FOI:s verksamhet. Faktum är att FOI:s huvudsakliga tillgångar är immateriella.

För att FOI ska ha möjlighet att fullgöra myndighetens uppdrag och leverera resultat till FOI:s huvuduppdragsgivare inom försvarssektorn behöver FOI värna sina immateriella tillgångar. FOI behåller därför i avtal och överenskommelser äganderätten till såväl bakgrundskunskap som forskningsresultat så att de immateriella tillgångarna kan användas för att bedriva fortsatt forskning, metod- och teknikutveckling samt nödvändig kunskapsuppbyggnad inom myndigheten. FOI kan via avtal och överenskommelser ge andra nyttjanderätt till FOI:s immateriella tillgångar så att FOI:s forskningsresultat kan nyttjas utanför försvarssektorn och främja annan forskning eller utveckling. Sådan nyttjanderätt lämnas dock i enlighet med de villkor som FOI uppställer för att säkerställa att nyttjandet inte hindrar FOI:s eget behov och användning. Nyttjandet får inte heller innebära att FOI:s huvuduppdragsgivare Försvarsmakten och Försvarets materielverk inte kan använda beställda resultat fritt i framtiden. FOI publicerar årligen en stor mängd rapporter som skyddas av upphovsrätten utan att nyttjanderätt lämnas.

Förordningen och nationell säkerhet

Det anges i artikel 3.2d att data som är skyddade av skäl som rör nationell säkerhet, försvar eller allmän säkerhet, inte omfattas av förordningen. FOI uppfattar att det är sekretessbelagd information som avses. FOI producerar i sin verksamhet som forskningsinstitut på totalförsvarsområdet, försvarsunderrättelsemyndighet och med Försvarsmakten som största uppdragsgivare, en stor mängd känslig information med anknytning till skydd av den nationella säkerheten och totalförsvaret som inte nödvändigtvis omfattas av sekretess enligt offentlighets- och sekretesslagen. Det är svårt att bedöma risker med tillgängliggörande och vidareutnyttjande av data, både utifrån aktuellt datainnehåll och ny kunskap som kan uppstå när data aggregeras från en eller flera myndigheter över tid. FOI ser med stor oro på utmaningarna att förutse vilken ny skyddsvärd information som kommer att uppstå och kan komma att lämnas ut när det digitala tillgängliggörandet ökar.

FOI föreslår att myndigheten tillsammans med övriga försvarsmyndigheter i ges rätt till undantag från förordningen genom att artikel 3.2 kompletteras med en punkt (f) om att detta kapitel inte ska tillämpas på data som innehas av försvarsmyndigheter. I annat fall finns risk för att uppgifter till men för rikets säkerhet kan komma att röjas. En sådan bestämmelse skulle dessutom göra tillämpningen av förordningen i Sverige mer i enlighet med hur förordningen kommer att tillämpas i andra länder som inte har en offentlighetsprincip som innebär att all information som inte är sekretessbelagd ska lämnas ut.

Delning av information och behörigt organ

I artikel 3.3 anges att bestämmelserna i kapitel II inte medför någon skyldighet för offentliga myndigheter att tillåta vidareutnyttjande av data och befriar inte heller

offentliga myndigheter från deras konfidentialitetskrav. Vidare beskrivs i artikel 7.3 samt skäl 21 att de behöriga organ som medlemsstaterna ska utse får anförtros uppgiften att bevilja tillgång till vidareutnyttjande av de kategorier av data som avses i artikel 3.1 om detta föreskrivs i sektorsspecifik unionslagstiftning eller i medlemsstaternas lagstiftning. FOI tolkar bestämmelsen i artikel 3.3. såsom att det är frivilligt och upp till varje offentlig myndighet att självständigt tillåta vidareutnyttjande av data, trots bestämmelsen i artikel 7.3. Om detta inte är en riktig tolkning bör detta förtydligas. Om artikel 7.3 innebär att ett behörigt organ kan göra en annan bedömning än den enskilda myndigheten i delningsfrågan motsätter sig FOI bestämmelsen.

Personuppgifter

I förordningen (artikel 5.3) anges att offentliga myndigheter får införa en skyldighet att vidareutnyttja endast förbehandlade data, vilket innefattar anonymisering eller pseudonymisering av personuppgifter eller radering av data som innehåller affärshemligheter. Fortsättningsvis används begreppet "icke-personuppgifter" i de villkor för vidareutnyttjande som stipuleras i artikel 5. Det är för FOI oklart om det är personuppgifter eller icke-personuppgifter som avses i skrivningarna om överföring till tredjeländer (artikel 5.11-13). Till exempel anges i artikel 5.13 att den offentliga myndigheten ska underrätta datainnehavaren om en eventuell tredjelandsoverföring. Detta förutsätter att den offentliga myndigheten besitter en nyckel som kan identifiera datainnehavaren i det data som vidareutnyttjaren fått tillgång till. Den aktuella informationen är därmed inte "icke-personuppgifter" utan personuppgifter enligt förordning (EU) 2016/679 (GDPR) då data kan hänföras till en fysisk person med kompletterande uppgifter (skäl 26). Samma problematik uppstår i artikel 30.5 då den offentliga myndigheten, den fysiska eller juridiska person, leverantören av datadelningstjänsten eller den erkända dataaltruismorganisationen ska underrätta datainnehavaren om förekomsten av en begäran från en förvaltningsmyndighet i ett tredjeland om att få tillgång till dess data. Detta kan endast ske om datainnehavaren är identifierad eller kan bli identifierad med kompletterande uppgifter.

På samma vis är det oklart vad som avses när villkor för tillhandahållande av datadelningstjänster beskrivs i artikel 11. Leverantören ska säkerställa och vidta åtgärder för att säkerställa en hög säkerhetsnivå för lagring och överföring av icke-personuppgifter. Även i artikel 30 om internationell tillgång hänvisas endast till icke-personuppgifter. FOI anser att det sker en sammanblandning mellan personuppgifter och icke-personuppgifter i förordningen och att det bör förtydligas att kraven även omfattar skydd av personuppgifter vid lagring och överföring. Det är även oklart vilken rättslig grund myndigheter ska använda enligt GDPR när den tillåter vidareutnyttjande av personuppgifter (jfr artikel 5.6). En annan fråga är på vilket sätt det är förenligt med finalitetsprincipen i GDPR att tillåta det vidareutnyttjande av personuppgifter som av allt att döma beskrivs i den aktuella förordningen.

Tredjelandsoverföring

FOI saknar inledningsvis en definition av vad som avses med tredje land enligt den remitterade förordningen. Rimligen avses med tredje land detsamma som avses enligt förordning (EU) 2016/679 (GDPR), dvs. länder utanför EU och EES, men detta framgår dock inte klart. Leverantörer av datadelningstjänster och enheter registrerade i registret över erkända dataaltruismorganisation kan vara etablerade utanför unionen om en rättslig företrädare utses i en av medlemsstaterna där tjänsterna erbjuds (t.ex. artikel

10.3, artikel 30). FOI instämmer i den problematik som EU-strategi för data (COM2020 66 final) konstaterar och ser stora utmaningar med tanke på aktuell utveckling inom EU vad gäller tredjelandsöverföringar och personuppgifter (EU-domen Schrems II). Leverantörer som är verksamma i EU kan omfattas av tredjeländers lagstiftning, vilken potentiellt inte är förenlig med EU-lagstiftning på området. FOI menar att det är förvånande att EU så villigt delar data med ursprung inom unionens medlemsländer med tredje land. Data med ursprung i unionens medlemsländer och som anges vara en dyrbar resurs riskerar alltså bli åtkomliga för tredjeländers jurisdiktioner som inte följer EU:s dataskyddsråd.

Delegation till kommissionen

I enlighet med vad FOI anför under rubriken Delning av information och behörigt organ om att ett beslut om att tillgängliggöra information alltid måste fattas av den aktuella myndigheten (jfr artikel 3.3) kan FOI inte tillstyrka en sådan bred och generell delegation till kommissionen angående bland annat bedömningen av säkerheten i tredje land (artikel 28 i kombination med artiklarna 5.9-5.11). I vart fall ska inte delegation kunna ges genom en underlåtenhet att invända mot en delegerad akt, se artikel 28.6.

FOI menar även att det behöver förtydligas vad som utgör ”mycket känsliga icke-personuppgifter” som kommissionen kan besluta om (artikel 5.11 i kombination med artikel 28).

Detta remissvar har beslutats av generaldirektör Jens Mattsson efter föredragning av projektledare Linda Eriksson. I den slutliga handläggningen har även jurist Åsa Berglund samt särskild rådgivare Mikael Wiklund deltagit.

Kista som ovan



Jens Mattsson



Linda Eriksson

Sändlista:

Försvarsdepartementet (fo.remissvar@regeringskansliet.se)
Anneli Hagdahl, (anneli.hagdahl@regeringskansliet.se)

Internt FOI:
FOI registrator
GD-sekreterare
Särskild rådgivare
Åsa Berglund
Hanna Lantz
Chefsjurist