Genomförande av EU:s dataförvaltningsförordning

Ds 2023:24

Regeringskansliet
Finansdepartementet

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

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

Omslag: Regeringskansliets standard
Tryck och remisshantering: Elanders Sverige AB, Stockholm 2023

ISBN 978-91-525-0671-4 (tryck)
ISBN 978-91-525-0672-1 (pdf)
ISSN 0284-6012

Finansdepartementet

Med anledning av att Europaparlamentet och rådet antog en europeisk dataförvaltningsförordning fick jag i oktober 2022 i uppdrag från Regeringskansliet att utreda hur EU-förordningen ska kompletteras i nationell rätt.

Jag får härmed överlämna promemorian Genomförande av EU:s dataförvaltningsförordning.

Göteborg i juli 2023.

Esmeralda Claesson

Innehåll

Sammanfattning

I promemorian lämnas förslag till genomförande av och komplettering till förordning (EU) 2022/868 av den 30 maj 2022 om europeisk dataförvaltningsförordning och om ändring av förordning (EU) 2018/1724 (dataförvaltningsakten), nedan dataförvaltningsförordningen. Bestämmelserna i EU-förordningen ska börja tillämpas den 24 september 2023.

Dataförvaltningsförordningen omfattar villkor för vidareutnyttjande av vissa typer av skyddade data från offentliga myndigheter, en ram för anmälan av och tillsyn över tillhandahållande av dataförmedlingstjänster, ett ramverk för frivillig registrering av och tillsyn över dataaltruismorganisationer samt inrättande av en europeisk datainnovationsstyrelse.

Det föreslås att förordningen genomförs genom en ny lag samt genom tillägg till lagen om offentliga sektorns tillgängliggörande av data för vidareutnyttjande.

Enligt dataförvaltningsförordningen ska en eller flera myndigheter utses till behöriga organ. Dessa ska bistå andra myndigheter som ska bevilja eller vägra tillgång till vissa kategorier av skyddade data för vidareutnyttjande. Myndigheten för digital förvaltning och Statistiska centralbyrån föreslås bli behöriga organ. Myndigheten för digital förvaltning ska vara huvudansvariga för uppgiften och också ha till uppgift att främja tillgängliggörande av skyddade data.

En gemensam informationspunkt ska inrättas enligt dataförvaltningsförordningen. Myndigheten för digital förvaltning föreslås tillhandahålla den gemensamma informationspunkten.

I dataförvaltningsförordningen finns det ramverk för leverantörer av dataförmedlingstjänster och för dataaltruismorganisationer. Post- och telestyrelsen föreslås bli s.k. behörig

myndighet för dessa. Uppgiften innebär att myndigheten ska ta emot anmälningar och ansökningar från dessa aktörer samt utöva tillsyn över dem.

Medlemsstaterna ska införa sanktioner för överträdelser av vissa artiklar i dataförvaltningsförordningen. Post- och telestyrelsen ska kunna besluta om en erinran mot leverantörer av dataförmedlingstjänster och dataaltruismorganisationer. Sanktionsavgift ska kunna beslutas för vissa överträdelser som leverantörer av dataförmedlingstjänster begår. Sanktionsavgift ska också kunna beslutas för överträdelser som vidareutnyttjare gör sig skyldiga till vid vissa tredjelandsöverföringar. Myndigheter som tillgängliggör vissa kategorier av skyddade data för vidareutnyttjande ska anmäla till tillsynsmyndigheten för dataförmedlingstjänster om de får kännedom om sådana överträdelser som kan leda till en sanktionsavgift.

Lagförslagen ska träda i kraft den 1 januari 2024.

1 Författningsförslag

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

Härigenom föreskrivs följande.

Inledande bestämmelse

1 § Denna lag kompletterar Europaparlamentets och rådets förordning (EU) 2022/868 av den 30 maj 2022 om europeisk dataförvaltning och om ändring av förordning (EU) 2018/1724 (dataförvaltningsakten), nedan EU:s dataförvaltningsförordning.

Termer och uttryck i lagen har samma betydelse som i EU:s dataförvaltningsförordning.

Tillsynsmyndighet

2 § Den myndighet som regeringen bestämmer ska vara tillsynsmyndighet enligt denna lag. Den myndighet som är tillsynsmyndighet enligt denna lag är behörig myndighet för dataförmedlingstjänster enligt artikel 13 EU:s dataförvaltningsförordning och behörig myndighet för registrering av dataaltruismorganisationer enligt artikel 23 EU:s dataförvaltningsförordning.

Informationsutbyte

3 § De myndigheter regeringen bestämmer ska på begäran lämna tillsynsmyndigheten de uppgifter som den behöver för att kunna utföra sitt tillsynsuppdrag enligt EU:s dataförvaltningsförordning.

Tillsynsmyndigheten ska på begäran lämna de uppgifter som andra myndigheter som regeringen bestämmer behöver för att kunna utföra tillsynsuppdrag enligt annan författning.

Erinran

4 § Tillsynsmyndigheten får meddela en erinran till en leverantör av dataförmedlingstjänster som bryter mot anmälningsskyldigheten enligt artikel 11, villkoren för tillhandahållande av dataförmedlingstjänster enligt artikel 12 eller villkoren för överföring av andra uppgifter än personuppgifter till tredjeland enligt artikel 31 EU:s dataförvaltningsförordning.

Tillsynsmyndigheten får meddela en erinran till en erkänd dataaltruismorganisation som bryter mot villkoren för registrering som erkänd dataaltruismorganisation i artiklarna 18, 20, 21 och 22 eller villkoren för överföring av andra uppgifter än personuppgifter till tredjeland enligt artikel 31 EU:s dataförvaltningsförordning.

Vite

5 § Tillsynsmyndigheten får förena förelägganden enligt artikel 14 EU:s dataförvaltningsförordning med vite.

Sanktionsavgift

6 § Tillsynsmyndigheten får ta ut en sanktionsavgift av en leverantör av en dataförmedlingstjänst vid överträdelser av

– anmälningsskyldigheten för leverantören av dataförmedlingstjänster enligt artikel 11,

– villkoren för tillhandahållande av dataförmedlingstjänster enligt artikel 12, eller

– villkoren för överföring av andra uppgifter än personuppgifter till tredjeland enligt artikel 31 EU:s dataförvaltningsförordning.

Tillsynsmyndigheten får ta ut en sanktionsavgift av en vidareutnyttjare för överträdelser av artikel 5.14 i EU:s dataförvaltningsförordning.

7 § En sanktionsavgift ska bestämmas till lägst 5 000 kronor och högst 10 000 000 kronor.

När avgiftens storlek bestäms ska särskild hänsyn tas till

1. överträdelsens art, allvar, omfattning och varaktighet,
2. eventuella åtgärder som leverantören av dataförmedlingstjänster eller vidareutnyttjaren vidtagit för att begränsa eller avhjälpa den skada som överträdelsen har orsakat,
3. tidigare överträdelser som leverantören av dataförmedlingstjänster eller vidareutnyttjaren har gjort sig skyldig till,
4. de ekonomiska vinster som leverantören av dataförmedlingstjänster eller vidareutnyttjaren gjort eller de förluster som de undvikit till följd av överträdelsen, och
5. andra försvårande eller förmildrande omständigheter.

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

8 § En sanktionsavgift får inte beslutas om överträdelsen omfattas av ett föreläggande som har förenats med vite och överträdelsen ligger till grund för en ansökan om utdömande av vitet.

9 § En sanktionsavgift får inte beslutas om den som avgiften ska tas ut av inte har fått tillfälle att yttra sig inom två år från den dag då överträdelsen ägde rum.

Ett beslut om sanktionsavgift ska delges.

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

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

indrivning av statliga fordringar m.m. Vid indrivning får verkställighet ske enligt utsökningsbalken.

En sanktionsavgift tillfaller staten.

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

Avgifter

12 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om skyldighet för leverantörer av dataförmedlingstjänster som omfattas av anmälningsskyldighet enligt artikel 11 EU:s dataförvaltningsförordning att betala avgift för tillsynsmyndighetens verksamhet enligt EU:s dataförvaltningsförordning och denna lag.

Överklagande

13 § Tillsynsmyndighetens beslut enligt artikel 14, 19 och 24 EU:s dataförvaltningsförordning eller enligt denna lag får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Denna lag träder i kraft den 1 januari 2024.

1.2 Förslag till lag om ändring i lagen (2022:818) om den offentliga sektorns tillgängliggörande av data

Härigenom föreskrivs i fråga om lag (2022:818) om den offentliga sektorns tillgängliggörande av data

dels att 1 kap. 2, 3, 4, 8 och 10 §§, 4 kap. 1 § samt 5 kap. 1 § ska ha följande lydelse,

dels att det ska införas sex nya paragrafer, 1 kap. 1 a § och 7 a §, 2 kap. 5 a och 6 a §§, 3 kap. 1 a § och 4 kap. 2 a §, och närmast före 2 kap. 6 a § en ny rubrik av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	1 kap.
	1 a §
	Denna lag kompletterar Europaparlamentets och rådets förordning (EU) 2022/868 av den 30 maj 2022 om europeisk dataförvaltning och om ändring av förordning (EU) 2018/1724 (dataförvaltningsakten), nedan EU:s dataförvaltningsförordning.
	2 §
Denna lag påverkar inte tillämpningen av bestämmelser i någon annan lag eller förordning som ger någon rätt att få tillgång till data eller som begränsar en sådan rätt.	Denna lag påverkar inte tillämpningen av bestämmelser i någon annan lag eller förordning som ger någon rätt att få tillgång till data *eller skyddade data* eller som begränsar en sådan rätt.

3 §

Om det i någon annan lag eller i en förordning finns mer långtgående krav i fråga om tillgängliggörande av data än i denna lag, ska de kraven tillämpas.	Om det i någon annan lag eller i en förordning finns mer långtgående krav i fråga om tillgängliggörande av data *eller skyddade data* än i denna lag, ska de kraven tillämpas.

4 §

I lagen avses med	
begäran om tillgängliggörande av data för vidareutnyttjande: en begäran om att data ska göras tillgängliga för vidareutnyttjande i enlighet med denna lag,	*begäran om tillgängliggörande av data för vidareutnyttjande*: en begäran om att data *eller skyddade data* ska göras tillgängliga för vidareutnyttjande i enlighet med denna lag *eller kapitel II EU:s dataförvaltningsförordning*,

bulknedladdning: nedladdning av en avgränsad datamängd,

data: information i digitalt format oberoende av medium,

dynamiska data: data som uppdateras ofta eller i realtid för att vara aktuella och relevanta att vidareutnyttja,

forskningsdata: data som till någon del är offentligt finansierade, som samlas in eller framställs inom ramen för vetenskaplig forskningsverksamhet och som görs direkt tillgängliga för vidareutnyttjande genom en dataplattform som är allmänt åtkomlig,

gränssnitt: en regeluppsättning för dynamiskt datautbyte mellan programvaror,

maskinläsbart format: ett filformat som är strukturerat på ett sådant sätt att det enkelt kan läsas av ett datorprogram,

offentligt företag: ett företag som en eller flera myndigheter har ett bestämmande inflytande över och som är verksamt

- inom de sektorer som framgår av 2 kap. 1 § och 5–8 §§ lagen (2016:1146) om upphandling inom försörjningssektorerna,

- som ett kollektivtrafikföretag enligt Europaparlamentets och rådets förordning (EG) nr 1370/2007 av den 23 oktober 2007 om

kollektivtrafik på järnväg och väg och om upphävande av rådets förordning (EEG) nr 1191/69 och (EEG) nr 1107/70,

- som ett lufttrafikföretag som har allmän trafikplikt enligt artikel 16 i Europaparlamentets och rådets förordning (EG) nr 1008/2008 av den 24 september 2008 om gemensamma regler för tillhandahållande av lufttrafik i gemenskapen, eller

- som ett rederi inom gemenskapen som uppfyller förpliktelser vid allmän trafik enligt artikel 4 i rådets förordning (EEG) nr 3577/92 av den 7 december 1992 om tillämpning av principen om frihet att tillhandahålla tjänster på sjötransportområdet inom medlemsstaterna (cabotage),

offentligt styrt organ: ett sådant organ som avses i 1 kap. 18 § lagen (2016:1145) om offentlig upphandling eller en sammanslutning av sådana organ,

skyddade data: sådana kategorier av skyddade data som avses i artikel 3.1 EU:s dataförvaltningsförordning,

vidareutnyttjande: bearbetning av data från den offentliga sektorn för valfritt ändamål,

värdefull datamängd: data som förtecknas i en genomförandeakt som har meddelats med stöd av artikel 14.1 i öppna data-direktivet,

öppna data-direktivet: Europaparlamentets och rådets direktiv (EU) 2019/1024 av den 20 juni 2019 om öppna data och vidareutnyttjande av information från den offentliga sektorn.

7 a §

Bestämmelserna om vidareutnyttjande av skyddade data ska endast tillämpas av myndigheter, dock inte av kulturinstitutioner och utbildningsinstitutioner.

8 §

Lagen ska tillämpas

1. när någon som har rätt att få tillgång till data enligt någon

1. när någon som har rätt att få tillgång till data *eller skyddade*

annan lag eller förordning framställer en begäran om tillgängliggörande av data för vidareutnyttjande,	*data* enligt någon annan lag eller förordning framställer en begäran om tillgängliggörande av data för vidareutnyttjande,
2. när en myndighet eller ett offentligt företag på eget initiativ tillgängliggör data som omfattas av lagen i syfte att de ska kunna vidareutnyttjas, *eller*	2. när en myndighet eller ett offentligt företag på eget initiativ tillgängliggör data som omfattas av lagen i syfte att de ska kunna vidareutnyttjas,
	3. när en myndighet på eget initiativ tillgängliggör skyddade data som omfattas av lagen i syfte att de ska kunna vidareutnyttjas, eller
3. när data lämnas till en statlig eller kommunal myndighet som ska använda dem i en konkurrensutsatt verksamhet som avser tillhandahållande av data.	*4*. när data lämnas till en statlig eller kommunal myndighet som ska använda dem i en konkurrensutsatt verksamhet som avser tillhandahållande av data.

Trots första stycket ska lagen inte tillämpas

1. när data, i andra fall än som avses i första stycket 3, lämnas

a) mellan statliga och kommunala myndigheter,

b) från ett organ som enligt 1 kap. 5 § andra stycket jämställs med en myndighet eller ett offentligt företag till en statlig eller kommunal myndighet, eller

2. när en statlig eller kommunal myndighet tillhandahåller data i en konkurrensutsatt verksamhet.

10 §

Lagen gäller inte för data som

1. omfattas av en sådan ensamrätt som följer av patentlagen (1967:837), mönsterskyddslagen (1970:485), lagen (1992:1685) om skydd för kretsmönster för halvledarprodukter, växtförädlarrättslagen (1997:306), varumärkeslagen (2010:1877) eller lagen (2018:1653) om företagsnamn,

2. tredje man innehar rätt till enligt lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk,

3. utgörs av datorprogram, eller
4. utgörs av logotyper, heraldiska vapen eller insignier.

Första stycket ska inte tillämpas avseende sådana kategorier av skyddade data som framgår av artikel 3.1 c i EU:s dataförvaltningsförordning.

2 kap.

5 a §

En myndighet som tillgängliggör skyddade data för vidareutnyttjande ska ställa upp villkor för vidareutnyttjandet i enlighet med artikel 5 i EU:s dataförvaltningsförordning.

En myndighet som tillgängliggör konfidentiella data till en vidareutnyttjare som avser att överföra dem till tredje land i enlighet med artikel 5.10 i EU:s dataförvaltningsförordning är skyldig att anmäla de överträdelser av artikel 5.14 som myndigheten får kännedom om till tillsynsmyndigheten enligt lag (2023:000) med kompletterande bestämmelser till EU:s dataförvaltningsförordning.

Förteckning över skyddade data som görs tillgängliga

6 a §

Den myndighet som regeringen bestämmer ska tillhandahålla en gemensam informationspunkt enligt artikel 8 i EU:s dataförvaltningsförordning.

En myndighet som tillgängliggör skyddade data för vidareutnyttjande ska informera den myndighet som tillhandahåller den gemensamma informationspunkten om sådana data och villkoren för vidareutnyttjande av dessa.

3 kap.

1 a §

En myndighet som innehar skyddade data får endast ge någon en exklusiv rätt att vidareutnyttja dessa data i den mån det är tillåtet enligt artikel 4 i EU:s dataförvaltningsförordning.

4 kap.

1 §

En myndighet eller ett offentligt företag som har rätt att ta ut en avgift för att tillgängliggöra data	En myndighet eller ett offentligt företag som har rätt att ta ut en avgift för att tillgängliggöra data

för vidareutnyttjande får inte beräkna den till ett högre belopp än vad som följer av 2–6 §§.	*eller skyddade data* för vidareutnyttjande får inte beräkna den till ett högre belopp än vad som följer av 2–6 §§.
	2 a §
	Vid tillgängliggörande av skyddade data får en avgift, utöver vad som följer av 2 § första stycket första meningen, också täcka sådana kostnader som framgår av artikel 6.5 i EU:s dataförvaltningsförordning.

5 kap.

1 §

En myndighet ska inom fyra veckor avgöra ett ärende till följd av en begäran om tillgängliggörande av data för vidareutnyttjande.

Om en sådan begäran avser skyddade data ska ärendet avgöras inom åtta veckor.

Tidsfristen får förlängas med ytterligare fyra veckor, om en begäran är omfattande eller komplicerad. Myndigheten ska underrätta sökanden om förlängningen och redovisa skälen för den senast tre veckor från den dag då begäran kom in.

Denna lag träder i kraft den 1 januari 2024.

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

Härigenom föreskrivs följande.

Inledande bestämmelse

1 § Denna förordning innehåller bestämmelser som kompletterar

1. Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), här benämnd EU:s dataskyddsförordning, och

2. lagen (2023:000) med kompletterande bestämmelser till EU:s dataförvaltningsförordning.

Tillsynsmyndighet

2 § Post- och telestyrelsen är tillsynsmyndighet enligt lagen med kompletterande bestämmelser till EU:s dataförvaltningsförordning.

Informationsutbyte

3 § Integritetsskyddsmyndigheten och Konkurrensverket ska på begäran lämna tillsynsmyndigheten de uppgifter som den behöver för att kunna utföra sitt tillsynsuppdrag enligt EU:s dataförvaltningsförordning.

Tillsynsmyndigheten ska på begäran lämna Integritetsskyddsmyndigheten de uppgifter myndigheterna behöver för att kunna utföra uppgiften som nationell dataskyddsmyndighet enligt 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) och lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

Tillsynsmyndigheten ska på begäran lämna Konkurrensverket de uppgifter myndigheten behöver för att kunna utföra uppgiften som nationell konkurrensmyndighet enligt rådets förordning (EG) nr 1/2003 av den 16 december 2002 om tillämpning av konkurrensreglerna i artiklarna 81 och 82 i fördraget och konkurrenslagen (2008:579).

Avgift

4 § Tillsynsmyndigheten ska årligen ta ut en proportionerlig avgift från leverantörer av dataförmedlingstjänster enligt 12 § lagen (2023:000) med kompletterande bestämmelser till EU:s dataförvaltningsförordning.

Post- och telestyrelsen får meddela de närmare föreskrifter som behövs om avgiften.

Denna förordning träder i kraft den 1 januari 2024.

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

Härigenom föreskrivs att 4 och 19 §§ förordning (2007:951) med instruktion för Post- och telestyrelsen ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*

4 §

Post- och telestyrelsen har till uppgift att

1. främja tillgången till säkra och effektiva elektroniska kommunikationer, inbegripet att se till att samhällsomfattande tjänster finns tillgängliga, och att främja tillgången till ett brett urval av elektroniska kommunikationstjänster,
2. främja utbyggnaden av och följa tillgången till bredband och mobiltäckning i alla delar av landet, inbegripet att skapa förutsättningar för samverkan mellan myndigheter som kan bidra till utbyggnaden av bredband,
3. svara för att möjligheterna till radiokommunikation och andra användningar av radiovågor utnyttjas effektivt,
4. svara för att nummer ur nationella nummerplaner utnyttjas på ett effektivt sätt,
5. främja en effektiv konkurrens,
6. övervaka pris- och tjänsteutvecklingen,
7. bedriva informationsverksamhet riktad till konsumenter,
8. följa utvecklingen när det gäller säkerhet vid elektronisk kommunikation och uppkomsten av eventuella miljö- och hälsorisker,
9. pröva frågor om tillstånd och skyldigheter, fastställa och analysera marknader samt utöva tillsyn och pröva tvister enligt lagen (2022:482) om elektronisk kommunikation,
10. meddela föreskrifter enligt förordningen (2022:511) om elektronisk kommunikation,
11. upprätta och offentliggöra planer för frekvensfördelning till ledning för radioanvändningen samt offentliggöra information av

allmänt intresse om rättigheter, villkor, förfaranden och avgifter som rör radiospektrumanvändningen,

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

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

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

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

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

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

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

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

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

21. vara tillsynsmyndighet enligt lagen (2018:1174) om informationssäkerhet för

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

21. vara tillsynsmyndighet enligt lagen (2018:1174) om informationssäkerhet för

samhällsviktiga och digitala tjänster.	samhällsviktiga och digitala tjänster, *och* *22. vara tillsynsmyndighet enligt lagen (2023:000) med kompletterande bestämmelser till EU:s dataförvaltningsförordning.*

19 §

Bestämmelser om avgifter för Post- och telestyrelsens verksamhet finns i

– 4 kap. 21 § postlagen (2010:1045),

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

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

– 15 § radioutrustningslagen (2016:392),

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

– 7 § lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering, *och*	– 7 § lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering,
– förordningen (2016:602) om finansiering av Post- och telestyrelsens verksamhet.	– förordningen (2016:602) om finansiering av Post- och telestyrelsens verksamhet, *och* – 12 § lagen (2023:000) med *kompletterande bestämmelser till EU:s dataförvaltnings-förordning.*

Denna förordning träder i kraft den 1 januari 2024.

1.5 Förslag till förordning om ändring i förordning (2016:822) med instruktion för Statistiska centralbyrån

Härigenom föreskrivs att 2 § förordning (2016:822) med instruktion för Statistiska centralbyrån ska ha följande lydelse.

Nuvarande lydelse *Föreslagen lydelse*

2 §

Myndigheten ska

1. vara nationell statistikbyrå med den innebörd som anges i Europaparlamentets och rådets förordning (EG) nr 223/2009 av den 11 mars 2009 om europeisk statistik och om upphävande av Europaparlamentets och rådets förordning (EG, Euratom) nr 1101/2008 om utlämnande av insynsskyddade statistiska uppgifter till Europeiska gemenskapernas statistikkontor, rådets förordning (EG) nr 322/97 om gemenskapsstatistik och rådets beslut 89/382/EEG, Euratom om inrättande av en kommitté för Europeiska gemenskapernas statistiska program, i lydelsen enligt Europaparlamentets och rådets förordning (EU) 2015/759,
2. utföra de uppgifter gällande årsrapporter som Sverige har enligt artikel 11.4 i Europaparlamentets och rådets förordning (EG) nr 223/2009,
3. göra långsiktiga prognoser inom arbetsmarknads-, befolknings- och utbildningsområdet,
4. vara nationell koordinator för Internationella valutafondens gemensamma datastandard i Sverige,
5. verka för samarbete mellan de statistikansvariga myndigheterna,
6. ge råd och stöd till statistikansvariga myndigheter i principiella frågor om den officiella statistikens kvalitet och i frågor om att underlätta uppgiftslämnandet,
7. senast den 31 mars varje år lämna en rapport till regeringen om systemet för den officiella statistiken, med en analys av de utvärderingar av kvaliteten som de statistikansvariga myndigheterna

ska göra enligt 13 a § förordningen (2001:100) om den officiella statistiken,

8. föra en förteckning över statistikansvariga myndigheters statistikprodukter,

9. sammanställa en årlig publiceringsplan för den officiella statistiken, *och*

10. förvalta och utveckla det fördelningsanalytiska statistiksystemet för inkomster och transfereringar.

9. sammanställa en årlig publiceringsplan för den officiella statistiken,

10. förvalta och utveckla det fördelningsanalytiska statistiksystemet för inkomster och transfereringar, *och*

11. vara behörigt organ enligt artikel 7 Europaparlamentets och rådets förordning (EU) 2022/868 av den 30 maj 2022 om europeisk dataförvaltning och om ändring av förordning (EU) 2918/1724 (dataförvaltningsakten).

Denna förordning träder i kraft den 1 januari 2024.

1.6 Förslag till förordning om ändring i förordning (2018:1486) med instruktion för Myndigheten för digital förvaltning

Härigenom föreskrivs att 6 och 6 a §§ förordning (2018:1486) ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
6 §	
Myndigheten ska också	
1. delta i och främja nationellt och internationellt standardiseringsarbete inom sitt verksamhetsområde,	
2. främja öppen och data-driven innovation samt tillgängliggörande och vidareutnyttjande av *öppna* data från den offentliga förvaltningen	2. främja öppen och data-driven innovation samt tillgängliggörande och vidareutnyttjande av data från den offentliga förvaltningen
3. främja att det vid förvaltningsgemensam utveckling av digitala tjänster tas hänsyn till användares behov,	
4. främja att information och tjänster som tillhandahålls digitalt av den offentliga förvaltningen är tillgängliga för alla oavsett funktionsförmåga,	
5. ge vägledning till den offentliga förvaltningen i frågor om digitala investeringar inom ramen för den förvaltningsgemensamma digitaliseringen, och	
6. ge vägledning till den offentliga förvaltningen i juridiska frågor inom ramen för den förvaltningsgemensamma digitaliseringen. Förordning (2022:821).	
6 a §	
Myndigheten ska digitalt publicera en sådan förteckning över data som har gjorts tillgängliga eller sökbara på internet som anges i 2 kap. 6 § lagen (2022:818) om den offentliga sektorns tillgängliggörande av data. Myndigheten får meddela närmare föreskrifter om	

innehållet i och utformningen av förteckningen och om den information som ska lämnas om data som görs tillgängliga eller sökbara i förteckningen.

Myndigheten ska också digitalt publicera en sådan förteckning över de myndigheter som är skyldiga att ta ut en avgift vid tillgängliggörande av data som anges i 4 kap. 9 § lagen om den offentliga sektorns tillgängliggörande av data.

Myndigheten ska tillhandahålla en gemensam informationspunkt i enlighet med artikel 8 Europaparlamentets och rådets förordning (EU) 2022/868 av den 30 maj 2022 om europeisk dataförvaltning och om ändring av förordning (EU) 2918/1724 (dataförvaltningsakten).

Denna förordning träder i kraft den 1 januari 2024.

2 Bakgrund

2.1 Uppdraget

Europaparlamentet och rådet har antagit förordning (EU) 2022/868 av den 30 maj 2022 om europeisk dataförvaltningsförordning och om ändring av förordning (EU) 2018/1724 (dataförvaltningsakten), nedan dataförvaltningsförordningen. Bestämmelserna i EU-förordningen ska börja tillämpas den 24 september 2023. Förordningstexten finns i bilaga 1.

Dataförvaltningsförordningen omfattar villkor för vidareutnyttjande av vissa typer av skyddade data från offentliga myndigheter, en ram för anmälan av och tillsyn över tillhandahållande av dataförmedlartjänster, ett ramverk för frivillig registrering av och tillsyn över dataaltruismorganisationer samt inrättande av en europeisk datainnovationsstyrelse. Dataförvaltningsförordningen är en del av genomförandet av EU:s datastrategi.

Inom Finansdepartementet har en sakkunnig utredare haft i uppdrag att analysera och vid behov lämna förslag på hur EU-förordningen ska kompletteras i nationell rätt (I 2022:D). I denna promemoria redogörs för utredarens slutsatser och förslag.

En EU-förordning är bindande och direkt tillämplig i varje medlemsstat. En sådan rättsakt varken ska eller får genomföras eller transformeras till nationell rätt, och medlemsstaterna får inte utfärda bestämmelser i sådana frågor som regleras i en EU-förordning. Det är endast om svensk rätt anses strida mot en EU-förordning, om den föreskriver en skyldighet eller en möjlighet att vidta nationella lagstiftningsåtgärder eller då det behövs andra åtgärder till stöd för en EU-förordnings syfte som ändringar i svensk rätt aktualiseras. En sådan åtgärd kan exempelvis vara att införa regler av verkställande karaktär för att en EU-förordnings bestämmelser ska fungera i

praktiken, t.ex. i fråga om vilken eller vilka nationella myndigheter eller andra organ som ska hantera förordningen.

Denna promemoria syftar till att analysera vilka kompletteringar som krävs i nationell rätt för att dataförvaltningsförordningen ska vara genomförd i Sverige. En central del av analysen är att utreda vilka myndigheter som påverkas av förordningen och vilka myndigheter som föreslås få nya uppgifter med anledning av förordningen.

2.2 Inledning

Den digitala tekniken förändrar människors liv, från hur vi kommunicerar till hur vi lever och arbetar. Digitaliseringen kan lösa många av de utmaningar som människor står inför och kan öppna möjligheter när det t.ex. gäller att skapa jobb, främja utbildning, stimulera konkurrenskraft och innovation samt att bekämpa klimatförändringarna och möjliggöra en grön omställning.

Under det senaste årtiondet har den digitala tekniken förändrat ekonomin och samhället genom sin inverkan på alla verksamheter och det dagliga livet. I centrum för den omvandlingen står data. Datadriven innovation kommer att medföra enorma fördelar för både unionsmedborgare och ekonomin, t.ex. genom förbättrad medicin och precisionsmedicin, genom tillhandahållande av ny mobilitet och genom dess bidrag till den europeiska gröna given. För att göra den datadrivna ekonomin inkluderande för alla unionsmedborgare måste den digitala klyftan minska, kvinnors deltagande i dataekonomin stimuleras och europeisk spetskompetens inom tekniksektorn främjas.

För att europeiska samhällen och ekonomier ska kunna anpassas till den digitala tidsåldern har EU åtagit sig att skapa en säker digital miljö för människor och företag på ett sätt som är inkluderande och tillgängligt för alla. Det innebär att man möjliggör en digital omställning som garanterar EU:s värden och skyddar medborgarnas säkerhet och grundläggande rättigheter samtidigt som man stärker EU:s digitala suveränitet.

2.3 Sveriges digitaliseringspolitik

Målet för digitaliseringspolitiken är att Sverige ska vara bäst i världen på att använda digitaliseringens möjligheter (prop. 2011/12:1, utg.omr. 22, bet. 2011/12:TU1, rskr. 2011/12:87). Regeringens mål för digitaliseringen är en ökad digitalisering av den offentliga förvaltningen och att undanröja hinder för ökad digitalisering. Målet är att delningen av data ska öka.

2.3.1 Nationell datastrategi för Sverige

I oktober 2021 antogs en nationell datastrategi för Sverige, Data – en underutnyttjad resurs för Sverige (I2021/02739). Strategin sammanfattar ett antal regeringsbeslut med uppdrag som fattades under året med finansiering från bl.a. det nationella innovationsrådet och som utgör ett komplement till den nationella digitaliserings-strategin och AI-inriktningen och syftar till att främja olika former av öppen och kontrollerad datadelning för ökad tillgång till data för bl.a. artificiell intelligens och digital innovation (prop. 2021:22:225 s. 62).

Datastrategin beslutades med motivet att följa upp EU:s ambition att gå i spetsen för utvecklingen av ett datadrivet samhälle. Strategin syftar till att öka tillgången till data och därigenom stärka Sveriges konkurrenskraft genom att bättre nyttja digitala datatillgångar. Målet är att Sverige ska vara en ledande datadelningsnation inom AI och digital innovation för att stärka välfärden, svensk konkurrenskraft och bidra till ett hållbart samhälle.

2.4 EU:s digitaliseringspolitik

2.4.1 En digital europeisk inre marknad

”Den digitala inre marknaden” och strategin för denna presenterades år 2015 som en av kommissionens prioriteringar (Meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén, En strategi för en inre digital marknad i Europa, COM/2015/0192). Tanken var att komma till rätta med den fragmentering och de

hinder som finns på den digitala inre marknaden och därigenom skapa de bästa förutsättningarna för att göra Europa världsledande inom den digitala ekonomin.

En inre marknad som till fullo drar nytta av digitaliseringens möjligheter kan bidra till stärkt konkurrenskraft och hållbar tillväxt. Som ett led i att genomföra strategin för en digital inre marknad informerade kommissionen år 2017 om satsningen på att skapa en europeisk dataekonomi (Meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén, ”Att skapa en europeisk dataekonomi”, COM(2017) 9 final). Kommissionen konstaterade att information i dag är en viktig resurs för att skapa ekonomisk tillväxt, arbete och samhällsutveckling. Vidare menade kommissionen att information bär på enorm potential för ny innovation och optimering av processer och beslutsfattande inom en rad olika områden, t.ex. hälsosektorn, energisektorn, smarta städer och transportsystem och att allt större datamängder produceras av den nya teknikens maskiner och processer som sakernas internet, framtidens fabriker och autonoma, uppkopplade system. Kommissionen framhöll också i strategin för den inre digitala marknaden att dataekonomin kommer att kräva ramar som möjliggör att digital information kan användas genom hela värdekedjan i vetenskaps-, samhälls- och näringssyfte.

2.4.2 EU:s datastrategi

Kommissionens meddelande om en datastrategi för EU kom i februari 2020 (COM (2020) 66, Meddelande från Kommissionen till Europaparlamentet, Rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén om En EU-strategi för data).

Meddelandet innehåller förslag till åtgärder som syftar till att göra EU till den mest attraktiva, säkraste, mest dynamiska och mest snabbrörliga datadrivna ekonomin i världen. Meningen är att Europa genom bättre användning av data som resurs ska förbättra beslutsfattande och livskvalitet för samtliga medborgare. Datastrategin tar upp ett antal åtgärder och investeringar som behöver genomföras under kommande år för att uppnå de i meddelandet uppsatta målen samt stärka Europas internationella

konkurrenskraft bl.a. inom artificiell intelligens och annan digital innovation. Kommissionens mål är att till 2030 tillskapa ett gemensamt europeiskt dataområde och en fungerande och säker inre marknad för data.

En inre marknad för data ska göra EU mer konkurrenskraftigt på global nivå och möjliggöra innovativa processer, produkter och tjänster. Industriella och kommersiella samt offentligt hållna data är centrala drivkrafter för den digitala ekonomin.

EU ska bli en attraktiv, säker och dynamisk dataekonomi genom att fastställa tydliga och rättvisa regler för tillgång till och vidareutnyttjande av data, investera i nästa generations standarder, verktyg och infrastrukturer för att lagra och behandla data, förena krafterna genom en europeisk molnsammanslutning, samla europeiska data inom nyckelsektorer genom gemensamma och kompatibla EU-omfattande dataområden och att ge användarna rättigheter, verktyg och färdigheter att behålla full kontroll över sina data.

Dataekonomin måste byggas på ett sätt som möjliggör välmående företag, särskilt mikroföretag och små och medelstora företag samt nystartade företag, där neutral dataåtkomst, dataportabilitet och interoperabilitet säkerställs och inlåsningseffekter undviks. I EU-strategin för data har kommissionen beskrivit visionen om ett gemensamt europeiskt dataområde, som innebär en inre marknad för data, där data kan användas i enlighet med gällande lagstiftning oavsett var i unionen de fysiskt lagras. Detta kan enligt skäl 2 till dataförvaltningsförordningen vara avgörande för den snabba utvecklingen av teknik för artificiell intelligens.

Genom genomförandet av de olika åtgärderna i EU:s datastrategi ska mer data göras tillgängliga för användning i ekonomin och samhället, samtidigt som de som genererar uppgifterna behåller kontrollen. Dataförvaltningsförordningen är den första förordningen som genomförs som har sin grund i EU:s datastrategi. Viktiga rättsakter som föregått dataförvaltningsförordningen är den allmänna dataskyddsförordningen samt öppna data-direktivet.

Meddelandet om en EU-strategi för data innehåller referenser till meddelandet om vitboken om AI, och beskriver behovet av samlade europeiska insatser för att effektivare nyttja data som en strategisk resurs. Detta för att hantera gemensamma samhällsutmaningar i en stark internationell konkurrens från USA och Kina samt ledande

plattformsföretag. Tillgång till samt kontroll över relevanta data, baserat på gemensamma regelverk och standarder, är av strategisk betydelse för utvecklingen av digital innovation, särskilt artificiell intelligens, inom EU. Som exempel på åtgärder för kontroll över data nämns europeiska initiativ till molntjänster. Vidare nämns vikten av att investera i kompetens samt att fokusera på att locka fler kvinnor till branschen.

Kommissionen anser att EU:s teknologiska framtid är avhängigt förmågan att hantera värdet av data genom en europeisk modell, samt genom strukturer och politik för data under kommande år. Kommissionen lyfter bl.a. fram dataskyddsförordningen, cybersäkerhetsakten och inrättandet av en kodex för elektronisk kommunikation som betydelsefulla rättsliga grunder för en säker, trygg och snabbrörlig dataekonomi. Likaså betonas investeringar i digital infrastruktur och lagstiftning inom vissa sektorer och domäner, bl.a. för intelligenta transportsystem, som angelägna för bättre tillgång till data inom EU. Kommissionens vision går bl.a. ut på att skapa europeiska datautrymmen, som ska kunna stödja utvecklingen inom samhällssektorer som tillverkning, hälsa och mobilitet, med beaktande av klimatutmaningarna och grundläggande värden för medborgarna.

I strategin lyfter kommissionen att de vill stödja inrättande av olika gemensamma europeiska dataområden, bl.a. för hälsa, energi och jordbruk.

2.4.3 Det digitala decenniet och den digitala kompassen

EU-kommissionen har utropat 2020-talet till det digitala årtiondet. Vägen till det digitala decenniet är EU:s policyprogram för den digitala omställningen (Meddelande från kommissionen till Europaparlamentet, rådet europeiska ekonomiska och sociala kommittén samt regionkommittén Digital kompass 2030: den europeiska vägen in i det digitala decenniet, COM[2021] 118). Där finns specifika digitala mål och delmål som ska uppnås senast 2030. Programmet lägger fokus vid digitala färdigheter och utbildning och struktureras kring fyra huvudområden. De två första fokuserar på digital kapacitet inom infrastruktur och inom utbildning och

färdigheter, och de två andra fokuserar på den digitala omställningen av företag och offentliga tjänster.

Meddelandet om den digitala kompassen beskriver en styrstruktur i form av ett program för en digital politik innehållandes konkreta mål för 2030, uppföljning och övervakningssystem samt mekanismer för att främja multinationella projekt.

2.4.4 Programmet för ett digitalt Europa (DIGITAL)

Programmet för ett digitalt Europa regleras i Europaparlamentets och rådets förordning (EU) 2021/694 av den 29 april 2021 om inrättande av programmet för ett digitalt Europa och om upphävande av beslut (EU) 2015/2240 och det pågår under 2021–2027. Programmet har en totalbudget på 7,6 miljarder euro och syftar till att stödja den inre marknaden genom att bygga kapacitet och infrastruktur inom EU med fokus på att underlätta bred användning av digital teknik och sätta resultat från forskning på marknaden.

Programmet för ett digitalt Europa utgör ett komplement till en rad andra program som stöder den digitala omvandlingen som Horisont Europa och de digitala aspekterna av Fonden för ett sammanlänkat Europa (CEF2).

Projekt med investeringar till och finansiering av inrättande dataområden i enlighet med vad som föreskrivs i EU:s datastrategi utlyses genom bl.a. Programmet för ett digitalt Europa och Horisont Europa. De gemensamma europeiska dataområdena kan beskrivas som bestående av dels de rättsliga, organisatoriska och administrativa förutsättningarna för kontrollerad och säker datadelning, dels de tekniska och infrastrukturella förutsättningarna. Vissa dataområden ska regleras och styras genom EU-förordningar, medan inrättandet av andra kan förväntas ske utan EU-reglering. Ett exempel på ett dataområde som ska styras av en EU-förordning är hälsodataområdet där kommissionen tagit fram ett förslag till förordning (COM(2022) 196 Meddelande från kommissionen och rådet - Ett europeiskt hälsodataområde: tillvarata kraften hos hälsodata för människor, patienter och innovation), se vidare avsnitt 2.6.4.

2.5 Genomförd EU-lagstiftning på digitaliseringsområdet

2.5.1 Öppna data-direktivet och datalagen

Europaparlamentets och rådets direktiv (EU) 2019/1024 av den 20 juni 2019 om öppna data och vidareutnyttjande av information från den offentliga sektorn, nedan öppna data-direktivet, är en omarbetning av Europaparlamentets och rådets direktiv 2003/98/EG om vidareutnyttjande av information från den offentliga sektorn (PSI-direktivet).

Öppna data-direktivets övergripande syfte är att främja användningen av öppna data och stimulera innovation inom produkter och tjänster genom vidareutnyttjande av information som tillgängliggörs av den offentliga sektorn. Direktivet har anpassats till de senaste framstegen inom digital teknik och ska ytterligare främja digital innovation, särskilt beträffande artificiell intelligens (jfr skäl 3). Direktivets reglering strävar mot att hantera kvarstående och nya hinder som motverkar ett brett vidareutnyttjande av information.

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

Öppna data-direktivet omfattar inte uppgifter med insynsskydd för statistiska och kommersiella uppgifter och data som ingår i verk eller andra alster till vilka tredje man innehar immateriella rättigheter. Data som rör affärshemligheter inbegriper data som skyddas av företagshemligheter, skyddad know-how och annan information vars otillbörliga röjande skulle påverka företagets marknadsställning eller finansiella sundhet omfattas enligt skäl 10 inte heller.

Dataförvaltningsförordningens kapitel II omfattar villkor för vidareutnyttjande från offentliga myndigheter av vissa typer av just sådana typer av skyddade data som öppna data-direktivet inte omfattade. Detta kapitel i förordningen avhandlas i avsnitt 4.

2.5.2 DSA

EU har antagit en förordning om den inre marknaden för digitala tjänster, Europaparlamentets och rådets förordning (EU) 2022/2065 av den 19 oktober 2022 om en inre marknad för digitala tjänster och om ändring av direktiv 2000/31/EG (förordningen om digitala tjänster, nedan kallad DSA). I förordningen fastställs harmoniserade regler för tillhandahållandet av förmedlingstjänster på den inre marknaden. Den innehåller bestämmelser om villkorat undantag från ansvar för leverantörer av sådana tjänster och om särskilda krav på tillbörlig aktsamhet som är anpassade för specifika kategorier av leverantörer. Den innehåller även regler för genomförandet och kontrollen av efterlevnaden av förordningen, även vad gäller samarbete och samordning mellan behöriga myndigheter. Slutligen fastställer den ett ramverk för samarbete och efterlevnadskontroll mellan kommissionen och nationella myndigheter (SOU 2023:2 s. 9).

I juni 2022 tillsattes en utredning för att lämna förslag på åtgärder med anledning av förslaget till DSA. Utredningen kom i januari 2023 med delbetänkandet *En inre marknad för digitala tjänster – ansvarsfördelningen mellan myndigheter* (SOU 2023:02). I detta återfinns förslag på vilken eller vilka myndigheter som bör utses till behöriga myndigheter enligt förordningen och vilken myndighet som bör utses till samordnare för digitala tjänster. De återstående frågor som omfattas av uppdraget kommer att behandlas i det slutbetänkande som ska redovisas senast den 9 juni 2023.

2.6 Kommande EU-lagstiftning på digitaliseringsområdet

2.6.1 Kommande AI-förordning

Den 21 april 2021 presenterade kommissionen ett förslag till en förordning om harmoniserade regler för artificiell intelligens (AI) inom ramen för strategin för det digitala Europa. Kommissionen annonserade i Vitboken om artificiell intelligens, som presenterades den 19 februari 2020, ambitionen att föreslå ett rättsligt ramverk för AI med utgångspunkt i etiska riktlinjer för utveckling och användning av AI.

Syftet med förslaget till förordning är att harmonisera regler för AI inom EU, stärka den inre marknadens konkurrenskraft och funktion samt att undvika fragmentering på den inre marknaden, skydda hälsa, säkerhet och grundläggande rättigheter, främja de positiva aspekterna av AI och säkerställa fri rörlighet av AI-system.

2.6.2 Kommande datarättsförordningen

Den 23 februari 2022 presenterade kommissionen ett förslag till en förordning om harmoniserade regler för rättvis tillgång till och användning av data från bl.a. uppkopplade produkter, s.k. sakernas internet, inom ramen för den europeiska datastrategin. Förordningen benämns datarättsförordningen.

Det övergripande syftet med förordningen är att möjliggöra en bättre fördelning av värden och nyttor från den typ av data som genereras av olika uppkopplade produkter på ett rättvist sätt mellan aktörerna i dataekonomin och att främja tillgång och användning av data.

Förordningen följer dataförvaltningsförordningen som det andra stora lagstiftningsinitiativet som utgår från EU:s datastrategi, där dataförvaltningsförordningen var det första. Dataförvaltningsförordningen syftar till att skapa processer och strukturer för att underlätta datadelning för företag, individer och myndigheter. Datarättsförordningen ska i sin tur klargöra vem som kan skapa värde från data och under vilka förutsättningar. Enligt kommissionen syftar förslaget till att främja fullbordandet av den inre marknaden för data, där data från den offentliga sektorn, företag och enskilda används på bästa möjliga sätt, samtidigt som rättigheterna i förhållande till sådana data och de investeringar som görs för att samla in dem respekteras.

2.6.3 Kommande interoperabilitetsförordning

Förslaget till förordningen om ett interoperabelt Europa presenterades den 18 november 2022 av kommissionen. Det föreskriver utveckling av det redan utformade europeiska ramverket för interoperabilitet (EIF) och är tänkt att stärka den gränsöverskridande interoperabiliteten och samarbeten inom den

offentliga sektorn på den inre marknaden. Förslaget innehåller en styrningsmodell som gemensamt har arbetats fram av medlemsstaterna och EU-institutionerna. Styrningsmodellen ska ge berörda aktörer möjlighet att uttrycka sina synpunkter och är tänkt att stödja delning och återanvändning av bl.a. data. Detta ska vidare bidra till gemensamma lösningar för interoperabilitet i EU, exempelvis för gemensamma europeiska dataområden.

2.6.4 Kommande förordning om det europeiska hälsodataområdet

Den 3 maj 2022 presenterade kommissionen sitt förslag till en förordning med tillhörande meddelande om det europeiska hälsodataområdet, inom ramen för den europeiska datastrategin.

Syftet med kommissionens förslag till förordning är dels att ge enskilda inom EU en ökad kontroll över sina hälsodata inom vården (primäranvändning), dels att göra det lättare att dela och få tillgång till olika typer av hälsodata för såväl primäranvändning som för bl.a. forskning, innovation och beslutsfattande, s.k. sekundäranvändning.

3 Närliggande rättsområden

Dataförvaltningsförordningen gränsar i olika delar till flera olika rättsområden. Vissa av dem påverkar hela förordningen medan andra bara har betydelse för tolkningen och förståelsen för vissa specifika delar. All hantering som dataförvaltningsförordningen reglerar omfattas t.ex. av dataskyddsförordningen om aktuella data innehåller personuppgifter.

Vidareutnyttjande av skyddade data gränsar därutöver mot regler om bl.a. tillgång till allmänna handlingar, sekretess och förvaltningsrätt. Skyddade data i förordningens mening är skyddade enligt olika författningar, bl.a. offentlighets- och sekretesslagen, dataskyddsförordningen och immaterialrätten.

Ramverket för dataförmedlingstjänster gränsar också mot både dataskyddsreglerna och konkurrensrätten medan ramverket för dataaltruism framför allt gränsar mot dataskyddsreglerna.

Nedan följer en övergripande beskrivning av de olika rättsområden som har betydelse för förståelsen och tolkningen av dataförvaltningsförordningens regler och hur dessa kan kompletteras i nationell rätt.

3.1 Handlingsoffentlighet och sekretess

Allmänhetens rätt till tillgång till allmänna handlingar (handlingsoffentligheten) är grundlagsskyddad och regleras i 2 kap. tryckfrihetsförordningen (TF). Syftet med bestämmelserna är rent generellt att främja ett fritt meningsutbyte och en allsidig upplysning. Rätten att ta del av allmänna handlingar fungerar också som ett viktigt medel för kontroll av offentliga organs verksamhet, t.ex. handläggningsrutiner och effektivitet. Under årens lopp har

offentlighetsprincipen fått ökad betydelse för uttag av allmänna handlingar för kommersiella ändamål.

Vem som helst har rätt att med stöd av 2 kap. 1 § TF ta del av allmänna handlingar. Denna rätt omfattar inte bara fysiska personer utan även privaträttsliga juridiska personer (se RÅ 2003 ref. 83).

Regelverket fick i huvudsak sitt nuvarande innehåll under 1970-talet, vilket innebär att reglerna inte är anpassade till den digitala utvecklingen. Med handling avses enligt tryckfrihetsförordningen 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 § TF). Handlingen är allmän om den förvaras hos en myndighet och är inkommen till eller upprättad hos myndigheten (2 kap. 4 § TF). Med myndighet jämställs i detta avseende riksdagen och beslutande kommunal församling (2 kap. 5 § TF).

Vissa typer av handlingar är inte allmänna. Detta gäller exempelvis handlingar som förvaras hos en myndighet endast som ett led i en teknisk bearbetning eller teknisk lagring för någon annans räkning. Inte heller säkerhetskopior eller handlingar som ingår i bibliotek är allmänna handlingar (2 kap. 13 och 14 §§ TF).

Myndigheter ska ta hänsyn till handlingsoffentligheten när de organiserar sina allmänna handlingar, se 4 kap. 1 § offentlighets- och sekretesslagen (2009:4000) (OSL). Regler om hur allmänna handlingar ska bevaras samt om gallring finns i arkivlagen (1990:782). Se även 2 kap. 23 § TF och 4 kap. 4 § OSL. Bestämmelsernas syfte är att garantera allmänhetens rätt att få tillgång till allmänna handlingar.

3.1.1 Utlämnande av allmän handling

En allmän handling ska som huvudregel genast, eller så snart det är möjligt, och utan avgift lämnas ut så att sökanden kan ta del av handlingen på stället. Detta gäller inte om handlingen innehåller uppgifter som är sekretessbelagda. Om någon del av handlingen är sekretessbelagd, ska de delar av handlingen som inte är sekretessbelagda tillhandahållas i avskrift eller kopia (2 kap. 15 § TF).

Den som vill ta del av en allmän handling har även enligt 2 kap. 16 § TF rätt att mot avgift få en avskrift eller kopia av handlingen.

Den avgift som avses regleras för statliga myndigheter i avgiftsförordningen. Kommunerna fastställer motsvarande avgifter i sin verksamhet utifrån självkostnadsprincipen. Avgiften får inte täcka kostnader för framtagande och återställande av handlingen, eftersom en allmän handling enligt 2 kap. 15 § TF ska tillhandahållas på stället kostnadsfritt (RÅ 1985 2:9). Handlingsoffentligheten innebär emellertid inte att en enskild har rätt att få ut handlingar i digital form. Det s.k. utskriftsundantaget i 2 kap. 16 § TF innebär att en myndighet inte är skyldig att lämna ut handlingen elektroniskt, om inte detta följer av lag. Utskriftsundantaget är inte något förbud mot att lämna ut en digital kopia av en viss handling, men enskilda myndigheters registerförfattningar kan däremot utgöra hinder mot att lämna ut sådana kopior, t.ex. 10 § lagen (2000:224) om fastighetsregister. Det finns endast ett fåtal bestämmelser om skyldighet att lämna ut handlingar i digital form, t.ex. 13 kap. 1 § lagen (2004:297) om bank- och finansieringsrörelse.

3.1.2 Utlämnande av uppgifter

Tryckfrihetsförordningen reglerar utlämnande av allmänna handlingar. I OSL finns det också regler om utlämnande av uppgifter. Enligt 6 kap. 4 § OSL har en enskild rätt att på begäran få ut en uppgift ur en allmän handling som förvaras hos myndigheten, om inte uppgiften är sekretessbelagd.

Ett beslut att avslå en begäran från en enskild om att få ta del av en uppgift ur en allmän handling är, till skillnad från ett beslut om avslag om utlämnande av allmän handling, inte överklagbart (6 kap. 7–9 §§ OSL).

3.1.3 Sekretess

Rätten att ta del av allmänna handlingar kan enligt 2 kap. 2 § TF bara begränsas av sekretess. Begränsningar får endast göras med hänsyn till vissa sekretessgrunder och ska framgå av OSL eller annan lag som den lagen hänvisar till.

Med sekretess menas förbud att röja en uppgift, vare sig det sker muntligen, genom utlämnande av allmän handling eller på något annat sätt. Sekretess kan alltså avse både tystnadsplikt och

handlingssekretess, vilket innebär att inte bara en myndighets utlämnande av allmänna handlingar begränsas, utan även en myndighets tillgängliggörande av information utan en föregående begäran. Otillåtet röjande av en sekretessbelagd uppgift är enligt 20 kap. 3 § brottsbalken (1962:700) straffsanktionerat som brott mot tystnadsplikt.

I OSL finns bestämmelser som syftar till att säkerställa skyddet för uppgifter om enskildas personliga eller ekonomiska förhållanden, liksom skyddet för allmänna intressen.

I detta sammanhang finns anledning att särskilt nämna att sekretess gäller för personuppgift om en myndighet kan anta att uppgiften efter utlämnandet kommer att behandlas i strid med dataskyddsregleringen (21 kap. 7 § OSL).

Förbehåll

En allmän handling som omfattas av sekretess kan under vissa förutsättningar lämnas ut med villkor, s.k. förbehåll, som inskränker rätten att använda den information som finns i handlingen.

Bestämmelsen i 10 kap. 14 § OSL om förbehåll möjliggör för myndigheter att lämna ut uppgifter som är sekretessbelagd för att ett utlämnande skulle kunna orsaka skada, men eller annan olägenhet. Ett utlämnande av uppgifterna kan ske under förutsättning att den risk för skada, men eller annan olägenhet som hindrar att uppgifterna lämnas till den enskilde kan undanröjas genom förbehållet. Ett förbehåll kan avse ett förbud mot att lämna uppgifterna vidare eller att nyttja dem. Förbehållet medför att tystnadsplikt uppkommer för den som tagit emot uppgifterna, vilket inskränker rätten att meddela och offentliggöra uppgifterna (meddelarfrihet). Ett röjande av uppgifterna kan medföra straffansvar för brott mot tystnadsplikt.

Det finns emellertid begränsningar kring när och hur ett förbehåll får ställas upp. För det första får ett förbehåll inte meddelas i förväg utan ska föregås av en prövning i varje enskilt fall och avse konkreta uppgifter. För det andra ska ett förbehåll meddelas som ett formligt beslut, dvs. det ska dokumenteras och innehålla en överklagande-hänvisning. För det tredje ska uppgiftsutlämnandet ske till en

utpekad fysisk person. Det går alltså inte att i avtal reglera generella förbehåll.

Ett beslut av en myndighet om att lämna ut en allmän handling med förbehåll som inskränker rätten att förfoga över den kan överklagas (2 kap. 19 § TF och 6 kap. 7–9 §§ OSL).

3.1.4 Tillgång till allmänna handlingar och dataförvaltningsförordningen

Information som samlas in eller framställs i den offentliga sektorn är en stor tillgång för samhället. Möjligheten att utnyttja sådan information vidare har genom offentlighetsprincipen gamla anor i Sverige. Digitaliseringen av offentlig förvaltning och nya tekniska lösningar för att ta del av information av olika slag gör att de praktiska möjligheterna att vidareutnyttja information har ökat markant.

Allmänhetens rätt att få tillgång till offentliga handlingar kan betraktas som ett allmänt intresse enligt skäl 11 till förordningen. Med hänsyn till den roll som allmänhetens rätt att få tillgång till offentliga handlingar och öppenheten spelar i ett demokratiskt samhälle har dataförvaltningsförordningen avgränsats så att den inte påverkar tillämpningen av nationell rätt om beviljande av tillgång till och utlämnande av allmänna handlingar, artikel 1.2 andra stycket punkten a. Dataförvaltningsförordningen påverkar därför inte tillämpningen av reglerna om handlingsoffentlighet och sekretess. Däremot kan utlämnande av allmänna handlingar enligt TF vara grunden för ett tillgängliggörande av skyddade data enligt dataförvaltningsförordningen. Mer om det i avsnitt 4.

3.2 Skydd för personlig integritet

3.2.1 FN:s förklaring och deklaration

Det internationella arbetet för mänskliga rättigheter tar sin utgångspunkt i den allmänna förklaring om de mänskliga rättigheterna som FN antog 1948. I artikel 12 anges bl.a. att ingen får utsättas för godtyckligt ingripande i fråga om privatliv och att var och en har rätt till lagens skydd mot sådana ingripanden och

angrepp. Rättigheterna i förklaringen om de mänskliga rättigheterna har senare förts in och vidareutvecklats i ett antal konventioner som är bindande för de anslutna staterna, däribland Sverige. Artikel 12 i förklaringen återfinns i artikel 17 i 1966 års FN-konvention om medborgerliga och politiska rättigheter.

3.2.2 Europakonventionen och rättighetsstadgan

Enligt artikel 8 i Europeiska konventionen den 4 november 1950 angående skydd för de mänskliga rättigheterna och de grundläggande friheterna har var och en rätt till skydd för bl.a. sitt privat- och familjeliv. Artikeln ger enligt Europadomstolens praxis upphov inte bara till en förpliktelse för det allmänna att avhålla sig från omotiverade inskränkningar, utan även en skyldighet för det allmänna att se till att enskilda även i förhållande till andra enskilda tillförsäkras en rätt till skydd för sitt privat- och familjeliv.

Den personliga integriteten skyddas också av Europeiska unionens stadga om de grundläggande rättigheterna 2010/C 83/02. I artikel 3, 7 och 8 slås bl.a. fast att var och en har rätt till integritet, respekt för sitt privat- och familjeliv samt skydd av sina personuppgifter.

3.2.3 Regeringsformen

Den personliga integriteteten skyddas av regeringsformen (1974:152). Av målsättningsstadgandet i 1 kap. 2 § följer att det allmänna ska värna den enskildes privat- och familjeliv. Målsättningsstadgandet anger ett viktigt mål för den samhälleliga verksamheten, men är inte rättsligt bindande för det allmänna. I 2 kap. finns däremot rättsligt bindande föreskrifter om grundläggande fri- och rättigheter. Av 2 kap. 6 § andra stycket framgår att var och en är 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.

3.2.4 Dataskydd

Dataskyddsregleringen utgör ett starkt skydd för den enskilde avseende hur både myndigheter och andra enskilda verksamheter behandlar personuppgifter.

Dataskyddsförordningen och dataskyddslagen

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), nedan dataskyddsförordningen, utgör en generell reglering för behandling av personuppgifter inom EU. Förordningen, som är direkt tillämplig, ska tillämpas på sådan behandling av personuppgifter som helt eller delvis sker på automatisk väg, och på annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register. I förordningen regleras bl.a. grundläggande principer för behandling av personuppgifter, den registrerades rättigheter, personuppgiftsansvar, överföring av personuppgifter, tillsyn över personuppgiftsbehandling, rätten för enskilda att få tillgång till rättsmedel och sanktioner mot ansvariga som inte lever upp till förordningens krav.

Från dataskyddsförordningens tillämpningsområde undantas personuppgiftsbehandling som utförs av behöriga myndigheter i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inkluderande skydd mot samt förebyggande och förhindrande av hot mot den allmänna säkerheten. Personuppgiftsbehandling för dessa syften omfattas i stället av 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.[1]

[1] Direktivet har genomförts i svensk rätt i huvudsak genom brottsdatalagen (2018:1177). Lagen kompletteras av brottsdataförordningen (2018:1202), som genomför vissa detaljbestämmelser i direktivet. Brottsdatalagen är subsidiär i förhållande till annan lag eller förordning. De myndigheter som ska tillämpa brottsdatalagen har i de flesta fall särskilda

Nedan finns en översiktlig beskrivning av regleringen i dataskyddsförordningen. Brottsdatalagen (2018:1177) och andra lagar som genomförde direktivet finns inte med.

I Sverige kompletteras dataskyddsförordningen av lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen) och förordningen (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning. Lagen med tillhörande förordning förtydligar under vilka förutsättningar personuppgifter får behandlas med stöd av dataskyddsförordningen.

Dataskyddslagen är subsidiär i förhållande till annan lag eller förordning, vilket innebär att avvikande bestämmelser i registerförfattningar har företräde, 1 kap. 6 §. Lagen – och dataskyddsförordningen – ska inte heller tillämpas i den utsträckning det skulle strida mot TF eller yttrandefrihetsgrundlagen, 1 kap. 7 § (se även artikel 85.1 och 86 i förordningen). Myndigheter kan alltså utan hinder av dataskyddsförordningen på begäran från en enskild lämna ut allmänna handlingar i enlighet med 2 kap. TF, såvida handlingarna inte innehåller sekretessbelagda uppgifter.[2] Om handlingen inte lämnas ut på papper behöver sättet som handlingen tillgängliggörs digitalt dock uppfylla dataskyddsreglerna.

När det gäller myndigheters tillgängliggörande av information på eget initiativ, t.ex. genom att göra allmänna handlingar tillgängliga för vidareutnyttjande, ska dataskyddsförordningen och dataskyddslagen tillämpas fullt ut. Detta gäller även vid överföring av personuppgifter mellan myndigheter enligt offentlighets- och sekretesslagen (Sören Öman, Dataskyddsförordningen (GDPR) m.m., Norstedts Juridik, s. 657ff).

registerförfattningar som gäller utöver brottsdatalagen och som innehåller preciseringar, undantag eller avvikelser från bestämmelserna i den lagen, t.ex. bestämmelser om längsta tid för behandling och sanktionsavgifter.

[2] Att notera är också att det finns en bestämmelse i 21 kap. 7 § OSL som säger att sekretess gäller för en uppgift om det kan antas att uppgiften efter ett utlämnande kommer att behandlas i strid med dataskyddsförordningen och dataskyddslagen.

Grundläggande principer för personuppgiftsbehandling

Grundläggande krav vid behandling

All behandling av personuppgifter måste uppfylla vissa grundläggande krav som framgår av artikel 5.1 i dataskyddsförordningen. Personuppgifter ska behandlas på ett lagligt, korrekt och öppet sätt. Uppgifterna ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål (ändamålsbegränsning). Uppgifterna ska vidare vara adekvata, relevanta och inte för omfattande i förhållande till ändamålen (uppgiftsminimering) samt korrekta och, om det är nödvändigt, uppdaterade. Alla rimliga åtgärder ska vidtas för att säkerställa att felaktiga personuppgifter raderas eller rättas utan dröjsmål. Personuppgifter får inte heller förvaras under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen och de ska skyddas genom lämpliga säkerhetsåtgärder.

Det är den personuppgiftsansvarige som ska säkerställa att kraven följs vid behandlingen av uppgifterna, artikel 5.2 i dataskyddsförordningen.

Rättslig grund

För att en behandling av personuppgifter ska vara laglig måste den vila på en rättslig grund enligt artikel 6.1 i dataskyddsförordningen. De rättsliga grunderna är samtycke (beskrivs närmare nedan), avtal, rättslig förpliktelse, grundläggande intresse, allmänt intresse, myndighetsutövning och – såvitt avser behandling som utförs av enskilda – intresseavvägning. Personuppgiftsbehandlingen ska även vara nödvändig.

Om behandlingen utförs med stöd av någon av de rättsliga grunderna rättslig förpliktelse, allmänt intresse eller myndighetsutövning måste denna vara fastställd i unionsrätten eller i nationell rätt i enlighet med artikel 6.3 i dataskyddsförordningen.

Samtycke

Samtycke enligt definitionen i dataskyddsförordningen är varje slag av frivillig, specifik, informerad och otvetydig viljeyttring, genom vilken den registrerade, antingen genom ett uttalande eller genom en entydig bekräftande handling, godtagbar behandling av personuppgifter som rör honom eller henne. Ett sådant samtycke kan sedan vara den rättsliga grunden för behandlingen av personuppgifter, artikel 6.1 a dataskyddsförordningen. I artikel 7 regleras villkoren för samtycke. Två viktiga principer gällande samtycke enligt dataskyddsförordningen är att samtycket ska vara frivilligt och att det ska gå att återkalla. Med frivilligt menas att den registrerade har ett genuint fritt val och kontroll över sina personuppgifter. Samtycket blir därför ogiltigt om någon har utsatts för påverkan. Den registrerade får inte heller drabbas av negativa konsekvenser om han eller hon inte lämnar sitt samtycke. Samtycket får heller inte vara en obligatorisk del av avtalsvillkor. Det ska vara lika lätt att återkalla ett samtycke som att lämna det. Detta är särskilt viktigt när det gäller barn. Om det är svårt att återkalla samtycket är det inte giltigt. Om den registrerade inte kan eller får återkalla sitt samtycke utan att drabbas av negativa konsekvenser är samtycket inte frivilligt.

3.2.5 Dataskyddsreglerna och dataförvaltningsförordningen

Tanken med dataförvaltningsförordningen är att skapa goda förutsättningar för vidareutnyttjande, dataförmedling och dataaltruism, utan att för den saken inkräkta på den personliga integriteten. Det slås därför fast redan i artikel 1.3 att befintlig unionsrätt och nationell rätt som avser skydd av personuppgifter ska tillämpas fullt ut, inklusive tillsynsmyndigheters befogenheter och behörigheter. Detta gäller enligt skäl 4 även när personuppgifter och andra data än personuppgifter i en datamängd är oupplösligt sammanlänkade. Av samma skäl framgår också uttryckligen att dataförvaltningsförordningen i synnerhet inte ska tolkas som att den skapar en ny rättslig grund för behandling av personuppgifter eller att den påverkar informationskraven i befintlig dataskyddslagstiftning och då framför allt dataskyddsförordningen.

Om andra än tillsynsmyndigheterna på dataskyddsområdet utses som behöriga myndigheter för olika delar av dataförvaltnings-

förordningens områden så ska enligt skäl 4 deras uppdrag utformas så att det inte påverkar dataskyddsmyndigheternas tillsynsbefogenheter.

I flera delar av förordningen nämns olika skyddsåtgärder som kan vidtas för information, t.ex. anonymisering, differentiell integritet, generalisering, undertryckande och randomisering, användning av syntetiska data eller liknande metoder. Sådana skyddsåtgärder kan vidtas för att uppfylla kraven på bl.a. uppgiftsminimering och skyddsåtgärder enligt dataskyddsförordningen, i tillämpliga fall tillsammans med en konsekvensbedömning avseende dataskydd. Tillämpningen av sådan teknik, tillsammans med övergripande konsekvensbedömningar avseende dataskydd och andra skyddsåtgärder, kan enligt skäl 8 bidra till större säkerhet i användningen och vidareutnyttjandet av personuppgifter och bör kunna säkerställa att företagsdata som rör affärshemligheter kan vidareutnyttjas för forsknings-, innovations- och statistikändamål på ett säkert sätt.

3.3 Kommersiella uppgifter med insynsskydd

Affärshemlighet kan ses som ett samlingsbegrepp för olika typer av hemlig information i näringslivet, innefattande företagshemligheter och yrkeshemligheter. Den hemliga informationen kan vara skyddad eller oskyddad. Regler som rör området finns på olika ställen, t.ex. i lag (2018:558) om företagshemligheter (FHL), rättegångsbalken (1942:740) (RB), konkurrenslagen (2008:579), nedan KKL, och arbetsmiljölagen (1977:1160).

3.3.1 Företagshemligheter

Lagen om företagshemligheter innehåller bestämmelser om skadestånd, vitesförbud och straff vid obehöriga angrepp på företagshemligheter. Lagen genomför delvis Europaparlamentets och rådets direktiv 2016/943/EU av den 8 juni 2016 om skydd mot att icke röjd know-how och företagsinformation (företagshemligheter) olagligen anskaffas, utnyttjas och röjs.

FHL definierar vad som är en företagshemlighet och vad som är ett obehörigt angrepp av densamma. För att det ska vara fråga om en företagshemlighet måste fyra kriterier vara uppfyllda. Det ska röra

sig om affärs- eller driftsförhållanden som inte är allmänt kända, som ägaren har vidtagit rimliga åtgärder för att hemlighålla och som skadar ägaren i förhållande till sina konkurrenter om de avslöjas eller kommer i orätta händer, 2 § första stycket.

Erfarenheter och färdigheter som en arbetstagare har fått vid normal yrkesutövning är inte en företagshemlighet. Inte heller är information om något som utgör ett brott eller annat allvarligt missförhållande en företagshemlighet, 2 § andra stycket.

Att behålla information eller kunskap som företagshemlighet kan i vissa fall vara ett alternativ till att söka patent. Patent ger förvisso ensamrätt till en uppfinning under 20 år, men ett patent innebär också att uppfinningen offentliggörs. Som företagshemlighet kan informationen/kunskapen stanna inom företaget, men det innebär i sin tur en risk att någon annan kommer på samma eller en snarlik lösning eftersom det då inte finns en ensamrätt till den.

3.3.2 Yrkeshemligheter

Yrkeshemligheter regleras inte på ett sådant samlat sätt som företagshemligheter. I stället finns det på olika ställen regler som avser yrkeshemligheter.

I rättegångsbalken återfinns bestämmelser om yrkeshemligheter på åtskilliga ställen. De flesta har med bevisning att göra och reglerar t.ex. befrielse från skyldighet att avslöja yrkeshemlighet eller möjlighet till stängda dörrar i domstol för att skydda sådana uppgifter.

Ett vittne kan enligt 36 kap. 6 § RB att helt avstå från att avge en utsaga, om utsagan skulle avslöja en yrkeshemlighet. Samma rätt föreligger också för part (vid förhör under sanningsförsäkran) genom 37 kap. 3 § andra stycket RB som hänvisar till 36 kap. 6 § RB samt för parts- och domstolssakkunnig 40 kap. 19 § andra stycket RB som hänvisar till 36 kap. 6 § RB resp. 40 kap. 4 § punkten 3. Enligt vad Processlagberedningen uttalade (se NJA II 1943 s. 472) omfattar yrkeshemlighet fabrikationssätt, anordning, affärsförhållande eller annat som kan anses såsom något för ett visst affärsföretag egendomligt och beträffande vilket innehavaren har ett skäligt anspråk att det inte uppenbaras. Beredningen hänvisade i det sammanhanget till lagen (1931:152) med vissa bestämmelser om

illojal konkurrens, som har ersatts av FHL. Den i FHL intagna definitionen på begreppet företagshemlighet torde enligt bl.a. kommentaren till 36 kap. 6 § RB i allt väsentligt överensstämma med begreppet yrkeshemlighet enligt 1931 års lag. Enligt rättsfallet NJA 1995 s. 347 har begreppet företagshemlighet i vart fall inte en vidare innebörd än uttrycket yrkeshemlighet. Enligt 36 kap. 6 § tredje stycket RB gäller ett undantag från ett vittnes rätt att vägra uttala sig om yrkeshemlighet om det finns synnerlig anledning att vittnet hörs om denna (SOU 2017:45 s. 272).

I arbetsmiljölagen finns reglerat att den som utsetts till bl.a. skyddsombud, studerandeskyddsombud eller ledamot i en skyddskommitté inte obehörigen får röja eller utnyttja vad han eller hon under uppdraget har fått veta om bl.a. yrkeshemlighet, arbetsförfarande eller affärsförhållande, 7 kap. 13 §. Under vissa omständigheter får uppgifterna enligt andra stycket samma paragraf lämnas vidare till vissa utpekade personer, och tystnadsplikten följer då med.

3.3.3 Affärshemligheter och dataförvaltningsförordningen

Vidareutnyttjande av uppgifter som innehåller kommersiella uppgifter som har insynsskydd enligt framförallt något av de regelverk som beskrivs ovan, t.ex. affärs, yrkes- eller företagshemligheter är en av de kategorier som ramverket för tillgängliggörande av skyddade data i dataförvaltningsförordningen omfattar. Sådant vidareutnyttjande ska enligt skäl 10 ske utan att det påverkar tillämpningen av direktiv (EU) 2016/943, som fastställer ramen för tillåtet anskaffande, användande eller röjande av företagshemligheter. Direktivet infördes i Sverige i huvudsak genom FHL.

Om data som begärs anses vara konfidentiella i enlighet med unionsrätten eller nationell rätt om affärshemligheter ska de offentliga myndigheterna säkerställa att dessa konfidentiella data inte röjs till följd av att vidareutnyttjande tillåts, artikel 5.8 i dataförvaltningsförordningen.

3.4 Statistiksekretess

Enligt 24 kap. 8 § OSL gäller sekretess i sådan särskild verksamhet hos myndighet som avser framställning av statistik för uppgift som avser enskilds personliga eller ekonomiska förhållanden och som kan hänföras till den enskilde. Härigenom skyddas inte bara sådana uppgifter som innehåller identitetsbeteckningar som namn och personnummer på en enskild utan även uppgifter som över huvud taget kan – direkt eller indirekt – hänföras till en viss enskild (prop. 2013/14:162 s. 6).

Statistiksekretessen är enligt huvudregeln i första och andra styckena absolut. I tredje stycket behandlas de undantagsfall där ett omvänt skaderekvisit gäller, dvs. det råder en presumtion för sekretess. I fråga om bestämmelsens hela tillämpningsområde gäller undantag från den s.k. generalklausulen i 10 kap. 27 § och det råder inte meddelarfrihet. För statistiksekretessen är inte ändamålet med uppgiften avgörande utan den verksamhet i vilken den förekommer. Det kan leda till att en uppgift hos en myndighet är offentlig inom en handläggande avdelning men sekretessbelagd inom en avdelning som framställer statistik (Lagkommentar 24 kap. 8 § OSL, Lisa Englund Krafft, Karnov).

Det saknas anvisningar för hur en sådan särskild verksamhet som paragrafen avser ska se ut eller vara organiserad och en bedömning får göras i varje enskilt fall. Viss ledning kan hämtas från uttalanden av regeringen i frågan. I proposition om ändring i sekretesslagen (1980:100), m.m. anfördes bl.a. att förutsättningarna för statistiksekretess är att statistikframställningen sker utan anknytning till något ärende och att verksamheten är organiserad som en egen enhet eller liknande. Saknas en särskild statistikenhet kan statistiksekretessen ändå gälla om verksamheten med framställning av statistik på annat sätt är avgränsad från annan verksamhet.

Uttrycket statistik definieras varken i OSL eller i någon annan lagstiftning. I allmänt språkbruk används ”statistik” huvudsakligen i två olika betydelser. Den ena betydelsen av statistik är såsom en beteckning på en vetenskaplig disciplin. Ursprungligen menades med statistik en vetenskap som behandlade rådande förhållanden, i synnerhet politiska, sociala och ekonomiska förhållanden, inom en stat eller olika stater. Statistiken som vetenskaplig disciplin kom

senare att även inom fler områden behandla metoder för insamling, bearbetning, redovisning och analys av data. Statistik kan även avse sammanställningar av data, vanligen i tabeller eller liknande, sammanställningar som ofta åstadkoms med de olika metoder för insamling, bearbetning, redovisning och analys som utvecklats inom den statistiska vetenskapen (prop. 2013/14:162 s. 8).

3.4.1 Statistiksekretess och dataförvaltningsförordningen

Vidareutnyttjande av data som är skyddade på grund av insynsskydd för statistiska uppgifter är en av de kategorier som ramverket för tillgängliggörande av skyddade data i kapitel II dataförvaltningsförordningen omfattar. Sådant vidareutnyttjande ska ske utan att det påverkar tillämpningen nationell rätt som avser statistiksekretess, artikel 3.3 a i dataförvaltningsförordningen.

3.5 Immateriella rättigheter

Immaterialrätten är ett rättsområde som rör rättsligt skydd för litteratur, konst, vetenskap, teknik, industriell formgivning, design, varumärken och andra kännetecken m.m. Skyddet är reglerat i olika lagar och består i stora drag av fyra delar

1. **Upphovsrätten** skyddar bl.a. musik, film, litteratur, brukskonst och andra litterära eller konstnärliga verk, källkoden till datorprogram m.m. Upphovsrätt regleras i lag (1960:729) om upphovsrätt till litterära och konstnärliga verk, nedan URL.
2. **Patent** är ett skydd för en ny, teknisk lösning på ett problem. Patent regleras i patentlagen (1967:837).
3. **Varumärkesskydd** är ett skydd för ett kännetecken för ett företag, en produkt eller tjänst. Det kan bestå av exempelvis ord, figurer, bokstäver/siffror, personnamn eller slogans. Det kan också vara en specifik utformning av själva produkten, s.k. förpackningsutstyrslar. Varumärkesskydd regleras i varumärkeslagen (2010:1877).
4. **Mönsterskydd/designskydd**, skyddar utseendet och formen på en produkt, men inte själva funktionen. Mönsterskydd regleras i mönsterskyddslagen (1970:485).

Det finns ett antal gemensamma strukturella drag mellan de olika immaterialrättsliga lagarna där grunden är att den eller de som tagit fram ett verk, en uppfinning, ett varumärke eller ett mönster ges ensamrätt till det under vissa förutsättningar och under viss tid. Lagarna har även rent praktiska beröringspunkter. En och samma företeelse omfattas inte sällan av flera typer av skydd, t.ex. kan formgivningen av en viss industriprodukt omfattas av både upphovsrätt och mönsterrätt och kanske kan dess form eller utstyrsel även skyddas som varumärke (Se Levin & Hellstadius, Lärobok i immaterialrätt Upphovsrätt, Patenträtt, Mönsterrätt, Kännetecknensrätt - I Sverige, EU och internationellt (2016, Norstedts), s. 24).

3.5.1 Upphovsrätt

Allmänt om upphovsrätt

Upphovsrätt gäller som huvudregel för litterära och konstnärliga verk oavsett i vilken form dessa har kommit till uttryck och regleras i URL. För att upphovsrätt ska föreligga krävs en viss grad av självständighet och originalitet, s.k. verkshöjd (Se Olsson & Rosén, Upphovsrättslagstiftningen En kommentar, Norstedts Juridik 2019, kommentaren till 1 kap. 1 § URL).

I myndigheternas verksamheter förekommer ett stort antal verk och andra alster som kan vara föremål för upphovsrätt eller närstående rättigheter. Rätten för enskilda att ta del av allmänna handlingar gäller även för handlingar som är upphovsrättsligt skyddade, 2 kap. 26 b § URL. Det finns undantag från detta gällande vissa typer av handlingar som lämnats in till en myndighet utan upphovsmannens samtycke, 31 kap. 23 § OSL. Den person som fått ut handlingen får däremot inte någon rätt att utnyttja verket utöver vad upphovsrättslagen medger. Den fria användningen av allmänna handlingar kan alltså begränsas av upphovsrättslig reglering, 1 kap. 11 § TF. Myndigheter som har upphovsrätt till en handling kan därför ställa upp villkor för vidareutnyttjandet av handlingen i enlighet med reglerna i upphovsrättslagen.

Upphovsrättslagen gör skillnad mellan upphovsrätt för handlingar som har upprättats hos myndigheten och handlingar som har kommit in till myndigheten. Upphovsrätten till handlingar som

kommer in till en myndighet innehas i huvudsak av någon annan än myndigheten (SOU 2020:55 s. 81).

Upphovsrätt till upprättade handlingar

Vissa kategorier av handlingar av stats- eller förvaltningsrättslig karaktär som upprättats av en myndighet – författningar, beslut, yttranden och officiella översättningar av sådana handlingar – skyddas normalt inte av upphovsrätt och får återges helt fritt, 1 kap. 9 § URL. Detta gäller inte för kartor, alster av bildkonst, musikaliska verk eller diktverk som ingår i en sådan handling. Har ett verk av denna typ tagits in i exempelvis ett beslut omfattas det av upphovsrätt, men upphovsrätten är inskränkt eftersom verken, med undantag av kartor, får återges fritt enligt 2 kap. 26 a § första stycket URL. Upphovsrättsmannen har emellertid rätt till ersättning. Upphovsrätt gäller även till ett verk som ingår i en bilaga till ett myndighetsbeslut, om beslutet avser utlämnande av en allmän handling där verket ingår i handlingen. Verket behåller alltså sitt upphovsrättsliga skydd trots att det blir en del av myndighetens beslut.

Andra upprättade myndighetshandlingar än de av stats- eller förvaltningsrättslig karaktär, t.ex. handböcker, skyddas som huvudregel av upphovsrätt, men även sådana handlingar får enligt 2 kap. 26 a § andra stycket URL återges fritt. Undantag från rätten till fri återgivning görs dock i 2 kap. 26 a § tredje stycket URL för vissa kategorier av handlingar som har ansetts behöva samma upphovsrättsliga skydd som inom den privata sektorn. Det rör sig bl.a. om kartor, tekniska förebilder, datorprogram och handlingar som tillhandahålls allmänheten i samband med myndighetens affärsverksamhet. För att framställa exemplar av sådana handlingar eller för att göra dem tillgängliga krävs rättighetshavarens tillstånd.

Upphovsrätt gäller alltså fullt ut för kartor, oavsett om dessa framställts i myndighetens offentliga verksamhet eller i dess affärsverksamhet. Kartor kan därför inte fritt återges utan myndighetens tillstånd. En förutsättning för det upphovsrättsliga skyddet är emellertid att kartan uppnår verkshöjd. Det är oklart om kartdata som används för automatiserad kartritning utgör kartor i

upphovsrättslig mening och därmed omfattas av undantagen i 1 kap. 9 § och 2 kap. 26 a § URL (SOU 2020:55 s. 82).

Andra immateriella rättigheter

Utöver det upphovsrättsliga skyddet kan det i handlingar som finns hos myndigheter förekomma sådant som är föremål för annat immaterialrättsligt skydd, t.ex. skydd för varumärken eller mönster som begränsar rätten att fritt vidareutnyttja handlingen. Detta kan förekomma i såväl upprättade som inkomna handlingar och rättigheterna kan tillkomma såväl myndigheter som tredje man.

3.5.2 Immaterialrätt och dataförvaltningsförordningen

Tillgängliggörande för vidareutnyttjande enligt kapitel II dataförvaltningsförordningen avser bl.a. data som är skyddade på grund av skydd av tredje parts immateriella rättigheter, artikel 3.1c.

Kapitel II ska dock inte tillämpas på data som innehas av public service-bolag eller av kulturinstitutioner, såsom bibliotek, arkiv och museer samt orkestrar, operor, baletter och teatrar, eller utbildningsinstitutioner. Detta enligt skäl 12 eftersom dessa till övervägande del omfattas av tredje parts immateriella rättigheter.

Data som skyddas av immateriella rättigheter är alltså en sådan kategori av skyddade data som kapitel II omfattar. Vidareutnyttjande av data ska dock endast tillåtas i enlighet med immateriella rättigheter, artikel 5.7.

3.6 Säkerhetsskydd

3.6.1 Säkerhetsskyddslagen

Säkerhetsskydd innebär bl.a. förebyggande åtgärder för att skydda säkerhetskänslig verksamhet mot spionerі, sabotage, terroristbrott och andra brott. Kraven på säkerhetsskyddet har förändrats genom utvecklingen i omvärlden och på informationsteknikområdet, ökningen av säkerhetskänslig verksamhet som bedrivs i enskild regi och en ökad internationell samverkan. För att stärka säkerhetsskyddet gjordes en översyn som resulterade i en ny

säkerhetsskyddslag (2018:585) som trädde i kraft den 1 april 2019. Den nya lagen gäller för den som till någon del bedriver verksamhet som är av betydelse för Sveriges säkerhet eller som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd, s.k. säkerhetskänslig verksamhet, 1 kap. 1 §.

Säkerhetsskyddet omfattar inte bara skydd av säkerhetskänslig verksamhet, utan även skydd av säkerhetsskyddsklassificerade uppgifter. En uppgift är säkerhetsskyddsklassificerad om den rör säkerhetskänslig verksamhet och därför omfattas av sekretess enligt offentlighets- och sekretesslagen, eller skulle ha omfattats av sekretess om den lagen hade varit tillämplig, 1 kap. 2 §. Det andra ledet i bestämmelsen tar sikte på enskilda verksamhetsutövare som normalt inte omfattas av offentlighets- och sekretesslagens regler. Lagen innehåller krav på olika säkerhetsskyddsåtgärder i form av informationssäkerhet, fysisk säkerhet och personalsäkerhet för de aktörer som bedriver säkerhetskänslig verksamhet.

Säkerhetsskyddsklassificerade uppgifter delas in i olika säkerhetsskyddsklasser utifrån den skada som ett röjande av uppgiften kan medföra för Sveriges säkerhet, 2 kap. 5 §. Det finns fyra olika säkerhetsskyddsklasser: kvalificerat hemlig vid en synnerligen allvarlig skada, hemlig vid en allvarlig skada, konfidentiell vid en inte obetydlig skada och begränsat hemlig vid endast ringa skada.

3.6.2 Informationssäkerhet

Åtgärder inom informationssäkerhet ska företas dels för att förebygga att säkerhetsskyddsklassificerade uppgifter obehörigen röjs, ändras, görs otillgängliga eller förstörs, dels för att förebygga skadlig inverkan i övrigt på uppgifter och informationssystem som gäller säkerhetskänslig verksamhet, 2 kap. 2 §. Tillämpningsområdet för säkerhetsskyddsåtgärden informationssäkerhet har utvidgats till att även avse skydd av uppgifter och informationssystem som inte utgör eller innehåller säkerhetsskyddsklassificerade uppgifter, men som har ett högt skyddsvärde av andra skäl. Detta eftersom det ökande informationsflödet innebär att viktiga samhällsfunktioner blir alltmer beroende av tillförlitliga och säkra digitala system som en garanti för att information är korrekt och tillgänglig (prop. 2017/18:89 s. 67f).

Säkerhetsskyddslagen och de krav på informationssäkerhet som ställs upp där gäller bara för de mest skyddsvärda verksamheterna. Krav på informationssäkerhet som gäller för samtliga statliga myndigheter finns emellertid i förordningen (2022:524) om statliga myndigheters beredskap. Av 13 § framgår att varje myndighet ansvarar för att sina informationshanteringssystem uppfyller sådana grundläggande och särskilda säkerhetskrav att myndighetens verksamhet kan utföras på ett tillfredsställande sätt och att behovet av säkra ledningssystem för informationssäkerhet särskilt ska beaktas. Förordningen kompletteras av föreskrifterna om informationssäkerhet för statliga myndigheter, om säkerhetsåtgärder i informationssystem för statliga myndigheter och om rapportering av it-incidenter för statliga myndigheter från Myndigheten för samhällsskydd och beredskap (MSBFS 2020:6, 2020:7 och 2020:8). I föreskrifterna finns ytterligare reglering kring utformning av informationssystem samt krav på myndigheternas informationssäkerhetsarbete, bl.a. gällande incident- och kontinuitetshantering.

För kommuner och regioner finns inte motsvarande reglering om informationssäkerhet som för statliga myndigheter. I lagen (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap med tillhörande förordning, finns bestämmelser om vilka åtgärder kommuner och regioner ska vidta för att hantera krissituationer i fred för att kunna minska sårbarheten i sin verksamhet. Regleringen innehåller emellertid inte några specifika bestämmelser om informationssäkerhet i bemärkelsen säker informationshantering.

3.6.3 Säkerhetsskydd och dataförvaltningsförordningen

Dataförvaltningsförordningens bestämmelser påverkar inte medlemsstaternas befogenheter när det gäller allmän säkerhet, försvar och nationell säkerhet, artikel 1.5. Det nationella regelverk som finns kring bl.a. säkerhetsskydd och informationssäkerhet påverkas därför inte av reglerna i dataförvaltningsförordningen, utan dessa gäller fullt ut på samma sätt som tidigare.

I kapitel II dataförvaltningsförordningen finns bestämmelser om hur vissa typer av skyddade data hos offentliga myndigheter kan

tillgängliggöras för vidareutnyttjande. Ingen av de kategorier av skyddade data som förordningen omfattar avser data som skyddas på grund av säkerhetsskydd. Vid bedömningen av om data kan göras tillgänglig ska en offentlig myndighet alltid beakta både säkerhetsskyddslagen och annan lagstiftning avseende informationssäkerhet. Dataförvaltningsförordningen påverkar inte detta.

I kapitel III och IV dataförvaltningsförordningen finns ramverk för leverantörer av dataförmedlingstjänster och dataaltruismorganisationer. För dessa båda finns krav bl.a. gällande säkerhet i förordningen. Om dessa leverantörer eller organisationer också träffas av befintliga regelverk avseende säkerhetsskydd eller informationssäkerhet så påverkar inte dataförvaltningsförordningens krav några av de skyldigheter som följer av t.ex. säkerhetsskyddslagen.

3.7 Konkurrensrätt

3.7.1 Konkurrenslagen

Konkurrensrätten regleras i Sverige primärt i konkurrenslagen med tillhörande konkurrensförordning (2021:87). Lagen syftar till att undanröja och motverka hinder för en effektiv konkurrens i fråga om produktion av handel med varor, tjänster och andra nyttigheter. Konkurrenslagen syftar till att generellt skydda samhällsekonomin och konsumenterna. Lagen är tillämplig på alla företag i hela näringslivet och i fråga om all produktion av och handel med varor, tjänster och andra nyttigheter. Själva företagsbegreppet utgör emellertid en viss begränsning av tillämpningsområdet.

Konkurrenslagen bygger i huvudsak på den konkurrensrättsliga förbudsprincipen. Principen innebär att vissa konkurrensbegränsningar i sig är skadliga och därför ska vara förbjudna. Lagens materiella bestämmelser är i huvudsak utformade med EU-rätten som förebild. Avsikten är att konkurrenslagen i materiellt hänseende ska likna EU-rättens konkurrensregler så mycket som möjligt vilket innebär att EU-domstolarnas praxis har betydelse för lagens tillämpning (prop. 2022/23:21 s. 6).

De materiella bestämmelserna i konkurrenslagen är inriktade på att motverka tre slag av åtgärder som kan skada konkurrensens effektivitet. Dels finns två förbudsbestämmelser, en som förbjuder

konkurrensbegränsande samarbete mellan företag och en som förbjuder företag med en dominerande ställning att missbruka sin marknadsmakt. Enligt 2 kap. 1 § KKL och art. 101 i fördraget om Europeiska unionens funktionssätt är det förbjudet med konkurrensbegränsande samarbete mellan företag som märkbart hindrar, begränsar eller snedvrider konkurrensen. Reglerna förbjuder t.ex. överenskommelser om priser, informationsutbyte eller exklusivitetsavtal. Enligt 2 kap. 7 § KKL och art. 102 i fördraget om Europeiska unionens funktionssätt är det förbjudet för företag med en dominerande ställning att missbruka sin marknadsmakt. Företaget får t.ex. inte försvåra för nya aktörer att ta sig in på marknaden eller genom underprissättning. Vidare finns bestämmelser med mer strukturella åtgärder avseende förbud mot företagskoncentration, 4 kap. 1 § KKL.

Konkurrenslagen innehåller också en regel som gör det möjligt att pröva konkurrenskonflikter som uppstår när staten, en kommun eller en region säljer varor och tjänster på marknaden i konkurrens med privata aktörer, 3 kap. 27 §, förbud mot konkurrensbegränsande offentlig säljverksamhet. Den regeln kompletterar förbuden mot konkurrensbegränsande samarbete respektive missbruk av dominerande ställning.

3.7.2 Konkurrensrätten och dataförvaltningsförordningen

Dataförvaltningsförordningen är som beskrivs i avsnitt 2.4.2 en del av EU:s datastrategi och en första pusselbit för att få den europeiska datamarknaden på plats. Syftet med datastrategin och inrättandet av den europeiska datamarknaden är att uppnå bättre transparens och sund konkurrens och därmed skapa bättre livsvillkor och innovation. Dataförvaltningsförordningen ska bidra till detta mål genom att skapa bättre tillit till marknaden, särskilt när det gäller dataförmedlartjänster. Genom att ställa krav på dessa tjänsters utformning och att särskilja på rollerna som tillhandahållare av data och förmedlare av data och konsument av data så hoppas man på att skapa bättre förutsättningar för en sund konkurrens.

I en rapport om datadelning och konkurrenskraft från europa.data.eu belyses frågan om hur datadelning och konkurrensrätten hänger samman. Rapporten tar avstamp i EU:s

datastrategi. I rapporten beskrivs att EU:s konkurrensrätt använts upprepade gånger för att komma åt konkurrensbegränsande praxis inom datahantering, t.ex. skulle artikel 101 kunna tillämpas när en datainnehavare använder datadelningsavtal som förhindrar eller begränsar utvecklingen av nya tjänster som skulle kunna byggas på tillgängliga data. Det finns dock risker med att tolka konkurrensreglerna alltför strikt då det i stället skulle kunna leda till negativa effekter på konkurrens och innovation. I en situation där en datainnehavare vägrar att göra data tillgängliga för en tredje part är i stället artikel 102 mer relevant. Det kräver dock att man kan fastslå vilken den relevanta datamarknaden är vilket inte är helt lätt när det kommer till datamarknader (Sharing Data (Anti-)Competitively – Will European data holders need to change their ways under the proposed new data legislation? Data.europa.eu, s. 7). Även om konkurrensrätten alltså redan i dag kan hantera vissa av de problem som kan uppstå så kan den inte lösa allt. Det beror bl.a. på att konkurrensreglerna är generella och inte specifikt anpassade till datamarknaden. Komplexiteten i att tillämpa konkurrensrätten (och begrepp som en marknad, dominerande position eller väsentlig anläggning) på en datamiljö gör resultatet oförutsägbart. Dessutom är konkurrensrätten inte utformad för att ta itu med alla möjliga utmaningar i detalj. Därför har i stället nya rättsakter tagits fram för att hantera olika aspekter (Sharing Data (Anti-)Competitively – Will European data holders need to change their ways under the proposed new data legislation? Data.europa.eu, s. 10).

I en studie framtagen av Generaldirektoratet för rättsliga frågor och konsumentfrågor fann man att nuvarande praxis för datadelning i EU var suboptimal ur ett ekonomiskt perspektiv, *Study on model contract terms and fairness control in data sharing and in cloud contracts and on data access rights* European commission Directorate-General for Justice and Consumers Directorate A — Civil and commercial justice, April 2022. Marknadsmisslyckanden som identifierades uppstår specifikt när det saknas konkurrens om data, och dataleverantörer befinner sig i en datamonopolsituation. Otillräcklig datadelning har en direkt koppling till bristande konkurrens. Studien noterade också att marknadsmisslyckanden kan inträffa när en datainnehavare kan implementera en värdekedjemodell som möjliggör gatekeeping. I dessa fall är nya tjänster eller produkter inhiberade på grund av en datainnehavare

vars samarbete krävs för att få tillgång till relevant information. Denna observation är också relevant i ljuset av analysen av EU:s konkurrenslagstiftning ovan, eftersom det är en utmaning som tillämpningen av EUF-fördraget sannolikt inte skulle kunna täcka på lämpligt sätt. Den ekonomiska effekten är betydande, och studien uppskattade att optimal datadelning kan utlösa ytterligare 185 miljarder euro i vinst under en period på 10 år (2021–2030).

Marknaden för datadelning är enligt rapporten inte optimalt konkurrensutsatt, och tillämpningen av traditionell konkurrensrätt har inte kunnat lösa detta problem, vilket leder till tydlig och betydande ekonomiska skador för företag och samhället som helhet.

En av slutsatserna i rapporten är att de olika rättsakter som kommit på dataområdet på senare tid och som är under förhandling inte påverkar eller förändrar den befintliga konkurrensrätten. I stället skapar de i praktiken en kompletterande rättslig ram som starkt påverkar hur bristande konkurrens kan åtgärdas.

En central faktor för tillit och för ökad datadelning är alltså att en sund konkurrens upprätthålls. I förordningen finns därför återkommande skrivningar gällande konkurrens, både i artiklar och beaktandeskäl. På flera ställen, t.ex. i skäl 37 och 60 och i artikel 1.4, fastslås att tillämpning av förordningen ska ske i enlighet med gällande lagstiftning på konkurrensområdet och inte påverka tillämpningen av dessa regler. Vidare finns det skrivningar i t.ex. skäl 13, 15, 25 och 33 samt i artikel 5.2 och 12.l om att tillämpning ska ske så att inte villkor ställs upp som bl.a. begränsar konkurrensen.

Behöriga myndigheter för dataförmedlartjänster och behöriga myndigheter för dataaltruismorganisationer ska också enligt artikel 11.7, 13.3 och 26.2 utföra sina uppdrag så att de inte snedvrider konkurrensen samt att deras befogenheter inte ska påverka befogenheten för de nationella konkurrensmyndigheterna.

3.8 SDG-förordningen

Europaparlamentets och rådets förordning (EU) 2018/1724 av den 2 oktober 2018 om inrättande av en gemensam digital ingång för tillhandahållande av information, förfaranden samt hjälp- och problemlösningstjänster och om ändring av förordning (EU) nr 1024/2012, den s.k. SDG-förordning, beslutades den 2 oktober

2018. SDG står för single digital gateway, den engelska beteckningen för gemensam digital ingång. Förordningen utgör en del av EU:s strategi för den inre marknaden och den fria rörligheten för människor, varor, tjänster och kapital. Med stöd av förordningen ska en gemensam digital ingång inrättas i syfte att minska den administrativa bördan för privatpersoner och företag när de utövar sin rätt till fri rörlighet och utför ärenden eller bedriver verksamhet över gränserna. Ingången ska integreras i Europeiska kommissionens befintliga portal Ditt Europa och fungera som en central kontaktpunkt där länkar ger tillgång till webbsidor med information, förfaranden samt hjälp- och problemlösningstjänster som är publicerade på nationell nivå eller EU-nivå (prop. 2021/22:66 s. 5).

Genom den gemensamma digitala ingången ska privatpersoner och företag få tillgång till bl.a.:

- information om rättigheter, skyldigheter och regler som gäller vid utövandet av rättigheter inom de områden av den inre marknaden som anges i bilaga I till förordningen,
- information om förfaranden som finns tillgängliga online och offline samt länkar till onlineförfaranden, inklusive sådana förfaranden som omfattas av bilaga II till förordningen, och
- information om och länkar till de hjälp- och problemlösningstjänster som omfattas av bilaga III till förordningen.

Den information som görs tillgänglig via ingången ska uppfylla vissa språk- och kvalitetskrav enligt artiklarna 9–11 i förordningen. Kraven syftar bl.a. till att den information som presenteras ska vara användarvänlig, begriplig och korrekt.

Med förfarande avses en sekvens av handlingar som en användare måste utföra för att t.ex. erhålla ett beslut från en behörig myndighet, artikel 3.3. Förordningen skiljer på sådana förfaranden som omfattas av bilaga II och andra förfaranden som har inrättats på nationell nivå och som omfattas av förordningens tillämpningsområde. De förfaranden som förtecknas i bilaga II ska, om de har inrättats i en medlemsstat, göras tillgängliga helt online, artikel 6.

Europeiska kommissionen ska i samarbete med medlemsstaterna, för de förfaranden som omfattas av bilaga II till förordningen, inrätta ett tekniskt system för automatiskt utbyte av bevis mellan de behöriga myndigheterna i olika medlemsstater, artikel 14. Med bevis

avses dokument eller data, inbegripet text eller ljud, bildinspelningar eller audiovisuella inspelningar, oavsett vilket medium som använts, artikel 3.5.

Ingången ska också ge tillgång till de hjälp- och problemlösningstjänster som förtecknas i bilaga III till förordningen samt till eventuella motsvarande tjänster som har tillgängliggjorts på frivillig väg, artikel 7.2 och 7.3. Hjälp- och problemlösningstjänsterna i bilaga III avser redan befintliga tjänster, vars primära reglering finns i andra EU-rättsakter.

Varje medlemsstat ska utse en eller flera nationella samordnare. En nationell samordnare ska bl.a. fungera som kontaktpunkt för alla frågor som rör ingången och främja en enhetlig tillämpning av artiklarna 9–16, artikel 28.1 a och b. En nationell samordnare har ett övergripande ansvar att tillhandahålla länkarna till den information, de förfaranden samt de hjälp- och problemlösningstjänster som finns tillgängliga på de webbsidor som förvaltas av behöriga myndigheter. Vidare ska en nationell samordnare parallellt med kommissionen regelbundet följa upp att informationen och tjänsterna uppfyller EU-förordningens kvalitetskrav, artiklarna 17.1 och 19.3.

En behörig myndighet är en myndighet eller ett organ i en medlemsstat som inrättats på nationell, regional eller lokal nivå och som har specifikt ansvar när det gäller den information, de förfaranden samt de hjälp- och problemlösningstjänster som omfattas av EU-förordningen, artikel 3.4.

3.8.1 SDG ska börja tillämpas stegvis

SDG-förordningen trädde i kraft den 12 december 2018 och ska börja tillämpas stegvis, artikel 39. Den 12 december 2020 inrättades den gemensamma digitala ingången och fr.o.m. denna tidpunkt ska samtliga behöriga myndigheter förutom kommunala myndigheter tillhandahålla information om de rättigheter, skyldigheter och regler som anges i bilaga I till SDG-förordningen. Även information om förfaranden, inklusive de förfaranden som anges i bilaga II, ska finnas tillgänglig från denna tidpunkt liksom information och länkar till de hjälp- och problemlösningstjänster som anges i bilaga III. För kommunala myndigheter inträder skyldigheten att som behöriga

myndigheter tillgängliggöra information och hjälp- och problemlösningstjänster den 12 december 2022. De förfaranden som omfattas av EU-förordningen ska fr.o.m. den 12 december 2023 finnas tillgängliga via ingången.

3.8.2 Lag och förordning med kompletterande bestämmelser

En ny lag infördes i Sverige för att komplettera SDG-förordningen, lag (2022:126) med kompletterande bestämmelser till EU:s förordning om en gemensam digital ingång. I lagen finns bemyndiganden för regeringen att bl.a. meddela föreskrifter om vilka kommunala myndigheter och enskilda organ som ska vara behöriga myndigheter eller nationella samordnare enligt SDG-förordningen. Det finns också bestämmelser om vilka artiklar i SDG-förordningen som en behörig myndighet ska uppfylla, utöver de bestämmelser som uttryckligen riktar sig till de behöriga myndigheterna. Slutligen finns en informationsskyldighet för behöriga myndigheter.

Ansvarsfördelningen har därutöver tydliggjorts i förordning (2022:127) med kompletterande bestämmelser till EU:s förordning om en gemensam digital ingång. I förordningens bilaga finns en lista över behöriga myndigheter.

3.8.3 SDG och dataförvaltningsförordningen

Genom dataförvaltningsförordningens artikel 36 genomfördes en utökning av SDG-förordningens tillämpningsområde. I artikeln justeras bilaga II till SDG-förordningen så att förfarandena Anmälan som leverantör av dataförmedlingstjänst och Registrering som dataaltruismorganisation som är erkänd i unionen omfattas av bilaga II.

Det innebär att dessa förfaranden ska göras tillgängliga helt online, vilket innebär att en användare kan gå igenom alla led i förfarandet elektroniskt och på distans.

4 Vidareutnyttjande av skyddade data från myndigheter

4.1 Inledning

Information som samlas in eller framställs i den offentliga sektorn är en stor tillgång för samhället. Möjligheten att utnyttja sådan information vidare har genom offentlighetsprincipen gamla anor i Sverige. Digitaliseringen av den offentliga sektorn och nya tekniska lösningar för att ta del av information av olika slag gör att de praktiska möjligheterna att vidareutnyttja information har ökat markant.

Den information som skapas av myndigheter är framför allt till nytta inom den verksamhet som tar fram den, men kan även vara till gagn i andra sammanhang. En myndighet själv eller andra aktörer kan sammanställa eller förädla informationen. På så vis kan informationen användas för andra ändamål och få ett värde inte bara för ursprungsverksamheten utan även för andra myndigheter eller intressenter. Även information som isolerat sett inte har något värde utanför en viss myndighet kan i en sammanställning, där information från olika verksamheter har länkats ihop, få ett värde. En sådan förädlad version av information kan vara värdefull i en bredare krets, vilket medför att ursprungsinformationen i sig också blir attraktiv att ha tillgång till. Information från den offentliga sektorn kan alltså många gånger ha ett betydande värde för enskilda eller företag. Genom att sammanställa och bearbeta information och göra den sökbar är det möjligt att utveckla nya tjänster som gör att informationen kan användas av fler. Att fler aktörer får möjlighet att ta del av information från offentlig verksamhet främjar insyn i förvaltningen och ger en ökad delaktighet och bidrar därmed till en demokratisk utveckling. Genom att bidra till förbättrad effektivitet

kan en ökad tillgång till information även ha positiva samhällsekonomiska effekter.

Tanken att data som har tagits fram eller samlats in av offentliga myndigheter eller andra enheter på offentliga budgetars bekostnad bör gynna samhället har länge varit en del av unionens politik. Öppna data-direktivet hade till syfte att säkerställa att myndigheter gör en större del av de data de producerar lätt tillgängliga för användning och vidareutnyttjande. Vissa kategorier av data, såsom data som rör affärshemligheter, insynsskyddade statistiska data och data som skyddas av tredje parts immateriella rättigheter, inbegripet företagshemligheter och personuppgifter, i offentliga databaser görs dock ofta inte tillgängliga, inte ens för forskning eller innovativ verksamhet i allmänhetens intresse, trots att sådan tillgänglighet är möjligt i enlighet med tillämplig unionsrätt, särskilt dataskyddsreglerna. På grund av sådana datas känslighet måste vissa tekniska och rättsliga förfarandekrav uppfyllas innan de görs tillgängliga, inte minst för att säkerställa att andra personers rättigheter till sådana data iakttas eller för att begränsa den negativa effekten på de grundläggande rättigheterna, principen om icke-diskriminering och dataskyddet. Det är vanligen tidsödande och kunskapsintensivt att uppfylla sådana krav. Detta har enligt kommissionen lett till ett otillräckligt nyttjande av sådana skyddade data. För att underlätta privata och offentliga enheters användning av skyddade data för europeisk forskning och innovation behövs enligt skäl 6 till dataförvaltningsförordningen tydliga villkor över hela unionen för tillgång till och användning av skyddade data.

Kapitel II i dataförvaltningsförordningen avser just detta. Här regleras vidareutnyttjande av vissa kategorier av skyddade data som innehas av offentliga myndigheter. Kapitlet ger inte en ny dataskyddsrättslig grund för att dela skyddade data. Inte heller innebär det skyldigheter att tillgängliggöra sådana data. I stället införs villkor för hur ett sådant tillgängliggörande får se ut i de fall sådana data kan tillgängliggöras för vidareutnyttjande enligt befintliga regler.

I framtagandet av förordning har kommissionen inspirerats av principer för datahantering och vidareutnyttjande som tagits fram för forskningsdata. FAIR-principerna innebär att forskningsdata ska gå att hitta, det ska finnas information om hur man får tillgång till dem, de ska vara kompatibla med andra data, och de ska vara möjliga

att återanvända. FAIR är en förkortning som står för Findable, Accessible, Interoperable och Reusable. FAIR-principerna används i arbetet för öppen vetenskap och beskriver några centrala riktlinjer för god datahantering och öppen tillgång till forskningsdata. FAIR bygger på att data ska vara så öppen som möjligt men stängd när nödvändigt.

Reglerna om tillgängliggörande av skyddade data för vidareutnyttjande har en stark koppling till det tidigare genomförda öppna data-direktivet.

I avsnitt 4.2 finns en beskrivning av hur regelverket för vidareutnyttjande av skyddade data ser ut i kapitel II dataförvaltningsförordningen. Därefter följer analyser och bedömningar av olika frågor om tillämpning och implementering i svensk rätt. Frågan om vilka myndigheter som föreslås utses till behöriga organ respektive tillhandahålla en gemensam informationspunkt behandlas i varsina avsnitt.

4.2 Reglering i dataförvaltningsförordningen

I kapitel II dataförvaltningsförordningen finns villkor och ramar för vidareutnyttjande av skyddade data som innehas av offentliga myndigheter. Kapitlet kan ses som en komplettering till öppna data-direktivet och en vidareutveckling gällande det rättsliga ramverket för att kunna tillgängliggöra offentligt producerade data för vidareutnyttjande.

4.2.1 Tillämpningsområde och avgränsningar

Bestämmelserna i kapitel II träffar offentliga myndigheter, artikel 3.1. Med det avses statliga, regionala eller lokala myndigheter och offentligrättsliga organ, eller sammanslutningar av en eller flera sådana myndigheter eller offentligrättsliga organ, artikel 2.18. Offentligrättsliga organ är juridiska personer som har inrättats för att tillgodose behov av allmänt intresse och som till största del finansieras av statliga, regionala eller kommunala myndigheter, eller står under administrativ tillsyn av myndigheter eller av ett kontrollorgan som till mer än hälften utses av sådana myndigheter, artikel 2.19.

Bestämmelserna ska inte tillämpas på offentliga företag, public service-bolag, kulturinstitutioner och utbildningsinstitutioner, artikel 3.2.

Med offentliga företag avses enligt definitionen i artikel 2.19 företag som offentliga myndigheter har ett direkt eller indirekt bestämmande inflytande över.

Kulturinstitutioner beskrivs som institutioner så som bibliotek, arkiv och museer samt orkestrar, operor, baletter och teatrar. Anledningen till att dessa är undantagna från tillämpningsområdet är att de verk och handlingar som dessa innehar till övervägande del omfattas av tredje parts immateriella rättigheter.

Utbildningsinstitutioner definieras inte särskilt i dataförvaltningsförordningen. Begreppet kan vara svårt att tolka för de institutioner som delvis bedriver utbildning, men också annan verksamhet såsom exempelvis forskning. Av skäl 12 framgår att forskning kan bedrivas av offentliga myndigheter och att förordningen då bara ska tillämpas på dem enbart i deras egenskap av organisation som bedriver forskning. Detta är dock inte alltid en enkel gränsdragning att göra. Forskning och undervisning bedrivs ofta samlat på svenska universitet och högskolor. Universitetsbiblioteken är ofta både utbildning- och forskningsbibliotek.

Begreppet offentlig myndighet i förordningen, med avgränsningen mot offentliga företag, stämmer väl överens med begreppet myndighet i RF som också är det som används vid tillämpningen av tillgång till allmänna handlingar enligt 2 kap. TF. Myndigheter är de organ som ingår i den offentligrättsliga statliga och kommunala organisationen. Regeringen, ämbetsverken, domstolarna och de kommunala nämnderna är exempel på myndigheter. Riksdagen, landstingen och kommunfullmäktige är inte myndigheter, men dessa beslutande församlingar jämställs uttryckligen med myndigheter när det gäller bestämmelserna om rätten att ta del av allmänna handlingar, 2 kap. 5 § TF.

Vidare är inte bolag, föreningar och stiftelser myndigheter ens om staten eller en kommun helt äger eller bestämmer över dem. Vissa sådana juridiska personer jämställs dock med myndigheter vid tillämpning av rätten att ta del av allmänna handlingar genom bestämmelser i OSL, 2 kap. 3 och 4 §§ OSL. (Se Lenberg, Tansjö & Geijer, Offentlighets- och sekretesslagen En kommentar (2022, version 26, JUNO), under rubriken Myndighetsbegreppet).

Vissa kategorier av skyddade data

Bestämmelserna i kapitel II avser data som myndigheter innehar som är skyddade på grund av
- insynsskydd för kommersiella uppgifter inklusive affärs-, yrkes- och företagshemligheter,
- insynsskydd för statistiska uppgifter,
- skydd för tredje parts immateriella rättigheter, eller
- skydd av personuppgifter, om sådana data inte omfattas av tillämpningsområdet för öppna data-direktivet.

Kapitlet är inte tillämpbart på data som innehas av myndigheter och som är skyddade av skäl som rör allmän säkerhet, försvar eller nationell säkerhet, artikel 3.2 d. Detta innebär att data som är skyddade av flera skäl varav ett är ett sådant skäl som är undantaget inte träffas av bestämmelserna i förordningen. Om en myndighet bedriver affärsverksamhet ska bestämmelserna inte tillämpas på data inom den verksamheten, artikel 3.2 e.

Vidareutnyttjande

Kapitlet reglerar tillgängliggörande av data för vidareutnyttjande. Med vidareutnyttjande avses fysiska eller juridiska personers användning av data som innehas av offentliga myndigheter för andra ändamål än de ursprungliga ändamålen inom den offentliga verksamheten, artikel 2.2. Utbyte av data mellan offentliga myndigheter som sker i samband med deras offentliga verksamhet omfattas däremot inte av definitionen.

4.2.2 Förbud mot exklusiva avtal

Avtal eller praxis som ger exklusiv rätt till vidareutnyttjande av den aktuella typen av data är som utgångspunkt förbjudet enligt art. 4. Skulle ett exklusivt avtal vara nödvändigt för tillhandahållandet av en tjänst eller en produkt av allmänt intresse så är det tillåtet i upp till tolv månader. Bestämmelserna kan ses som en komplettering till EU:s konkurrensreglering.

Exklusiva avtal som ingåtts redan innan förordningen beslutades får inte förnyas. Om sådana gäller på obestämd tid bör de upphöra att gälla senast 30 månader efter att förordningen träder i kraft enligt skäl 14. Om avtal som ingåtts innan förordningen beslutades innehåller avtalsvillkor som inte uppfyller villkoren i artikel 4.2 och 3 så ska de upphöra att gälla när de löper ut och som senast den 24 december 2024, 15 månader efter att förordningen träder i kraft, artikel 4.6.

4.2.3 Villkor

Vidareutnyttjande av data ska bara tillåtas av myndigheten på ett sätt som säkerställer att uppgifternas skyddade karaktär bevaras. I artikel 5 regleras vilka villkor som får ställas upp när offentliga myndigheter tillgängliggör de särskilda kategorierna av skyddade data för vidareutnyttjande. Villkoren ska vara icke-diskriminerande, transparenta, proportionerliga och objektivt motiverade med hänsyn till kategorierna av data, vidareutnyttjandets syfte och typerna av data. Villkoren får inte begränsa konkurrensen. Villkoren för vidareutnyttjande ska offentliggöras via den gemensamma informationspunkt som ska inrättas enligt artikel 8.

De krav som kan föreskrivas av offentliga myndigheter omfattar olika skyddsåtgärder för att upprätthålla datans aktuella skydd. Det avser bl.a. anonymisering av personuppgifter, ändringar av uppgifter innehållande affärshemligheter eller immateriella rättigheter, att tillgång till och vidareutnyttjande ska ske i en säker behandlingsmiljö som tillhandahålls och kontrolleras av myndigheten eller att tillgång till och vidareutnyttjande av data i vissa fall ska ske i bestämda fysiska lokaler där den säkra behandlingsmiljön är belägen.

Om vidareutnyttjande tillåts genom en säker behandlingsmiljö, på distans eller i fysiska lokaler, ska myndigheten införa villkor som bevarar integriteten för de tekniska systemens funktionssätt i den säkra behandlingsmiljön. Myndigheten ska också förbehålla sig rätten att verifiera processen, metoderna och alla resultat från den behandling av data som görs av vidareutnyttjaren för att bevara integriteten i dataskyddet och förbehålla sig rätten att förbjuda användning av resultat som innehåller information som hotar tredje parters rättigheter och intressen, artikel 5.4.

Det ska vara förbjudet för vidareutnyttjaren att återidentifiera de registrerade, och vidareutnyttjaren ska vidta åtgärder för att förhindra att det sker. Denna ska också informera den utlämnande myndigheten om alla uppgiftsincidenter om det sker.

Överföring av icke-personuppgifter till tredje land

Om vidareutnyttjaren avser överföra icke-personuppgifter till tredje land ska den underrätta den utlämnande myndigheten om detta i samband med begäran. Tillstånd till sådant vidareutnyttjande får bara ske efter tillstånd från den juridiska person vars rättigheter och intressen kan påverkas, art. 5.9. Därutöver finns ett antal villkor som vidareutnyttjaren ska åta sig i avtal vid överföring av data till tredje land, art. 5.10. För överföring av personuppgifter till tredje land gäller i stället dataskyddsregleringen av detta fullt ut.

Kommissionen får ta fram standardavtalsklausuler för detta i en genomförandeakt. Kommissionen kan också anta genomförandeakter för att intyga ett visst tredjelands rättsliga, tillsynsmässiga och verksamhetsmässiga arrangemang på ett tillfredställande sätt säkerställer skydd för immateriella rättigheter och affärshemligheter, att dessa tillämpas och verkställs på ett effektivt sätt och att det omfattar effektiva rättsmedel, artikel 5.11 andra stycket.

4.2.4 Avgifter för vidareutnyttjande

Offentliga myndigheter som tillåter ett vidareutnyttjande av sådana data som avses i artikel 3.1 får enligt artikel 6 ta ut en avgift. Avgifterna ska vara transparenta, icke-diskriminerande, proportionella och objektivt motiverade. Avgifterna får inte begränsa konkurrensen. Avgifterna ska kunna härledas till kostnaderna för att genomföra förfarandet för begäran om vidareutnyttjande och vara begränsade till nödvändiga kostnader i samband med vissa i artikeln utpekade åtgärder.

Offentliga myndigheter som tar ut avgifter måste säkerställa att dessa kan betalas online med hjälp av allmänt tillgängliga gränsöverskridande betaltjänster, artikel 6.3.

När offentliga myndigheter tar ut avgifter ska de vidta åtgärder för att ge incitament till vidareutnyttjande av skyddade data för icke-kommersiella ändamål så som vetenskaplig forskning. Vidare ska man ge incitament till vidareutnyttjande av små och medelstora företag och uppstartsföretag. Detta kan ske genom att tillgängliggörande sker med nedsatt avgift eller avgiftsfritt. Kriterier och metoder för avgifter ska fastställas av medlemsstaterna, artikel 6.6.

4.2.5 Behöriga organ

Varje medlemsstat ska enligt artikel 7 utse ett eller flera behöriga organ för att bistå de offentliga myndigheterna som hanterar begäran om vidareutnyttjande. Biståndet ska enligt art. 7.4 innefatta följande:

- Tekniskt stöd för att tillhandahålla en säker behandlingsmiljö för att ge tillgång till vidareutnyttjande av data.
- Vägledning och tekniskt stöd om hur data bäst kan struktureras.
- Tekniskt stöd för pseudonymisering (dvs. att som säkerhetsåtgärd ersätta personuppgifter med något annat som exempelvis en kod) och för att säkerställa att databehandling sker på ett sätt som effektivt bevarar integriteten, konfidentialiteten, dataintegriteten (dvs. skyddet av data mot bl.a. förvanskning och obehörig tillgång) och tillgängligheten för den information som finns i den aktuella datan. Det kan t.ex. vara teknik för anonymisering, generalisering, undertryckande och randomisering eller andra integritetsbevarande metoder eller metoder för radering av kommersiellt känslig information.
- Bistånd till offentliga myndigheter i de fall de ska stödja vidareutnyttjare när de begär samtycke till vidareutnyttjande eller datainnehavares tillstånd.
- Bistånd vid bedömning av tillräcklighet i avtalsmässiga åtaganden.

De behöriga organen får ges befogenhet att bevilja tillgång till de kategorier av data som avses i artikel 3.1. De ska i sådana fall tillämpa samma artiklar som de offentliga myndigheterna annars skulle tillämpa vid beviljandet.

4.2.6 Gemensam informationspunkt

Medlemsstaterna ska etablera en informationspunkt som stöd för vidareutnyttjare i att finna lämpliga data.

All relevant information om tillämpningen av artiklarna 5 och 6 avseende villkor för vidareutnyttjande och om avgifter ska finnas tillgänglig och lätt åtkomlig via den gemensamma informationspunkten. För detta ska medlemsstaterna inrätta ett nytt organ eller utse ett befintligt organ. Informationspunkten ska vara behörig att ta emot förfrågningar eller ansökningar om vidareutnyttjande.

I den gemensamma informationspunkten ska det finnas en sökbar tillgångsförteckning som innehåller en översikt över alla tillgängliga datakällor tillsammans med relevant information som beskriver tillgängliga data samt villkoren för vidareutnyttjandet av dessa, artikel 8.2.

Kommissionen ska inrätta en europeisk gemensam åtkomstspunkt med ett sökbart register över tillgängliga data i nationella gemensamma informationspunkter, artikel 8.4.

Den gemensamma informationspunkten ska också kunna ta emot förfrågningar eller ansökningar om vidareutnyttjande av skyddade data och vidareförmedla dessa till de myndigheter som innehar aktuella data, artikel 8.2.

4.2.7 Hantering av begäran om vidareutnyttjande

Offentliga myndigheter som får en begäran om vidareutnyttjande av de kategorier av skyddade data som avses i art. 3.1 ska fatta beslut om begäran inom två månader från det att begäran mottogs, artikel 8.1. I nationell rätt får föreskrivas kortare tid. Det finns i artikel 8.1 andra stycket möjlighet att förlänga tiden för hantering av begäran med ytterligare högst 30 dagar vid exceptionellt omfattande eller komplicerade begäran. Sökanden ska i sådant fall underrättas om detta tillsammans med skälen för det.

Fysiska eller juridiska personer som påverkas av ett beslut ska ha en effektiv rätt till överprövning av en opartisk myndighet, artikel 9.2. Hur denna överprövning ska se ut ska regleras i nationell rätt.

4.3 Vidareutnyttjande av skyddade data och dataskydd

Ramverket i dataförvaltningsförordningen om tillgängliggörande av skyddade data för vidareutnyttjande har många beröringspunkter med dataskyddsreglerna. Som beskrivs i avsnitt 3.2.5 påverkar inte dataförvaltningsförordningen tillämpningen av befintlig unionsrätt och nationell rätt som avser skydd för personuppgifter. Dataskyddsreglerna ska därför tillämpas fullt ut. Detta gäller enligt skäl 4 även när personuppgifter och andra data än personuppgifter i en datamängd är oupplösligt sammanlänkade.

Nedan följer en beskrivning av vissa centrala dataskyddsrättsliga aspekter som myndigheter som ska bedöma en begäran om att vidareutnyttja skyddade data behöver beakta. Uppräkningen ska inte ses som en uttömmande uppräkning av dataskyddsrättsliga frågor som kan aktualiseras.

4.3.1 Finalitetsprincipen

I artikel 5.1 b dataskyddsförordningen anges att personuppgifter ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. Detta är principen om ändamålsbegränsning, eller finalitetsprincipen. I artikel 6.4 dataskyddsförordningen ges ledning i hur bedömningen av förenligheten med insamlingsändamålen ska göras.

Denna begränsning är relevant i förhållande till varje behandling som den personuppgiftsansvarige utför efter själva insamlingen. Varje efterföljande behandlingsåtgärd, inklusive den tekniska bearbetning och lagring som ofta är oundviklig när uppgifter har samlats in, utgör nämligen en ytterligare behandling (dvs. vidarebehandling) i dataskyddsförordningens mening. Att vidta skyddsåtgärder enligt dataförvaltningsförordningens kapitel II och att tillgängliggöra data är också sådan ytterligare behandling. Detta gäller oavsett om denna behandling sker för samma ändamål som det för vilka uppgifterna samlades in eller för något annat ändamål. Det är viktigt att notera att det är i förhållande till det ursprungliga insamlingsändamålet som varje vidarebehandling ska prövas, inte mot det ändamål för vilket den senaste vidarebehandlingen utfördes.

Den nya behandlingen kräver enligt dataskyddsförordningen inte någon annan rättslig grund än den med stöd av vilken den ursprungliga insamlingen medgavs, skäl 50 till förordningen.

4.3.2 Skyddsåtgärder ur ett dataskyddsperspektiv

För att kunna bevilja tillgång till skyddade data ska olika typer av skyddsåtgärder vidtas inför att data görs tillgängligt. I dataförvaltningsförordningens artikel 5 räknas sådana villkor upp som myndigheter kan ställa upp. I artikel 7 beskrivs hur behöriga organ kan stötta vid dessa olika åtgärder.

All behandling av personuppgifter ska uppfylla kraven i dataskyddsreglerna, primärt dataskyddsförordningen. Av artikel 4.2 dataskyddsförordningen framgår att ”behandling” bl.a. omfattar åtgärder som vidtas beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt.

Att i enlighet med dataförvaltningsförordningen vidta olika skyddsåtgärder på datamängder som innehåller personuppgifter och att tillgängliggöra data som innehåller personuppgifter är personuppgiftsbehandlingar i dataskyddsförordningens mening. När sådana åtgärder vidtas med data som innehåller personuppgifter behöver kraven i dataskyddsförordningen vara uppfyllda. Det behöver bl.a. finnas en rättslig grund enligt artikel 6 för behandlingen. Dataförvaltningsförordningens regelverk utgör enligt skäl 4 inte en sådan rättslig grund. En sådan rättslig grund skulle i stället t.ex. kunna vara en uppgift av allmänt intresse om det kan bedömas som att tillhandahållandet omfattas av den utlämnande myndighetens uppgift i instruktion och regleringsbrev eller annan verksamhetsreglering tillsammans med serviceskyldigheten enligt förvaltningslagen.

Två skyddsåtgärder som nämns i dataförvaltningsförordningen är anonymisering och pseudonymisering. Dessa två åtgärder bör viktas olika av myndigheter när de bedömer vidareutnyttjandet ur ett dataskyddsperspektiv. Anonymisering utgör ett sätt att främja vidareutnyttjande av information från den offentliga sektorn ur ett konkurrensfrämjande perspektiv, samtidigt som den uppfyller de

olika kraven i dataskyddslagstiftningen, eftersom dataskyddsförordningen inte är tillämplig på ”anonym information”, såsom den definieras i skäl 26 i dataskyddsförordningen. När det däremot gäller information som har pseudonymiserats (vilket skulle kunna leda till avanonymisering av fysiska personer med hjälp av ytterligare information) så ska den fortfarande betraktas som personuppgifter, vilket innebär att andra åtgärder som krävs enligt dataskyddslagstiftningen ska vidtas. Samtidigt är psedonymisering en skyddsåtgärd enligt dataskyddsförordningen och den minskar riskerna för de registrerade, och offentliga myndigheter och vidareutnyttjare får hjälp att uppfylla kraven på dataskydd, särskilt principerna om inbyggt dataskydd och dataskydd som standard samt uppgiftsminimering (gemensamt yttrande 03/2021 från EDPB och EDPS om förslaget till Europaparlamentets och rådets förordning om dataförvaltning [dataförvaltningsakten], punkt 91). Dataskyddsreglerna gäller dock endast för information som hänför sig till en identifierad eller identifierbar person, och de är därmed inte tillämpliga på personuppgifter som anonymiserats på ett sådant sätt att en fysisk person inte längre är identifierbar.[3]

Villkoren för vidareutnyttjande av data bör begränsas till vad som är nödvändigt för att skydda tredje parts rättigheter och intressen i data och integriteten hos de offentliga myndigheternas it- och kommunikationssystem. Offentliga myndigheter bör tillämpa sådana villkor som bäst gagnar vidareutnyttjarens intressen utan att detta leder till en oproportionerlig börda för de offentliga myndigheterna. Villkoren för vidareutnyttjande av data bör utformas på ett sätt som säkerställer effektiva skyddsåtgärder för personuppgifter. Före överföring bör personuppgifter vara anonymiserade på ett sådant sätt att de registrerade inte kan identifieras, och data som innehåller affärshemligheter bör ändras på ett sådant sätt att ingen konfidentiell information lämnas ut. Om tillhandahållandet av anonymiserade eller ändrade data inte skulle tillgodose vidareutnyttjarens behov, förutsatt att eventuella krav på att genomföra en konsekvensbedömning avseende dataskydd och samråda med tillsynsmyndigheten enligt artiklarna 35 och 36 i dataskyddsförordningen uppfylls och om riskerna för de registrerades rättigheter och deras intressen är minimala, kan det

[3] Jfr definitionen av personuppgift i artikel 4.1 dataskyddsförordningen. Se också skäl 8 till dataförvaltningsförordningen.

enligt skäl 15 första stycket dataförvaltningsförordningen tillåtas att vidareutnyttja uppgifterna på plats eller på distans inom en säker behandlingsmiljö.

4.3.3 Skyddsåtgärder – allmän handling och sekretess

Dataförvaltningsförordningen påverkar inte nationella bestämmelser om sekretess, inte heller sådan sekretess som avser de kategorier av skyddade data som kapitel II avser. Det innebär att t.ex. statistiksekretess och affärssekretess samt dataskyddssekretess i 21 kap. 7 § OSL inte påverkas utan ska tillämpas på samma sätt som i dag även efter att dataförvaltningsförordningen ska börja tillämpas. Vid genomförandet av öppna data-direktivet hanterades frågan om hur sekretessförbehåll påverkades av direktivet och den nya datalagen. Den svenska lagstiftaren har i konsekvens med direktivets tillämpningsområdesformulering uttalat att sekretessförbehåll enligt 10 kap. 14 § OSL inte påverkas av lagen (prop. 2021/22:225 s. 71), jfr 1 kap. 2 § datalagen. Eftersom inte heller dataförvaltningsförordningen påverkar nationella bestämmelser om tillgång och sekretess kan ett förbehåll att inte lämna uppgiften vidare enligt 10 kap. 14 § OSL inte vara ett sådant villkor som avses i artikel 5 i dataförvaltningsförordningen.

I skäl 7 beskrivs olika tekniker som kan användas för att skydda eller ta bort personuppgifter ur en datamängd såsom t.ex. generalisering, undertryckande och randomisering. Om en myndighet skulle bearbeta känsliga uppgifter med någon av dessa metoder så skulle resultatet av bearbetningen sannolikt anses vara en ny handling skild från handlingen med de känsliga uppgifterna i obearbetad form. De moderna metoder som avses i dataförvaltningsförordningen skiljer sig från traditionell maskning enligt svensk sekretesslagstiftning där det vanligen är den handling där de känsliga uppgifterna ursprungligen finns som blir föremål för utlämnande. Bearbetningen, dvs. användandet av nämnda metoder, torde aldrig kunna ses som sådana rutinbetonade åtgärder som avses i 2 kap. 6 § andra stycket TF. Någon skyldighet att använda metoderna och i praktiken framställa nya handlingar eller data som kan göras tillgänglig för vidareutnyttjande finns inte, varken i dataförvaltningsförordningen eller i svensk rätt.

Att någon skyldighet inte föreligger innebär inte att det finns hinder mot det. Av legalitetsprincipen följer emellertid att det bör finnas rättsligt stöd även för en myndighets frivilliga verksamhet att åtminstone mer regelmässigt använda skyddsbevarande metoder på begäran. Det rättsliga stödet återfinns normalt i myndighetens instruktion eller regleringsbrev, informationsskyldighet enligt annan verksamhetsförfattning jämte serviceskyldigheten i förvaltningslagen.

4.4 Kompletterande regler i nationell rätt

I dataförvaltningsförordningens kapitel II om tillgängliggörande av skyddade data för vidareutnyttjande finns vissa skyldigheter och möjligheter för medlemsstaterna att reglera vissa frågor i nationell rätt.

4.4.1 Datalagen ska komplettera dataförvaltningsförordningens regler om vidareutnyttjande av skyddade data

Förslag: Bestämmelser som ska genomföra och komplettera dataförvaltningsförordningens kapitel II om vidareutnyttjande av vissa kategorier av skyddade data som innehas av myndigheter ska infogas i svensk lag.

Skälen för förslaget: Artikel 6, 7, 8 och 9 i kapitel II dataförvaltningsförordningen innehåller skyldigheter och möjligheter till kompletterande nationell lagstiftning gällande vidareutnyttjande av skyddade data från myndigheter. De avser tillgängliggörande av data för vidareutnyttjande och handläggning av sådana ärenden, villkor för vidareutnyttjande, förteckningar över tillgängliga data, avgifter och överklagandehantering. Kapitel II i dataförvaltningsförordningen har ett nära samband med regleringen i öppna data-direktivet och datalagen, som genomför direktivet i svensk rätt. De delar som ska införas i svensk rätt passar väl in i den befintliga strukturen i datalagen.

Många myndigheter träffas av både öppna data-direktivet och kapitel II i dataförvaltningsförordningen. Båda dessa regelverk avser

vidareutnyttjande av data som tillhandahålls från olika delar av offentlig sektor, men de avser olika typer av data. Vilka som omfattas av regelverken skiljer sig också delvis åt. Dataförvaltningsförordningens kapitel II omfattar bara myndigheter medan öppna data-direktivet också omfattar t.ex. offentliga företag.

För att både myndigheter och vidareutnyttjare samlat ska kunna utläsa vad som gäller vid tillgängliggörande av data för vidareutnyttjande är det lämpligt att regelverken hålls samlade i svensk rätt. Datalagen reglerar hur myndigheter ska tillgängliggöra öppna data för vidareutnyttjande, avgifter för sådant tillgängliggörande samt handläggningen av begäran om att få vidareutnyttja sådana data.

Alternativet till att införa kompletterande bestämmelser i datalagen hade varit att ta fram en ny lag som reglerar tillgängliggörande av just de aktuella kategorierna av skyddade data. Det skulle innebära att fler delar som är lika gällande tillgängliggörande av data oavsett om det rör öppna data eller vissa typer av skyddade data hade behövt regleras parallellt i båda regelverken. Det skulle leda till onödig dubbelreglering.

4.4.2 Ord och uttryck i datalagen

Förslag: Definitionen av uttrycket begäran om tillgängliggörande av data för vidareutnyttjande ska utvidgas till att även omfatta av skyddade data som görs tillgängliga enligt dataförvaltningsförordningen.

Uttrycken skyddade data och EU:s dataförvaltningsförordning ska införas i lagen.

Skälen för förslaget: I datalagen finns i 1 kap. 4 § en lista med ord och uttryck och definitionerna av dessa. Definitionerna har i tillämpliga fall utgångspunkt i öppna data-direktivet (prop. 2021/22:225 s. 73–75). Flera av begreppen förekommer också i dataförvaltningsförordningen. Andra begrepp förekommer inte uttryckligen i dataförvaltningsförordningen, men har betydelse för hur de kompletterande bestämmelser som föreslås i denna promemoria ska tillämpas. Om datalagen ska innehålla kompletterande bestämmelser till dataförvaltningsförordningen så

är det viktigt att det inte finns oklarheter gällande vad olika begrepp betyder.

Orden data och vidareutnyttjande definieras i såväl datalagen som i artikel 2 i dataförvaltningsförordningen.

Uttrycket begäran om tillgängliggörande av data för vidareutnyttjande är centralt också för tillämpningen av datalagen i relation till kapitel II dataförvaltningsförordningen.

Data

Definitionerna av data i dataförvaltningsförordningen och datalagen skiljer sig åt språkligt. De innehåller dock samma element och de språkliga skillnaderna innebär inte att betydelsen av begreppet data är olika i dataförvaltningsförordningen och datalagen. Någon ändring av begreppet data i datalagen behövs därför inte.

Data definieras i dataförvaltningsförordningen som varje digital återgivning av handlingar, fakta eller information och varje sammanställning av sådana handlingar, sådana fakta eller sådan information, däribland i form av ljudinspelningar, bildinspelningar eller audiovisuella inspelningar.

I datalagen definieras data som information i digitalt format oberoende av medium.

Definitionen i datalagen avser information, medan dataförvaltningsförordningen avser handlingar, fakta och information eller sammanställningar av dessa. Av förarbetena till datalagen framgår att begreppet information valts framför t.ex. handlingar som genomgående begrepp eftersom det är bredare. Med information avses allt innehåll, eller varje del av ett sådant innehåll, i en informationsmängd som kan vara föremål för tillgängliggörande och vidareutnyttjande enligt datalagen (SOU 2020:55 s. 124 och 125). Information i datalagens mening ska därför anses omfatta såväl handlingar som fakta.

I dataförvaltningsförordningens definition anges varje digital återgivning, medan datalagens definition anger information i digitalt format. Båda definitionerna avgränsar alltså begreppet till att avse digital information.

Båda definitionerna hanterar också frågan om vissa format. Av dataförvaltningsförordningens begrepp framgår att det avser varje

återgivning och att det kan innefatta information i form av ljudinspelningar, bildinspelningar eller audiovisuella inspelningar. Av datalagen framgår i stället att det är oberoende av medium.

Vidareutnyttjande

Begreppet vidareutnyttjande och vilka avgränsningar det omfattar skiljer sig åt i struktur mellan dataförvaltningsförordningen och datalagen. I dataförvaltningsförordningen är vissa begränsningar av tillämpningsområdet inbyggda i själva definitionen, medan sådana begränsningar av tillämpningen i datalagen placerats i andra paragrafer än de där ord och uttryck definieras. Det innebär att de skillnader som finns mellan själva definitionerna inte får någon betydelse vid tillämpningen utifrån andra regleringar av begränsningar. Definitionen av vidareutnyttjande i datalagen behöver därför inte justeras.

Vidareutnyttjande definieras i dataförvaltningsförordningen som fysiska eller juridiska personers användning av data som innehas av offentliga myndigheter för andra kommersiella eller icke-kommersiella ändamål än det ursprungliga ändamål inom den offentliga verksamheten för vilket de framställdes, med undantag för utbyte av data mellan offentliga myndigheter som enbart sker i samband med deras offentliga verksamhet.

I datalagen definieras vidareutnyttjande som bearbetning av data från den offentliga sektorn för valfritt ändamål.

Datalagens definition gäller den offentliga sektorn. Begreppet offentliga sektorn används också i 1 kap. 1 § där lagens syfte slås fast till att avse den offentliga sektorns tillgängliggörande av data. Vad som omfattas av begreppet framgår i sin tur av vilka som ska tillämpa lagen i dess nuvarande omfattning. Som beskrivits ovan är det utöver myndigheter också offentliga företag, offentligt styrda organ i vissa fall, universitet och högskolor under statligt huvudmannaskap, universitets- och högskolebibliotek, huvudmän enligt skollagen (2010:800) och public service-bolag. Avgränsningen av vilka som ska tillämpa bestämmelsen har i datalagen alltså inte gjorts i definitionen av vidareutnyttjande, utan i en annan bestämmelse som reglerar hur lagen ska tillämpas. I dataförvaltningsförordningens definition finns avgränsningen av vilka subjekt som ska tillämpa reglerna också

införd i begreppet vidareutnyttjande som bara omfattar data från offentliga myndigheter.

Definitionen i dataförvaltningsförordningen avser användning av data medan definitionen i datalagen avser bearbetning av data. En bearbetning av data enligt kan innebära att någon skapar, utvecklar eller testar produkter, tjänster, kunskaper, idéer eller andra företeelser. Att någon endast tar del av data för att tillgodogöra sig det informationsbärande innehållet, exempelvis i kunskapshöjande syfte, utgör inte ett vidareutnyttjande i datalagens mening (prop. 2021/22:225 s. 75).

I dataförvaltningsförordningen avser vidareutnyttjande sådant som sker för andra kommersiella eller icke-kommersiella ändamål än det ursprungliga ändamål för vilket de framställdes. I datalagen handlar det i stället om valfritt ändamål. Effekten är densamma av dessa båda beskrivningar, men datalagens ram kan anses vara något vidare då den avser valfritt ändamål.

I dataförvaltningsförordningens definition är utbyte av data mellan offentliga myndigheter som enbart sker i samband med deras offentliga verksamhet undantagen. Motsvarande skrivning finns inte i definitionen i datalagen. En sådan avgränsning finns i stället i 1 kap. 8 § andra stycket datalagen.

Nya ord och uttryck som bör föras in

Datalagen ska komplettera kapitel II i dataförvaltningsförordningen. Kapitlet avser vidareutnyttjande av vissa kategorier av skyddade data som innehas av offentliga myndigheter. Datalagen omfattar vidareutnyttjande av data i en bredare bemärkelse.

Begränsningen av vilken data som omfattas av datalagen återfinns under rubriken Undantag för vissa data i 1 kap. 9 och 10 §§ datalagen. Begränsningen omfattar dels data som någon har rätt till tillgång till som part, dels data som omfattas av immateriella rättigheter. Frågan om immateriella rättigheter och omfattningen av datalagen hanteras särskilt i avsnitt 4.4.4. De kategorier av skyddade data som dataförvaltningsförordningen omfattar ska hanteras enligt den och de särskilda kompletterande regler som avser dataförvaltningsförordningen. Det behövs därför ett uttryck för att beskriva vilka data som avses. I dataförvaltningsförordningen

används uttrycket kategorier av data som avses i artikel 3.1. Detta är en bra definition för ett uttryck, men det är något omständligt att använda genomgående i datalagen som uttryck.

Något sammanhållande begrepp för alla fyra skyddsgrunder finns inte. Vissa kategorier av skyddade data är det uttryck som återfinns i rubriken till kapitel II i dataförvaltningsförordningen. Vissa kategorier visar på att det avser data som är skyddade på olika grunder. Det pekar dock inte ut vilka kategorier av skyddade data som avses. Uttrycket är också långt och otympligt. Uttrycket skyddade data är ett mer luftigt uttryck. Det kan dock uppfattas som oprecist och som att det omfattar alla typer av skyddade data, inte bara de som räknas upp i artikel 3.1 förordningen. Genom en tydlig definition av uttrycket skyddade data i lagen kan den risken undanröjas Skyddade data bedöms därför vara ett ändamålsenligt begrepp.

Det behöver i datalagen finnas hänvisningar till dataförvaltningsförordningen. Hänvisningar till dataförvaltningsförordningen i lagen bör vara utformade på så sätt att den avser förordningen i den vid varje tidpunkt gällande lydelsen, s.k. dynamisk hänvisning. Förordningen kan då ändras utan att de kompletterande nationella bestämmelserna behöver justeras.

Begäran om tillgängliggörande av data för vidareutnyttjande

Med uttrycket begäran om tillgängliggörande av data för vidareutnyttjande avses enligt datalagen en begäran om att data ska göras tillgängliga för vidareutnyttjande i enlighet med den lagen. Begreppet används sedan i 1 kap. 8 § där lagens tillämpningsområde regleras, i rubriken till kapitel 5 samt i 5 kap. 1 och 3 §§.

Som redogjorts för ovan bör ett nytt uttryck införas för att definiera de kategorier av data som kapitel II dataförvaltningsförordningen avser och där förordningens regler ska gälla jämte vissa bestämmelser i datalagen. Uttrycket kommer att läggas till i flera paragrafer i lagen för att genomföra förordningen.

En del som ska genomföras i lagen är nationella regler för handläggning av ärenden om begäran av tillgängliggörande för vidareutnyttjande också för de särskilda kategorierna av skyddade data. Alla de tre paragrafer där uttrycket begäran om

tillgängliggörande av data för vidareutnyttjande behöver omfatta sådana begäran också för skyddade data enligt dataförvaltningsförordningen. Att införa ett nytt uttryck som avsåg sådana begäran bara för skyddade data är därför inte nödvändigt. Det skulle också riskera att bli svårtillgängligt och onödigt krångligt. I stället bör definitionen av begreppet utökas så att det är klart att det avser också begäran enligt dataförvaltningsförordningens kapitel II.

Begäran om tillgängliggörande av data för vidareutnyttjande bör därför justeras till att avse en begäran om att data eller skyddade data ska göras tillgängliga för vidareutnyttjande i enlighet med datalagen eller kapitel II dataförvaltningsförordningen.

4.4.3 Tillämpningsområde datalagen

Förslag: Vilka som ska tillämpa de bestämmelser i datalagen som blir tillämpliga för vidareutnyttjande av skyddade data ska regleras i lagen.

Skälen för förslaget: Öppna data-direktivet omfattade inte bara data som innehas av offentliga myndigheter utan också vissa data som innehas av vissa offentliga företag och vissa forskningsdata (jfr art. 1.1 öppna data-direktivet). Dataförvaltningsförordningens bestämmelser om vidareutnyttjande av skyddade data avser alltså inte bara vissa andra typer av data utan de träffar också färre tillhandahållare.

Bestämmelserna i kapitel II dataförvaltningsförordningen träffar offentliga myndigheter (artikel 3.1). Med det avses statliga, regionala eller lokala myndigheter och offentligrättsliga organ, eller sammanslutningar av en eller flera sådana myndigheter eller offentligrättsliga organ. Bestämmelserna ska inte tillämpas på

– offentliga företag,
– public service-bolag,
– kulturinstitutioner och
– utbildningsinstitutioner (artikel 3.2).

Med offentliga företag avses enligt definitionen i artikel 2.19 företag som offentliga myndigheter har ett direkt eller indirekt bestämmande inflytande över. Definitionen stämmer delvis överens

med motsvarande definition i öppna data-direktivet, men inte fullt ut, jämför artikel 1.1b öppna data-direktivet och 1 kap. 4 § datalagen.

Public service-bolag omfattas inte heller av öppna data-direktivet, se artikel 1.2 i öppna data-direktivet och 1 kap. 7 § 3 p. datalagen. Att notera är att det i de engelska versionerna av både öppna data-direktivet och dataförvaltningsförordningen står public service broadcasters. I de svenska översättningarna skiljer det sig åt mellan offentliga radio- och tv-företag i öppna data-direktivet och public service-bolag i dataförvaltningsförordningen. I datalagen har det definierats som radio- eller tv-företag vars sändningsverksamhet finansieras med public service-avgift enligt lagen (2018:1893) om finansiering av radio och tv i allmänhetens tjänst.

Kulturinstitutioner beskrivs som institutioner så som bibliotek, arkiv och museer samt orkestrar, operor, baletter och teatrar. I datalagen är kulturinstitutioner också undantagna, förutom när det gäller bibliotek, museer och arkiv. Dessa omfattas alltså av öppna data-direktivet och därmed datalagen, jämför med artikel 1.2 öppna data-direktivet och 1 kap. 7 § 1 p. datalagen. Tillämpningsområdet för dataförvaltningsförordningen är alltså mer begränsat än för öppna data-direktivet i denna del.

I öppna data-direktivet finns inte utbildningsinstitutioner med som begrepp. Däremot finns begreppet utbildningsanstalter med i både beaktandeskäl och artiklar i direktivet, jämför med skäl 31 och artikel 1.2 k öppna data-direktivet. Ett av fokusområdena i öppna data-direktivet är forskningsdata (artikel 1.1 c och 10), varför information som innehas av vissa utbildnings- och forskningsinstitutioner omfattas av direktivets tillämpningsområde om informationen i fråga avser sådan forskningsdata som omfattas av direktivet. Det gäller för utbildningsinstitutioner, men enbart universitet och högskolor eftersom utbildningsinstitutioner som bedriver högst gymnasieutbildning undantas, se artikel 1.2.k. Vidare gäller detta för de organisationer som bedriver eller finansierar forskning, inklusive de organisationer som inrättats för överföring av forskningsresultat, se artikel 1.2.l. Annan information från dessa typer av organ än forskningsdata ska dock undantas från tillämpningsområdet (SOU 2020:55 s. 175).

Tillämpningsområdet för dataförvältningsförordningen och datalagen skiljer sig alltså åt på det sätt att tillämpningsområdet för dataförvaltningsförordningen är snävare. Det behöver därför finnas

en ny paragraf i datalagen som anger vilka som ska tillämpa de bestämmelser i datalagen som kompletterar kapitel II i dataförvaltningsförordningen.

4.4.4 Datalagen ska omfatta data som skyddas av tredje parts immateriella rättigheter i vissa delar

Förslag: Undantaget i datalagens tillämpningsområde för tredje parts immateriella rättigheter ska inte gälla för de nya bestämmelser som avser skyddade data.

Skälen för förslaget: En av de kategorier av skyddade data som kapitel II i dataförvaltningsförordningen omfattar är enligt artikel 3.1 c data som är skyddade på grund av skydd av tredje parts immateriella rättigheter.

I datalagen anges under rubriken Undantag för vissa data i 1 kapitlet 10 § att datalagen inte omfattar data som

1. omfattas av en sådan ensamrätt som följer av patentlagen (1967:837), mönsterskyddslagen (1970:485), lagen (1992:1685) om skydd för kretsmönster för halvledarprodukter, växtförädlarrättslagen (1997:306), varumärkeslagen (2010:1877) eller lagen (2018:1653) om företagsnamn,
2. tredje man innehar rätt till enligt lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk,
3. utgörs av datorprogram, eller
4. utgörs av logotyper, heraldiska vapen eller insignier.

Data som är skyddade på grund av tredje parts immateriella rättigheter i den bemärkelse som avses i artikel 3.1 c dataförvaltningsförordningen är alltså undantagna från datalagens tillämpningsområde genom 1 kap. 10 §.

För att datalagen ska kunna tillämpas för vidareutnyttjande av skyddade data enligt dataförvaltningsförordningen behöver lagens tillämpningsområde utökas. Avsikten är dock inte att ge befintligt regelverk i datalagen ett bredare tillämpningsområde. Utökningen bör därför bara gälla vid tillämpning i enlighet med dataförvaltningsförordningen och för skyddade data.

4.4.5 Begränsningar i dataförvaltningsförordningen och datalagen

Kapitel II dataförvaltningsförordningen avser tillgängliggörande av data för vidareutnyttjande. Med vidareutnyttjande avses enligt definitionen i artikel 2.2 fysiska eller juridiska personers användning av data som innehas av offentliga myndigheter för andra ändamål än de ursprungliga ändamålen inom den offentliga verksamheten. Utbyte av data mellan offentliga myndigheter som sker i samband med deras offentliga verksamhet omfattas däremot inte av definitionen. Närmare om definitionen av vidareutnyttjande i avsnitt 4.4.2.

Kapitlet ska vidare inte tillämpas på data som innehas av offentliga myndigheter och som är skyddade av skäl som rör allmän säkerhet, försvar eller nationell säkerhet, artikel 3.2 d. Detta innebär att data som är skyddade av flera skäl varav ett är ett sådant skäl som är undantaget inte träffas av bestämmelserna i förordningen.

Tillgängliggörande av data enligt datalagen ska bara ske i den utsträckning som krav på informationssäkerhet och skydd av personuppgifter kan upprätthållas och under förutsättning att det inte innebär risker för Sveriges säkerhet, 2 kap. 1 §. Datalagen har därför en begränsning som motsvarar den som följer av dataförvaltningsförordningens artikel 3.2 d. Någon justering av tillämpningsområdet i datalagen krävs därför inte.

4.4.6 Exklusiva avtal i datalagen

Förslag: Datalagens bestämmelser om exklusiv rätt att vidareutnyttja data ska inte tillämpas på skyddade data.

För skyddade data gäller i stället dataförvaltningsförordningens bestämmelser om exklusiva avtal.

Skälen för förslaget: Både i datalagen och dataförvaltningsförordningen finns begränsningar avseende exklusiva avtal om vidareutnyttjande av data. Reglerna är på flera punkter snarlika. Utgångspunkten är att exklusiva avtal inte är tillåtna, utom om det är nödvändigt för att en tjänst av allmänt intresse ska kunna tillhandahållas, jfr artikel 4.1 och 2 samt 3 kap. 1 § första stycket datalagen.

Vid tillhandahållande av skyddade data för vidareutnyttjande ska myndigheter tillämpa reglerna om förbud mot exklusiva avtal i dataförvaltningsförordningen, inte reglerna i datalagen. En hänvisning till reglerna om exklusiva avtal i dataförvaltningsförordningen bör därför för tydlighetens skull föras in i datalagen.

4.5 Behandling av begäran om vidareutnyttjande

Genom öppna data-direktivet och datalagen har en ram för tillgängliggörande av data från offentlig förvaltning för vidareutnyttjande inrättats. Regelverket i kapitel II dataförvaltningsförordningen är en påbyggnad på detta befintliga regelverk. I förarbetena till datalagen finns noggranna överväganden avseende bl.a. relationen mellan befintliga regler om utlämnande av allmän handling i TF och serviceskyldigheten i förvaltningslagen, om vilka begrepp som ska användas och hur ärenden om begäran om tillgång till data för vidareutnyttjande ska hanteras. I allt väsentligt kan det befintliga regelverket och de bedömningar som gjorts vid införandet av datalagen appliceras också på kapitel II dataförvaltningsförordningen. Det finns dock vissa skillnader och vissa delar som behöver regleras särskilt.

Dataförvaltningsförordningens regler om tillgängliggörande av skyddade data innebär inte att det föreligger någon skyldighet för myndigheter att tillgängliggöra sådana data för vidareutnyttjande. I de fall myndigheten gör sådana data tillgängliga för vidareutnyttjande, antingen på grund av en skyldighet i annan lag eller frivilligt, ska dock förordningens kapitel II tillämpas.

4.5.1 Tillgång till information påverkas inte av dataförvaltningsförordningen

Bestämmelserna i kapitel II dataförvaltningsförordningen ger inte en rätt att få tillgång till och vidareutnyttja skyddade data, utan de syftar till att ge en uppsättning harmoniserade grundläggande förutsättningar under vilka vidareutnyttjande av sådana data kan tillåtas. Rätten att vidareutnyttja information och begränsningar i denna följer av svensk rätt. Dataförvaltningsförordningen påverkar inte dessa regler, jfr. artikel 1.2.

Dataförvaltningsförordningens regler om tillgängliggörande av data för vidareutnyttjande ger inte någon rätt till tillgång till information, utan regelverket avser frågan om *hur* information kan och ska tillhandahållas, dvs. frågor om avgifter och andra villkor för tillgängliggörande. I de fall skyddade data görs tillgängliga för vidareutnyttjande ska kapitel II i förordningen och de kompletterande bestämmelser som föreslås i denna promemoria tillämpas.

Innan frågan om tillgängliggörande av skyddade data för vidareutnyttjande kan behandlas måste därför först frågan om tillgång till informationen hanteras. Myndigheten ska i den delen bedöma tillgången till informationen i enlighet med regler i TF, OSL och andra författningar som reglerar tillgången till den aktuella informationen. Först om det efter en sådan prövning finns utrymme att ge tillgång till informationen kan frågan om att tillgängliggöra skyddade data aktualiseras. I annat fall faller frågan om tillgängliggörande för vidareutnyttjande. Förhållandet mellan frågan om begäran om information och begäran om tillgängliggörande av data för vidareutnyttjande ska förstås på samma sätt som för öppna data-direktivet, se SOU 2020:55 avsnitt 8.4 och 8.5 samt figur 1 och 2.

Syftet med bestämmelserna sammanfaller delvis med 2 kap. TF, bl.a. vad gäller att öka insynen för allmänheten i den offentliga förvaltningen. Dataförvaltningsförordningen har dock, liksom öppna data-direktivet som ligger till grund för datalagen, också andra mål som är närmare knutna till de ekonomiska värden som information från myndigheter innehåller, exempelvis i form av ökad innovation av produkter och tjänster.

4.5.2 Tillgängliggörande av data på olika sätt

Information som offentliga myndigheter innehar kan lämna myndigheterna och bli tillgängliga för vidareutnyttjande på två olika sätt. Information kan dels bli tillgänglig för vidareutnyttjande genom att myndigheten på ett proaktivt sätt tillgängliggör den digitalt, i första hand online. Information kan också göras tillgänglig för vidareutnyttjande efter en förfrågan.

Datalagens bestämmelser om vidareutnyttjande av information från offentliga myndigheter bygger i huvudsak på tryckfrihetsförordningens bestämmelser om handlingsoffentlighet.

Tillgängliggörande av öppna data enligt datalagen kan ske både på myndighetens egna initiativ, eller som ett led i att fullgöra en skyldighet, ofta efter begäran. Ett sådant tillgängliggörande kan bli aktuellt också för information som lämnas ut enligt 2 kap. TF (SOU 2020:55, s. 161 och 162). Med tillgängliggöra avses i datalagen att en myndighet eller ett offentligt företag ger tillgång till information, oavsett om det görs frivilligt eller på grund av en skyldighet i annan författning. Ett tillgängliggörande förutsätter således inte att det sker på viss rättlig grund.

För att de kategorier av skyddade data som kapitel II dataförvaltningsförordningen avser ska kunna göras tillgängliga för vidareutnyttjande behöver den offentliga myndigheten vidta vissa skyddsåtgärder och i normalfallet ställa upp vissa villkor för vidareutnyttjandet. Sådana skyddade data kan därför inte tillhandahållas utan en begäran.

Utlämnande efter begäran

Utmärkande för en begäran om utlämnande är att den är riktad till en myndighet och att det förväntas att myndigheten reagerar på något individualiserat sätt. Av den anledningen är nedladdning av information från en webbplats inte en begäran om att information ska göras tillgänglig.

Om den information som efterfrågas i ett enskilt fall redan finns tillgänglig på annat sätt, exempelvis genom att den har publicerats på myndighetens webbplats ska frågan om tillgång till informationen hanteras som en begäran om utlämnande och därefter frågan om tillgång för vidareutnyttjande som en begäran om tillgängliggörande för vidareutnyttjande.

En begäran om tillgång till information hanteras i svensk rätt i första hand genom bestämmelser i 2 kap. TF och 6 kap. OSL. Om det inte finns några hinder i form av sekretess kommer en sådan begäran att resultera i ett utlämnande, som ett led i att myndigheten fullgör en författningsreglerad skyldighet. I normalfallet är det fråga om ett utlämnande av en allmän handling med stöd av 2 kap. TF eller en uppgift enligt 6 kap. OSL.

Tillgängliggörande som en serviceåtgärd efter en begäran

Det kan finnas tillfällen då den information som efterfrågas inte kan lämnas ut enligt 2 kap. TF eller 6 kap. OSL, men myndigheten ändå – som en serviceåtgärd – vill göra den tillgänglig. Ett exempel kan vara att det skulle kräva mer än rutinbetonade åtgärder för att sammanställa en potentiell handling. Ett annat tänkbart scenario är att sökanden uttryckligen vill att myndigheten tillhandahåller informationen inom ramen för sin serviceskyldighet (jfr JO:s beslut, 1996/97, s. 484). Någon skyldighet för myndigheterna att göra informationen tillgänglig saknas vid dessa förhållanden.

Vid ett utlämnande med stöd av offentlighetsprincipen finns, på grund av utskriftsundantaget i 2 kap. 16 § TF, inte någon skyldighet att tillhandahålla informationen i ett digitalt format. Om den ändå tillhandahålls digitalt sker det som en serviceåtgärd. Sedan datalagen trädde i kraft är myndigheternas möjlighet att, vid en begäran om vidareutnyttjande, fritt avgöra om information ska tillhandahållas i ett visst format begränsat i de fall begäran avser sådana data som lagen omfattar (jfr prop. 2021/22:225 s. 39 och SOU 2020:55 s. 132).

4.5.3 Vidareutnyttjande av skyddade data förutsätter att informationen kan lämnas ut

Förslag: Datalagen ska tillämpas när någon som har rätt att få tillgång till skyddade data enligt någon annan lag eller förordning begär att dessa data ska tillgängliggöras för vidareutnyttjande. Lagen ska också tillämpas när en myndighet på eget initiativ tillgängliggör data som omfattas av lagen i syfte att de ska kunna vidareutnyttjas.

Skälen för förslaget: Innan frågan om tillgängliggörande av skyddade data för vidareutnyttjande kan behandlas måste först frågan om tillgång till den aktuella informationen hanteras. Myndigheten ska i den delen bedöma tillgången till informationen i enlighet med regler i TF, OSL och andra författningar som reglerar tillgången till den aktuella informationen. Först om det efter en sådan prövning finns utrymme att ge tillgång till informationen kan frågan om att tillgängliggöra skyddade data aktualiseras. I annat fall faller frågan om tillgängliggörande för vidareutnyttjande.

Avgränsningen i datalagen avseende vilket informationsinnehåll som faller inom lagens tillämpningsområde följer av öppna data-direktivet, och den avser information. Skälen för detta är flera, bl.a. att handling enligt TF utgår från att innehållet har fixerats vid någon form av medium samt att man velat undvika att det svenska handlingsbegreppet skulle kunna bli föremål för tolkning av EU-domstolen. Vidare slipper man genom frikopplingen från handlings-begreppet de osäkerhetsmoment som kan finnas kring hur digital information förhåller sig till handlingsbegreppet (SOU 2020:55 s. 122 och 123). Dataförvaltningsförordningen avser liksom öppna data-direktivet information i en bredare bemärkelse.

Information som myndigheter gör tillgänglig får som huvudregel vidareutnyttjas fritt utan restriktioner. Denna rättighet är grundlags-skyddad avseende sådan information som har lämnats ut efter en begäran om allmän handling enligt 2 kap. TF, men ett fritt vidareutnyttjande gäller även enligt en svensk allmän princip för information som har tillgängliggjorts på frivillig väg. Det är alltså inte dataförvaltningsförordningen eller datalagen som ger rätt att vidareutnyttja information (SOU 2020:55 s. 159 och 160).

Det kan emellertid finnas rättsliga begränsningar i möjligheten att vidareutnyttja information. Exempelvis kan det vara fråga om ett förbehåll enligt 10 kap. 14 § OSL som begränsar den enskildes rätt att sprida informationen vidare eller att ett vidareutnyttjande skulle strida mot finalitetsprincipen i dataskyddslagstiftningen. Sådana begränsningar följer direkt av författning och ska inte sammanblandas med det förhållandet att en myndighet ställer upp villkor för ett vidareutnyttjande med stöd av en författning, t.ex. lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk (upphovsrättslagen, URL).

Begränsningar i rätten att vidareutnyttja information som omfattas av de kategorier av skyddade data som kapitel II dataförvaltningsförordningen avser, liksom begränsningar av rätten att ställa upp villkor för vidareutnyttjande, följer alltså inte av dataförvaltningsförordningen utan av nationell reglering, t.ex. offentlighets- och sekretesslagen (2009:400), upphovsrättslagen, dataskyddsförordningen eller en registerförfattning (SOU 2020:55 s. 160). Dataförvaltningsförordningen innehåller ramar för hur villkor kan utformas om myndigheten ska tillåta ett vidareutnyttjande av sådana skyddade data. Myndigheten är inte

enligt dataförvaltningsförordningen skyldig att tillhandahålla data för vidareutnyttjande. Finns det inte i annan lagstiftning krav på att vissa skyddade data ska göras tillgängligt för vidareutnyttjande så är det upp till myndigheten att avgöra om data kan göras tillgängligt för vidareutnyttjande med hjälp av de villkor som finns i artikel 5.

Ett av syftena med dataförvaltningsförordningens kapitel II är, liksom det var med öppna data-direktivet, att säkerställa att de villkor som ställs upp ska vara objektiva, proportionella och icke-diskriminerande, att avgifter följer vissa principer samt att information tillhandahålls i format som underlättar ett vidareutnyttjande. Förordningens krav i dessa delar ska tillämpas inte bara på sådan information som utgör skyddade data enligt artikel 3.1 som myndigheter tillgängliggör på eget initiativ, utan även på sådan information som har lämnats ut med stöd av 2 kap. TF eller som tillgängliggörs på grund av en skyldighet som anges i en annan författning när det sker på ett sätt som innebär ett vidareutnyttjande enligt artikel 2.2 dataförvaltningsförordningen.

4.5.4 Handläggning av ärenden om vidareutnyttjande

Förslag: En begäran om vidareutnyttjande av skyddade data ska hanteras på samma sätt som begäran om vidareutnyttjande enligt datalagen.

Ärenden om tillgängliggörande av skyddade data ska avgöras inom åtta veckor från det att begäran mottogs. Ärenden med exceptionellt omfattande eller komplicerade begäran får förlängas med som mest fyra veckor.

Skälen för förslag: I artikel 9.1 dataförvaltningsförordningen anges att ett ärende med en begäran om vidareutnyttjande av skyddade data ska avgöras inom två månader från dagen för mottagen begäran, såvida inte kortare tidsfrister fastställs i nationell rätt.

I datalagen 5 kap. 1 § anges att ett ärende till följd av en begäran om tillgängliggörande av data för vidareutnyttjande ska avgöras inom fyra veckor. Tiden för att hantera ett ärende i datalagen är alltså ungefär hälften så lång som den maximalt får vara för ärenden om skyddade data enligt dataförvaltningsförordningen.

En begäran om vidareutnyttjande av skyddade data är till sin natur mer komplex än en begäran om vidareutnyttjande av andra data. Detta eftersom skyddsåtgärder alltid måste vidtas och villkor för vidareutnyttjandet ställas upp. Det vore därför inte lämpligt att ställa upp allt för korta tider för hantering av ärenden, utan dessa bör få ta längre tid att handlägga. Den svenska regleringen av handläggningstiden bör därför i princip motsvara den längsta tiden i förordningen. I datalagen är dock handläggningstiden beskriven i veckor, inte månader. För att inte i samma lagrum ha olika tidsmått bör därför tiden för hantering av ärenden som avser skyddade data sättas till åtta veckor.

Exceptionellt omfattande eller komplicerade begäran om vidareutnyttjande tar längre tid att handlägga. Handläggningen av ett sådant ärende får därför enligt dataförvaltningsförordningen artikel 9.1 andra stycket förlängas med högst 30 dagar. I datalagen är tidsfristerna uttryckta i veckor och inte i dagar och förlängning tillåten med som mest fyra veckor. Denna tid motsvarar i princip de 30 dagar som dataförvaltningsförordningen tillåter. För att inte i onödan komplicera regleringen av tidsfrister bör samma tid gälla för förlängning av handläggningstiden för ärenden om vidareutnyttjande av skyddade data enligt dataförvaltningsförordningen som för data i andra fall.

4.5.5 Anmälan av överträdelser som vidareutnyttjare gör sig skyldig till vid tredjelandsöverföringar

Förslag: En myndighet som överfört konfidentiella data till en vidareutnyttjare som avser att överföra dessa till tredjeland ska anmäla överträdelser av förordningens villkor för tredjelandsöverföringar som vidareutnyttjaren gör sig skyldig till och som myndigheten får kännedom om till den behöriga myndigheten för dataförmedlingstjänster.

Skälen för förslaget: Enligt artikel 5.10 får en myndighet överföra konfidentiella data som inte är personuppgifter eller immaterialrättsligt skyddat material till en vidareutnyttjare som avser att föra ut dessa till tredje land bara under vissa förutsättningar.

För data som innehåller personuppgifter gäller de dataskyddsrättsliga reglerna om tredjelandsöverföringar som framför allt återfinns i kapitel V dataskyddsförordningen. För data som innehåller immaterialrättsligt skyddat material ska i stället immaterialrättsliga regler gällande tredjelandsöverföringar tillämpas.

Om en myndighet medger tillgång till konfidentiella data för vidareutnyttjande till en vidareutnyttjare som avser att överföra uppgifterna till tredje land ska myndigheten enligt artikel 5. 10 ställa upp villkor där det framgår att vidareutnyttjaren åtar sig vissa skyldigheter.

Kommissionen får anta ett antal olika typer av genomförandeakter gällande vidareutnyttjande av sådana data i tredje land. Dels får kommissionen anta genomförandeakter med standardavtalsklausuler för fullgörande av de aktuella villkoren, artikel 5.11. Kommissionen får också anta genomförandeakter i vilka det intygas att ett visst tredjelands rättsliga, tillsynsmässiga och verkställighetsmässiga arrangemang säkerställer det skydd som krävs, tillämpas och verkställs på ett effektivt sätt och omfattar effektiva rättsmedel, artikel 5.12. Det finns vidare i artikel 5.13 en hänvisning till att det i andra unionslagstiftningsakter kan finnas begränsningar i hur data kan överföras till tredjeland, t.ex. för att inte äventyra unionens offentligpolitiska mål om säkerhet och folkhälsa. Om en sådan akt antas ska kommissionen anta delegerade akter för att fastställa särskilda villkor som ska tillämpas i de fallen.

Den som beviljas rätten att vidareutnyttja icke-personuppgifter får enligt artikel 5.14 bara överföra dessa till tredjeland om kraven i artikel 5.10, 5.12 och 5.13 uppfylls. Om en vidareutnyttjare bryter mot artikel 5.14 ska den enligt artikel 34 kunna träffas av en sanktion. Sanktionen bör beslutas av den behöriga myndigheten för dataförmedlingstjänster, se avsnitt 5.8.8.

För att den behöriga myndigheten ska kunna besluta om sanktioner behöver den få kännedom om överträdelser av artikel 5.14. Den myndighet som lämnat ut data är den som kan ha kännedom om sådana överträdelser. Myndigheten bör därför ha skyldighet att anmäla sådana överträdelser till den behöriga myndigheten.

En anmälan bör innehålla de uppgifter om överträdelsen som tillsynsmyndigheten behöver för att kunna besluta om sanktioner. Uppgifter om vidareutnyttjaren ska framgå av anmälan. Vidare bör

den innefatta en beskrivning av de data som lämnats ut, vilka villkor som ställts upp för vidareutnyttjandet och överföringen till tredje land, en redogörelse för den eller de överträdelser som vidareutnyttjaren gjort sig skyldig till samt vilka effekter överträdelsen gett. Uppgifter om hur överträdelsen upptäcktes och hur allvarlig den är, vilken omfattning den har och under hur lång tid överträdelsen pågått ska finnas med i anmälan då det är aktuellt. Om myndigheten har kännedom om tidigare överträdelser som viderutnyttjaren gjort sig skyldig till ska det ingå i anmälan. Likaså uppgifter om ekonomiska vinster eller förluster som undvikits som överträdelsen inneburit för vidareutnyttjaren. Myndigheten ska därutöver inkludera andra försvårande eller förmildrande omständigheter som kan ha betydelse för bedömningen av en sanktionsavgift.

4.5.6 Bistå vidareutnyttjare

Enligt artikel 5.6 ska offentliga myndigheter i vissa fall bistå den som begär tillgång till skyddade data. Av artikeln framgår att om myndigheten inte kan tillåta vidareutnyttjande, t.ex. på grund av att skyddet av personuppgifter eller en affärshemlighet inte kan garanteras, kan vidareutnyttjaren försöka söka samtycke eller tillstånd direkt från de berörda personerna eller enheterna. Det ska då enligt artikeln ske med bistånd från myndigheten. Myndigheten ska göra sitt yttersta för att bistå vidareutnyttjaren, men bara i den utsträckning som det är tillåtet i enlighet med unionsrätt och nationell rätt. Det finns både i nationell rätt och unionsrätten vissa begränsningar för myndigheter att bistå med detta.

Serviceskyldigheten i förvaltningslagen

I vilken utsträckning myndigheter i Sverige kan bistå den som begär att få tillgång till data för vidareutnyttjande styrs av myndighetens uppgift så som den framgår i myndighetens instruktion och regleringsbrev och annan verksamhetsreglering, t.ex. register-författningar. Bestämmelser om service i samband med tillhandahållande av allmänna handlingar finns i 2 kap. 15 § TF samt i 4 kap. och 6 kap. 4 och 6 §§ OSL. Därutöver ska myndigheterna i

handläggning av ärenden följa förvaltningslagen (2017:900), nedan FL. Enligt 6 § FL har myndigheterna en viss serviceskyldighet som innebär att myndigheterna ska lämna den enskilde sådan hjälp att han eller hon kan ta till vara sina intressen. Hjälpen ska ges i den utsträckning som det är lämpligt med hänsyn till frågans art, den enskildes behov av hjälp och myndighetens verksamhet. Hjälp ska också ges utan onödigt dröjsmål.

Med serviceskyldigheten avses att den enskilde inte ska behöva ha någon särskild sakkunskap innan den kontaktar myndigheten. Det förhållande att en enskild inte är nöjd med svaret från en myndighet innebär inte att serviceskyldigheten åsidosatts (JO beslut 2009-03-27, dnr 4716-2008). Den hjälp som ska lämnas är exempelvis hur man fyller i blanketter eller gör en ansökan, om en framställan är ofullständig eller oklar samt att hänvisa till rätt myndighet om någon av misstag lämnat in till fel. Rätten att få hjälp är inte begränsad till viss form. Detta innebär inte att myndigheternas serviceskyldighet därmed ska anses omfatta exempelvis rådgivning av sådant slag som privata ombud med juridisk specialkompetens inom ett visst område tillhandahåller åt enskilda individer och företag. Serviceskyldigheten ska inte heller uppfattas som ett krav på myndigheterna att alltid se till att enskilda kan undvika tidsödande arbete. Utgångspunkten är att servicenivån måste anpassas till förutsättningarna i det enskilda fallet. Att närmare precisera hur omfattande hjälp en myndighet bör ge enskilda i olika typsituationer har inte ansetts lämpligt eller praktiskt möjligt. Inte heller att ange vilka åtgärder som myndigheten bör vidta för att kunna svara på en viss fråga (prop. 2016/17:180 s. 66 och 67).

Den typ av bistånd som beskrivs i artikel 5.6 kan i många fall vara sådan att den faller utanför myndigheternas skyldigheter enligt instruktioner, verksamhetsreglering och serviceskyldigheten enligt förvaltningslagen. Det är viktigt att understryka att regleringen i artikel 5.6 inte ger myndigheterna en skyldighet att bistå vidareutnyttjare annat än i den mån det är tillåtet i enlighet med unionsrätt och nationell rätt. Serviceskyldigheten i FL innefattar normalt inte den typ av bistånd som avses i artikel 5.6.

Samtycke

Om den data som begäran avser innehåller personuppgifter och biståndet avser inhämtande av samtycke från de registrerade finns också dataskyddsrättsliga aspekter som behöver beaktas.

En av de rättsliga grunderna i dataskyddsförordningen är samtycke, artikel 6.1 a. Ett sådant samtycke ska vara frivilligt och det ska kunna återkallas när som helst. För att ett samtycke ska kunna vara frivilligt krävs det att maktförhållandet mellan den registrerade och den personuppgiftsansvariga är jämlikt. Av skäl 42 till dataskyddsförordningen framgår att ett samtycke inte bör betraktas som frivilligt om den registrerade inte har någon genuin eller fri valmöjlighet eller inte utan problem kan vägra eller ta tillbaka sitt samtycke. Av skäl 43 till dataskyddsförordningen framgår bl.a. följande:

> För att säkerställa att samtycket lämnas frivilligt bör det inte utgöra giltig rättslig grund för behandling av personuppgifter i ett särskilt fall där det råder betydande ojämlikhet mellan den registrerade och den personuppgiftsansvarige, särskilt om den personuppgiftsansvarige är en offentlig myndighet och det därför är osannolikt att samtycket har lämnats frivilligt när det gäller alla förhållanden som denna särskilda situation omfattar.

Såsom framgår av skäl 43 kan det råda sådan betydande ojämlikhet mellan den registrerade och en myndighet som personuppgiftsansvarig att det är osannolikt att samtycke kan lämnas frivilligt (Dataskyddsförordningen (GDPR) m.m. En kommentar Öman, Sören, kommentar till art 4.11).

Denna problematik kvarstår om samtycke samlas in av myndigheten för annans räkning. Detta oavsett om ett sådant samtycke skulle tas in vid insamlandet av uppgifterna eller i efterhand. Utöver att behandling som sådan behöver uppfylla alla krav i dataskyddsförordningen, inklusive att det ska finnas en rättslig grund för myndigheten, så finns det risk att det samtycke som tas in inte är frivilligt och därmed inte kan ses som ett giltigt samtycke ur ett dataskyddsrättsligt perspektiv och därmed inte en giltig rättslig grund.

4.5.7 Incidenter

Som beskrivits i avsnitt 4.3.2 ska personuppgifter som utgångspunkt anonymiseras innan de lämnas ut för vidareutnyttjande, eller annars lämnas ut i en säker behandlingsmiljö. Detta framgår av skäl 15. Det ska enligt artikel 5.5 sedan vara förbjudet för vidareutnyttjare att återidentifiera de registrerade som uppgifterna gäller, och vidareutnyttjarna ska vidta tekniska och operativa åtgärder för att förhindra återidentifiering. Skulle det ändå ske ska de underrätta den offentliga myndigheten om alla uppgiftsincidenter som leder till att berörda registrerade återidentifieras.

En sådan incident skulle också kunna vara en personuppgiftsincident enligt dataskyddsförordningen. En personuppgiftsincident är en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats. En personuppgiftsincident ska i vissa fall anmälas till Integritetsskyddsmyndigheten som är tillsynsmyndighet inom 72 timmar efter att den personuppgiftsansvariga fått vetskap om den, artikel 33 dataskyddsförordningen. Den registrerade ska också informeras om personuppgiftsincidenten i vissa fall, artikel 34 dataskyddsförordningen.

En uppgiftsincident enligt dataförvaltningsförordningen skulle också kunna vara en incident som berör säkerhet för information i annan reglering. Det finns t.ex. skyldigheter att rapportera vissa incidenter till Myndigheten för samhällsskydd och beredskap (MSB) i enlighet med föreskrifter från MSB.[4]

4.5.8 Avgifter för vidareutnyttjare

Offentliga myndigheter som tillåter vidareutnyttjande av data får enligt dataförvaltningsförordningen ta ut en avgift för det enligt artikel 6.1. Enligt avgiftsförordningen (1992:191) får en myndighet ta ut avgifter för varor och tjänster som den tillhandahåller bara om det framgår av en lag eller förordning. Rätten att ta ut en avgift för

[4] Genom det s.k. NIS2-direktivet utökas tillämpningsområdet för det tidigare NIS-direktivet som ställer krav på åtgärder för en hög gemensam cybersäkerhetsnivå i unionen. Genom implementering av NIS2-direktivet kan ytterligare nya incidenter och rapporteringsskyldigheter tillkomma.

tillgängliggörande av skyddade data för vidareutnyttjande följer av dataförvaltningsförordningen vilken är direkt tillämplig i Sverige och därmed motsvarar lag. Kriterier och metoden för beräkning av avgifter ska fastställas av medlemsstaten och offentliggöras, artikel 6.6.

När myndigheter tar ut avgifter ska de enligt artikel 6.4 vidta åtgärder för att ge incitament till vidareutnyttjande av skyddade data för icke-kommersiella ändamål. Vidare ska myndigheterna ge incitament till vidareutnyttjande av små och medelstora företag och uppstartsföretag, det civila samhället och utbildningsanstalter. Incitament till vidareutnyttjande kan ske genom att tillgängliggörande sker med nedsatt avgift eller avgiftsfritt.

Offentliga myndigheter som tar ut avgifter måste säkerställa att dessa kan betalas online med hjälp av allmänt tillgängliga gränsöverskridande betaltjänster, artikel 6.3. Liknande krav ställs i andra EU-rättsakter, t.ex. SDG-förordningen artikel 13.2 e och 16 c. Trots detta har ännu inte alla myndigheter tillgång till sådana betaltjänster.

Att myndigheter får ta ut en avgift för tillgängliggörande av skyddade data är alltså redan reglerat i dataförvaltningsförordningen. De frågor som behöver hanteras i svensk rätt är dels hur sådana avgifter ska se ut och beräknas och om det ska finnas nedsatta avgifter eller avgiftsfri tillgång för att främja visst vidareutnyttjande.

Avgifter i datalagen

I öppna data-direktivet infördes en huvudregel om att vidareutnyttjande av data ska vara avgiftsfritt (artikel 6.1). Syftet var att motverka att avgiftsuttag blir ett betydande hinder för vidareutnyttjande av data, i synnerhet för nystartade eller små och medelstora företag (jfr skäl 36). Huvudregeln kompletterades dock av flera undantag.

Avgifter regleras i datalagen i kapitel 4. Där framgår vissa kriterier för beräkning av avgifter för olika typer av data i 2–6 §§. Av 4 kap. 2 § framgår att en avgift får tas ut enligt marginalkostnadsprincipen och därmed inte får sättas till ett högre belopp än vad som behövs för att täcka kostnaderna för att reproducera, tillgängliggöra och sprida data och för att avidentifiera personuppgifter. Också

dataförvaltningsförordningens reglering av avgifter följer en slags marginalkostnadsprincip.

Kostnader för att avidentifiera eller anonymisera personuppgifter får räknas in i marginalkostnaden i den utsträckning en sådan åtgärd inte enbart syftar till att maskera sekretessbelagda uppgifter. Med avidentifiering avses i detta sammanhang samtliga metoder och tekniker för att avidentifiera eller anonymisera personuppgifter (prop. 2021/22:225 s. 90).

Forskningsdata ska tillgängliggöras avgiftsfritt, 3 §. Värdefulla datamängder ska också som huvudregel tillgängliggöras kostnadsfritt, utom i vissa undantagsfall, 4–6 §§. I 7 § regleras att myndigheter och offentliga företag ska kunna ange grunder för hur avgifter beräknats och att information om avgifter i vissa fall ska publiceras. Vidare ges Digg föreskriftsrätt över en förteckning av vilka myndigheter som är skyldiga att ta ut en avgift vid tillgängliggörande av data för vidareutnyttjande, 9 § jämte 6 a § andra stycket förordning (2018:1486) med instruktion för Myndigheten för digital förvaltning.

4.5.9 Avgiftens storlek

Förslag: En avgift för tillgängliggörande av skyddade data ska kunna härledas från kostnader för att genomföra förfarandet för begäran om vidareutnyttjande. De kostnader som ska kunna ligga till grund för beräkningen av avgift ska vara begränsat till kostnader för

- reproduktion, tillhandahållande och spridning av data,
- klarering av upphovsrätt,
- anonymisering eller andra former av framställning av personuppgifter och affärshemligheter,
- underhåll av säkra behandlingsmiljöer,
- förvärvande av rättigheter från tredje part och
- visst bistånd till vidareutnyttjare.

Skälen för förslaget: Kriterier och metoden för beräkning av avgifter ska fastställas av medlemsstaten och offentliggöras, artikel

6.6. Avgiftsprinciperna som fastställs ska tillämpas när information görs tillgänglig enligt dataförvaltningsförordningens kapitel II, oavsett på vilken grund det görs (jfr SOU 2020:55 s. 285).

Avgifter ska vara transparenta, icke-diskriminerande, proportionella och objektivt motiverade och de får inte begränsa konkurrensen, artikel 6.2. Avgifterna ska enligt artikel 6.5 härledas från kostnaderna för att genomföra förfarandet för begäran om vidareutnyttjande, och de ska vara begränsade till nödvändiga kostnader i samband med

– reproduktion, tillhandahållande och spridning av data,
– klarering av upphovsrätt,
– anonymisering eller andra former av framställning av personuppgifter och affärshemligheter,
– underhåll av den säkra behandlingsmiljön,
– förvärvande av rätten att tillåta vidareutnyttjande, och
– bistånd till vidareutnyttjare som begär de registrerades samtycke och tillstånd från datainnehavare vars rättigheter och intressen kan påverkas av vidareutnyttjandet.

Samtliga dessa kostnader avser sådana nödvändiga åtgärder som offentliga myndigheter kan behöva vidta för att kunna göra skyddade data tillgängliga för vidareutnyttjande. Vad varje punkt omfattar och i vilken mån den ska läggas till grund för en avgift bedöms i separata avsnitt nedan.

Den som vill ta del av en allmän handling har även enligt 2 kap. 16 § TF rätt att mot avgift få en avskrift eller kopia av handlingen. Den avgift som avses regleras för statliga myndigheter i avgiftsförordningen. Avgiftsförordningen innehåller fastställda avgifter som ska tillämpas när allmänna handlingar tillhandahålls i pappersform. Motsvarande reglering saknas när informationen tillhandahålls i elektronisk form och myndigheter tar inom ramen för det skönsmässiga utrymme som det generella bemyndigandet i 4 § 8 avgiftsförordningen medger ut vitt skilda avgifter för samma eller samma typ av digital information (SOU 2020:82 s. 12). Kommunerna fastställer motsvarande avgifter i sin verksamhet utifrån självkostnadsprincipen. Avgiften får inte täcka kostnader för framtagande och återställande av handlingen, eftersom en allmän handling enligt 2 kap. 15 § TF ska tillhandahållas på stället kostnadsfritt. Det är därför viktigt att kriterierna och metoden också

för beräkning av avgifter för att tillgängliggöra skyddade data för vidareutnyttjande just avser kostnader förknippade med detta, inte för framtagande av själva handlingen.

Liksom andra delar som rör tillgängliggörande av skyddade data bör kompletterande reglering införas i datalagen.

Reproduktion, tillhandahållande och spridning

Kostnader för reproduktion, tillhandahållande och spridning av data är ett begrepp som återfinns både i dataförvaltningsförordningen och öppna data-direktivet och som finns infört i datalagen 4 kap. 2 § och den bör omfatta också avgifter för skyddade data.

Med detta avses att även kostnader för att formatera eller verifiera data, liksom kostnader för material och programmering får räknas in i marginalkostnaden. Avgiftsunderlaget får även avse kostnader för utveckling och drift av en tjänst som möjliggör att data tillgängliggörs, exempelvis via internet. Kostnader för spridning kan också omfatta användarstöd. Däremot får kostnader för att samla in data eller förvalta system där data förvaras inte räknas in i avgiftsunderlaget (prop. 2021/22:225 s. 90).

Riksdagen har beslutat om en enhetlig princip för prissättning av information som myndigheter tillhandahåller i elektronisk form (prop. 1997/98:136, bet. 1997/98:KU 31, rskr. 1997/98:294). Principen innebär att avgifter som tas ut med stöd av 4 § första stycket 8 avgiftsförordningen inte får överstiga kostnaden för att ”ta fram och distribuera” informationen. I detta ingår samtliga kostnader för att hantera beställningen, bl.a. materialkostnader, kostnader för programmering, bearbetning och distribution samt kostnader som är kopplade till debitering. Öppna data-utredningen ansåg, i likhet med Ekonomistyrningsverket (ESV), att denna prissättningsprincip ska gälla som utgångpunkt (SOU 2020:55 s. 288 och 289). Detta bör gälla också vid fastställandet av avgiftsprinciper för dataförvaltningsförordningens kapitel II.

När det gäller uttrycket ”ta fram” kan det exempelvis vara fråga om att göra sådana rutinbetonade sammanställningar som en myndighet är skyldig att göra vid en begäran om utlämnande av allmän handling. Begreppet motsvaras närmast av kostnader för reproduktion.

Begreppen ”tillhandahålla och sprida” enligt artikel 6.5 a motsvaras av ”distribuera” i datalagen och samma bedömning bör göras för dataförvaltningsförordningen (SOU 2020:55 s. 289). Det kan innefatta åtgärder så exempelvis att formatera informationen.

En särskild fråga är om overhead-kostnader (OH-kostnader) ska ingå i de kostnader som omfattas av att reproducera, tillhandahålla och sprida uppgifter för vidareutnyttjande. OH-kostnader avser normalt gemensamma, eller indirekta, kostnader som inte är kopplade till en enskild begäran. Det kan exempelvis vara kostnader för ledning, administrativt stöd och lokaler. ESV bedömer att ett exkluderande av sådana kostnader skulle bidra till att främja vidareutnyttjande av information (ESV 2015:63 s. 21). Öppna data-utredningen gjorde samma bedömning (SOU 2020:55 s. 289 och 290) och den bör gälla även för dataförvaltningsförordningen. Det kan finnas gränsfall och frågan om vilka OH-kostnader som kan medräknas får bedömas i det enskilda fallet.

Klarering av upphovsrätt

En av de kategorier av skyddade data som kapitel II omfattar är upphovsrättsligt skyddat material. För att kunna göra sådant tillgängligt för vidareutnyttjande kan upphovsrätten behöva klareras hos rättighetsinnehavaren. Att klarera upphovsrätten innebär att alla som har rättigheter ger sitt tillstånd till användningen, t.ex. genom en licens eller ett avtal. Klarering av upphovsrätt kan typiskt sätt medföra kostnader. Sådana kostnader är en direkt kostnad som kan uppstå. Det skulle inte vara rimligt att den utlämnande myndigheten skulle bära en sådan kostnad. En avgift bör därför kunna täcka sådana kostnader. Klarering av upphovsrätter innebär också arbetsinsatser för den utlämnande myndigheten som hanterar detta. Dessa ska också kunna omfattas.

Datalagen omfattar inte upphovsrättsligt skyddat material och någon bestämmelse som motsvarar detta finns inte. Datalagen bör därför kompletteras med bestämmelser om att avgifter som tas ut enligt dataförvaltningsförordningen ska kunna innefatta kostnader för klarering av upphovsrätt.

Anonymisering eller andra former av framställning av personuppgifter och affärshemligheter

Kostnader för anonymisering och andra former av framställningar av både personuppgifter och affärshemligheter ska också kunna omfattas av en avgift, artikel 6.5 c. Detta avser något annat än reproduktion enligt artikel 6.5 a dataförvaltningsförordningen vilket behandlas ovan.

Vad som avses med framställning i sammanhanget är inte helt givet. I den engelska versionen används i stället begreppet ”preparation” vilket snarare synes avse bearbetning av data.

De olika åtgärder som avses med punkten är sådana som kan vidtas av myndigheter enligt artikel 5 för att bevara uppgifters skyddade karaktär. En sådan åtgärd är att personuppgifter anonymiseras, artikel 5.3 a i. Affärshemligheter, inbegripet företagshemligheter, kan skyddas genom att de ändras, aggregeras eller behandlas med någon annan metod för kontroll, artikel 5.3 a ii. Kontroll bör i det här sammanhanget förstås som kontroll av att affärshemligheten inte avslöjas, i den engelska versionen används uttrycket ”any other method of disclosure control”. Syftet med åtgärden är enligt skäl 15 att uppgifterna ska ändras på ett sådant sätt att ingen konfidentiell information lämnas ut. EU-lagstiftaren bedömer i skäl 7 i dataförvaltningsförordningen att de tekniker som utvecklats för integritetsskyddsändamål även bör kunna användas för att skydda affärshemligheter.

En avgift enligt datalagen 4 kap. 2 § första stycket får omfatta kostnader för avidentifiering av personuppgifter, vilket får sägas motsvara anonymisering. Bestämmelsen grundar sig på artikel 6.1 i öppna data-direktivet som ger stöd för att avgiften täcker även kostnaderna för ”avidentifiering av personuppgifter och åtgärder för att skydda konfidentiell affärsinformation”. Kostnader för att skydda konfidentiell affärsinformation får dock i datalagen bara ingå i avgiftsunderlaget för offentliga företag och offentligt styrda organ, med vilket avses t.ex. statliga och kommunala bolag (prop. 2021/22:225 s. 49-50). Dessa omfattas inte av dataförvaltningsförordningen som ju bara omfattar myndigheter.

Datalagen behöver därför kompletteras med en skrivning som ger myndigheter rätt att inkludera kostnader för sådana skyddsåtgärder som de vidtar för att bearbeta data med personuppgifter eller

affärshemligheter så att de kan tillgängliggöras för vidareutnyttjande.

Underhåll av den säkra behandlingsmiljön

Tillhandahållande av skyddade data i en säker behandlingsmiljö, antingen på distans eller i de fysiska lokaler där den säkra behandlingsmiljön är belägen, är en av de skyddsåtgärder som offentliga myndigheter kan använda enligt artikel 5.3 b och c för att kunna tillgängliggöra skyddade data för vidareutnyttjande. En avgift kan omfatta de direkta kostnader som kan uppstå för att tillhandahålla en sådan säker behandlingsmiljö redan genom kostnader för att tillhandahålla data som beskrivits ovan.

Det finns också möjlighet att i avgiften också ta med kostnader som är nödvändiga för underhåll av den säkra behandlingsmiljön. Det kan vara kostnader för exempelvis supportavtal för hårdvara, nyinköp för att ersätta befintlig hårdvara när garantin gått ut, uppgraderings- och supportavtal för programvarulicenser och personalkostnader för säkerhetspatchningar, backuper, uppgraderingar och annat underhåll. Sådana kostnader ska kunna omfattas av avgifterna som offentliga myndigheter tar ut.

Datalagen omfattar i dag inte tillhandahållande i en säker behandlingsmiljö och kostnader för underhåll av dessa saknas därför. Datalagen bör följaktligen kompletteras med att avgifter som tas ut enligt dataförvaltningsförordningen ska kunna innefatta kostnader för underhåll av en säker behandlingsmiljö.

Förvärvande av rätten att tillåta vidareutnyttjande från tredje part

Liksom för klarering av upphovsrätt så kan andra direkta kostnader för att förvärva en rätt från tredje part för att tillåta ett vidareutnyttjande uppstå.

Det kan inte uteslutas att det skulle kunna uppstå sådana direkta kostnader som avses i förordningen och att en möjlighet att ta ut avgifter för sådana kostnader därför bör införas

Av samma skäl som klarering av upphovsrätt bör kunna omfattas av de avgifter som myndigheter får ta ut, så bör kostnader för förvärvande av tredje parts rättigheter omfattas.

Datalagen omfattar i dag inte något som motsvarar förvärvande av rätt från tredje part. Datalagen bör därför kompletteras med att avgifter som tas ut enligt dataförvaltningsförordningen ska kunna innefatta kostnader för förvärvande av rätt att tillåta vidareutnyttjande från tredje part.

Bistånd till vidareutnyttjare

Som beskrivits i avsnitt 4.5.6 är utrymmet för behöriga myndigheter att bistå vidareutnyttjare som begär registrerades samtycke och datainnehavares tillstånd begränsat på flera sätt. I den mån sådant bistånd ges är det dock lämpligt att en avgift också ska kunna täcka detta. Utifrån de generella begränsningar som finns är det svårt att ge exempel på vad ett sådant bistånd kan innefatta.

Datalagen omfattar i dag inte sådant bistånd till vidareutnyttjare. Datalagen bör därför kompletteras med att avgifter som tas ut enligt dataförvaltningsförordningen ska kunna innefatta kostnader för bistånd till vidareutnyttjare i enlighet med artikel 5.6.

Om en myndighet i samband med att den hanterar en begäran om tillgång till skyddade data för vidareutnyttjande ger stöd i enlighet med FL så kan den inte ta ut en avgift enligt förordningen för det biståndet.

4.5.10 Inga undantag för avgiftsuttag

Bedömning: Några särskilda undantag från skyldigheten att ta ut avgifter för vidareutnyttjande av skyddade data bör inte införas.

Skälen för bedömningen: När myndigheter tar ut avgifter ska de enligt artikel 6.4 vidta åtgärder för att ge incitament till vidareutnyttjande av skyddade data för icke-kommersiella ändamål. Med det avses bl.a. vetenskaplig forskning. Att notera är att vidareutnyttjande enligt definitionen i artikel 2 inte omfattar utbyte av data mellan offentliga myndigheter som enbart sker i samband med deras offentliga verksamhet. Sådant utbyte av data som sker

mellan myndigheter för användning av forskning hos den ena myndigheten som har forskningsuppdrag, t.ex. högskolor och universitet eller Brottsförebyggande rådet, omfattas inte av reglerna i dataförvaltningsförordningens kapitel II.

Vidare ska myndigheterna ge incitament till vidareutnyttjande av små och medelstora företag och uppstartsföretag, det civila samhället och utbildningsanstalter.

Incitament till vidareutnyttjande kan ske genom att tillgängliggörande sker med nedsatt avgift eller avgiftsfritt. Den offentliga myndigheten som tillhandahåller data och som sätter en lägre avgift får upprätta en förteckning över data som tillgängliggörs till en nedsatt avgift eller kostnadsfritt för vissa aktörer får tas fram, artikel 6.4 sista meningen.

I datalagen finns gällande tillgängliggörande av data för vidareutnyttjande begränsningar avseende vilka typer av data som får avgiftsbeläggas. Möjligheten att begränsa avgiftsuttaget i dataförvaltningsförordningen avser i stället vem som begär tillgång för vidareutnyttjande och för vilka syften. Att införa en begränsning av avgiftsuttag på andra grunder än redan befintliga skulle kunna innebär att regelverket blir väldigt komplext och svårtillgängligt.

Lantmäteriet fick i uppdrag av regeringen att i samverkan med berörda aktörer identifiera värdefulla datamängder enligt öppna data-direktivet. Rapporten Tillgängliggörande av särskilt värdefulla datamängder Delrapport till regeringsuppdrag I2019/01415/DF att analysera konsekvenser av myndigheters tillgängliggörande av värdefulla datamängder i enlighet med Europaparlamentets och rådets direktiv om öppna data och vidareutnyttjande av information från den offentliga sektorn avser öppna data och värdefulla datamängder, men flera av de grundläggande resonemangen gällande avgifter för tillgång till data är aktuella att titta på även för skyddade data.

Höga kostnader för offentlig information begränsar förutsättningarna att vidareutnyttja data och därmed antal aktörer som kan utveckla nya produkter och tjänster. Genom att tillhandahålla data fritt sänks trösklarna för att nyttja data vilket möjliggör att fler kan göra det och skapa större sammanlagd nytta. I innovationens natur ligger att utvecklingen inte sällan uppstår inom oförutsägbara områden – varför den fria tillgången till data är av särskild vikt. Den fria tillgången till data minimerar kostnaden att

kombinera olika datamängder och bidrar därmed till att skapa ny kunskap och nya insikter inom tidigare oförutsägbara applikationsområden.

Lantmäteriet konstaterade bl.a. följande avseende frågan om avgifter:

> Flera av de föreslagna datamängderna finansieras idag via avgifter. Detta innebär att den som ska nyttja data måste betala och förhålla sig till ett antal restriktioner. Denna tröskel innebär att många beslut ute i samhället inte baseras på den bästa möjliga data som finns. Idag begränsas många företags utveckling av att de på grund av höga datakostnader istället tvingas använda inaktuella uppgifter eller data med låg upplösning – trots att data av högre kvalitet finns.

Som beskrivits ovan innebär inte bestämmelserna i dataförvaltningsförordningen någon skyldighet för offentliga myndigheter att tillgängliggöra skyddade data för vidareutnyttjande. I de fall det i annan lagstiftning finns en sådan skyldighet eller det annars är möjligt att medge sådant vidareutnyttjande i enlighet med befintlig lagstiftning så ska det ske i enlighet med ramverket i kapitel II dataförvaltningsförordningen. Avgifter är då ett viktigt sätt för offentliga myndigheter att kunna täcka kostnader som uppstår i samband med tillgängliggörande av skyddade data. Om möjligheten att ta ut avgifter i vissa fall begränsas skulle det kunna få motsatt effekt och i stället innebära en risk för att skyddade data inte tillgängliggörs för vidareutnyttjande i samma utsträckning.

Någon särskild reglering för att tillhandahållande ska ske med nedsatt avgift eller avgiftsfritt bör därför inte införas.

4.5.11 Överprövning av beslut

Förslag: Beslut efter begäran om vidareutnyttjande av skyddade data enligt dataförvaltningsförordningen ska kunna överklagas till allmän förvaltningsdomstol.

Skälen för förslaget: Av artikel 9.2 följer att fysiska eller juridiska personer som direkt påverkas av ett beslut efter en begäran om vidareutnyttjande av skyddade data ska ha effektiv rätt till överprövning. Denna rätt till överprövning ska föreskrivas i

nationell rätt och inbegripa möjlighet till omprövning av en opartisk myndighet som besitter lämplig sakkunskap.

Förordningen varken förordar eller kräver att en överprövning av ett beslut om tillgängliggörande av skyddade data för vidareutnyttjande ska göras av en domstol. En effektiv och rättssäker ordning talar dock för att överprövning av en myndighets beslut bör ske inom ramen för det befintliga systemet för överklagande av förvaltningsbeslut, dvs. med förvaltningsrätten som första instans.

I datalagen finns en befintlig bestämmelse för överklagandehantering av beslut om vidareutnyttjande i 5 kap. 4 §. Denna bestämmelse omfattar de krav som behöver ställas på en möjlighet till överprövning enligt dataförvaltningsförordningens art. 9.2. Det finns ingen anledning att göra andra bedömningar eller överväganden än de som gjordes i samband med utformandet av bestämmelsen inför införandet (se prop. 2021/22:225 s. 59, 60 och 95). Den befintliga bestämmelsen om överlagande i 5 kap. 4 § datalagen bör därför också tillämpas för beslut om vidareutnyttjande enligt dataförvaltningsförordningen.

Frågan är vem som kan överklaga myndighetens beslut. Av förordningen framgår att det ska vara de som direkt eller indirekt påverkas av ett beslut om att medge eller vägra tillgång till skyddade data för vidareutnyttjande.

Enligt 42 § FL får ett beslut överklagas av den som beslutet angår, om det har gått honom eller henne emot. Ett beslut får enligt 41 § FL överklagas om beslutet kan antas påverka någons situation på ett inte obetydligt sätt. I 40 § samma lag anges att beslut överklagas till allmän förvaltningsdomstol och att prövningstillstånd krävs vid överklagande till kammarrätten. Klagorätt enligt förvaltningslagen tillkommer alltså den som beslutet angår, om beslutet har gått denne emot.

Den som direkt påverkas av ett beslut om tillgång till skyddade data för vidareutnyttjande kan vara den som begär tillgång till sådana data. Den har också möjlighet att klaga på ett beslut om att medge eller vägra tillgång till informationen enligt 2 kap. TF. För sådana beslut anses inte den som sekretessen avser vara en som beslutet angår, och denne har inte rätt att klaga på ett sådant beslut om tillgång till information.

Den som skyddet för den aktuella datamängden avser skulle dock kunna påverkas direkt av ett sådant beslut, t.ex. om den vars affärshemligheter ingår eller den som innehar upphovsrätt till datan anser att dennes affärshemlighet eller upphovsrätt inte blivit tillräckligt skyddad vid tillgängliggörandet. I sådana fall bör denna ha rätt att överklaga beslutet enligt artikel 9.2. Den som påverkas direkt av beslutet bör också anses vara en som beslutet angår i förvaltningslagens mening vid tillämpningen av överklagande-bestämmelsen i datalagen för ärenden om tillgängliggörande av skyddade data.

4.6 Behöriga organ

Varje medlemsstat ska enligt dataförvaltningsförordningen utse ett eller flera behöriga organ, artikel 7. Dessa får vara behöriga för särskilda sektorer.

Ett behörigt organ ska bistå de offentliga myndigheter som beviljar eller vägrar tillgång för vidareutnyttjande av de typer av skyddade data som kapitel II avser. Behöriga organ får också ges befogenhet att bevilja tillgång till vidareutnyttjande.

Behöriga organ ska ha tillräckliga juridiska, ekonomiska och tekniska resurser och personalresurser för att utföra de uppgifter som de anförtrotts, inbegripet de nödvändiga tekniska kunskaperna för att kunna följa relevant unionsrätt eller nationell rätt om systemen för tillgång till de kategorier av data som avses i artikel 3.1.

Det är alltid den utlämnande myndigheten själv som är ansvarig för den behandling som genomförs och för att ett tillgängliggörande är tillåtet utifrån all tillämplig lagstiftning så som t.ex. dataskyddsregler, immaterialrätten, säkerhetsskyddsregler eller sekretessbestämmelser. Det är den utlämnande myndigheten som är personuppgiftsansvarig för all behandling, och det är den utlämnande myndigheten som handlägger ärendet med begäran om tillgängliggörande för vidareutnyttjande. De myndigheter som ska tillgängliggöra skyddade data för vidareutnyttjande behöver också själva bygga upp den rättsliga, tekniska och organisatoriska kompetens som krävs för detta.

Frågan om att bevilja eller vägra tillgång till skyddade data för vidareutnyttjande och bedömning av tillåtligheten och lämpligheten

av det ansvarar den myndighet som innehar aktuella data för självständigt. Samma sak gäller för frågan om vilka skyddsåtgärder som kan och bör vidtas för att uppnå ett fullgott skydd vid vidareutnyttjande. Det är den myndighet som innehar data som är personuppgiftsansvarig och som ansvarar för rättsliga och säkerhetsmässiga bedömningar fullt ut, liksom att myndigheten själv bär ansvar för vilka tekniska åtgärder som vidtas och att dessa är tillräckliga för att upprätthålla skyddet samt att dessa är korrekt utförda.

I rollen som behörigt organ ligger ett ansvar att bistå andra myndigheter utifrån sin egen kompetens. Det innebär som nämnts ovan inte att det behöriga organet har ansvar för att bedöma om det är möjligt tekniskt eller rättsligt eller om det är lämpligt att tillgängliggöra en viss datamängd för vidareutnyttjande. Det behöriga organet har heller inte ansvar för att kontrollera om vidtagna skyddsåtgärder är tillräckliga eller korrekt utförda.

Biståndet som behöriga organ ska ge ska, när så är nödvändigt, innefatta flera olika delar enligt artikel 7.4.

Medlemsstaterna får antingen inrätta nya behöriga organ eller förlita sig på befintliga myndigheter eller avdelningar inom offentliga myndigheter.

4.6.1 Behöriga organ ska inte kunna bevilja tillgång för vidareutnyttjande för andra myndigheters räkning

Bedömning: Behöriga organ bör inte ges befogenhet att bevilja tillgång till skyddade data för andra offentliga myndigheters räkning.

Skälen för bedömningen: De behöriga organen får ges befogenhet att bevilja tillgång till vidareutnyttjande av skyddade data, artikel 7.2. Frågan om huruvida skyddade data kan göras tillgängliga för vidareutnyttjande kräver en mängd olika överväganden. Som första steg ska en prövning göras av om informationen kan göras tillgänglig i enlighet med regler i bl.a. 2 kap. TF och i OSL. Om informationen kan lämnas ut ska därefter bedömningar göras av om och i så fall hur data kan göras tillgänglig för vidareutnyttjande och vilka villkor som ska ställas upp. Det är

inte lämpligt att någon annan myndighet än den som innehar data gör en sådan prövning och beviljar tillgång till data för annan myndighets räkning. En sådan befogenhet bör inte ges till de behöriga organen i Sverige.

4.6.2 Kompetenser för behöriga organ

I rollen som behörigt organ finns det utifrån beskrivningen i artikel 7.4 av vad rollen innebär vissa förmågor som den eller de myndighet som ska utses behöver besitta.

Sammanställningen nedan har tagits fram i samverkan med Nobareg, en nordisk-baltisk arbetsgrupp skapad på uppdrag av nordiska ministerrådet för att samverka kring implementering av relevant EU-lagstiftning på digitaliseringsområdet, däribland dataförvaltningsförordningen. Länderna företräds av handläggare och experter från myndigheter eller departement. Sverige deltar genom en företrädare för Myndigheten för digital förvaltning (Digg).

Teknisk kompetens

Rollen som behörigt organ innebär att man ska bistå myndigheter med tekniskt stöd i flera olika delar. Bistånd ska ges i hur data bäst kan struktureras och lagras så att dessa data är lättillgängliga. Tekniskt stöd ska också ges för psedonymisering och andra åtgärder som bevarar integritet, konfidentialitet, dataintegritet och tillgänglighet för data. Det kan handla om exempelvis teknik för anonymisering, generalisering eller randomisering, eller av radering av kommersiellt känslig information som affärshemligheter eller immaterialrättsligt skyddat material. Uppräkningen i förordningen är en exemplifiering av sådana integritetsfrämjande och skyddande åtgärder som kan vidtas.

För att kunna bistå med tekniskt stöd i dessa olika delar krävs att det finns en hög teknisk kompetens gällande datahantering och datadelning. Denna kompetens bör vara praktisk och bygga på egna erfarenheter hos myndigheten i hantering av egna datamängder. Även teoretisk teknisk kompetens avseende vad som är ”best practice” är mycket värdefullt.

Vidare krävs att det finns en teknisk kompetens gällande säkerhet.

Säker behandlingsmiljö

Behöriga organ ska ge tekniskt stöd i tillhandahållande av en säker behandlingsmiljö. Biståndet ska inte bestå i att det behöriga organet ska tillhandahålla en säker behandlingsmiljö för andra myndigheter att nyttja, utan stöd i hur en sådan miljö kan konstrueras och hanteras. Egen erfarenhet av att ta fram och tillhandahålla en säker behandlingsmiljö och de tekniska, rättsliga och administrativa aspekter det medför är därför centralt i rollen som behörigt organ.

Rådgivning

Rollen som behörigt organ består i att bistå andra myndigheter och ge dessa råd och stöd. Det är därför bra om den myndighet som ges uppdraget har vana av att vara rådgivande och att stötta andra myndigheter i vissa frågor. Om befintliga sådana uppgifter finns på en myndighet finns också rutiner och strukturer för detta som kan användas.

Det är den myndighet som innehar skyddade data och som ska bedöma om den kan göra den tillgänglig för vidareutnyttjande som ytterst är ansvarig för bedömningarna som ska göras. I rollen som rådgivare är det viktigt att förhålla sig neutral och självständig.

Rättslig kompetens

Behöriga organ ska bistå andra myndigheter när de i sin tur ska stödja en vidareutnyttjare som ska begära registrerades samtycke eller datainnehavares tillstånd till vidareutnyttjande. Behöriga organ ska också bistå i bedömningen av om avtalsmässiga åtaganden är tillräckliga vid viss tredjelandsöverföring enligt artikel 5.10. För dessa uppgifter krävs att det finns en rättslig kompetens på området hos det behöriga organet.

Rättsliga frågor som kan uppkomma kan röra dataskydd, immaterialrätt, affärshemligheter, insynsskydd för statistik,

förvaltningsrätt, offentlighet och sekretess samt säkerhetsskydd och cybersäkerhet. Eftersom krav på att utse en behörig myndighet ställs i en EU-förordning är det centralt att ha förståelse för EU-rättens metod och systematik. Förmåga hos myndigheten att bidra med kompetens inom dessa rättsområden är därför önskvärd.

4.6.3 Andra länders bedömningar

Flera länder uppger att de kommer att utse sina statistikmyndigheter till behöriga organ. Bl.a. Nederländerna, Danmark och Polen avser att utse sina statistikmyndigheter till behöriga organ. Skälet för detta är att statistikmyndigheterna besitter mycket goda kunskaper i hantering av stora mängder skyddade data och hur sådana data på ett säkert sätt kan göras tillgänglig. Statistikmyndigheterna har också i många länder tillgång till skyddade behandlingsmiljöer. Vidare bedöms statistikmyndigheterna själva vara en av de myndigheterna som träffas av regleringen i förordningens kapitel II.

Många av de länder som inte utser sina statistikmyndigheter kommer i stället att lämna uppgiften till en digitaliseringsmyndighet. Bl.a. Finland och Norge kommer att utse sina digitaliseringsmyndigheter till behöriga organ.

En del länder kommer att utse en myndighet inom hälso- och sjukvårdsområdet som sektorsansvarigt behörigt organ på hälso- och sjukvårdsområdet. Bl.a. Finland och Danmark kommer att utse myndigheter inom hälso- och sjukvårdsområdet till sektorsansvariga behöriga organ. Skälet för detta är att hälsodata kan bli aktuella att tillhandahålla för vidareutnyttjande under regelverket.

4.6.4 Befintliga myndigheter ska utses till behöriga organ

Bedömning: Sverige bör inte inrätta nya myndigheter för att utföra uppgiften som behörigt organ enligt dataförvaltningsförordningen, utan utse en befintlig myndighet eller flera befintliga myndigheter.

Skälen för bedömningen: I artikel 7 anges att medlemsstaterna för uppgiften som behöriga organ får inrätta ett eller flera nya

behöriga organ eller förlita sig på befintliga offentliga myndigheter eller interna avdelningar inom offentliga myndigheter.

Uppgiften som behörigt organ är begränsad till att bistå andra myndigheter som beviljar eller vägrar tillgång till skyddade data för vidareutnyttjande. Det har undersökts i vilken utsträckning myndigheter innehar data som omfattas av regelverket och som de tillgängliggör för vidareutnyttjande för att få en uppfattning om hur omfattande hanteringen kan förväntas bli. De tillfrågade myndigheterna bedömer bara i enstaka fall och för vissa datamängder att regelverket kan bli aktuellt. Uppgiften som behörigt organ förväntas därför inte bli omfattande. Att inrätta nya myndigheter är kostsamt och komplext. De kompetenser som krävs för uppgiften finns hos befintliga myndigheter. Uppgiften bör därför fördelas på befintliga myndigheter.

De myndigheter som har skyddade data behöver bygga upp kompetens kring möjligheter att tillgängliggöra sådana data, vilket ytterligare talar för att inga nya myndigheter ska inrättas för uppgiften.

4.6.5 Aktuella myndigheter för uppgiften som behörigt organ

Uppgiften som behörigt organ bör tilldelas en eller flera befintliga myndigheter i Sverige. Den eller de myndigheter som ska få denna uppgift behöver kunna bistå med de kompetenser som uppgiften innefattar.

De myndigheter som bedöms som aktuella för uppgiften är dels Myndigheten för digital förvaltning, dels Statistiska centralbyrån. Nedan följer en övergripande beskrivning av de två myndigheterna och deras nuvarande uppgifter och vilka kompetenser de innehar.

Myndigheten för digital förvaltning (Digg)

Myndigheten för digital förvaltning (Digg) är en myndighet under Finansdepartementet som har till uppgift att samordna och stödja den förvaltningsgemensamma digitaliseringen i syfte att göra den offentliga förvaltningen mer effektiv och ändamålsenlig. Digg:s uppgift finns beskrivet i förordning (2018:1486) med instruktion för Myndigheten för digital förvaltning.

Digg:s huvudsakliga uppgift är att:

1. Samordna och stödja den förvaltningsgemensamma digitaliseringen.
2. Ansvara för den förvaltningsgemensamma infrastrukturen.
3. Bistå regeringen med underlag för den offentliga förvaltningen och av samhällets digitalisering. I detta ingår att följa upp, analysera och beskriva den utvecklingen.

Inom ramen för Digg:s instruktionsenliga uppgifter ligger också att främja öppen och datadriven innovation samt tillgängliggörande och vidareutnyttjande av öppna data från den offentliga förvaltningen, att ge vägledning till den offentliga förvaltningen i frågor om digitala investeringar inom ramen för den förvaltningsgemensamma digitaliseringen, och att ge vägledning till den offentliga förvaltningen i juridiska frågor inom ramen för den förvaltningsgemensamma digitaliseringen.

Digg ska tillhandahålla vägledning i frågor som rör tillgängliggörande av information för vidareutnyttjande i enlighet med öppna data-direktivet. Digg hade ett särskilt uppdrag att främja delning och nyttiggörande av data.[5] Vidare ansvarar Digg för att digitalt publicera en sådan förteckning över data som har gjorts tillgängliga eller sökbara på internet som anges i 2 kap. 6 § datalagen. Denna förteckning finns tillgänglig i Sveriges dataportal som Digg tillhandahåller. Myndigheten har föreskriftsrätt avseende innehållet i och utformningen av förteckningen och om den information som ska lämnas om data som görs tillgängliga eller sökbara i förteckningen. Myndigheten ska också digitalt publicera en sådan förteckning över de myndigheter som är skyldiga att ta ut en avgift vid tillgängliggörande av data som anges i 4 kap. 9 § datalagen.

Sedan 2020 har Digg ett publikt och öppet diskussionsforum kopplat till Sveriges dataportal.[6] Forumet ger en möjlighet för dataproducenter och dataanvändare att nyttja varandras erfarenheter och knyta nya värdefulla kontakter samt nyttja erfarenheter för hur andra gjort i sitt eget arbete för att på så sätt höja kvaliteten och

[5] Regeringsuppdraget I2021/01826 Uppdraget slutredovisades i januari 2023 i rapporten Uppdrag att främja delning och nyttiggörande av data.
[6] Slutrapport regeringsuppdrag I2021/01826, Uppdrag att främja delning och nyttiggörande av data, Myndigheten för digital förvaltning.

effektivisera det egna arbetet. Detta forum kan vara ett värdefullt verktyg i rollen som behörigt organ.

Digg ansvarar för att etablera en förvaltningsgemensam digital infrastruktur för informationsutbyte och ett nationellt ramverk för grunddata. Inom ramen för Ena, Sveriges digitala infrastruktur som Digg ansvarar för, har bl.a. olika s.k. byggblock tagits fram. Inom Ena har även ett nytt metodstöd i form av en rekommendation för aggregerade data tagits fram för offentliga aktörer som tillgängliggör data antingen som öppna data eller genom kontrollerad datadelning. Digg:s roll i Ena och de vägledningar och ansvar som myndigheten redan idag har är en bra grund för fortsatt stöd avseende tillgängliggörande också av skyddade data.

Digg har vidare en befintlig uppgift att ge rättsligt stöd till den offentliga förvaltningen inom digitalisering. Detta stöd är fortfarande delvis under uppbyggnad. Digg har genom tidigare genomförda uppdrag bl.a. avseende att främja offentliga aktörers förmåga att dela och nyttiggöra data upparbetad kompetens i närliggande rättsliga frågor.[7]

Statskontoret har fått i uppdrag att genomföra en myndighetsanalys av Digg.[8] Inom uppdraget ska Statskontoret bl.a. analysera hur Digg fullgör sina uppgifter i förhållande till instruktion, regleringsbrev, regeringsuppdrag och resurser samt ändamålsenligheten och effektiviteten i myndighetens interna ledning, styrning och uppföljning. Statskontoret ska vid behov lämna förslag på åtgärder som kan vidtas för att stärka myndighetens förutsättningar att fullgöra sina uppgifter och uppdrag. Uppdraget ska redovisas senast den 1 december 2023.

Statistiska centralbyrån (SCB)

Statistiska centralbyrån (SCB) är en myndighet under Finansdepartementet som har till huvudsaklig uppgift att utveckla, framställa och sprida officiell statistik och annan statlig statistik

[7] Under uppdragstiden har Digg deltagit i flera olika forum, exempelvis nätverksträffar, event och konferenser, med syfte att både dela med sig av kunskap och erfarenheter samt för att motivera offentliga aktörer att dela sina data. Digg har även både skapat partnerskap och nätverk samt deltagit i redan etablerade nätverk för att främja datadelning och användningen av data och andra digitala resurser. Se vidare Slutrapport regeringsuppdrag I2021/01826, Uppdrag att främja delning och nyttiggörande av data, Myndigheten för digital förvaltning.
[8] https://www.statskontoret.se/pagaende-uppdrag/myndighetsanalys-av-myndigheten-for--digital-forvaltning-digg/

samt för att samordna systemet för den officiella statistiken. Myndighetens uppgifter framgår av förordning (2016:822) med instruktion för Statistiska centralbyrån. SCB är Sveriges nationella statistikbyrå inom det europeiska statistiksystemet.

Det övergripande målet med verksamheten är att producera officiell statistik av god kvalitet som är lättillgänglig för användarna. SCB har informationsförsörjning som en del av kärnverksamheten. Det finns därför en god grundläggande kunskap om tillgängliggörande av information.

Den statistik SCB framställer används som underlag för bl.a. beslutsfattande, debatt och forskning. Inom ramen för myndighetens verksamhet utförs uppdrag från bl.a. regeringen och olika myndigheter, men SCB har även kunder i det privata näringslivet och bland forskare.

När det gäller att samla in och förädla data har SCB hög metodkompetens och ett brett ämneskunnande. Myndigheten använder modern teknik och verkar för att arbeta kostnadseffektivt. SCB besitter i sin roll som statistikmyndighet mycket bra kunskaper om hantering av stora datamängder som skyddas av statistiksekretess och att bearbeta sådana data så att den kan göras tillgänglig. SCB har god kunskap om olika integritetsfrämjande tekniker så som pseudonymisering, anonymisering, generalisering, randomisering osv. Vissa av dessa tekniker använder SCB i sin verksamhet till vardags. Andra tekniker använder de inte själva i någon större omfattning, i de fallen finns kunskapen om metoderna på en mer teoretisk nivå.

Mona

MONA (Microdata Online Access) är sedan 2007 SCB:s standardverktyg för tillgängliggörande av mikrodata för forsknings- och statistikändamål och är en del av SCB:s uppdragsverksamhet. MONA syftar till att öka tillgängligheten till mikrodata samtidigt som säkerhet och sekretess i hanteringen stärks.

SCB har genom MONA en framtagen säker behandlingsmiljö. Denna används för att tillgängliggöra data som skyddas av statistiksekretess från SCB för bl.a. forskare. Villkor ställs då upp för hur data får användas. I vissa fall när den som tar del av data i MONA

också behöver data från andra aktörer, t.ex. en annan myndighet, låter SCB dessa tillgängliggöra data via MONA också. Vid tillhandahållande av MONA för andra aktörers data är SCB den aktörens personuppgiftsbiträde. MONA tillhandahålls bara för andra myndigheter eller aktörer att tillgängliggöra data i de fall det redan rör ett ärende där SCB själva tillgängliggör data i MONA.

4.6.6 Digg och SCB ska utses till behöriga organ

Förslag: Både Myndigheten för digital förvaltning och Statistiska centralbyrån ska utses som behöriga organ enligt artikel 7. De ska gemensamt ansvara för att sektorsövergripande bistå myndigheter som ska bevilja eller vägra tillgång till skyddade data för vidareutnyttjande i enlighet med ramverket i kapitel II dataförvaltningsförordningen.

Myndigheten för digital förvaltning ska ha huvudansvar och samordningsansvar för uppgiften.

Skälen för förslaget: Frågan om att bevilja eller vägra tillgång till skyddade data för vidareutnyttjande och bedömning av tillåtligheten och lämpligheten av det ansvarar den myndighet som innehar aktuella data för självständigt.

Behöriga organ enligt dataförvaltningsförordningen ska kunna bistå den myndighet som innehar skyddade data med råd och kunskap. Uppgiften att vara behörigt organ och bistå offentliga myndigheter som ska tillgängliggöra skyddade data för vidareutnyttjande innefattar som beskrivs ovan ett bistånd på flera olika sätt och kräver många olika kompetenser.

Digg:s kompetenser

Digg har till uppgift att stödja den förvaltningsgemensamma digitaliseringen. De har inom ramen för detta till uppgift att främja tillgängliggörande av öppna data. Digg har befintliga ansvar för delar från öppna data-direktivet. Regelverket för vidareutnyttjande av skyddade data har ett tätt samband med öppna data-direktivet. Digg har bl.a. genomfört livesändningar om öppna data-lagen, publicerat

artiklar på ämnet på dataportalen samt stöd och vägledning. Att ge stöd åt myndigheter för att de ska kunna tillgängliggöra skyddade data för vidareutnyttjande ligger därmed väldigt nära redan befintliga uppgifter. Det finns därför samordningsvinster med att utse Digg till behörigt organ enligt artikel 7.

Uppgiften att vara behörigt organ och bistå offentliga myndigheter som ska tillgängliggöra skyddade data för vidareutnyttjande innefattar som beskrivs ovan ett bistånd på en relativt konkret teknisk nivå. Detta ställer krav på att den myndighet som anförtros uppgiften besitter konkret kunskap om hur stora mängder skyddade data på bästa sätt ska hanteras och behandlas för att kunna vidta tillräckliga skyddsåtgärder vid tillgängliggörande. Tekniska kunskaper har Digg förvisso då det på myndigheten finns en bred teknisk kompetens eftersom myndigheten tillhandahåller förvaltningsgemensam infrastruktur. Myndigheten hanterar data bl.a. inom ramen för tillhandahållande av förvaltningsgemensamma tekniska lösningar för säker digital kommunikation (SDK). Myndigheten har dock inte vana av att använda olika integritetsfrämjande tekniker så som psedonymisering på data.

Digg har till uppgift att samordna frågor om gemensamma standarder, format, specifikationer och liknande krav i den offentliga förvaltningens elektroniska informationsutbyte, 4 § 2 punkten förordningen (2018:1486) med instruktion för Myndigheten för digital förvaltning.

Ett verktyg för att kunna tillhandahålla skyddade data är att göra det i en säker behandlingsmiljö. Digg har inte tillgång en sådan säker behandlingsmiljö och har inte någon upparbetad kunskap kring utveckling och tillhandahållande av en sådan säker behandlingsmiljö.

Digg föreslås få ansvar för den gemensamma informationspunkten i Sveriges dataportal enligt artikel 8, se avsnitt 4.7. Det finns goda samordningsfördelar med att hålla ihop de uppgifter som ges enligt art. 7 och 8 hos en och samma myndighet.

SCB:s kompetenser

I dataförvaltningsförordningen nämns olika typer av integritetsfrämjande tekniker som kan användas för att kunna göra skyddade data tillgängliga för vidareutnyttjande. Det handlar exempelvis om

anonymisering, generalisering, undertryckande och randomisering. SCB använder vissa av dessa tekniker i sin vardagliga hantering av datamängder, medan andra används i mer begränsad omfattning. Det finns därför en praktisk och teknisk kunskap inom myndigheten gällande flera integritetsfrämjande metoder.

Som nämnts ovan är en central skyddsåtgärd som kan vidtas för att tillgängliggöra skyddade data för vidareutnyttjande är att tillgängliggöra dessa i en skyddad behandlingsmiljö. SCB har i MONA en säker behandlingsmiljö. Detta innebär att SCB har en god kunskap i hur en sådan behandlingsmiljö kan konstrueras och användas, både ur tekniskt och rättsligt perspektiv.

Uppgiften som behörigt organ passar inte självklart in i grunduppgiften för myndigheten och resurser saknas att hantera tillkommande bestående uppgifter.

Digg och SCB:s samlade uppgifter och erfarenheter

Varken Digg eller SCB besitter tidigare erfarenhet och kunskap om alla nödvändiga delar av vad uppgiften som behörigt organ innefattar på egen hand. För att stödet till andra myndigheter ska finnas på plats så snart som möjligt, och för att det ska kunna ges på ett effektivt sätt är det centralt att i så stor utsträckning som möjligt nyttja befintliga myndigheters redan upparbetade kunskap och erfarenhet. Det är därför inte lämpligt att ge bara en av de aktuella myndigheterna uppgiften ensam.

Tillsammans har SCB och Digg den kunskap och erfarenhet som behöriga organ som ska ge stöd till andra myndigheter på en sektorsövergripande nivå behöver ha. Förordningen möjliggör att medlemsstaterna utser flera behöriga organ.

Både SCB och Digg bör därför utses till behöriga organ enligt artikel 7.

Digg bör vara huvudansvarig och samordna arbetet

Myndigheterna behöver samverka med varandra i uppbyggnaden av stödet. För att det ska kunna ske på bästa sätt är det lämpligt att en myndighet ges huvudansvar för uppgiften. Med utgångspunkt i

Digg:s grunduppgift är det mest naturligt att Digg utses som huvudansvarig för funktionen.

Utifrån de kompetenser och erfarenheter som Digg och SCB besitter som gör dem lämpliga att utse till behöriga organ bör Digg ha huvudansvaret för att bistå med vägledning och juridisk kompetens vid begäran om registrerades samtycke eller datainnehavares tillstånd samt vid bedömning av tillräckligheten i de avtalsmässiga åtagandena i enlighet med artikel 5.10.

Den kompetens som SCB besitter gör att det stöd som SCB kan ge andra myndigheter som ska tillgängliggöra skyddade data för vidareutnyttjande består i teknisk kompetens i datahantering och i hur man kan tillhandahålla en säker behandlingsmiljö. SCB bör vara huvudansvariga för att bistå med vägledning och tekniskt stöd gällande hur en säker behandlingsmiljö kan tillhandahållas, tekniskt stöd för psedonymisering och för att säkerställa databehandling på ett sätt som bevarar integriteten, konfidentialiteten, dataintegriteten och tillgängligheten för den information som finns i data. Det tekniska stödet ska bestå i att bistå med kunskap, inte att tillhandahålla tekniska lösningar eller vara en hjälpdesk för tekniska problem.

Frågor om hur data bäst kan struktureras och lagras så att de är lättillgängliga har både Digg och SCB kunskap om.

Uppdelningen av ansvar bör utöver frågan om huvudansvar inte ges för skarpa gränser i författning, utan rollerna bör utformas av myndigheterna tillsammans i samverkan med utgångspunkt i beskrivningen ovan.

Under uppbyggnaden av stödet som de behöriga organen ska kunna lämna kan det finnas behov av att få stöd ifrån andra myndigheter som har viss sakkunskap som de behöriga organen själva inte besitter och som kan behövas för ett bra genomförande av uppgiften. Något särskilt uppdrag för införandet bedöms dock inte behöva ges, varken till Digg eller SCB eller till andra myndigheter. Detta eftersom Digg enligt 10 § instruktionen för myndigheten ska samverka med den offentliga förvaltningen i syfte att främja utvecklingen inom sitt verksamhetsområde, Vidare ska alla myndigheter enligt 6 § andra stycket myndighetsförordningen (2007:515) samarbeta med andra myndigheter och ta till vara på de fördelar som kan vinnas av ett sådant samarbete. Det samarbete mellan myndigheter som behövs för att kunna få ett stöd på plats för

rollen som behörigt organ kan ske med stöd Digg:s instruktion och myndighetsförordningen.

4.6.7 Behöriga organ inom olika sektorer bör utredas vidare

Bedömning: Behöriga organ inom olika sektorer bör införas på sikt. För att kunna göra det behöver särskilda förutsättningar inom olika sektorer tas i beaktande vilket inte ingår i denna utredning. Regeringen bör därför utreda frågan vidare inom olika sektorer.

Skälen för bedömningen: Dataförvaltningsförordningen medger att behöriga organ utses för särskilda sektorer, artikel 7.1. För att ett behörigt organ ska kunna bistå med kvalitativ konkret stöd så krävs utöver den kunskap på en övergripande nivå som beskrivits i avsnitt 4.6.2 ovan också kunskaper om särskilda villkor och förutsättningar inom de olika sektorer och för de datamängder som är aktuella.

Inom Ena, Sveriges digitala infrastruktur, har ansvar för olika komponenter fördelats till olika myndigheter. Några myndigheter, Lantmäteriet, Bolagsverket, E-hälsomyndigheten, Skatteverket och Trafikverket har ansvar för olika grunddatadomäner. Ett antal kompetensområden har tagits fram och i dagsläget ansvarar Digg för samtliga utom kompetensområde arkiv som Riksarkivet ansvarar för. Vissa myndigheter har också fått ansvar för s.k. byggblock.[9]

Ett behörigt organ ska bl.a. ge vägledning i hur data bäst kan struktureras och lagras för att vara lättillgängligt. Bedömningen av detta kan skilja sig åt beroende på vad det rör sig om för data. Behöriga organ på sektorsnivå skulle kunna ge mer ändamålsenliga stöd för just olika typer av data. De befintliga ansvaren inom Ena skulle kunna vara en bra utgångspunkt vid utseende av sektorsansvariga behöriga organ.

En pågående utredning om sekundäranvändning av hälsodata[10] har tittat på frågan utifrån hälsodataområdet. Utredningen har tagit

[9] För byggblocken ansvarar just nu Digg, Skatteverket, Bolagsverket, Riksarkivet, Arbetsförmedlingen, Försäkringskassan och E-hälsomyndigheten. Mer om Ena och ansvarsfördelningen finns på https://www.digg.se/ledning-och-samordning/ena---sveriges-digitala-infrastruktur/ansvar-och-finansiering, 2023-03-31.
[10] S 2022:04 Utredningen om sekundäranvändning av hälsodata.

fram en promemoria med förslag på E-hälsomyndigheten som behörigt organ för hälsodatasektorn. Förslaget behandlas för närvarande inom Regeringskansliet.

För att få ut en större nytta av regleringen i dataförvaltningsförordningen bör behöriga organ utses på sektoriell nivå utöver de behöriga organ på övergripande nivå som föreslås i denna promemoria. Detta bör därför utredas vidare.

4.7 Gemensam informationspunkt

Medlemsstaterna ska tillhandahålla en gemensam informationspunkt enligt artikel 8. I denna ska information om tillämpningen av artikel 5 och 6 som avser villkor för vidareutnyttjande och avgifter finnas tillgänglig.

Medlemsstaterna kan inrätta ett nytt organ eller utse ett befintligt som gemensam informationspunkt.

I den gemensamma informationspunkten ska det finnas en sökbar tillgångsförteckning som innehåller en översikt över alla tillgängliga datakällor tillsammans med relevant information som beskriver tillgängliga data samt villkoren för vidareutnyttjandet av dessa.

Kommissionen ska inrätta en europeisk gemensam åtkomstspunkt med ett sökbart register över tillgängliga data i nationella gemensamma informationspunkter, artikel 8.4.

Den gemensamma informationspunkten ska också kunna ta emot förfrågningar eller ansökningar om vidareutnyttjande av skyddade data och vidareförmedla dessa till de myndigheter som innehar aktuella data, artikel 8.2.

4.7.1 Digg och Sveriges dataportal

Enligt datalagen 2 kap. 5 § ska Digg digitalt publicera en förteckning över sådana data som offentlig sektor på eget initiativ gjort tillgängliga eller sökbara på internet i syfte att de ska kunna vidareutnyttjas. Denna förteckning finns i Sveriges dataportal som Digg ansvarar för.

Sveriges dataportal är en etablerad webbplats som ger myndigheter, kommuner och regioner en möjlighet att synliggöra

sina delade data på ett centralt ställe och på ett strukturerat sätt. Sveriges dataportal ger också tillgång till data och stöd för att utveckla tjänster med datadriven innovation inom områdena data, API, AI och öppen källkod.

På Sveriges dataportal synliggörs data från en rad olika typer av organisationer och sektorer. Själva datan finns dock inte på portalen, utan enbart information om datamängder, dvs. metadata. Data hämtas i sin tur via länkar för nedladdning eller efterfrågas hos respektive organisation som ansvarar för sina egna datamängder. Ansvaret för att den publicerade informationen är korrekt, fullständig och aktuell har den organisation som äger informationen.

Data och API:er på Sveriges dataportal får användas på olika sätt, och det är den tillhandahållande organisationen som bestämmer vilka villkor som ska gälla för vidareutnyttjande. Det kan vara helt fri återanvändning, finnas krav på att användaren ska referera till den tillhandahållande organisationen när data används eller att en avgift ska betalas. Verksamheter som tillgängliggör data rekommenderas att använda Creative Commons version 4.0 för att rättighetsmärka eller licensiera sin data för att skapa tydliga ramar för användarna. Creative Commons är en ideell organisation som tagit fram ett system av licenser som syftar till att hjälpa de som skapar och vill dela med sig av sina verk (helt eller delvis).

Data som är publicerad på Sveriges dataportal ska vara av god kvalitet och användbar enligt ett antal framtagna nationella principer för att tillgängliggöra information.[11] Principerna syftar till att stödja arbetet med att tillgängliggöra och publicera information för vidareutnyttjande. Genom att etablera gemensamma principer som sträcker sig över sektorsgränser ska det möjliggöra för verksamheter att fatta mer likartade beslut och successivt få en mer likartad hantering inom den offentliga förvaltningen.

I slutet av november 2022 lanserade Digg en betaversion av Sveriges dataportal med nya komponenter. Här finns bl.a. en förteckning över datamängder, API:er, begrepp och specifikationer för att kunna hitta och utforska delade data samt konkret stöd kring AI genom en guide, ett självskattningsverktyg och praktiska exempel.

[11] Principerna finns beskrivna på dataportalen, https://www.digg.se/kunskap-och-stod/oppna-och-delade-data/offentliga-aktorer/nationella-principer-for-att-tillgangliggora-information, 2023-02-09.

Digg har genomfört tekniska förberedelser av Sveriges dataportal för att kunna importera forskningsdata och dataspecifikationer till webbplatsen. Genom en rad olika insatser har myndigheten arbetat för att det diskussionsforum som finns kopplat till Sveriges dataportal ska vara navet för publika diskussioner kring offentliga API:er och (öppna-) data samt andra digitala resurser.

I samarbete med Ena – Sveriges digitala infrastruktur som Digg ansvarar för – har även ett nytt metodstöd i form av en rekommendation för aggregerade data tagits fram för offentliga aktörer som tillgängliggör data antingen som öppna data eller genom kontrollerad datadelning.

4.7.2 Digg ska tillhandahålla den gemensamma informationspunkten

Förslag: Myndigheten för digital förvaltning ska tillhandahålla den gemensamma informationspunkten i Sverige.

Skälen för förslaget: I dataförvaltningsförordningen finns det krav på att medlemsstaterna ska tillhandahålla en gemensam informationspunkt för allmän information om villkor för vidareutnyttjande av skyddade data och avgifter för sådan tillgång samt en förteckning över tillgängliga data med specifika villkor.

I beaktandeskäl 26 lyfts att befintliga praktiska arrangemang, som t.ex. portaler för öppna data, skulle kunna användas också som gemensam informationspunkt för dataförvaltningsförordningen. För Sveriges del är det Digg som genom Sveriges dataportal tillhandahåller en sådan portal för öppna data. Portalen är inte bara en plats där data från en rad olika typer av organisationer och sektorer synliggörs för att dataanvändare ska kunna hitta den, tanken är också att Sveriges dataportal ska vara navet för publika diskussioner kring offentliga data och API:er samt andra digitala resurser.

För både myndigheter som innehar data som ska kunna vidareutnyttjas och för dataanvändare som vill hitta data är det lämpligt att använda en och samma portal oavsett om den data som avses är öppna data eller skyddade data. Samma myndighet som har ansvar för förteckningen av öppna data bör därför tillhandahålla den

gemensamma informationspunkten för dataförvaltningsförordningen.

4.7.3 Myndigheter som tillgängliggör skyddade data ska informera den gemensamma informationspunkten

Förslag: En myndighet som tillgängliggör skyddade data för vidareutnyttjande ska informera den myndighet som tillhandahåller den gemensamma informationspunkten om sådana data och villkoren för vidareutnyttjande av dessa.

Skälen för förslaget: I den gemensamma informationspunkten ska på elektronisk väg en sökbar tillgångsförteckning tillhandahållas. I den ska en översikt över alla tillgängliga datakällor finnas tillsammans med relevant information som beskriver tillgängliga data, inbegripet dataformat och datastorlek samt villkoren för vidareutnyttjande av dessa, artikel 8.2.

För att Digg som tillhandahåller den gemensamma informationspunkten ska kunna ha en sådan tillgångsförteckning behöver myndigheter som tillgängliggör data för vidareutnyttjande förse Digg med relevant information. De myndigheter som tillgängliggör skyddade data för vidareutnyttjande bör därför ha en skyldighet att informera Digg.

Med tillgängliggöra avses i datalagen att en myndighet eller ett offentligt företag ger tillgång till information, oavsett om det görs frivilligt eller på grund av en skyldighet i annan författning. Ett tillgängliggörande förutsätter således inte att det sker på viss rättlig grund. För att de kategorier av skyddade data som kapitel II dataförvaltningsförordningen avser ska kunna göras tillgängliga för vidareutnyttjande behöver den offentliga myndigheten vidta vissa skyddsåtgärder och i normalfallet ställa upp vissa villkor för vidareutnyttjandet. Sådana skyddade data kan därför inte tillhandahållas utan en begäran. Den myndighet som innehar skyddade data ska underrätta den gemensamma informationspunkten som sådana data som gjorts tillgängliga för vidareutnyttjande på begäran eller sådana data som myndigheten på eget initiativ identifierat och satt upp villkor för vidareutnyttjande för.

4.7.4 En begäran till informationspunkten inte en inkommen handling

Bedömning: En förfrågan eller ansökan om vidareutnyttjande av skyddade data som inkommer till den gemensamma informationspunkten för vidarebefordran till den myndighet som innehar aktuella data bör inte ses som inkommen till den myndighet som tillhandahåller den gemensamma informationspunkten.

Skälen för bedömningen: Den gemensamma informationspunkten ska vara behörig att ta emot förfrågningar eller ansökningar om vidareutnyttjande av skyddade data. Den gemensamma informationspunkten bör enligt skäl 26 kunna förlita sig på automatiska metoder när den överför förfrågningar eller ansökningar om vidareutnyttjande.

En åtgärd som en myndighet vidtar endast som ett led i en teknisk bearbetning eller teknisk lagring av en handling som en annan myndighet har tillhandahållit ska inte anses leda till att handlingen har kommit in till den mottagande myndigheten, 2 kap. 9 § tredje stycket TF. En handling som förvaras hos en myndighet endast som ett led i en teknisk bearbetning eller teknisk lagring för någon annans räkning anses inte som allmän handling hos den myndigheten, 2 kap. 13 § TF. Har en myndighet alltså bara till uppgift att tekniskt bearbeta eller lagra en upptagning för automatiserad behandling för någon annan myndighets eller en enskilds räkning, anses upptagningen inte vara en allmän handling hos den myndighet som bara har tekniska uppgifter i sammanhanget. Av praxis framgår att det väsentliga är om myndighetens enda syfte med handlingarna är teknisk bearbetning eller lagring. Om myndigheten, av tekniska eller administrativa skäl, har möjlighet att använda handlingarna på något annat sätt är bestämmelsen inte tillämplig (Se Lenberg, Tensjö & Geijer, Offentlighets- och sekretesslagen En kommentar [2022, version 26, JUNO], under rubriken 13–14 §§ Handlingar som inte anses som allmänna).

Den myndighet som tillhandahåller den gemensamma informationspunkten ska vid tillhandahållandet av den gemensamma informationspunkten kunna ta emot förfrågningar och ansökningar om vidareutnyttjande av data. En sådan förfrågan eller ansökan är en

handling. Dessa ska dock inte hanteras av den myndighet som tillhandahåller den gemensamma informationspunkten annat än för vidarebefordran till den aktuella myndigheten. Den myndighet som tillhandahåller den gemensamma informationspunkten kan automatisera dessa överföringar. En sådan förfrågan eller ansökan förvaras då i normalfallet bara som en led i en teknisk lagring i den gemensamma informationspunkten. Handling ska då inte anses som en inkommen handling hos den myndigheten.

5 Dataförmedlingstjänster och dataaltruism

5.1 Inledning

Kommissionen lyfter i konsekvensanalysen för dataförvaltningsförordningen att många företag i dag befarar att delning av data kan innebära en förlust av konkurrensfördelar och utgöra en risk för missbruk. I dataförvaltningsförordningens kapitel III finns därför en uppsättning regler för leverantörer av dataförmedlingstjänster för att säkerställa att de kommer att fungera som pålitliga organisatörer av datadelning. Syftet med ramverket är att öka tilliten till dataförmedlarna och att möjliggöra en konkurrensutsatt miljö för datadelning.

För att öka förtroendet för datadelning introduceras en modell som bygger på dataförmedlarnas neutralitet och transparens samtidigt som individer och företag får kontroll över sina data. Leverantörerna av dataförmedlingstjänster ska därför enligt skäl 33 fungera som förmedlare av data och inte själva använda de data som utbyts för några andra ändamål. Ramverket ger ett alternativ för datahantering från den praxis de s.k. big tech-bolagen arbetat fram, där deras kontroll över stora mängder data gett dem en hög grad av makt över marknaden. Regelverket ska enligt skäl 32 bidra till att säkerställa att såväl de registrerade och datainnehavarna som dataanvändarna får bättre kontroll över tillgången till och användningen av den data som är deras.

Dataaltruism handlar om att individer och företag ger sitt samtycke eller tillåtelse att tillgängliggöra data som de genererar – frivilligt och utan belöning – för att användas i allmänhetens intresse. Sådana uppgifter har en enorm potential för att främja forskning och utveckla bättre produkter och tjänster, inklusive inom områdena hälsa, miljö och mobilitet.

Som skäl för införande av ramverket för dataaltruism lyfter kommissionen att forskning tyder på att även om det i princip finns en vilja att engagera sig i dataaltruism, hämmas detta i praktiken av bristen på verktyg för datadelning. Kapitel IV i dataförvaltningsförordningen syftar till att skapa pålitliga verktyg som gör att data kan delas på ett enkelt sätt till gagn för samhället. Det ska skapa de rätta förutsättningarna för att försäkra individer och företag om att när de delar med sig av sin data kommer den att hanteras av pålitliga organisationer baserade på EU:s värderingar och principer. Enligt skäl 45 kan detta möjliggöra skapandet av datapooler av tillräcklig storlek för att möjliggöra dataanalys och maskininlärning, också över gränserna inom unionen.

5.2 Dataförmedlingstjänster och dataaltruism i dataförvaltningsförordningen

5.2.1 Dataförmedlingstjänster

Dataförmedlingstjänster regleras i kapitel III i dataförvaltningsförordningen. Kapitlet innehåller ett par bestämmelser som sätter ramar för tillämpningsområdet (artiklarna 10 och 15), regler om en anmälningsplikt för leverantörer av dataförmedlingstjänster (artikel 11), villkor för tillhandahållande av sådana tjänster (artikel 12) samt bestämmelser om behöriga myndigheter för dataförmedlingstjänster som ska hantera anmälningar och utöva tillsyn (artiklarna 13 och 14).

Definitioner och tillämpningsområde

En dataförmedlingstjänst är enligt definitionen i artikel 2.11 en tjänst som syftar till att med tekniska, rättsliga eller andra medel upprätta affärsförbindelser för datadelning mellan ett obestämt antal registrerade och datainnehavare, å ena sidan, och dataanvändare, å andra sidan, inbegripet för att utöva de registrerades rättigheter avseende personuppgifter, med uteslutande av åtminstone följande:

1. Tjänster som erhåller data från datainnehavare och aggregerar, berikar eller omvandlar data i syfte att avsevärt öka deras värde och licensierar användningen av resulterande data till

dataanvändare, utan att upprätta en affärsförbindelse mellan datainnehavare och dataanvändare.
2. Tjänster som är inriktade på förmedling av upphovsrättsligt skyddat innehåll.
3. Tjänster som uteslutande används av en datainnehavare för att möjliggöra användning av de data som den datainnehavaren innehar, eller som används av flera juridiska personer en sluten grupp, inbegripet leverantörs- eller kundrelationer eller samarbeten som grundar sig på avtal, särskilt sådana som har som huvudsakligt syfte att säkerställa funktionerna för föremål och enheter som är anslutna till sakernas internet.
4. Datadelningstjänster som erbjuds av offentliga myndigheter som inte syftar till att upprätta affärsförbindelser.

Dataförmedlingstjänster är med andra ord tjänster där data ska förmedlas på ett neutralt sätt utan att leverantören använder data och t.ex. förädlar eller omvandlar den. Tjänster som förmedlar upphovsrättsligt skyddat material är undantagna enligt punkten b) vilket innebär att exempelvis olika streamingtjänster för musik eller film inte omfattas, inte heller poddplattformar eller tjänster för ljud- eller e-böcker. Som framgår av punkten d) tillhandahåller myndigheter normalt inte dataförmedlingstjänster i förordningens mening.

En central del av definitionen är *datadelning*, som i sin tur i artikel 2 definieras som en registrerads eller datainnehavares tillhandahållande av data till en dataanvändare för gemensam eller individuell användning av dessa delade data, baserat på frivilliga avtal, unionsrätt eller nationell rätt, direkt eller via en förmedlare, t.ex. inom ramen för öppna eller kommersiella licenser mot en avgift eller kostnadsfritt.

De dataförmedlingstjänster som ska uppfylla kraven i kapitel III är enligt artikel 10 följande dataförmedlingstjänster:

1. Förmedlingstjänster mellan datainnehavare och potentiella dataanvändare, däribland tillhandahållandet av tekniska eller andra metoder för att möjliggöra sådana tjänster; dessa tjänster kan innefatta bilaterala eller multilaterala utbyten av data eller inrättandet av plattformar eller databaser som möjliggör utbyte eller gemensam användning av data, liksom inrättandet av annan

särskild infrastruktur för sammankoppling av datainnehavare med dataanvändare.

2. Förmedlingstjänster mellan de registrerade som önskar göra sina personuppgifter tillgängliga eller fysiska personer som önskar göra icke-personuppgifter tillgängliga, och potentiella dataanvändare, däribland tillhandahållandet av tekniska eller andra metoder för att möjliggöra sådana tjänster, och i synnerhet som möjliggör utövandet av de registrerades rättigheter som föreskrivs i dataskyddsförordningen.
3. Datakooperativs tjänster.

Kapitel III ska inte tillämpas på erkända dataaltruismorganisationer eller andra icke-vinstdrivande enheter, artikel 15.

Anmälningsplikt

Varje leverantör av dataförmedlingstjänster som träffas av beskrivningen i artikel 10 ska lämna en anmälan till en behörig myndighet och följa de krav som ställs på dataförmedlare i kapitel III. Anmälningsförfarandet regleras i artikel 11. Efter att anmälan har lämnats får leverantören inleda sin verksamhet.

Anmälan ska innehålla vissa specifika fastslagna uppgifter, så som exempelvis namn, adress, rättslig status, ägarstruktur, en offentlig webbplats med information om tjänsten och leverantören och en beskrivning av tjänsten, artikel 11.6. Leverantören ska enligt artikel 11.8 på begäran inom en vecka från att den lämnat en vederbörligen och fullständigt genomförd anmälan lämnats in kunna få en standardiserad förklaring om att anmälan lämnats in och att den innehåller alla uppgifter den ska. Leverantören ska också enligt artikel 11.9 på begäran kunna få en bekräftelse från den behöriga myndigheten på att den uppfyller kraven i artikel 11 och 12. Om ytterligare information behövs för att utfärda en sådan bekräftelse så har den behöriga myndigheten befogenhet att begära den med stöd av artikel 14.2. Leverantören kan efter att den fått en sådan bekräftelse använda beteckningen ”leverantör av dataförmedlingstjänster som är erkänd i unionen” samt en gemensam logotyp i sin kommunikation, artikel 11.9. Logotypen ska tas fram av kommissionen i en genomförandeakt.

Leverantören av dataförmedlingstjänsten ska underrätta den behöriga myndigheten om något av det som framgick av anmälan ändras eller om den upphör med verksamheten.

Avgift får tas ut för anmälan om det regleras i nationell rätt, artikel 11.11.

Kommissionen ska från den behöriga myndigheten underrättas om alla anmälningar av nya dataförmedlingstjänster och om ändringar eller upphörande av redan anmälda dataförmedlingstjänster.

Villkor för tillhandahållande av dataförmedlingstjänster

Dataförmedlingstjänster som omfattas av kapitel III ska uppfylla de villkor som framgår av artikel 12. Artikeln omfattar 15 punkter med olika villkor som avser såväl administrativa som tekniska och juridiska aspekter.

Ett centralt villkor som knyter an till själva definitionen av dataförmedlingstjänst är att data som förmedlingstjänsten tillhandahålls för inte får användas för andra ändamål än att ställa dem till användarnas förfogande. Dataförmedlingstjänsten måste också tillhandahållas genom en juridisk person som är separat från all övrig verksamhet som bedrivs av leverantören av tjänsten, artikel 12 a och skäl 33. Data som samlas in av leverantören avseende användning får bara användas av leverantören för utveckling av tjänsten.

De kommersiella villkoren, inklusive prissättningen, får inte knytas till om datainnehavaren eller användaren använder andra tjänster från samma leverantör. Tillgången till tjänsterna ska vara rättvis, transparent och icke-diskriminerande. Tjänsten får omfattas av erbjudanden av ytterligare verktyg eller tjänster för syftet att underlätta utbytet av data, exempelvis tillfällig lagring eller konvertering. Sådana verktyg får användas bara på uttrycklig begäran.

Leverantörer av dataförmedlingstjänster ska främja utbyta av data i det format som den erhåller data, och konvertering ska bara få ske om det ökar interoperabiliteten, som bl.a. rör förmågan att kunna kombinera data med andra datamängder t.ex. genom användande av gemensamma standarder för dataformat. Den ska också vidta

åtgärder för att säkerställa interoperabiliteten med andra leverantörer.

Det finns också villkor som avser säkerhetsåtgärder som ska vidtas både för att förhindra bedrägerier, för att behandlingen ska vara säker och för att förhindra att otillåtna överföringar av data görs. Leverantören har också en skyldighet att informera datainnehavare vid otillåten överföring av data.

Vid insolvens ska leverantören säkerställa en rimlig kontinuitet i tillhandahållandet av tjänsten genom att ha mekanismer på plats för att möjliggöra tillgång till data.

Det finns vidare villkor för behandling av personuppgifter och begäran av samtycke som knyter an till dataskyddsförordningens krav på transparens och tydlig, begriplig och lättåtkomlig information om behandlingen.

Leverantören ska föra logg över dataförmedlingsverksamheten.

Behörig myndighet och tillsyn

Medlemsstaterna ska utse en eller flera behöriga myndigheter för dataförmedlingstjänster, artikel 13. Den behöriga myndigheten ska ta emot anmälningar från leverantörer av dataförmedlingstjänster och underrätta kommissionen om anmälningarna.

Den behöriga myndigheten ska övervaka och utöva tillsyn över leverantörer av dataförmedlingstjänster och att dessa uppfyller villkoren. Tillsynen får bedrivas både på eget initiativ och på begäran av en fysisk eller juridisk person.

Befogenheten för den behöriga myndigheten ska inte påverka befogenheterna för den nationella dataskyddsmyndigheten konkurrensmyndigheten eller myndigheterna som ansvarar för cybersäkerhet. I Sverige är Integritetsskyddsmyndigheten dataskyddsmyndighet och Konkurrensverket konkurrens-myndighet. Flera olika myndigheter ansvar för olika delar av cybersäkerhetsarbetet. Regeringen har i beslut Fö2019/01330 uppdragit åt Försvarets radioanstalt (FRA), Försvarsmakten, Myndigheten för samhällsskydd och beredskap (MSB) och Säkerhetspolisen att inrätta Nationellt cybersäkerhetscenter. Arbetet sker i nära samverkan med Post- och telestyrelsen (PTS), Polismyndigheten och Försvarets materielverk. Den behöriga

myndigheten ska ha ett nära samarbete med dessa myndigheter och utbyta nödvändig information som behövs för att kunna utföra respektive uppgifter, artikel 13.3.

Den behöriga myndigheten har befogenhet att begära all information som är nödvändig för att kunna kontrollera uppfyllandet av kraven i kapitel III, artikel 14.2. En begäran om information ska vara proportionerlig och motiveras.

Om den behöriga myndigheten finner att en leverantör av dataförmedlingstjänster inte uppfyller kraven ska den underrätta leverantören om detta, och leverantören ska få möjlighet att yttra sig, artikel 14.3. Vid allvarligare överträdelser ska tillsynsmyndigheten kräva att överträdelsen upphör, artikel 14.4. Därutöver kan olika administrativa åtgärder vidtas, såsom förelägganden om att tillhandahållande av tjänsten skjuts upp eller avbryts eller ekonomiska sanktioner.

De behöriga myndigheterna för dataförmedlingstjänster i olika medlemsstater ska samarbeta och bistå varandra när det behövs, artikel 14.7. Sådant samarbete kan omfatta informationsutbyte mellan myndigheterna.

Av artikel 26 framgår krav som ställs på behöriga myndigheter. De ska vara juridiskt åtskilda och funktionellt oberoende av leverantörer av dataförmedlingstjänster. Ledande befattningshavare och personal som ansvarar för att utföra uppgifterna på myndigheten får inte vara personer som på något sätt är involverade i tjänsterna genom att t.ex. utveckla, tillhandahålla eller äga sådana tjänster. Detta hindrar inte att dataförmedlingstjänster används inom myndigheten för om det är nödvändigt för verksamheten, eller användning för personliga ändamål, artikel 26.3.

Myndigheten ska utföra sina uppgifter på ett opartiskt, transparent, konsekvent och tillförlitligt sätt och utan dröjsmål, artikel 26.2. Ledande befattningshavare och personal som är involverade i verksamheten får inte delta i någon verksamhet som kan påverka objektiviteten och integriteten i samband med bedömningar som de ska göra, artikel 26.4.

Överklagande och domstolsprocess

I kapitel V i dataförvaltningsförordningen finns bestämmelser om rätten att föra talan mot beslut från behöriga myndigheter för dataförmedlingstjänster och instrumenten att få rättslig prövning.

Fysiska och juridiska personer kan inkomma med klagomål mot leverantörer av dataförmedlingstjänster till den behöriga myndigheten, artikel 27. Klagomål kan framföras både individuellt och kollektivt. Den behöriga myndigheten ska underrätta klaganden om hur förfarandet fortskrider och vilka beslut som fattas, samt om rätten till ett effektivt rättsmedel enligt artikel 28.

I artikel 28 stadgas att fysiska och juridiska personer ska ha rätt till effektiva rättsmedel för sådana bindande beslut som den behöriga myndigheten för dataförmedlingstjänster kan fatta inom ramen för tillsynen. Förfaranden ska inledas i domstol i den medlemsstat där den aktuella behöriga myndigheten är belägen.

Om den behöriga myndigheten underlåter att agera på ett klagomål ska den som klagat ha rätt till omprövning hos en opartisk myndighet med rätt sakkunskap eller prövning i domstol.

5.2.2 Dataaltruism

I kapitel IV finns bestämmelser för att främja dataaltruism, data som på frivillig basis görs tillgänglig av individer eller företag i det allmännas intresse. Vid dataaltruism i förordningens mening ska den som delar med sig av sin data hela tiden ha information om hur deras data används. Detta till skillnad från datadonation där den som donerar data inte har insyn i hur denna sedan används.

Definitioner och tillämpningsområde

Dataaltruism definieras i artikel 2.16 som den frivilliga delningen av data på grundval av de registrerades samtycke till behandling av personuppgifter som rör dem eller tillstånd från datainnehavare att tillåta användning av deras icke-personuppgifter utan något krav på eller mottagande av ersättning utöver ersättning för de kostnader som de ådragit sig när de gör uppgifterna tillgängliga för mål av allmänintresse, t.ex. hälso- och sjukvård, bekämpande av

klimatförändringar, förbättring av mobiliteten, främjande av framställning och spridning av officiell statistik, förbättrat tillhandahållande av offentliga tjänster, politiskt beslutsfattande eller vetenskaplig forskning av allmänt intresse.

Dataaltruism omfattar alltså både personuppgifter och icke-personuppgifter, dvs. uppgifter som inte är personuppgifter, och grunden för delningen är samtycke när det gäller personuppgifter och tillstånd när det gäller icke-personuppgifter. Att notera är att definitionen av samtycke i artikel 2.5 i dataförvaltningsförordningen är knuten till samtycke enligt artikel 4.11 dataskyddsförordningen.

Registrering

Organisationer som vidtar dataaltruismåtgärder och uppfyller vissa villkor som ställs upp ska kunna ansöka om att registreras som en dataaltruismorganisation.

För att kvalificera sig för registrering i ett nationellt register ska organisationen uppfylla vissa krav uppställda i artikel 18. Organisationen ska vara en juridisk person som bildats för att uppfylla mål av allmänt intresse och bedriver verksamhet på icke-vinstdrivande grund och är fristående från enheter som bedriver verksamhet på vinstdrivande grund.

Registrering av dataaltruismorganisationer sker efter ansökan om registrering till en behörig myndighet. Vad ansökan ska innehålla och hur den ska handläggas regleras i förordningens artikel 19.

Ansökan ska innehålla vissa specifika fastslagna uppgifter, så som exempelvis namn, adress, rättslig status, organisationsnummer om sådant finns, stadgar, inkomstkällor, en offentlig webbplats med information om organisationen och verksamheten, de mål av allmänt intresse som organisationen ämnar främja när data samlas in och den typ av data som enheten avser behandla, artikel 19.4. När den behöriga myndigheten har utvärderat ansökan och konstaterat att organisationen uppfyller kraven ska den registreras i det offentliga registret, artikel 19.5.

Dataaltruismorganisationen ska underrätta den behöriga myndigheten om något av det som framgick av ansökan om registrering ändras, artikel 19.7.

Den behöriga myndigheten ska underrätta kommissionen om de dataaltruismorganisationer som registreras och om ändringar som sker, artikel 19.5 och 7.

Villkor att uppfylla

Dataaltruismorganisationen ska uppfylla de villkor som ställs upp i kapitel IV.

Transparenskrav

I artikel 20 finns transparenskrav. Där stadgas bl.a. att organisationen ska föra fullständiga och noggranna register över alla fysiska och juridiska personer som getts möjlighet att behandla data som organisationen innehar, datum eller varaktighet för behandlingen och ändamålet med den.

Den erkända dataaltruismorganisationen ska årligen sammanställa en verksamhetsrapport till den behöriga myndigheten. Denna ska innehålla information om organisationens verksamhet och en beskrivning av hur de mål av allmänt intresse för vilka uppgifter samlats in har främjats. Verksamhetsrapporten ska också innehålla en förteckning över alla fysiska och juridiska personer som tillåtits behandla den data som organisationen innehar tillsammans med en sammanfattande beskrivning av de mål av allmänt intresse som behandlingen är tänkt att uppnå. Den ska också innehålla en beskrivning av de tekniska metoder som använts, inklusive vilka metoder som använts för skydd av den personliga integriteten och dataskydd. Resultat som kan ha uppnåtts av de databehandlingar som tillåtits ska också finnas med i rapporten. Slutligen ska organisationen i rapporten också redogöra för inkomstkällor, och då i synnerhet intäkter från beviljande av tillgång till data, och utgifter.

Krav till skydd för registrerade och datainnehavare

I artikel 21 finns krav som syftar till att säkerställa skyddet för de registrerade och datainnehavare som delat sina data för altruistiska ändamål.

Den erkända dataaltruismorganisationen ska på ett klart och lättbegripligt sätt underrätta registrerade och datainnehavare om hur deras data behandlas. Den får inte använda data för några andra mål än de mål av allmänt intresse för vilka data den registrerade eller datainnehavaren tillåter. Vilseledande marknadsföring får inte användas. Dataaltruismorganisationen ska tillhandahålla verktyg för inhämtande av samtycke eller tillstånd samt för enkelt återkallande av dessa.

För behandlingen av data som innehåller personuppgifter gäller dataskyddsförordningens krav på säker behandling, information till de registrerade och personuppgiftsincidenter. I artikel 21 finns vissa motsvarande krav gällande icke-personuppgifter. Det stadgas att dataaltruismorganisationen ska vidta åtgärder för att säkerställa en lämplig säkerhetsnivå för lagring och behandling av icke-personuppgifter, samt att den ska informera datainnehavare vid otillåten överföring, tillgång eller användning av data som datainnehavaren delat.

Regelbok

Kommissionen ska genom en delegerad akt ta fram en regelbok för erkända dataaltruismorganisationer som de ska följa, artikel 22. Regelboken ska komplettera förordningen och den ska bl.a. hantera lämpliga informationskrav, lämpliga säkerhetsmässiga och tekniska krav, kommunikationsplaner för att öka medvetenhet om dataaltruism och rekommendationer om lämpliga interoperabilitets-standarder.

Kommissionen ska vidare ta fram ett formulär för samtycke till dataaltruism, artikel 25. Det är inte tvingande att använda formuläret.

Behörig myndighet och tillsyn

Varje medlemsstat ska utse en eller flera behöriga myndigheter för registrering av dataaltruismorganisationer, artikel 23. Dessa ska enligt artikel 17 föra ett nationellt register över erkända dataaltruismorganisationer. Kommissionen ska föra ett motsvarande register för hela unionen.

De behöriga myndigheterna ska övervaka och utöva tillsyn över att erkända dataaltruismorganisationer uppfyller i förordningen fastställda krav. Tillsynen får bedrivas både på eget initiativ och på begäran av en fysisk eller juridisk person.

Inom ramen för tillsynen har den behöriga myndigheten befogenhet att begära all information som är nödvändig för att kunna kontrollera uppfyllandet av kraven. En begäran om information ska vara proportionerlig och motiveras. Den behöriga myndigheten har befogenhet att kräva att överträdelser som upptäcks upphör. En erkänd dataaltruismorganisation ska också enligt artikel 24 kunna förlora sin rätt att använda beteckningen ”dataaltruismorganisation som är erkänd i unionen”. Därutöver kan olika administrativa åtgärder vidtas, såsom förelägganden om att överträdelser ska upphöra och sanktioner som medlemsstaterna ska besluta om.

De behöriga myndigheterna för dataaltruismorganisationer i olika medlemsstater ska samarbeta och bistå varandra när det behövs. Sådant samarbete kan omfatta informationsutbyte mellan myndigheterna.

Av artikel 26 framgår krav som ställs på behöriga myndigheter. De ska vara juridiskt åtskilda och funktionellt oberoende av erkända dataaltruismorganisationer. Myndigheten ska utföra sina uppgifter på ett opartiskt, transparent, konsekvent och tillförlitligt sätt och utan dröjsmål. Ledande befattningshavare och personal som är involverade i verksamheten får inte delta i någon verksamhet som kan påverka objektiviteten och integriteten i samband med bedömningar som de ska göra. Detta hindrar inte användning för personliga ändamål, artikel 26.3.

Överklagande och domstolsprocess

I kapitel V i förordningen finns bestämmelser om rätten att föra talan mot beslut från behöriga myndigheter för dataaltruismorganisationer och instrumenten att få rättslig prövning.

Fysiska och juridiska personer kan inkomma med klagomål mot erkända dataaltruismorganisationer till den behöriga myndigheten, artikel 27. Klagomål kan framföras både individuellt och kollektivt. Den behöriga myndigheten ska underrätta klaganden om hur

förfarandet fortskrider och vilka beslut som fattas, samt om rätten till ett effektivt rättsmedel enligt artikel 28.

I artikel 28 stadgas att fysiska och juridiska personer ska ha rätt till effektiva rättsmedel för sådana bindande beslut som den behöriga myndigheten för dataaltruismorganisationer kan fatta inom ramen för tillsynen. Förfaranden ska inledas i domstol i den medlemsstat där den aktuella behöriga myndigheten är belägen.

Om den behöriga myndigheten underlåter att agera på ett klagomål ska den som klagat ha rätt till omprövning hos en opartisk myndighet med rätt sakkunskap eller prövning i domstol.

5.2.3 Dataskydd och dataaltruism

Delning av data för altruistiska ändamål ska när det gäller personuppgifter ske genom samtycke. Definitionen av samtycke i dataförvaltningsförordningen är knuten till definitionen av samtycke i artikel 4.11 i dataskyddsförordningen. I artikel 7 dataskyddsförordningen finns villkor för samtycke enligt dataskyddsförordningen. Ett samtycke ska bl.a. vara frivilligt och det ska gå att återkalla när som helst. Samtycke är vidare en rättslig grund för behandling av personuppgifter enligt artikel 6.1 a dataskyddsförordningen. Ett samtycke gäller mellan den registrerade och den personuppgiftsansvarige som samlade in uppgifterna, i det här fallet den erkända dataaltruismorganisationen.

Syftet för en dataaltruismorganisation att samla in uppgifter är att själv använda uppgifterna för mål av allmänt intresse, eller att ge andra fysiska och juridiska personer möjlighet att behandla data för de mål av allmänt intresse för vilka uppgifterna samlades in. Det samtycke som den erkända dataaltruismorganisationen hämtat in avser bara behandlingen hos dataaltruismorganisationen själv. Om dataaltruismorganisationen själv ska behandla uppgifterna för mål av allmänt intresse så kan ett samtycke, rätt utformat, ge en rättslig grund för behandlingen. Om behandlingen i stället ska lämnas ut till annan för vidarebehandling så kan ett dataskyddsrättsligt samtycke inte omfatta vidarebehandlingen hos den andra aktören. Åtgärden att lämna ut uppgifterna för vidareutnyttjande kan dock, beroende på hur samtycket är formulerat, omfattas av samtycket.

I de fall uppgifterna lämnas ut från dataaltruismorganisationen till någon annan för behandling uppkommer frågan om vem som är personuppgiftsansvarig för vidarebehandlingen av uppgifterna. Om det är vidarebehandlaren som är ensamt personuppgiftsansvarig för behandlingen behöver den själv uppfylla alla krav på personuppgiftsbehandlingen i dataskyddsförordningen. Det ska bl.a. finnas en rättslig grund för behandlingen enligt artikel 6. Det samtycke som den registrerade lämnat till dataaltruism-organisationen kan inte utgöra rättslig grund för behandlingen hos vidareutnyttjaren.

Om vidarebehandlingen sker genom att de båda gemensamt fastställer ändamålen och medlen för behandlingen är de gemensamt personuppgiftsansvariga. De ska i så fall följa kraven på ett sådant gemensamt ansvar i artikel 26 dataskyddsförordningen.

Dataaltruismorganisationen har en skyldighet att informera den registrerade om hur dennes personuppgifter behandlas och till vilka de lämnas ut både enligt dataförvaltningsförordningen och dataskyddsförordningen. Dataaltruism i förordningens mening är inte datadonation där den som donerar data inte har insyn i hur denna sedan används, utan regelverket bygger på att den som delar med sig av sina data hela tiden kan följa vad uppgifterna används till.

Vidarebehandlaren har också en skyldighet att uppfylla kraven på information till de registrerade i dataskyddsförordningen. Bland annat ska information lämnas i enlighet med artikel 13 som gäller när information hämtats in från den registrerade. Skulle de vara gemensamt personuppgiftsansvariga finns i artikel 26 särskilda krav kring hur de registrerade ska informeras.

5.3 Kompletterande bestämmelser för dataförmedlingstjänster och dataaltruismorganisationer

Nedan beskrivs hur kompletterande bestämmelser om dataförmedlingstjänster och dataaltruismorganisationer föreslås regleras i svensk rätt.

5.3.1 En ny lag

Förslag: Det ska införas nationella regler om bl.a. avgifter, informationsutbyte, sanktioner och möjligheter att överklaga beslut. Detta behöver regleras i nationell författning. En ny lag benämnd lag med kompletterande bestämmelser till EU:s dataförvaltningsförordning ska införas.

Hänvisningar till dataförvaltningsförordningen i den nya lagen bör vara utformade på så sätt att de avser förordningen i den vid varje tidpunkt gällande lydelsen, s.k. dynamisk hänvisning.

Skälen för förslaget: Dataförmedlingstjänster är ett nytt begrepp i europeisk och svensk rätt. Detsamma gäller för dataaltruism. För att ramverket avseende dataförmedlingstjänster i kapitel III och avseende dataaltruismorganisationer enligt kapitel IV samt vissa förfaranderegler i kapitel V och tillhörande regler om sanktioner i kapitel IX dataförvaltningsförordningen ska vara genomförda i svensk rätt krävs att det införs nationella regler om bl.a. avgifter, register och sanktioner. Detta behöver regleras i nationell författning.

Reglerna om dataförmedlingstjänster i kapitel III data-förvaltningsförordningen gränsar till flera befintliga rätts-områden så exempelvis som konkurrensrätt och dataskydd. De har dock inte en sådan koppling till något av dessa områden att det skulle lämpa sig att införa kompletterande regler om dataförmedlings-tjänster i t.ex. konkurrenslagen eller dataskyddslagen.

Reglerna om dataaltruism gränsar i sin tur också till flera befintliga rättsområden, t.ex. dataskydd och marknadsföring. Inte heller här finns en sådan koppling till något av dessa områden att det skulle lämpa sig att införa kompletterande regler för dataaltruism-organisationer i t.ex. dataskyddslagen eller marknadsföringslagen.

Den s.k. datalagen där kompletterande bestämmelser avseende vidareutnyttjande av skyddade data enligt kapitel II dataförvaltningsförordningen föreslås införas är inte en lämplig plats. Datalagen reglerar tillgängliggörande av data från offentlig sektor för vidareutnyttjande. Reglerna avseende dataförmedlings-tjänster och dataaltruismorganisationer gäller visserligen användning av data, men inte på det sätt som avses i datalagen. Data som dataförmedlare förmedlar behöver inte komma från offentlig sektor,

och den behöver inte ha tillgängliggjorts för vidareutnyttjande på det sätt som avses i datalagen. Dataaltruismorganisationer samlar själva in data direkt från de som data avser och har som regel ingen anknytning till data som offentlig sektor tillgängliggör för vidareutnyttjande. Det finns inte några befintliga bestämmelser i datalagen som också behöver införas för dataaltruismorganisationer. Skulle reglerna införas i datalagen skulle den behöva byta rubrik, syfte och tillämpningsområde utöver att nya kapitel skulle behöva införas. En sådan genomgripande förändring skulle inte leda till tydlighet eller samordningsvinster utan snarare till ett svårtillämpat regelverk och onödigt komplexa hänvisningar.

Det bör därför införas en ny lag att komplettera dataförvaltningsförordningen i de delar som inte avser vidareutnyttjande av skyddade data från offentliga myndigheter.

Hänvisningar till dataförvaltningsförordningen i den nya lagen bör vara utformade på så sätt att de avser förordningen i den vid varje tidpunkt gällande lydelsen, s.k. dynamisk hänvisning. Förordningen kan då ändras utan att de kompletterande nationella bestämmelserna behöver justeras.

5.3.2 Ord och uttryck i lagen

Förslag: Ord och uttryck i den nya lagen ska ha samma betydelse som i dataförvaltningsförordningen.

Skälen för förslaget: I dataförvaltningsförordningen definieras flera centrala termer och begrepp som avser dataförmedling och dataaltruism i artikel 2. De begrepp som har särskild central betydelse för regleringen i kapitel III och IV dataförvaltningsförordningen är datadelning, dataförmedlingstjänst och dataaltruism. Andra begrepp definieras visserligen inte, men är av unionsrättslig karaktär och kan inte ges en särskild betydelse i nationell rätt, t.ex. begreppet tredjeland. Vissa begrepp hänför sig till annan EU-lagstiftning så som t.ex. registrerad och samtycke som är begrepp som har sin grund i dataskyddsförordningen och som definieras genom en hänvisning i dataförvaltningsförordningen.

Termer och uttryck som används i den nya lagen bör därför ha samma betydelse som i dataförvaltningsförordningen. Lagen utgör

endast ett komplement till dataförvaltningsförordningen. Det stora flertalet av de regler som ska tillämpas finns i dataförvaltningsförordningen och ska tillämpas direkt av myndigheter, företag och organisationer. Om förordningens definitioner infördes i den nya lagen skulle det kunna ge intrycket av att lagen är fristående från förordningen.[12]

5.3.3 Anmälningsförfarandet för dataförmedlingstjänster ska kunna avgiftsbeläggas

Förslag: Regeringen, eller den behöriga myndigheten efter bemyndigande från regeringen, får meddela föreskrifter om skyldighet för leverantörer av dataförmedlingstjänster att betala avgift för anmälningsförfarandet och därmed den behöriga myndighetens verksamhet som tillsynsmyndighet.

Bedömning: Nivån på avgiften bör ses över av den behöriga myndigheten efter tre år.

Skälen för förslaget och bedömningen

Anmälningsförfarandet för dataförmedlingstjänster får enligt dataförvaltningsförordningen avgiftsbeläggas i medlemsstaterna. Leverantörer av dataförmedlingstjänster ska sedan de anmält sig stå under tillsyn av den behöriga myndigheten. Avgiften får enligt artikel 11.11 dataförvaltningsförordningen omfatta administrativa kostnader för de behöriga myndigheternas övervakning av efterlevnaden och andra marknadskontrollåtgärder avseende anmälningar av leverantörer av dataförmedlingstjänster. Avgifter får därmed omfatta både anmälningsförfarandet och den efterföljande tillsynen.

[12] Jfr motsvarande bedömning avseende ord och uttryck i dataskyddsförordningen och den kompletterande dataskyddslagen, prop. 2017/18:105 s. 24-

Allmänt om avgifter för tillsyn

Tillsyn kan finansieras genom anslag till tillsynsmyndigheten eller avgifter. Finansieringen bör utformas på ett sådant sätt att både tillsynsobjekt och tillsynsorgan ges incitament att agera kostnadsmedvetet samt att utveckla en betryggande intern kontroll och styrning. Tillsyn bör i normalfallet finansieras genom avgifter (skr. 2009/10:79, s. 19).

Inom vissa områden kan det vara lämpligt att finansiera tillsynen via anslag. Det kan exempelvis vara fallet när kostnaderna för att administrera ett avgiftsuttag bedöms som höga i relation till avgiften i övrigt. Även fördelningspolitiska och effektivitetsmässiga eller andra skäl kan vara grund för att anslagsfinansiera tillsyn. Detta gäller särskilt när tillsynen avser statligt och kommunalt finansierad verksamhet (Tillsyn enligt NIS-direktivet – kostnader och finansiering, 2018:7, Statskontoret, s. 82).

En offentligrättslig avgift måste motsvaras av en tydlig motprestation, annars är det inte en avgift utan en skatt. Att avgiften ska motsvara de faktiska kostnaderna hänger samman med kravet på motprestation. Motprestationen definieras av de kostnader som enligt lag eller förordning ska täckas av avgiften. Om ingen kostnad uppstår finns heller ingen grund för en avgift (skr. 2009/10:79 s. 21).

En tillsynsavgift bör som huvudregel ha principen om full kostnadstäckning som ekonomiskt mål. Avgifterna bör vara lättbegripliga och förutsebara för tillsynsobjekten och ge incitament till avsedda beteenden hos tillsynsorganen och tillsynsobjekten. Avgifter bör inte vara konkurrenssnedvridande. Själva uttagandet av en avgift bör inte medföra höga administrativa kostnader för tillsynsorganet eller tillsynsobjekten (skr. 2009/10:79 s.20 och 21).

Avgift bör kunna tas ut från leverantörer av dataförmedlingstjänster

Den allmänna utgångspunkten är alltså att tillsynsverksamhet ska avgiftsfinansieras. Att inte avgiftsbelägga anmälningsförfarandet och tillsynen över området skulle gå emot grundprincipen om att tillsynsverksamhet ska avgiftsfinansieras och att tillsynsobjekten själva ska stå för kostnaden.

Anmälningsförfarandet bör därför kunna avgiftsbeläggas av den behöriga myndigheten.

Avgiften bör inte ha full kostnadstäckning som mål

När antalet tillsynsobjekt inte är fastställt blir möjligheten att uppskatta kostnaden per tillsyn osäker. Dessa osäkerhetsfaktorer kan leda till ett myndighetsinternt överskott eller underskott i finansieringen av tillsynen. Enligt avgiftsförordningen ska detta underskott respektive överskott balanseras efter räkenskapsårets slut, om det ekonomiska målet är full kostnadstäckning. Detta kan innebära att nytillkommande tillsynsobjekt kan få betala för tidigare års underskott (Tillsyn enligt NIS-direktivet – kostnader och finansiering, 2018:7, Statskontoret, s. 82).

Om ett tillsynsområde omfattar få tillsynsobjekt kan avgiften riskera att bli för hög. Det beror på att avgifterna ska beräknas så att den långsiktiga självkostnaden täcks, s.k. full kostnadstäckning. Detta gäller om inte regeringen har föreskrivit något annat. Det innebär att avgifterna ska beräknas så att intäkterna täcker kostnaderna på ett eller flera års sikt. Skulle de faktiska kostnaderna för tillsynen läggas på de leverantörer som kontrolleras riskerar avgiften att bli alldeles för hög.[13]

Ett skäl emot avgifter i allmänhet är enligt Tillsynsutredningen att sådana generellt sett har en viss hämmande effekt på näringsverksamhet genom att de innebär kostnader för utövarna. Exempelvis kan avgifter som är relativt höga i förhållande till företagens ekonomiska storlek hindra små företag från att vilja etablera sig på en marknad. Detta kan bli effekten av t.ex. tillståndsavgifter eller kombinerade tillstånds- och tillsynsavgifter (SOU 2004:100 s. 90).

[13] I samband med införandet av NIS-lagen utredde Statskontoret bl.a. frågan om huruvida tillsynen för NIS-lagen skulle avgiftsfinansieras. Inom ramen för utredningen genomförde de intervjuer med ett antal myndigheter. PTS lyfte i denna utredning att de har erfarenhet av avgiftsfinansierad tillsyn som fungerar väl på en marknad med ett stort antal aktiva tillsynsobjekt som avgiften kan fördelas på. Men PTS bedömde att det i det fallet var fråga om en marknad med få aktörer och att avgiftsfinansiering därför kunde vara olämplig, eftersom kostnaderna då blir stora per aktör. Det riskerar att bidra med incitament för företag att inte etablera sig på den svenska marknaden, utan att kanske hellre söka sig till länder som använder en skattefinansierad tillsyn. Utredningen redovisas i rapporten Tillsyn enligt NIS-direktivet – kostnader och finansiering, 2018:7, Statskontoret, sid. 81f.

Ett annat skäl som enligt Tillsynsutredningen talar emot avgiftsfinansiering är att det alltid innebär kostnader hos både tillsynsmyndigheten och tillsynsobjektet för att administrera avgiftssystemet. Administrationen omfattar bl.a. arbete med att beräkna storleken på avgifterna, budgetering och uppföljning av intäkter och kostnader, arbete med myndighetsföreskrifter om betalning, information och fakturering. Förutom kostnader för fakturering och annan administration kan systemet ibland också medföra kostnader för information till företagen om avgifterna eller om betalning. Avgiftssystemet måste också fortlöpande underhållas och anpassas till nya omvärldsfaktorer. Orimligt höga administrationskostnader för finansieringen minskar möjligheterna till avgiftsfinansiering av den egentliga tillsynen (SOU 2004:100 s. 90).

Avgiftsfinansiering av tillsynsverksamhet ska som huvudregel ha full kostnadstäckning som mål. När det gäller anmälningsförfarandet och tillsynen över dataförmedlingstjänster finns det dock faktorer som talar emot en sådan avgiftsmodell, i alla fall i nuläget. Framför allt finns det en betydande osäkerhet om hur stor marknaden för dataförmedlingstjänster är i dagsläget, och hur stor den kommer att vara på sikt. Om ett tillsynsområde omfattar få tillsynsobjekt kan avgiften riskera att bli för hög med full kostnadstäckning som mål. Det kan också ge hämmande effekter.

En avgift som införs bör därför inte ha full kostnadstäckning som mål då det innebär för stora osäkerhetsfaktorer och risk för negativa konsekvenser. Avgift bör i stället kunna tas ut på en proportionerlig nivå.

Närmare bestämmelser om avgiftssystemets utformning kan meddelas med stöd av bemyndigandet.

Det finns många osäkerhetsfaktorer gällande marknaden för dataförmedlingstjänster och hur denna kommer att utvecklas. Frågan om avgifter och dess utformning bör därför ses över när en sådan marknad har kunnat börja etablera sig. Nivån för avgifter och metoden för beräkning av dessa bör utvärderas av den behöriga myndigheten efter tre år då en marknad för dataförmedlingstjänster kan ha börjat etablera sig.

5.4 Behörig myndighet för dataförmedlingstjänster

Varje medlemsstat ska utse en eller flera behöriga myndigheter för dataförmedlingstjänster. Uppgiften som behörig myndighet för dataförmedlingstjänster omfattar olika delar. Dessa olika delar av uppgiften ställer krav på olika administrativa, tekniska och organisatoriska strukturer. En tidigare erfarenhet av liknande uppgifter inom den myndighet som ges uppgiften är en stor fördel, liksom upparbetad kompetens inom närliggande sakområden. Kompetenserna behöver inte finnas inom myndigheten sedan innan, men de behöver utvecklas för att kunna genomföra uppgiften.

Sammanställningen över vad uppgifterna innebär och vilka kompetenser som behövs har tagits fram i samverkan med Nobareg, en nordisk-baltisk arbetsgrupp skapad på uppdrag av nordiska ministerrådet för att samverka kring implementering av relevant EU-lagstiftning på digitaliseringsområdet, däribland dataförvaltningsförordningen. Länderna företräds av handläggare och experter från myndigheter eller departement. Sverige deltar genom en företrädare för Digg.

5.4.1 Uppgifter för behörig myndighet för dataförmedlingstjänster

Hantera anmälningar

Den behöriga myndigheten ska ta emot anmälningar från leverantörer av dataförmedlingstjänster. Att notera är att det rör sig om ett anmälningsförfarande, inte ett ansökningsförfarande. Den behöriga myndigheten behöver därför inte vidta åtgärder för att godkänna någon anmälan eller dylikt. Den behöriga myndigheten ska dock på begäran av leverantören inom en vecka från det att en komplett anmälan inkom utfärda en standardiserad förklaring som bekräftar att leverantören inkommit med en anmälan. Den behöriga myndigheten ska underrätta kommissionen på elektronisk väg om varje ny anmälan.

Att ta emot anmälningar från leverantörer av dataförmedlingstjänster är en central åtgärd som ska vidtas av den myndighet som är behörig myndighet för dataförmedlingstjänster. Att ha vana av att ta emot och bedöma olika typer av anmälningar kan därför ge stora

fördelar. En myndighet som redan gör detta kan nyttja befintliga system, processer och rutiner och den upparbetade kunskap som finns i myndigheten kring förfarandet och anpassa det till nya ärendeflöden.

Anmälningarna ska granskas för att se att de innehåller alla de uppgifter som krävs enligt art. 11.6, bl.a. namn och adress, uppgifter om bolagsform och ägarstruktur, en offentlig webbplats med viss information, kontaktperson och kontaktuppgifter, en beskrivning av dataförmedlingstjänsten samt beräknat startdatum för verksamheten.

En central fråga vid granskningen av anmälan är beskrivningen av tjänsten och om denna omfattas av definitionen av en dataförmedlingstjänst. En annan viktig aspekt är frågan om bolagsform och ägarstrukturer eftersom det finns krav på att dataförmedlingstjänsterna ska tillhandahållas i en separat juridisk person och att leverantören av dataförmedlingstjänster inte får använda de data för vilka dataförmedlingstjänsterna tillhandahålls för andra ändamål än att ställa dem till dataanvändarnas förfogande, artikel 12 a.

För att kunna göra dessa bedömningar är det centralt med kännedom inom de sakområden som är aktuella.

För dataförmedlingstjänster är en central aspekt att reglerna träffar näringsidkare och ställer villkor på utformningen av tjänster på den öppna marknaden. Kunskap om näringslivet och företagens villkor är därför viktigt. Detta avser både kunskap om de rättsliga ramar som gäller samt förståelse för marknadsfaktorer.

De villkor och definitioner som ska hanteras av myndigheten gränsar i flera delar mot konkurrensreglerna. Kunskap om konkurrensreglerna och en förståelse för faktorer som påverkar konkurrens och marknad är därför centralt.

Vissa av villkoren som avser dataförmedlingstjänsterna är av mer teknisk karaktär. Förståelse för datahantering och är därför också viktigt. Ytterligare andra villkor avser säkerhetskrav. Kunskap om säker datahantering och cybersäkerhet är därför också centralt för uppgiften.

Det finns vidare villkor som avser integritet och som gränsar mot dataskyddsreglerna. Kunskap om integritetsfrågor och grundläggande kunskap om dataskyddsreglerna och när de blir tillämpliga är därför också essentiellt.

Det regelverk som ska tillämpas av den behöriga myndigheten är i huvudsak dataförvaltningsförordningen. Kunskap inom och vana av att använda EU-rätten är därför också viktigt.

SDG-förordningen

Anmälningsförfarandet är ett förfarande som enligt artikel 36 omfattas av SDG-förordningen. Det innebär i korthet att förfarandet ska kunna genomföras digitalt med hjälp av en e-tjänst som ska vara tillgänglig gränsöverskridande inom unionen. Om e-tjänsten kräver legitimering så måste även andra medlemsstaters legitimeringar som uppfyller kraven i Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG, nedan eIDAS-förordningen, godtas. SDG-förordningen ska börja tillämpas i december 2023 i de delar som avser krav på e-tjänster.

Många myndigheter hanterar förfaranden som omfattas av SDG-förordningens bilaga II och de krav som följer av detta. Dessa myndigheter håller i nuläget på att utveckla och anpassa sina e-tjänster till de nya kraven. Det finns därför fördelar med om den myndighet som utses redan omfattas av SDG-förordningen och är en behörig myndighet enligt bilaga II till den. Om myndigheten som utses inte redan omfattas av SDG-förordningen kommer sannolikt utvecklingen av den e-tjänst som krävs att innebära större investeringar och mer omfattande rättsliga bedömningar inom myndigheten än om det ska utföras av en myndighet som redan omfattas.

Avgifter

Anmälningsförfarandet får avgiftsbeläggas i nationell rätt. Förslaget är att anmälningsförfarandet ska kunna avgiftsbeläggas i Sverige. Den behöriga myndigheten ska beräkna avgifter, ta ut avgifter och hantera dessa. Avgifter ska kunna betalas med hjälp av gränsöverskridande lösningar.

Att hantera avgifter som myndighet kräver både kunskap om hur avgifter ska beräknas samt praktiska och tekniska lösningar för att kunna begära och ta emot samt hantera avgifter. Om myndigheten som ges uppgiften som behörig myndighet har befintliga ärendehanteringar som är avgiftsbelagda så finns det fördelar med att kunna nyttja befintliga administrativa rutiner och processer samt tekniska lösningar.

Övervaka efterlevnad och utöva tillsyn

Den behöriga myndigheten ska övervaka och utöva tillsyn över leverantörerna av dataförmedlingstjänster och deras efterlevnad av kraven i kapitel III. Inom ramen för tillsynen ska olika åtgärder kunna vidtas så som underrättelser vid överträdelser, begäran om att överträdelser ska upphöra och andra administrativa åtgärder inklusive ekonomiska sanktioner.

Myndigheten ska ta emot och hantera klagomål från fysiska eller juridiska personer. Beslut som fattas inom ramen för uppgiften som behörig myndighet kan överklagas till domstol, och den behöriga myndigheten ska föra processen vidare där.

Vana av tillsynsuppdrag

Tillsynsuppgiften innehåller många olika delar. Tillsyn är en granskning för att kontrollera om krav och villkor uppfylls samt att vidta åtgärder för rättelser eller besluta om sanktioner vid eventuella överträdelser. Tillsynen ska utföras både självständigt baserat på bedömning av risker och efter klagomål.

Inom ramen för tillsynsuppdraget ska den behöriga myndigheten kunna identifiera vilka aktörer som ska granskas i ett tillsynsärende och vilka frågor som en tillsyn ska fokusera på särskilt.

En viktig del av att bedriva en effektiv tillsyn är att ge bra vägledning och information så att de som träffas av regelverket vet vad som gäller och får stöd i att göra rätt. Det kräver att det finns kanaler både för fast information och för frågor och vägledning i specifika fall. Tillsynsuppdraget innebär i det här fallet inga krav på förhandssamråd eller dylikt.

Vana av att besluta om sanktioner och processer i domstol

Den behöriga myndigheten för dataförmedlingstjänster ska inom ramen för sin roll som tillsynsmyndighet kunna besluta om sanktioner och hantera ärenden vidare i domstol. Att ha kunskap och vana av att hantera både sanktioner och domstolsprocesser är därför viktigt.

Samverkan med andra tillsynsmyndigheter

Den behöriga myndigheten ska ha ett nära samarbete med Integritetsskyddsmyndigheten, Konkurrensverket och myndigheterna som ansvarar för cybersäkerhet[14] och utbyta nödvändig information som behövs för att kunna utföra respektive uppgifter. De ska också samarbeta och utbyta information med sina motsvarigheter i andra medlemsstater.

Att myndigheter ska samverka med andra myndigheter följer av 6 § myndighetsförordningen. Erfarenhet av och vana av att samverka med andra myndigheter är därmed något som alla myndigheter kan förutsättas ha. Det kan dock finnas fördelar med att utse en myndighet som har befintlig samverkan med just de myndigheter som är aktuella i det här fallet.

Ingå i europeiska datainnovationsstyrelsen och arbete med kommissionen

Företrädare för den behöriga myndigheten ska ingå i den europeiska datainnovationsstyrelse som ska inrättas. Styrelsen ska agera som en expertgrupp och hantera ett antal olika frågor. Datainnovationsstyrelsen ska t.ex. rådge och bistå kommissionen i utarbetande av konsekvent praxis för de behöriga myndigheterna för dataförmedlingstjänster. Mer om den europeiska datainnovationsstyrelsen och dess arbetsuppgifter i avsnitt 6.

[14] I Sverige har flera olika myndigheter ansvar för olika delar av cybersäkerhetsarbetet. Försvarets radioanstalt (FRA), Försvarsmakten, Myndigheten för samhällsskydd och beredskap (MSB) och Säkerhetspolisen har inrättat ett nationellt cybersäkerhetscenter på uppdrag av regeringen. Arbetet sker i nära samverkan med Post- och telestyrelsen (PTS), Polismyndigheten och Försvarets materielverk.

Uppgiften som behörig myndighet innebär en kontinuerlig kontakt med kommissionen genom rapportering av anmälda leverantörer av dataförmedlingstjänster. Myndigheten ska också löpande samarbeta med sina motsvarigheter i andra medlemsstater. En upparbetad vana av internationellt samarbete och arbete mot kommissionen hos den myndighet som utses som behörig myndighet är därför en fördel.

5.4.2 Andra länders förslag

Vilka behöriga myndigheter andra länder avser att utse enligt artikel 13 förordningen skiljer sig åt ganska mycket åt mellan länderna.

Vissa medlemsstater avser att utse sina telekommyndigheter, bl.a. Danmark och Finland.[15] Andra kommer att låta sin konkurrens- och konsumentmyndighet vara behörig myndighet.[16]

Medlemsstater med digitaliseringsmyndigheter kommer i vissa fall att utse dessa. Vissa länder kommer att låta en och samma myndighet hantera alla nya myndighetsuppgifter som förordningen kräver även om rollerna omfattar väldigt olika frågor. Nationella statistikmyndigheter har därför varit på förslag i några medlemsstater.

Några enstaka medlemsstater överväger också att ge uppgiften som behörig myndighet till sin nationella dataskyddsmyndighet.[17]

I vissa länder kommer uppgiften som behörig myndighet att utföras av ett departement.[18]

En gemensam nämnare är att de flesta länder avser att utse samma behöriga myndigheter för dataförmedlingstjänster som för dataaltruismorganisationer.

[15] Danmark avser att utse den danska Erhversstyrelsen, vilket är ungefär näringslivsstyrelsen. De hanterar olika näringslivsfrågor, frågor om innovation och tillväxt samt ansvarar för telekomfrågor. Finland avser att utse Transport- och kommunikationsverket (Traficom). Traficom har ansvar för digitala förbindelser gällande bl.a. digital infrastruktur, tillstånd och frekvenser samt för vissa cybersäkerhetsfrågor. Därutöver hanterar de också frågor inom trafik och transport. Tjeckien avser att utse sin telekommyndighet (Czech Telecommunication Office), liksom Tyskland (Bundesnetzagentur).

[16] Nederländerna utser Autoriteit Consument & Markt som är en myndighet som hanterar både konkurrensfrågor och konsumentfrågor samt andra marknadsfrågor. Polen avser att utse sin konkurrens- och konsumentmyndighet Office of Competition and Cosumer Protection.

[17] Exempelvis Estland avser att utse sin dataskyddsmyndighet till behörig myndighet.

[18] Så är fallet i bl.a. Spanien och Belgien där motsvarigheten till finansdepartementet ska hantera uppgiften.

5.5 Behörig myndighet för registrering av dataaltruismorganisationer

Varje medlemsstat ska som beskrivits i avsnitt 5.2.2 utse en eller flera behöriga myndigheter för registrering av dataaltruism-organisationer. Nedan används det kortare begreppet behörig myndighet för dataaltruismorganisationer. Uppgiften som behörig myndighet för dataaltruismorganisationer omfattar olika delar. För att kunna utföra uppgiften som behörig myndighet för dataaltruismorganisationer krävs att olika kompetenser och administrativa och tekniska strukturer byggs upp. I avsnitt 5.5.1 beskrivs detta.

Sammanställningen har tagits fram i samverkan med Nobareg, se avsnitt 5.4.1.

5.5.1 Uppgiften som behörig myndighet för dataaltruismorganisationer

Registrering av dataaltruismorganisationer och förande av register

Den behöriga myndigheten ska föra ett uppdaterat offentligt nationellt register över erkända dataaltruismorganisationer.

Myndigheten ska ta emot ansökan om registrering från dataaltruismorganisationer och utvärdera denna. Om organisationen uppfyller kraven ska myndigheten registrera enheten i det nationella registret över erkända dataaltruismorganisationer.

Att ta emot ansökningar från dataaltruismorganisationer och föra ett register över de som uppfyller kraven är centrala åtgärder som ska vidtas av den myndighet som är behörig myndighet för dataaltruismorganisationer. Om den myndighet som utses som behörig myndighet har vana av och tekniska lösningar för att ta emot och bedöma olika typer av ansökningar och föra register kan det ge stora fördelar. Finns sådant på plats så kan befintliga system, processer och rutiner användas och anpassas för nya ärendeflöden.

Den behöriga myndigheten ska underrätta kommissionen löpande om alla registreringar i registret och underrättelser om ändringar. Det finns, till skillnad för sådana underrättelser om

leverantörer av dataförmedlingstjänster, inga formkrav för hur sådana underrättelser ska ske.

SDG-förordningen

Registreringsförfarandet är enligt artikel 36 ett förfarande som omfattas av SDG-förordningen. Det innebär i korthet att förfarandet ska kunna genomföras digitalt med hjälp av en e-tjänst som ska vara tillgänglig gränsöverskridande inom unionen. Om e-tjänsten kräver legitimering så måste även andra medlemsstaters legitimeringar som uppfyller kraven i eIDAS-förordningen godtas. Förordningen träder i de delar som avser krav på e-tjänster, i kraft i december 2023.

Många myndigheter hanterar förfaranden som omfattas av SDG-förordningens bilaga II och de krav som följer av detta. Dessa myndigheter håller i nuläget på att utveckla och anpassa sina e-tjänster till de nya kraven. Det finns därför fördelar med om den myndighet som utses redan omfattas av SDG-förordningen och är en behörig myndighet enligt bilaga II till den. Om myndigheten som utses inte redan omfattas av SDG-förordningen kommer sannolikt utvecklingen av den e-tjänst som krävs att innebära större investeringar och mer omfattande rättsliga bedömningar inom myndigheten än om det ska utföras av en myndighet som redan omfattas.

Närliggande befintlig uppgift och kunskap om sakområdet

För dataaltruismorganisationer är en central aspekt att reglerna träffar organisationer som bedriver verksamhet på icke-vinstdrivande grund för att uppfylla mål av allmänt intresse. Om den behöriga myndigheten har kunskap om hur bedömningar om vad som kan vara en icke-vinstdrivande verksamhet är det en fördel. Likaså frågan om vilka associationsformer som kan användas för sådana verksamheter. Den behöriga myndigheten behöver därför ha viss kunskap om olika associationsformer.

Den behöriga myndigheten kommer årligen att få en verksamhetsrapport som beskriver hur och vilka data som samlats in och använts och för vilka mål av allmänt intresse. Kunskap om vilka

uppgifter som kan anses vara för allmänt intresse är centralt för att kunna utvärdera dessa rapporter.

Likaså finns det krav som är av mer teknisk karaktär. Ytterligare andra villkor avser säkerhetskrav. Kunskap om säker datahantering är därför också viktigt för uppgiften.

De villkor som ska tillämpas av dataaltruismorganisationerna gränsar vad gäller personuppgifter mot dataskyddsreglerna. Samtycke ska bl.a. vara grunden för delning av personuppgifter för altruistiska ändamål. Dataförvaltningsförordningen påverkar inte tillämpligheten av dataskyddsförordningen och rollen som behörigt organ ska inte påverka dataskyddsmyndigheternas tillsyn. Den behöriga myndigheten behöver därför ha en grundläggande kunskap om dataskyddsreglerna och när dessa blir tillämpliga samt vilka frågor som faller inom dataskyddsmyndighetens tillsynsansvar.

Det regelverk som ska tillämpas av den behöriga myndigheten är i huvudsak dataförvaltningsförordningen. Kunskap inom och vana av att använda EU-rätten är därför också viktigt.

Övervaka efterlevnad och utöva tillsyn

Den behöriga myndigheten ska övervaka och utöva tillsyn över erkända dataaltruismorganisationer och deras efterlevnad av kraven i kapitel IV. En del av detta är att ta emot de årliga verksamhetsrapporterna som de erkända dataaltruism-organisationerna ska lämna enligt artikel 20.2. Inom ramen för tillsynen ska olika åtgärder kunna vidtas så som underrättelser vid överträdelser, begäran om att överträdelser ska upphöra och andra administrativa åtgärder inklusive sanktioner.

Myndigheten ska ta emot och hantera klagomål från fysiska eller juridiska personer. Beslut som fattas inom ramen för uppgiften som behörig myndighet kan överklagas till domstol, och den behöriga myndigheten ska föra processen vidare där.

Den behöriga myndigheten ska samarbeta och utbyta information med sina motsvarigheter i andra medlemsstater.

Vana av tillsynsuppdrag

Tillsynsuppgiften innehåller många olika delar. Tillsyn är en granskning för att kontrollera om krav och villkor uppfylls samt att vidta åtgärder för rättelser eller besluta om sanktioner vid eventuella överträdelser. Tillsynen ska utföras både självständigt baserat på bedömning av risker och efter klagomål.

Inom ramen för tillsynsuppdraget ska den behöriga myndigheten kunna identifiera vilka aktörer som ska granskas i ett tillsynsärende och vilka frågor som en tillsyn ska fokusera på särskilt.

En viktig del av att bedriva en effektiv tillsyn är att ge bra vägledning och information så att de som träffas av regelverket vet vad som gäller och får stöd i att göra rätt. Det kräver att det finns kanaler både för fast information och för frågor och vägledning i specifika fall. Tillsynsuppdraget innebär i det här fallet inga krav på förhandssamråd eller dylikt.

Ingå i europeiska datainnovationsstyrelsen och kontakt med kommissionen

Företrädare för den behöriga myndigheten ska ingå som en ordinarie deltagare i den europeiska datainnovationsstyrelse som ska inrättas. Styrelsen ska agera som en expertgrupp och hantera ett antal olika frågor. Datainnovationsstyrelsen ska t.ex. rådge och bistå kommissionen i utarbetande av en enhetlig praxis för dataaltruism inom unionen och tillämpningen av krav på erkända dataaltruismorganisationer. Kommissionen ska ta fram ett formulär för samtycke till dataaltruism och den europeiska datainnovationsstyrelsen ska rådge och bistå kommissionen i detta arbete.

Mer om den europeiska datainnovationsstyrelsen och dess arbetsuppgifter i kapitel 6. Uppgiften som behörig myndighet innebär en kontinuerlig kontakt med kommissionen genom rapportering av erkända dataaltruismorganisationer. Myndigheten ska också löpande samarbeta med sina motsvarigheter i andra medlemsstater.

5.5.2 Andra länders förslag

Vilka behöriga myndigheter andra länder avser att utse enligt artikel 23 i förordningen skiljer sig åt ganska mycket åt mellan länderna.

En gemensam nämnare är dock att de flesta medlemsstater avser att utse samma myndighet till behörig myndighet för dataaltruismorganisationer som för leverantörer av dataförmedlingstjänster, och att valet gjorts i första hand utifrån den myndighet som är bäst lämpad för rollen som behörig myndighet för dataförmedlingstjänster.

En beskrivning av vilka myndigheter andra länder föreslår finns i avsnitt 5.4.2.

5.6 Behöriga myndigheter – bedömningar och förslag

5.6.1 En befintlig myndighet som behörig myndighet för både dataförmedlingstjänster och dataaltruismorganisationer

Förslag: En och samma myndighet ska utses som behörig myndighet både för dataförmedlingstjänster och för dataaltruismorganisationer.

En ensam myndighet ska utses som behörig myndighet för dataförmedlingstjänster och för dataaltruismorganisationer.

En befintlig myndighet ska utföra uppgiften som behörig myndighet för dataförmedlingstjänster och för dataaltruismorganisationer.

Skälen för förslaget

Enligt förordningen ska varje medlemsstat utse en eller flera behöriga myndigheter för dataförmedlingstjänster för att utföra uppgifter i samband med anmälningsförfarandet samt att utöva tillsyn över leverantörerna. Vidare ska medlemsstaterna utse en eller flera behöriga myndigheter för erkända dataaltruismorganisationer för att utföra uppgifter i samband med ansökningsförfarandet samt

att utöva tillsyn över organisationerna. Medlemsstaterna får antingen inrätta en eller flera nya myndigheter eller förlita sig på befintliga, artikel 26.1. Uppgiften som behörig myndighet för dataförmedlingstjänster och dataaltruismorganisationer passar inte uppenbart in i någon befintlig myndighets uppgift. Bedömningen av vilken eller vilka myndigheter som bör utses får i stället göras utifrån vilken myndighet som har bäst förutsättningar för att utföra uppgiften utifrån befintliga uppgifter och förmågor.

Dataförvaltningsförordningen är den första lagstiftningsprodukten som är ett resultat av EU:s datastrategi. Som beskrivs i avsnitt 2.6 planeras för fler rättsakter på dataområdet framöver, så som t.ex. datarättsförordningen och AI-förordningen. Även inom ramen för dessa kommer det att finnas myndighetsuppgifter som ska utföras av nationella myndigheter. Genomförandet av EU:s datastrategi kommer att ställa krav på en bredare uppbyggnad av kunskap och förmåga på dataområdet hos myndigheter i Sverige. På sikt bör därför också frågan om fördelning av myndighetsuppgifter på dataområdet och uppbyggnaden av sådana kompetenser på myndigheter hanteras ur ett bredare strategiskt perspektiv. I denna promemoria görs bedömningar av vilken myndighet som bör utses för uppgiften bara utifrån kraven i dataförvaltningsförordningen.

Samma myndighet bör utses som behörig myndighet för dataförmedlingstjänster och för dataaltruismorganisationer

Uppgifterna för de behöriga myndigheterna för dataförmedlingstjänster och de behöriga myndigheterna för dataaltruismorganisationer får utföras av samma myndighet, artikel 26.1.

Uppgiften som behörig myndighet för dataförmedlingstjänster och uppgiften som behörig myndighet för dataaltruismorganisationer har många likheter. Kärnan i båda uppgifterna är att ta emot och hantera anmälningar och ansökningar för de företag och organisationer som omfattas av de respektive regelverken samt att utöva tillsyn över områdena. Den behöriga myndigheten ska kunna hantera klagomål och ska kunna utfärda sanktioner. Flera av reglerna gällande behöriga myndigheter, möjligheter att inge klagomål och överklaga beslut samt om sanktioner är också reglerade i samma artiklar i förordningen, artikel 26, 27 och 28. Båda förfarandena omfattas av SDG-förordningen, artikel 36. Detta visar på hur

snarlika ramverken och uppgifterna är. Vidare ska den behöriga myndigheten för båda uppgifterna representeras i den europeiska datainnovationsstyrelsen. De organisatoriska kraven för att kunna utföra uppgifterna är därför snarlika.

Uppgifterna i förordningen avser dock två olika tillsynsobjekt; leverantörer av dataförmedlingstjänster och erkända dataaltruism-organisationer. Respektive område har sina egna krav och villkor som ska vara uppfyllda, och de gränsar delvis mot olika befintliga rättsområden. De båda ramverken har dock det gemensamt att de på olika sätt syftar till att skapa förutsättningar för en ökad datadelning och inrättande av den europeiska datamarknaden.

Det finns i nuläget varken något större antal företag vars befintliga verksamhet träffas av definitionen av dataförmedlings-tjänster, eller organisationer som utför dataaltruismåtgärder i enlighet med förordningen. Det är därför sannolikt så att uppgifterna som behöriga myndigheter inte kommer att innebära någon större arbetsinsats, åtminstone inte inledningsvis.

Den större av de två uppgifterna kan förväntas bli behörig myndighet för dataförmedlingstjänster, varför den myndighet som är bäst lämpad för den uppgiften bör väga tyngst.

En och samma myndighet bör därför utses till behörig myndighet både för leverantörer av dataförmedlingstjänster enligt artikel 13 och för erkända dataaltruismorganisationer enligt artikel 23.

Den behöriga myndigheten ska ha tillräckliga ekonomiska resurser och personalresurser, inklusive nödvändiga tekniska kunskaper och resurser, för att kunna utföra sina uppgifter, artikel 26.5.

En enda myndighet bör utses

Sverige bör utse en ensam myndighet för uppgiften. Detta trots att tillsynen omfattar flera olika frågor och gränsar till flera olika rättsområden. Skälet för detta är framför allt att omfattningen av uppgifterna kan förväntas vara begränsad, både var för sig och tillsammans. En uppdelning av ansvar mellan olika myndigheter skulle skapa merarbete i form av samordning vilket i sig skulle kunna innebära mer arbete än vad myndighetsuppgiften som sådan innebär.

En befintlig myndighet bör utses

De centrala administrativa funktionerna för den behöriga myndigheten är att ta emot anmälningar och ansökningar om registrering samt att bedriva tillsyn. Det finns anledning att tro att ärendeflödet inte kommer att vara så stort, varken för dataförmedlingstjänsterna eller för dataaltruismorganisationerna, i alla fall under de första åren.

Det är mest effektivt att välja en myndighet som har så många befintliga kompetenser och strukturer på plats som möjligt. Skälet till detta är flera. Dels ska förordningen börja tillämpas relativt snart efter att den beslutats vilket ger kort om tid för att bygga upp helt nya rutiner, strukturer och kompetenser. Det kommer sannolikt inte heller att röra sig om stora ärendeflöden inledningsvis.

Att inrätta nya myndigheter är kostsamt och komplext. Att dessutom göra det för att hantera små ärendeflöden är dyrt och ineffektivt. De kompetenser som krävs för uppgiften finns hos befintliga myndigheter. Uppgiften bör därför fördelas på en befintlig myndighet.

5.6.2 Post- och telestyrelsen bör utses som behörig myndighet för dataförmedlingstjänster och dataaltruismorganisationer

Förslag: Post- och telestyrelsen ska utses till behörig myndighet för dataförmedlingstjänster och registrering av dataaltruismorganisationer.

Skälen för förslaget

Den behöriga myndigheten som utses för att övervaka leverantörer av dataförmedlingstjänster bör enligt skäl 44 väljas på grundval av sin kapacitet och sakkunskap avseende horisontellt eller sektorsbaserat datautbyte. Den behöriga myndigheten som utses för att övervaka erkända dataaltruismorganisationer bör enligt skäl 51 väljas på grundval av sin kapacitet och sakkunskap.

Den myndighet som redan har flest liknande administrativa och tekniska processer och mest upparbetad erfarenhet av de uppgifter och sakområden som är till nytta för utförandet av uppgifterna som behörig myndighet för både dataförmedlingstjänster och dataaltruismorganisationer är PTS. Nedan följer en beskrivning av myndighetens befintliga verksamhet och uppgift, därefter en bedömning av hur väl de nya uppgifterna passar in i myndighetens uppgift.

Post- och telestyrelsens uppgift

PTS är en förvaltningsmyndighet med ett samlat ansvar inom postområdet och området för elektronisk kommunikation. Myndigheten ska verka för att målen inom politiken för informationssamhället uppnås. Myndigheten ska, inom ramen för sina uppgifter enligt lagen (2022:482) om elektronisk kommunikation, nedan LEK, verka för att de mål som anges i lagen uppnås. Av PTS instruktion framgår även att myndigheten ska delta i nationellt och internationellt standardiseringsarbete. PTS är också en marknadskontrollmyndighet. PTS är vidare beredskaps-myndighet och sektorsansvarig myndighet enligt förordningen (2022:524) om statliga myndigheters beredskap. PTS är också en av de sju myndigheter som har uppgifter och förmågor inom cybersäkerhetsområdet och som samverkar med övriga inom Nationellt cybersäkerhetscenter.

PTS hanterar flera olika anmälnings- och registrerings-förfaranden, bl.a. anmälningar för elektroniska kommunikationsnät och -tjänster och tillstånd för paketförmedlingsverksamhet.

Myndigheten utövar tillsyn över ett flertal författningar på olika områden, t.ex. över postoperatörer, den svenska toppdomänen .se, elektronisk kommunikation, radiotillstånd och betrodda tjänster. PTS ansvarar för marknadskontroll av radioutrustning enligt radioutrustningslagen (2016:392). Inom ramen för tillsynen hanteras frågor som rör såväl integritet, säkerhet som konkurrens. PTS föreslås också blir samordnare för digitala tjänster enligt Europaparlamentets och rådets förordning (EU) 2022/2065 av den 19 oktober 2022 om en inre marknad för digitala tjänster och om ändring av direktiv 2000/31/EG, nedan DSA. Förslaget återfinns i

En inre marknad för digitala tjänster – ansvarsfördelning mellan myndigheter, SOU 2023:2. PTS har genom sina tillsynsuppgifter en bred vana av att arbeta med EU-rätt.

PTS har avgiftsfinansierad verksamhet, ca 65 procent av verksamheten finansieras genom avgifter. Det finns därför en väl upparbetad vana av att beräkna och hantera avgifter.

Myndigheten är en behörig myndighet enligt SDG-förordningen med ansvar för förfaranden enligt bilaga II. PTS har redan i dag ett antal e-tjänster. Flera av dessa finns tillgängliga genom verksamt.se. Verksamt.se skulle kunna vara en lämplig plattform också för anmälningsförfarandet för dataförmedlingstjänster och ansökningsförfarandet för registrering av dataaltruismorganisationer. PTS har befogenhet att besluta om sanktionsavgifter enligt LEK, NIS-lagen och säkerhetsskyddslagen. Det finns därför en uppbyggd kompetens om bedömning av lämpliga sanktioner samt beräkning av sanktionsavgifter och beslut om sådana.

Av relevans är även PTS omfattande och mångåriga erfarenhet av internationella samarbeten och internationell samordning, inte minst inom ramen för Organet för europeiska regleringsmyndigheter för elektronisk kommunikation (Berec), där även kommissionen deltar.

Bedömning av PTS lämplighet för rollerna

Sakkunskap

För att kunna utföra uppgiften som behörig myndighet för dataförmedlingstjänster och dataaltruismorganisationer behöver det finnas kunskap om relevanta sakområden. PTS hanterar frågor av direkt betydelse för näringslivet. Myndigheten planerar och fattar beslut t.ex. inom området radiospektrum, som kan ses som en naturresurs som staten fördelar, av stort ekonomiskt värde för företag och myndigheter.

De områden som är aktuella är framför allt konkurrens, datahantering, integritetsfrågor inklusive dataskydd, säkerhetsfrågor och viss associationsrätt. Inom ramen för sin befintliga uppgift ska PTS främja att marknaden för elektronisk kommunikation fungerar effektivt ur ett konkurrensperspektiv. Det innebär att det också på myndigheten finns befintlig kunskap inom

konkurrensområdet och om marknadsförutsättningar på området elektronisk kommunikation. På postområdet prövar PTS ansökningar från företag om tillstånd att bedriva postverksamhet Det finns därför en bra grundläggande förståelse för näringslivet och företagens villkor.

Inom ramen för befintliga tillsynsuppgifter hanterar PTS bl.a. tillsyn över integritet i elektroniska kommunikationsnät och kommunikationstjänster enligt 8 kap. 6, 8 och 9 §§, 9 kap. och 11 kap. 1 § LEK. Det innebär att det på myndigheten finns en god kännedom om integritetsfrågor och gränssnittet mot dataskyddsreglerna PTS ingår som samverkande myndighet i Nationellt cybersäkerhetscenter och utfärdar föreskrifter och allmänna råd inom säkerhetsskyddslagens område och utöver tillsyn över dessa.

PTS hanterar alltså i sin nuvarande tillsynsroll frågor rörande konkurrens, datahantering till viss del, integritetsfrågor och säkerhetsfrågor. Genom sin vana av att arbeta mot näringslivet finns också viss grundläggande kunskap gällande olika associationsformer.

Anmälnings- och ansökningsförfarande och SDG-förordningen

Den behöriga myndigheten behöver ha en rad administrativa, organisatoriska och tekniska förmågor. Dels ska den behöriga myndigheten kunna hantera ett anmälning- och registrerings-förfarande med efterföljande förande av register. PTS hanterar flera olika anmälnings- och registreringsförfaranden och har därmed befintliga rutiner, processer och system för sådan hantering

För dessa förfaranden behöver det också finnas e-tjänster som uppfyller SDG-förordningens krav. Myndigheten har redan i dag ett flertal e-tjänster. Eftersom PTS är en behörig myndighet enligt SDG-förordningen håller dessa också på att anpassas till de nya kraven. PTS kommer därför också ha tekniska lösningar som kan utnyttjas för nya e-tjänster och en upparbetad juridisk kompetens gällande SDG-förordningen.

Avgiftshantering

PTS är en till stora delar avgiftsfinansierad verksamhet. PTS har också föreskriftsrätt i olika utsträckning för flertalet avgifter som myndigheten kan ta ut. Det finns därför på myndigheten en väl upparbetad kunskap om avgiftsuttag såväl som rutiner, processer och tekniska lösningar för detta.

Tillsyn

PTS har en bred tillsynsvana med tillsyn över flera olika regelverk och olika tillsynsobjekt. PTS befintliga tillsynsuppgifter innebär att det finns en befintlig kunskap om tillsynsrollen och tillsynshantering inom myndigheten likväl som befintliga organisationer och processer som skulle kunna utnyttjas för nya tillsynsuppdrag. PTS deltar i Tillsynsforum, ett nätverk för statliga myndigheter med tillsynsuppgifter.

PTS har vidare inom ramen för befintlig tillsyn möjlighet att besluta om olika sanktioner, däribland sanktionsavgifter. Detta innebär att det finns en viss upparbetad erfarenhet av att göra bedömningar om lämpliga sanktioner för olika överträdelser samt viss vana av att fatta beslut och föra processer vidare i domstol.

PTS har inom ramen för de olika tillsynsrollerna vana av att samverka med de tillsynsmyndigheter som ramverket för dataförmedlingstjänster framförallt gränsar mot.

Inom ramen för sin befintliga uppgift ska PTS främja att marknaden för elektronisk kommunikation fungerar effektivt ur ett konkurrensperspektiv. Enligt instruktionen ska myndigheten samråda med berörda myndigheter och ta initiativ till löpande informationsutbyte. PTS ska vidare samverka med Konkurrensverket och inhämta yttranden från Konkurrensverket i vissa frågor enligt 1 och 5 kap. förordningen (2022:511) om elektronisk kommunikation. Det finns därför befintliga strukturer för samarbete med Konkurrensverket som kan nyttjas också för den samverkan som krävs i rollen som behörig myndighet för dataförmedlingstjänster.

PTS samverkar också med IMY i olika frågor inom ramen för befintlig tillsyn som rör integritet.

Den behöriga myndigheten ska också samverka med cybersäkerhetsmyndigheter. PTS har tillsynsansvar för samhällsviktiga tjänster inom sektorn digital infrastruktur samt för digitala tjänster. Myndigheten granskar om företagen uppfyller kraven i NIS-lagen och i föreskrifterna om säkerhetsåtgärder och incidentrapportering, framtagna av Myndigheten för samhällsskydd och beredskap (MSB). PTS har inom ramen för sin grunduppgift en nära samverkan med de myndigheter som är ansvariga inom ramen för Nationellt cybersäkerhetscenter.

Vana av europeiskt samarbete och kontakt med kommissionen

PTS har lång vana av att arbeta mot EU-kommissionen och att vara representanter i olika EU-sammanhang.

Myndigheten har också föreslagits få närliggande uppgifter för DSA som är ett annat EU-regelverk som rör digitalisering.[19] Det kan finnas samordningsvinster med att ansvaret för tillsynen för både dataförvaltningsförordningen och uppgiften som samordnare för digitala tjänster enligt DSA hanteras av samma myndighet.

Sammanfattning bedömning PTS

PTS har sakkunskap om för regelverket centrala områden, myndigheten har en vana av anmälningshantering och viss registerföring och den har en bred tillsynsvana. Det finns också en redan upparbetad samverkan med de angränsande tillsynsmyndigheter som den behöriga myndigheten behöver samarbete med. PTS har befogenhet att besluta om sanktionsavgifter och vana att processa i domstol. Myndigheten är också en behörig myndighet enligt SDG-förordningens bilaga II. PTS har vidare god vana av att arbeta mot EU-kommissionen och att vara representanter i olika EU-sammanhang. PTS bör därför utses till att vara behörig myndighet för dataförmedlingstjänster och dataaltruismorganisationer.

[19] PTS föreslås i delbetänkandet En inre marknad för digitala tjänster – ansvarsfördelning mellan myndigheter SOU 2023:2 få rollen som samordnare för digitala tjänster enligt artikel 49 förordningen om digitala tjänster (DSA).

5.6.3 Andra myndigheter som hade kunnat vara aktuella

Utifrån beskrivningen av de uppgifter som behöriga myndigheter för dataförmedlingstjänster och dataaltruismorganisationer ska utföra och de områden som myndigheten bör ha upparbetad vana av så finns det ett antal olika myndigheter skulle kunna vara lämpliga för rollen, men som inte föreslås i denna promemoria.

Flera myndigheter har närliggande uppgifter eller har kunskaper inom något centralt område, men har inte andra. Vid en genomgång av andra myndigheter än PTS bedöms inte någon annan myndighet ha en upparbetad vana av lika många av de aktuella uppgifterna eller samma upparbetade kompetens inom närliggande sakområden som PTS har.

Nedan följer en kortfattad beskrivning av myndigheter som har vana av vissa av de administrativa och de förmågor och sakkunskaper som krävs eller av andra skäl kan synes vara aktuella, men som inte bedöms som bäst lämpade för uppgiften.

Bolagsverket

Bolagsverkets huvudsakliga uppgift är att registrera och tillgängliggöra företagsinformation. Bolagsverkets har som grunduppgift att skapa förutsättningar för ett näringsliv med hög tillit. Det ligger i linje med det övergripande syftet med att inrätta ett ramverk för dataförmedlingstjänster. Bolagsverkets instruktionsenliga uppgift avser näringslivet vilket innebär att myndigheten har god kännedom om näringslivet, företagens villkor och förutsättningar som påverkar företagandet. Bolagsverket har också väldigt god kännedom om olika associationsformer.

Det finns på Bolagsverket en stor vana av att arbeta med anmälningar och att föra register. Myndigheten som är en behörig myndighet enligt SDG-förordningens bilaga II och den har flera e-tjänster och därmed vana av utveckling av e-tjänster. Bolagsverket är också en till stora delar avgiftsfinansierad myndighet med vana av avgiftshantering.

Bolagsverket har dock inte några befintliga tillsynsuppgifter och saknar därför grundläggande strukturer och organisation för tillsynsuppgifter. Tillsynsuppdraget ligger också långt ifrån myndighetens befintliga grunduppdrag. Bolagsverket har inte heller

befintliga uppgifter som ger specifik kunskap inom konkurrensområdet, datahantering och dataskydd utöver vad en myndighet behöver ha för sin interna hantering.

Bolagsverket säljer företagsdata och information och är därmed en aktör på den marknad där dataförmedlingstjänster agerar. Det skulle kunna innebära svårigheter för att agera som en neutral tillsynsmyndighet

Integritetsskyddsmyndigheten

Integritetsskyddsmyndigheten (IMY) är en förvaltningsmyndighet med huvudsaklig uppgift att arbeta för att människors grundläggande fri- och rättigheter skyddas i samband med behandling av personuppgifter och att underlätta det fria flödet av sådana uppgifter inom Europeiska unionen.

Relevant för dataförvaltningsförordningen och uppgiften som behörig myndighet är IMY:s uppdrag som tillsynsmyndighet för den allmänna dataskyddsförordningen i synnerhet och myndighetens kunskaper om integritetsfrågor i allmänhet. IMY är Sveriges nationella tillsynsmyndighet för behandling av personuppgifter. De granskar att bestämmelserna i dataskyddsförordningen, brottsdatalagen, kamerabevakningslagen och annan reglering på dataskyddsområdet följs, framför allt genom tillsyn. I IMY:s instruktion anges myndighetens tillsynsuppdrag.

Myndigheten har ingen anmälnings- eller registreringsverksamhet. Det finns heller inga ärenden som är avgiftsbelagda hos IMY idag.

Myndigheten har naturligtvis mycket goda kunskaper inom integritetsfrågor och dataskydd. Även frågor om säkerhet och datahantering ligger nära myndighetens grunduppgifter. Det finns ingen närmare kunskap om frågor som avser konkurrensrätt eller associationsformer.

IMY medverkar i det internationella samarbetet i flera olika sammanhang om dataskyddsfrågor bl.a. genom medverkan i den europeiska dataskyddsstyrelsen.

IMY ska som dataskyddsmyndighet vara fullständigt oberoende i utförandet av sina uppgifter och utövandet av sina befogenheter i enlighet med dataskyddsförordningen, se artikel 52.1 i

dataskyddsförordningen. Kravet på att en tillsynsmyndighet ska vara fullständigt oberoende innebär både att den ska vara fristående och självständig i förhållande till den verksamhet den är satt att övervaka och att det inte heller får förekomma någon påverkan eller instruktioner, direkt eller indirekt, från något annat håll, såsom från staten, se artikel 52.2 i dataskyddsförordningen, SOU 2016:65 s. 144 och EU-domstolens dom C-518/07.

Konkurrensverket

Konkurrensverket ska verka för en effektiv konkurrens i privat och offentlig verksamhet till nytta för konsumenterna och en effektiv offentlig upphandling till nytta för det allmänna och marknadens aktörer. Konkurrensverket har tillsynsansvar för konkurrenslagen och artiklarna 101 och 102 i fördraget om Europeiska unionens funktionsrätt.

Införandet av dataförmedlingstjänster syftar primärt till att skapa en bättre tillit och att komma åt bristande konkurrens på datadelningsmarknaden. Syftet ligger därmed i linje med det övergripande syftet med konkurrensrätten som Konkurrensverket ansvarar för att främja och utöva tillsyn över.

Konkurrensverket har tillsynsvana beträffande upphandlings- och konkurrensregelverket och befintliga befogenheter att besluta om konkurrensskadeavgift. Däremot har myndigheten inte några anmälnings- eller registreringsuppgifter. Myndigheten har inte heller några e-tjänster som liknar de som kommer att behöva tillhandahållas och är inte en behörig myndighet enligt SDG-förordningen. Konkurrensverket har heller inte några avgiftsbelagda förfaranden. Vidare saknar verket kunskap om relevanta sakområden. Konkurrensverkets nuvarande organisation baseras i grunden på att myndigheten förväntas vara expert på konkurrensrätten (konkurrenslagen och EU-fördragets konkurrensregler) oavsett inom vilken marknad och inom vilket sak- eller sektorsområde myndigheten för stunden utövar tillsyn. Myndigheten är alltså inte strukturerad eller anpassad för att över tid hålla kompetens inom specifika marknader och sakområden utan säkerställer nödvändig kompetens för stunden baserat på aktuella tillsynsärenden och uppdrag.

Konsumentverket

Konsumentverket är förvaltningsmyndighet för konsumentfrågor med ansvar för att bl.a. utöva tillsyn, inklusive marknadskontroll, enligt de konsumentskyddande regler som ligger inom myndighetens ansvarsområde. Verket ska även tillgängliggöra information och vägledning om konsumenters rättigheter och skyldigheter samt annan information som ger konsumenter goda förutsättningar att ta till vara sina intressen, om ingen annan myndighet har den uppgiften. Utöver detta ska verket stärka konsumenternas ställning på marknaden. Konsumentverket är i dag enligt 1 och 3 §§ förordningen (2009:607) med instruktion för Konsumentverket kontaktmyndighet inom EU för samarbete i konsumentrelaterade frågor som rör informationssamhällets tjänster enligt lagen (2002:562) om elektronisk handel och andra informationssamhällets tjänster (e-handelslagen) och utövar tillsyn enligt samma lag.

Konsumentverket bedriver tillsyn mot företag gällande bl.a. marknadsföring, varor och tjänsters säkerhet och avtalsvillkor i vissa fall. Myndigheten har dock inga registreringsförfaranden och ingen avgiftsbelagd verksamhet. Konsumentverket är en behörig myndighet enligt SDG-förordningen.

Myndigheten för digital förvaltning (Digg)

Digg har till uppgift att samordna och stödja den förvaltningsgemensamma digitaliseringen i syfte att göra den offentliga förvaltningen mer effektiv och ändamålsenlig.

Dataförvaltningsförordningen som helhet ligger nära de huvudsakliga frågor som Digg ansvarar för inom digitaliseringen av den offentliga förvaltningen. Som beskrivs i avsnitt 4 föreslås också Digg få vissa uppgifter kopplade till kapitel II i dataförvaltnings-förordningen.

Digg har viss tillsynsvana i och med att de idag är tillsynsmyndighet över lagen (2018:1937) om tillgänglighet till digital offentlig service, den s.k. DOS-lagen. Uppgiften är inriktad på tillsyn över offentlig förvaltning och inte över den privata sektorn. Myndigheten har inte genomfört uppgiften i den utsträckning som krävs enligt direktivet och genomförandebeslut

för direktivet (Årsredovisning 2022 Myndigheten för digital förvaltning, avsnitt 1.4.1.1).

Digg har inte något registreringsförfarande som liknar de som nu ska införas. Digg hanterar vissa avgifter inom e-legitimationsområdet.

Digg är nationell samordnare för Sverige för SDG-förordningen. Det innebär att det finns mycket goda kunskaper om SDG-förordningen och dess krav. Digg är dock inte själva en behörig myndighet enligt förordningen och har inte själva några e-tjänster som omfattas av förordningen.

Tillväxtverket

Tillväxtverket är en statlig myndighet som har regeringens uppdrag att främja hållbar näringslivsutveckling och regional tillväxt samt att genomföra delar av den europeiska sammanhållningspolitiken.

Den övergripande målsättningen med att införa den nya rollen som dataförmedlingstjänst är att skapa större tillit och ge förutsättningar för en mer hållbar och bättre konkurrensutsatt marknad som kan leda till innovation. Tillväxtverket har visserligen kunskaper om näringslivets förutsättningar, företagens villkor och förutsättningar som påverkar företagandet, men har sällan rådighet över företagandets ramvillkor. Tillväxtverket saknar dessutom specifik sakkunskap avseende horisontellt eller sektorsbaserat datautbyte.

Tillväxtverket har inte heller några befintliga tillsynsuppdrag, och inte heller några registrerings- eller anmälningsuppgifter. Med anledning av coronaviruset infördes 2020 ett tillfälligt förstärkt system med s.k. korttidspermittering där Tillväxtverket pekades ut som ansvarig myndighet (prop. 2021/22:77 s. 12). Tillväxtverket behövde på kort tid rekrytera personal och bygga upp en helt ny organisation för både ansökningar, utbetalningar och tillsyn. Omfattningen av stödet ställde stora krav på Tillväxtverket som är en mindre myndighet. Sedan 1 april 2022 hanteras korttidsstödet i stället av Skatteverket. Skälet för att uppgiften flyttades över var att det ansågs mera effektivt, bl.a. på grund av att Skatteverket har en etablerad verksamhet för kontroll (prop. 2021/22:77 s. 14). Den organisation och erfarenhet av tillsynsverksamhet som

Tillväxtverket haft finns därför inte kvar, och de personalresurser som hanterade uppgiften har lämnat myndigheten. Det saknas därför, trots denna erfarenhet i närtid, befintliga strukturer och resurser för tillsynsverksamhet.

Sammanfattning andra myndigheter

Som framgår av redogörelsen ovan finns det ett antal myndigheter utöver PTS som har en upparbetad vana och kompetens både avseende vissa administrativa förfaranden och vissa sakområden som skulle kunna användas vid fullgörandet av uppgifterna som behörig myndighet för dataförmedlingstjänster och dataaltruism-organisationer. Jämfört med PTS finns det dock ingen annan myndighet som redan har så många av de önskvärda processerna och kompetenserna som kan utnyttjas vid uppbyggnaden av den nya uppgiften på plats. Detta gäller både i avseendet kunskap inom olika sakområden samt vad gäller organisatoriska, administrativa och tekniska förmågor.

Konkurrensverket är expertmyndighet när det gäller den generella konkurrensrätten och dess tillämpning. På samma sätt har IMY bäst kunskaper inom integritets- och dataskyddsfrågor. I övrigt finns det inga särskilda sakkunskaper som talar för någon av myndigheterna.

Inte heller när det kommer till mer organisatoriska och administrativa förmågor är det någon annan myndighet som har samma bredd som PTS. Bara en av de aktuella myndigheterna har vana av olika anmälnings- och registreringsförfaranden, Bolagsverket. Bolagsverket har dock inga tillsynsuppdrag. Det finns andra myndigheter som i stället har tillsynsuppgifter som en central uppgift inom sitt befintliga uppdrag, t.ex. IMY, Konkurrensverket och Konsumentverket. Dessa myndigheters tillsynsverksamhet avser dock mer avgränsade frågor jämfört med PTS som utövar tillsyn över en mängd olika regelverk med olika aspekter så som konkurrens, integritet och säkerhet. IMY, Konkurrensverket och Konsumentverket har inte heller någon vana av olika anmälnings-förfaranden på det sätt som avses för leverantörer av dataförmedlingstjänster. De har heller ingen vana av avgiftshantering och inga befintliga e-tjänster att bygga vidare på.

IMY har därutöver ett särskilt oberoende i sin roll enligt dataskyddsförordningen som är viktigt att värna.

Digg saknar erfarenhet av och processer för många av de centrala uppgifter som krävs. Digg:s grunduppdrag avser primärt digitaliseringen av den offentliga förvaltningen. Uppgiften som behörig myndighet för dataförmedlingstjänster avser registrering och anmälning samt kontroll av företag och organisationer, inte offentlig förvaltning. Myndigheten har inte närmare kunskap om näringslivet eller företagens villkor och inte heller inom flera av de specifika sakområdena så som konkurrensrätt och associationsrätt. Myndigheten saknar erfarenhet och organisation för anmälningshantering och registerföring. Digg har en mindre tillsynsuppgift över den s.k. DOS-lagen, men denna har inte utförts den utsträckning som krävs enligt direktivet och genomförandebeslut för direktivet. Det skulle också kunna finnas svårigheter med att kombinera rollen som tillsynsmyndighet över dataförmedlingstjänster och dataaltruismorganisationer med tillhandahållandet av dataportalen. Den samordningsvinst som finns med att utse en redan behörig myndighet enligt SDG-förordningen för rollerna i dataförvaltningsförordningen finns inte eftersom den inte är en behörig myndighet enligt den förordningen. Att Digg besitter goda kunskaper i datahantering och digitalisering samt SDG-förordningen väger inte upp för dessa nackdelar.

Tillväxtverket har inte erfarenhet av anmälningsförfaranden eller befintliga strukturer eller resurser för tillsynsuppgifter. Att syftet med regelverket är i linje med myndighetens huvuduppgift och att det finns god kunskap om näringslivet väger inte upp för detta. Myndigheten är liten till storleken och har redan idag ett tämligen spretigt uppdrag med många olika komponenter. Att addera denna uppgift skulle kunna riskera att leda till fragmentering hos myndigheten. Tillsynsrollen skulle också kunna vara svår att kombinera med den roll som finansiär som Tillväxtverket har.

Sammantaget är ingen annan myndighet lika lämplig som behörig myndighet för dataförmedlingstjänster och dataaltruism-organisationer som PTS. PTS bedöms därför vara det överlägset lämpligaste alternativet.

5.7 Reglering av uppgift som behörig myndighet

Uppgifterna som behörig myndighet för dataförmedlartjänster och dataaltruismorganisationer avser i stora drag att ta emot anmälningar respektive registreringar, föra register över företag och organisationer samt att utöva tillsyn med alla delar som det omfattar.

I avsnitten som följer finns en genomgång av vilka kompletteringar som behövs i nationell rätt för dessa olika delar samt förslag på hur sådan reglering kan se ut.

5.7.1 Tillsyn

I regeringens skrivelse till riksdagen, En tydlig, rättssäker och effektiv tillsyn, skr. 2009/10:79, redovisas generella bedömningar av hur en tillsynsreglering bör vara utformad. Skrivelsen är avsedd att vara ett stöd och en vägledning vid bl.a. översyn av materiella regelverk av olika slag.

Begreppet tillsyn bör främst användas för verksamhet som avser självständig granskning för att kontrollera om tillsynsobjekt uppfyller krav som följer av lagar och andra bindande föreskrifter och vid behov kan leda till beslut om åtgärder som syftar till att åstadkomma rättelse av den objektsansvarige (skr. 2009/10:79 s. 14). Det är viktigt att tillsynsuppgiften ges tydliga ramar. Om tillsynsorganen saknar tillräckliga möjligheter att ingripa blir tillsynen ineffektiv. En väl fungerande tillsyn förbättrar förutsättningarna för en sund konkurrens.

Ramverket för tillsyn över både dataförmedlingstjänster och erkända dataaltruismorganisationer finns i dataförvaltningsförordningens kapitel III och IV. Utveckling av praxis för hur olika krav i förordningen ska tolkas av de behöriga myndigheterna kommer också att ske i den europeiska datainnovationsstyrelsen som ska inrättas. En närmare redogörelse för den och dess arbetsuppgifter finns i avsnitt 6.

Tillsyn över dataförmedlingstjänster ska ske på tillsynsmyndighetens eget initiativ, artikel 14.1 första meningen. Av artikel 14.1 andra meningen framgår att tillsyn också får inledas på grundval av en begäran från en fysisk eller juridisk person.

På samma sätt ska tillsyn över erkända dataaltruismorganisationer ske på tillsynsmyndighetens eget initiativ enligt

artikel 24.1 första meningen. Också gällande erkända dataaltruismorganisationer får tillsynsmyndigheten inleda tillsyn på begäran av en fysisk eller juridisk person, artikel 24.1 andra meningen.

Fysiska och juridiska personer har också enligt artikel 27 rätt att inkomma med klagomål mot både leverantörer av dataförmedlingstjänster och erkända dataaltruismorganisationer till den behöriga myndigheten. Ett sådant klagomål kan också leda till att den behöriga myndigheten inleder tillsyn. Närmare om klagomål i avsnitt 5.7.3 och 5.8.13.

5.7.2 Samverkan med andra tillsynsmyndigheter behöver inte regleras särskilt

Bedömning: Samverkan mellan behörig myndighet och IMY, Konkurrensverket och andra cybersäkerhetsmyndigheter behöver inte regleras särskilt.

Skälen för bedömningen: Samordning mellan tillsynsorgan är viktig, framför allt för att tillsynen ska vara effektiv, men även för att den tillsynspliktiga verksamheten inte ska störas mer än nödvändigt. Kontakter med och besök av tillsynsorgan är en del av de administrativa krav som många verksamheter behöver uppfylla. Särskilt betungande är detta för små och mindre näringsidkare. Tillsynsobjektets kontakter med tillsynsorgan kan bli än mer svåröverskådlig av att verksamheten som bedrivs är tillsynspliktig enligt flera olika regelverk. För att underlätta för tillsynsobjekten bör tillsynsorganen därför samverka, utan att för den skull sänka ambitionsnivån för tillsynen. Samtidigt ska tillsynsverksamheten bedrivas effektivt och samverkan ska inte vara kostnadsdrivande. Snarare kan en god samordning mellan tillsynsorgan öka effektiviteten och förenkla kommunikation.

Tillsynsuppgifterna för dataförmedlingstjänster och dataaltruismorganisationer gränsar mot flera andra tillsynsuppgifter. I förordningen stadgas att det är särskilt viktigt att den behöriga myndigheten för dataförmedlingstjänster etablerar ett starkt samarbete med den nationella dataskyddsmyndigheten, den nationella konkurrensmyndigheten och de nationella cybersäkerhetsmyndigheterna.

Enligt 8 § FL ska en myndighet inom sitt verksamhetsområde samverka med andra myndigheter. Krav på samarbete mellan statliga myndigheter finns även i myndighetsförordningen. I 6 § anges att förvaltningsmyndigheter under regeringen ska verka för att genom samarbete med myndigheter och andra ta till vara de fördelar som kan vinnas för enskilda samt för staten som helhet. I 26 § anges vidare att en myndighet inom ramen för sitt utredningsansvar kan begära ett yttrande från en annan myndighet. Dessa regler kring samordning gäller även i fråga om tillsyn. Reglering av samverkan mellan de aktuella tillsynsmyndigheterna är inte nödvändig, utan denna reglering bedöms som tillräcklig (jfr. skr. 2009/10:79 s. 24).

5.7.3 Klagomål

Bedömning: Det behövs inga särskilda författningsbestämmelser om fysiska eller juridiska personers rätt att lämna in klagomål eller om tillsynsmyndighetens skyldigheter att handlägga sådana klagomål inom rimlig tid.

Skälen för bedömningen: Fysiska och juridiska personer ska enligt artikel 27.1 dataförvaltningsförordningen ha rätt att inkomma med klagomål till den behöriga myndigheten för dataförmedlingstjänster mot en leverantör av dataförmedlingstjänster, eller till den behöriga myndigheten för dataaltruismorganisationer mot en erkänd dataaltruismorganisation. Den behöriga myndigheten ska enligt artikel 27.2 dataförvaltningsförordningen underrätta klaganden om hur förfarandet fortskrider och vilka beslut som fattas. Klaganden ska också informeras om möjligheten att överklaga.

Fysiska och juridiska personers rätt att inkomma med klagomål till tillsynsmyndigheten regleras därmed direkt i förordningen. Tillsynsmyndighetens skyldighet att behandla ett sådant klagomål följer av att myndigheten ska underrätta den som klagat om hur förfarandet fortskrider och vilket beslut som fattas. Någon reglering av rätten att lämna in ett klagomål eller skyldigheten för tillsynsmyndigheten att hantera detta behövs därför inte.

Om den behöriga myndigheten underlåter att vidta åtgärder med anledning av klagomålet ska berörda fysiska och juridiska personer

ha rätt till ett effektivt rättsmedel eller en tillgång till omprövning av en opartisk myndighet som besitter sakkunskap, artikel 28.3. Någon tidsgräns för när sådan underrättelse ska lämnas finns inte. Inte heller finns det någon tidsgräns för när ett slutligt besked om vilka eventuella åtgärder gentemot en leverantör av dataförmedlingstjänster eller en erkänd dataaltruismorganisation som klagomålet i förlängningen leder till. Bestämmelsen syftar till att stävja passivitet hos tillsynsmyndigheten och säkerställer att den klagande hålls underrättad om handläggningen av ärendet.

Ett uppenbart ogrundat klagomål bör kunna besvaras av tillsynsmyndigheten utan att några särskilda åtgärder vidtas och inom en kortare tid, i vart fall inom några månader. I andra fall kan tillsynsmyndigheten ha anledning att utnyttja sina tillsynsbefogenheter enligt artikel 14 eller 24. Besked om huruvida sådan tillsyn ska utövas eller inte bör i princip också kunna lämnas till den som lämnat klagomålet inom några månader. I de undantagsfall ett sådant besked inte kan ges bör tillsynsmyndigheten i vart fall kunna lämna besked om hur ärendet fortskrider. Tillsynsmyndighetens informationsplikt gentemot den klagande är då uppfylld.

Vid sidan av dataförvaltningsförordningens direkt tillämpliga bestämmelser om tillsynsmyndighetens skyldigheter att handlägga klagomål gäller skyndsamhetskrav och informationsskyldighet enligt förvaltningslagens allmänna bestämmelser. För det undantagsfall att den klagande inte skulle få något besked från tillsynsmyndigheten rörande klagomålet inom rimlig tid, kan den registrerade vända sig till Riksdagens ombudsmän och göra en anmälan om brister i handläggningen.

Riksdagens ombudsmän har också befogenhet att väcka åtal om tjänstefel. Om den klagande anser att tillsynsmyndighetens dröjsmål lett till skada kan denne också begära skadestånd enligt skadeståndslagen, antingen genom att väcka talan i allmän domstol eller genom att framställa kravet direkt till myndigheten. Enligt förordningen (1995:1301) om handläggning av skadeståndsanspråk mot staten kan en skadelidande få ett sådant skadeståndskrav prövat inom ramen för statens frivilliga skadereglering.

Slutligen bör det noteras att även 12 § förvaltningslagen, som ger den enskilde rätt att föra en dröjsmålstalan mot myndigheten vid långsam handläggning, skulle kunna aktualiseras i ett ärende som initierats genom ett klagomål, men då avseende tillsyns-

myndighetens slutliga avgörande. Detta förutsätter dock att den klagande anses ha ställning som part i förvaltningslagens mening.

Sammanfattningsvis bedöms svensk rätt innehålla effektiva rättsmedel som är tillgängliga för den klagande om tillsynsmyndigheten inte skulle uppfylla sin informationsskyldighet enligt dataförvaltningsförordningen.

5.7.4 Associationsformer för dataaltruismorganisationer

För att kvalificera sig för registrering i ett nationellt register över erkända dataaltruismorganisationer ska organisationen uppfylla vissa krav uppställda i artikel 18. Organisationen ska vara en juridisk person som bildats för att uppfylla mål av allmänt intresse och bedriver verksamhet på icke-vinstdrivande grund och är fristående från enheter som driver verksamhet på vinstdrivande grund. Detta krav påverkar vilka svenska associationsformer som är möjliga att använda för en erkänd dataaltruismorganisation. Det är inte möjligt att på förhand uteslutande avgöra vilka associationsformer som är möjliga att använda för att uppfylla kraven. Frågan regleras direkt i förordningen och det är EU-domstolen som ytterst har att uttolka innebörden av den.

Den organisation som ansöker om att registreras som en erkänd dataaltruismorganisation bör redogöra för hur den uppfyller kraven som en vägledning för den behöriga myndigheten.

En enskild näringsverksamhet uppfyller inte kraven då det inte är en juridisk person. Aktiebolag är som huvudregel vinstdrivande, 3 kap. 3 § aktiebolagslagen (2005:551). Ett privat aktiebolag kan vara ett aktiebolag med särskild vinstutdelningsbegränsning enligt bestämmelser i kap. 32 aktiebolagslagen.

Idéburna organisationer som regleras i lag (2022:900) om registrering av idéburna organisationer kan vara icke-vinstdrivande associationer. En idéburen organisation är en juridisk person som uteslutande har ett allmännyttigt syfte, 2 §. En idéburen organisation ska bedriva offentligt finansierad välfärdsverksamhet eller ha för avsikt att bedriva sådan verksamhet, 3 §. Staten, en region eller kommun får dock inte ha ett rättsligt bestämmande inflytande över organisationen. En idéburen organisation som uppfyller kraven

ska registreras hos Kammarkollegiet som också utövar tillsyn över de idéburna organisationerna.

En ideell förening har ett ideellt ändamål men kan bedriva ekonomisk verksamhet för att främja sitt ideella ändamål. Sådana föreningar kan bedriva icke vinstdrivande verksamhet. Det finns ingen särskild civilrättslig lagstiftning som reglerar ideella föreningar, men det finns rättspraxis kring vad som räknas som ideell förening och hur en ideell förening bildas. Även stiftelser bedriver som utgångspunkt icke vinstdrivande verksamhet.

5.8 Sanktioner

Medlemsstaterna ska enligt artikel 34 i förordningen fastställa sanktioner för överträdelser av vissa bestämmelser i dataförvaltningsförordningen. Sanktionerna ska vara effektiva, proportionella och avskräckande.

Stora skillnader mellan sanktionsreglerna i olika medlemsstater skulle kunna snedvrida konkurrensen på den inre marknaden. I det avseendet skulle det enligt skäl 55 vara fördelaktigt med en harmonisering av sanktionsreglerna. Medlemsstaterna ska i sina regler om sanktioner ta hänsyn till den europeiska datainnovationsstyrelsens rekommendationer, artikel 34.1. Några sådana finns ännu inte på plats då styrelsen inrättas först när förordningen ska börja tillämpas den 24 september 2023.

5.8.1 Överträdelser som ska ge en sanktion

Medlemsstaterna ska införa sanktioner för överträdelser av skyldigheter om överföring av icke-personuppgifter till tredjeländer enligt artiklarna 5.14 och 31. I artikel 5.14 regleras ramarna för tredjelandsöverföringar för den som vidareutnyttjar vissa kategorier av skyddade data från offentliga myndigheter enligt kapitel II förordningen. I artikel 31 regleras internationell tillgång till och överföring av icke-personuppgifter och den träffar såväl offentliga myndigheter, vidareutnyttjare av skyddade data enligt kapitel II som leverantörer av dataförmedlingstjänster och erkända dataaltruism-organisationer.

Sanktioner ska också kunna utgå vid överträdelser mot anmälningsskyldigheten för dataförmedlingstjänster enligt artikel 11 och villkoren för tillhandahållande av sådana tjänster enligt artikel 12. Av artikel 14.4 framgår också att den behöriga myndigheten för dataförmedlingstjänster genom administrativa förfaranden får ålägga leverantörerna avskräckande ekonomiska sanktioner. Dessa får inbegripa löpande viten och sanktioner med retroaktiv verkan.

Överträdelser av villkoren för registrering som erkänd dataaltruismorganisation enligt artiklarna 18, 20, 21 och 22 ska också kunna ge sanktion.

Det anges inte i förordningen att någon ska ha tillsynsansvar över vidareutnyttjare av skyddade data. För dataförmedlingstjänster och dataaltruismorganisationer ska den behöriga myndigheten ha tillsynsansvar.

5.8.2 Generellt om sanktioner

Det finns ingen legaldefinition av begreppet sanktion. En sanktion ska ha ett handlingsdirigerande eller bestraffande syfte. Sanktioner kan sägas omfatta alla former av påföljder som kan följa på ett rättsstridigt handlande. De sanktionsverktyg som normalt står till buds för staten är straff och sanktionsavgifter samt vite, förbud och återkallelse av tillstånd.

Sanktioner vid tillsyn bör vara proportionerliga i förhållande till de konstaterade bristerna. De olika möjligheter till sanktioner som är tillgängliga för ett tillsynsorgan bör därför kunna användas vid såväl mindre som mer allvarliga brister i en verksamhet. Ingripandena kan då anpassas till den enskilda situationen (skr. 2009/10:79 s. 41).

När en konstaterad brist är allvarlig bör verksamheten antingen kunna få sitt tillstånd återkallat eller, vid verksamhet som inte är tillståndspliktig, förbjudas.

Ingripanden vid tillsyn har inte enbart ett bestraffande syfte. De ska även ha en framåtsyftande funktion och tillse att regler följs i framtiden. Samtidigt är det viktigt att tillsynsorganen kan ingripa mot regelöverträdelser där överträdelsen inte går att göra ogjord (skr. 2009/10:79 s. 42).

5.8.3 Överträdelser ska inte vara straffbelagda

Bedömning: Överträdelser av dataförvaltningsförordningen bör inte vara straffsanktionerade.

Skälen för bedömningen: Kriminalisering som metod för att försöka hindra överträdelser av olika normer i samhället bör användas med försiktighet. Ett skäl till detta är att en alltför omfattande kriminalisering riskerar att undergräva straffsystemets brottsavhållande verkan, särskilt om rättsväsendet inte kan beivra alla brott på ett effektivt sätt. Ett annat skäl är att kriminalisering innebär påtagliga inskränkningar i medborgarnas valfrihet och ingripande tvångsåtgärder mot dem som begår brott.

När det gäller överträdelser av reglerna i dataförvaltningsförordningen utgör straff inte en särskilt effektiv sanktion, eftersom det i många fall är svårt att identifiera en fysisk person som ansvarig för överträdelsen samt att leda i bevis att denne haft uppsåt eller varit oaktsam på det sätt som krävs för straffbarhet.

Att i stället införa tillräckligt avskräckande sanktioner som kan drabba företag eller organisation som inte följer förordningen bör ha en hög avskräckande effekt och leda till att efterlevnaden av regelverket prioriteras högt.

Vidare kan införandet av straff aktualisera det dubbelprövningsförbud som gäller enligt Europakonventionen och EU:s stadga om de grundläggande rättigheterna samt göra det svårt för leverantörer av dataförmedlingstjänster och dataaltruismorganisationer att förutse vilken sanktion som kan komma i fråga för vilken överträdelse.

Dessa omständigheter talar för att överträdelser av dataförvaltningsförordningen inte bör straffsanktioneras.

5.8.4 Förelägganden mot dataförmedlingstjänster ska kunna förenas med vite

Förslag: Den behöriga myndigheten ska kunna förena sina förelägganden mot leverantörer av dataförmedlingstjänster enligt artikel 14 dataförvaltningsförordningen med vite.

Skälen för förslaget: Av artikel 14.4 framgår att den behöriga myndigheten för dataförmedlingstjänster genom administrativa förfaranden får ålägga leverantörerna avskräckande ekonomiska sanktioner. Dessa får inbegripa löpande viten och sanktioner med retroaktiv verkan.

Att ha möjlighet att hämta in uppgifter från den objektsansvarige är ett viktigt redskap i all slags tillsynsverksamhet. De inhämtade uppgifterna ingår i underlaget för tillsynsorganets granskning och beslut. En sådan möjlighet finns gentemot leverantörer av dataförmedlingstjänster i artikel 14.2. Om den som uppgiftsskyldigheten åvilar motsätter sig att lämna ut uppgifter bör denne vid vite kunna föreläggas att uppfylla sin skyldighet.

Om den behöriga myndigheten finner att en leverantör av en dataförmedlingstjänst inte uppfyller ett eller flera krav ska den meddela leverantören detta och ge den möjlighet att yttra sig, artikel 14.3. Ett sådant meddelande är inte ett föreläggande och ska därför inte kunna förenas med vite.

Ett tillsynsorgan bör ha en möjlighet att besluta om förelägganden i enskilda fall. Möjligheten att utforma föreläggandet för att kunna styra beteendet hos den objektsansvarige bör vara brett och i princip ansluta till tillsynens omfattning. Föreläggandets utformning skapar möjligheter för tillsynsorganet att anpassa ett ingripande efter vad som är behövligt ur sektorslagens perspektiv. Ett åtgärdsföreläggande bör kunna förenas med vite (skr. 2009/10:79 s. 44).

I dataförvaltningsförordningen finns möjligheter att utfärda ett sådant åtgärdsföreläggande till leverantörer av dataförmedlingstjänster i enlighet med artikel 14.4. Dessa bör kunna förenas med vite.

Dubbelprövningsförbudet kan aktualiseras då vite utdöms för gärningar som också kan leda till sanktionsavgifter. Frågan behandlas i avsnitt 5.8.11.

Föreläggande av vite ska ske i enlighet med lagen (1985:206) om viten, vilken bl.a. innebär att vitesförelägganden ska delges (2 §) och att utdömande av viten prövas av förvaltningsrätt på ansökan av den myndighet som utfärdat vitesföreläggandet (6 §).

5.8.5 Den behöriga myndigheten ska kunna utfärda erinran

Förslag: Den behöriga myndigheten ska kunna utfärda en erinran mot leverantörer av dataförmedlingstjänster och dataaltruism-organisationer.

Skälen för förslaget: För en hög regelefterlevnad på lång sikt är det viktigt att kontakterna mellan tillsynsmyndigheten och tillsynsobjekten sker med förtroende och respekt, vilket främjas av ett stort inslag av kommunikation. Innan ett ingripande görs kan det i vissa fall vara aktuellt med påpekanden och rekommendationer för att få till stånd en frivillig rättelse.

I dataförvaltningsförordningen finns möjligheter för den behöriga myndigheten att inom ramen för tillsynen meddela en leverantör av en dataförmedlingstjänst eller dataaltruism-organisation som inte uppfyller tillämpliga krav om de iakttagelser som gjorts och ge dem möjlighet att yttra sig inom 30 dagar, artikel 14.3 respektive 24.3.

Den behöriga myndigheten har vidare möjlighet att kräva att leverantör av en dataförmedlingstjänst inte inleder sin verksamhet eller upphör med verksamheten vid en viss tidpunkt eller omedelbart, artikel 14.4 b och c. Den behöriga myndigheten får också besluta att återkalla rätten att använda beteckningen ”dataaltruismorganisation som är erkänd i unionen”, artikel 24.5.

Beslut av detta slag innebär att den tillsynspliktiga verksamheten måste upphöra och utgör därför de allvarligaste ingripande-åtgärderna vid tillsyn. När det föreligger klara skäl för att återkalla rätten att använda beteckningen respektive att förbjuda en viss verksamhet, men där det av omständigheterna i det enskilda fallet framgår att det föreligger särskilda skäl att underlåta detta, kan en lämplig form av ingripande vara att utfärda en varning eller en erinran (skr. 2009/10:79 s. 43f).

Den behöriga myndigheten bör därför kunna utfärda en erinran. Erinran ska kunna användas vid sådana överträdelser som tillsynsmyndigheten bedömer behöver resultera i någon sanktion men där det inte finns skäl att besluta om att dataförmedlings-tjänsten ska avbrytas eller att dataaltruismorganisationen inte längre ska få vara registrerad som en erkänd sådan. För dataförmedlings-

tjänster kan i stället sanktionsavgifter vara en lämplig sanktion vid allvarligare överträdelser, se vidare i avsnittet nedan.

5.8.6 Sanktionsavgifter för leverantörer av dataförmedlingstjänster

Förslag: Den behöriga myndigheten för dataförmedlingstjänster får ta ut en sanktionsavgift från en leverantör av en dataförmedlingstjänst för överträdelser mot anmälningsskyldigheten, villkoren för tillhandahållande och för villkoren för överföring av icke-personuppgifter till tredjeland i dataförvaltningsförordning.

Skälen för förslaget: Tillsynsarbetet för dataförmedlingstjänster behöver vara både framåtsyftande för att åstadkomma förbättringar på marknaden för dataförmedlingstjänster och att ingripa mot tidigare fel och brister.

Leverantörer av dataförmedlingstjänster måste arbeta systematiskt, kontinuerligt och framåtsyftande för att leva upp till kraven i dataförvaltningsförordningen. Leverantörer av dataförmedlingstjänster är vinstdrivande företag som verkar i konkurrens med varandra. Det är därför nödvändigt att regleringen är utformad så att den ger aktörerna tillräckliga drivkrafter att följa de krav som uppställs.

Ett föreläggande enligt artikel 14 dataförvaltningsförordningen, med eller utan vite, är en åtgärd som kan vidtas först i efterhand när en överträdelse redan har skett. Det syftar endast till att åstadkomma framtida rättelse. Om en aktör på eget initiativ åtgärdar påtalade brister under handläggningen av ett tillsynsärende blir ett föreläggande inte aktuellt.

Erinran är en sanktion som också omfattar överträdelser som redan skett. Detta är fullt tillräckligt som sanktion vid vissa överträdelser, men det kan också finnas behov av sanktioner som ger mer kännbar effekt även ekonomiskt. En sanktionsavgift är en lämplig sådan sanktion som ger möjlighet att ingripa i efterhand mot en överträdelse som skett. Om sådana verktyg saknas riskerar man att skapa en marknad där aktörer inte vidtar åtgärder innan tillsynsmyndigheten vidtar tillsynsåtgärder. Vidare finns det

möjligheter för aktörer att undvika att vidta förebyggande åtgärder i enlighet med förordningen som egentligen skulle vara motiverade om inte sanktionsavgifter finns.

En sanktionsavgift riktar sig mot en konstaterad överträdelse av en författningsbestämmelse. Om sanktionsavgiften innebär en risk för en kostnad eller förlust som väger tyngre än den besparing som görs genom att regelverket inte följs skapar avgiften incitament att undvika överträdelser.

Utformningen av en sanktionsavgift vid tillsyn bör uppfylla de principer om sanktionsavgifters användningsområde och utformning som angavs i förarbetena till bestämmelsen om förverkande i 36 kap. 4 § brottsbalken (prop. 1981/82:142 s. 77). Enligt dessa principer bör sanktionsavgifter användas inom områden där regelöverträdelser är särskilt frekventa eller där det föreligger speciella svårigheter med att beräkna storleken av den vinst eller besparing som uppnås i det enskilda fallet. Avgifter bör vidare endast förekomma inom speciella och klart avgränsade rättsområden där det relativt lätt kan fastställas om en överträdelse skett eller inte. Sanktionsavgifter bör kunna beräknas utifrån parametrar som gör det möjligt att i förväg förutse och fastställa avgiftens storlek (skr. 2009/10:79 s. 46).

Överträdelser som får leda till sanktionsavgift

Sanktionsavgifter bör kunna komma i fråga för leverantörer av dataförmedlingstjänster för överträdelser mot anmälningsskyldigheten enligt artikel 11, villkoren för tillhandahållande enligt artikel 12 dataförvaltningsförordningen samt för villkoren för överföring av icke-personuppgifter till tredjeland enligt artikel 31. Det är för överträdelser av dessa artiklar som leverantörer av dataförmedlingstjänster gör sig skyldiga till som sanktioner ska införas enligt artikel 34.

Sanktionsavgiftssystemet bör bygga på strikt ansvar

Huvudregeln är att sanktionsavgifter bygger på strikt ansvar, dvs. att avgiften tas ut oberoende av om överträdelsen har skett med uppsåt eller berott på oaktsamhet. När det gäller de överträdelser som nu är

aktuella finns det ett starkt stöd för en presumtion om att överträdelser inte förekommer annat än som en följd av uppsåt eller oaktsamhet. Det finns därför inte skäl att frångå huvudregeln om strikt ansvar.

Tillsynsmyndigheten bör besluta om sanktionsavgift

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

En fördel med att tillsynsmyndigheten fattar beslut är att handläggningen kan bli snabbare eftersom inte flera myndigheter måste delta i hanteringen.

Den föreslagna sanktionsavgiftsbestämmelsen bygger på strikt ansvar. Det är tillsynsmyndigheten, PTS, som i första hand kommer att få kännedom om överträdelser av bestämmelserna, som också har bäst förutsättningar att utreda och bedöma om någon inte har följt det gällande regelverket. Det bör vidare beaktas att PTS har befogenheter att besluta om sanktionsavgifter på andra områden, både enligt 12 kap. LEK och 29 § NIS-lagen.

Sammanfattningsvis bör det vara tillsynsmyndigheten som beslutar om sanktionsavgift enligt den nya lagen.

5.8.7 Sanktionsavgift ska inte kunna tas ut av dataaltruismorganisationer

Bedömning: Sanktionsavgifter bör inte kunna tas ut av dataaltruismorganisationer.

Skälen för bedömningen: Sanktionsavgifter bör inte kunna tas ut av dataaltruismorganisationer. Detta för att ramverket för dataaltruismorganisationer är ett frivilligt ramverk. Dataaltruism-

organisationer är vidare icke-vinstdrivande organisationer. Alltför hårda sanktioner med potentiellt starka ekonomiska effekter riskerar att bli oproportionerlig för sådana organisationer. Erinran bedöms jämte de åtgärder som dataförvaltningsförordningen erbjuder som tillräckligt.

5.8.8 Sanktionsavgifter för vidareutnyttjare

Förslag: Den behöriga myndigheten för dataförmedlingstjänster får ta ut en sanktionsavgift från en vidareutnyttjare för överträdelser mot villkoren för överföring av konfidentiella data till tredjeland i dataförvaltningsförordningen.

Skälen för förslaget: En myndighet som överför s.k. konfidentiella data till en vidareutnyttjande för överföring till tredjeland får bara göra det i enlighet med vissa krav i artikel 5. Med konfidentiella data avses data som skyddas som affärshemligheter (se avsnitt 3.3) eller av statistiksekretess (se avsnitt 3.4), artikel 5.8. Data som innehåller personuppgifter eller immaterialrättsligt skyddat material är inte konfidentiella data enligt art. 5.10. Om en vidareutnyttjare som får tillgång till konfidentiella data för överföring till tredje land bryter mot artikel 5.14, som i sin tur hänvisar tillbaka till artikel 5.10, 5.12 och 5.13, ska den kunna träffas av en sanktion enligt artikel 34.

Det finns ingen tillsynsmyndighet som ska övervaka regelverket i kapitel II där artikel 5 återfinns. Medlemsstaterna ska själva bedöma vem som lämpligast ska kunna besluta om sanktioner för överträdelser av artikel 5.14.

En överträdelse av bestämmelsen innebär en risk för att konfidentiella uppgifter hanteras felaktigt och kommer i orätta händer. Den sanktion som bör bli aktuell är därför sanktionsavgift. Någon annan mildare sanktion bör inte införas.

Alla andra sanktioner som ska kunna utgå enligt förordningen avser leverantörer av dataförmedlingstjänster och dataaltruism-organisationer. Det är den behöriga myndigheten som utövar tillsyn över dessa som kan besluta om sådana sanktioner, och dessa beslut ska sedan kunna överklagas till allmän förvaltningsdomstol. Den behöriga myndigheten bör därför också vara den som fattar beslut

om sanktionsavgift för överträdelser mot artikel 5.14. Det bör ske efter anmälan av den myndighet som lämnade ut konfidentiella data för vidareutnyttjande eftersom det är den myndigheten som har kännedom om när data lämnats ut för överföring till tredje land och därmed kan få kännedom om överträdelser. Myndigheten bör ha skyldighet att göra en sådan anmälan om den får kännedom om en överträdelse av artikel 5.14, se avsnitt 4.5.5.

Genom att låta den behöriga myndigheten för dataförmedlingstjänster besluta om sanktionsavgifter samlas alla sanktionsmöjligheter enligt dataförvaltningsförordningen hos ett organ och i en och samma lag.

Ett alternativ till att låta den behöriga myndigheten för dataförmedlingstjänster fatta beslut om sanktionsavgifter skulle vara att ge de behöriga organen eller ett av de behöriga organen enligt artikel 7 befogenhet att fatta sådana beslut. En sådan uppgift ligger dock långt ifrån uppgiften som behörigt organ som i stället avser stöd till utlämnande myndigheter. Ingen av de myndigheter som föreslås för uppgiften har heller i dag någon sådan befintlig uppgift där de beslutar om sanktioner. Av skäl 26 framgår också att de behöriga organen inte bör ha någon tillsynsfunktion.

Ett annat alternativ hade varit att ge de myndigheter som medger att konfidentiella data får överföras till tredje land befogenhet att besluta om en sanktion vid överträdelser. Vid en sådan konstruktion skulle det vara svårt att få till en sammanhållen tillämpning av regelverket då det potentiellt skulle behöva kunna tillämpas av en stor mängd myndigheter.

5.8.9 Sanktionsavgiftens storlek

Förslag: Sanktionsavgiften ska bestämmas till lägst 5 000 kronor och högst 10 000 000 kronor.

Skälen för förslaget: Sanktionsavgifter kan vara utformade på olika sätt. De kan avse på förhand bestämda belopp, oavsett vem som begått överträdelsen, ett beloppsintervall eller vara kopplade till årsomsättning i näringsverksamhet. Överträdelser av de bestämmelser som ska kopplas till sanktionsavgiftssystemet kan vara av högst varierande art och karaktär. Bestämmelserna bör därför

utformas så att en sanktionsavgift i varje enskilt fall kan tas ut med ett proportionellt belopp. Ett system med ett bestämt beloppsintervall bedöms därför vara lämpligast.

För att uppfylla kravet på effektiva, proportionella och avskräckande sanktioner bör beloppsintervallet vara förhållandevis stort. Tillsynsmyndigheten får då möjlighet att göra en nyanserad bedömning i det enskilda fallet när avgiftens storlek ska bestämmas.

Beloppsintervallet varierar mellan olika rättsområden. På miljöområdet och arbetsmiljöområdet är intervallet 1 000–1 000 000 kronor. I lagarna på produktsäkerhetsområdet är intervallet normalt 5 000–5 000 000 kronor. Enligt resegarantilagen (2018:1218) är intervallet 5 000–10 000 000 kronor. Enligt spellagen (2018:1138) är beloppet lägst 5 000 kronor och högst 10 procent av licenshavarens årsomsättning. För upphandlingsskadeavgift enligt lagen (2016:1145) om offentlig upphandling gäller ett intervall om 10 000 – 10 000 000 kronor. I både LEK och NIS-lagen har det lägsta beloppet satts till 5 000 kronor och det högsta till 10 000 000 kronor.

Eftersom det inte finns någon befintlig marknad är det svårt att avgöra vilka beloppsgränser som kan vara rimliga. Dataförmedlingstjänster kommer att kunna erbjudas av såväl mikroföretag som av stora globala företag. Intervallet måste därför vara stort på en möjlig sanktionsavgift. Utifrån detta är bedömningen att en rimlig lägsta nivå på sanktionsavgiften är 5 000 kronor. För att avgiften ska få en tillräckligt avskräckande effekt för alla aktörer krävs att den övre gränsen för avgiften sätts relativt högt. För att kunna ge utrymme för en effektiv, proportionell och avskräckande sanktion även vid allvarliga överträdelser bör det högsta beloppet vara 10 000 000 kronor.

Sanktionsavgift bör sammanfattningsvis kunna tas ut med lägst 5 000 kronor och högst 10 000 000 kronor.

5.8.10 Hur sanktionsavgiften ska bestämmas i det enskilda fallet

Förslag: När avgiftens storlek bestäms ska särskild hänsyn tas till

1. överträdelsens art, allvar, omfattning och varaktighet,

5. eventuella åtgärder som leverantören av dataförmedlingstjänster vidtagit för att begränsa eller avhjälpa den skada som överträdelsen har orsakat,
6. tidigare överträdelser som leverantören av dataförmedlingstjänster har gjort sig skyldig till,
7. de ekonomiska vinster som leverantören av dataförmedlingstjänster gjort eller de förluster som de undvikit till följd av överträdelsen, och
8. andra försvårande eller förmildrande omständigheter.

Tillsynsmyndigheten ska få avstå från att ta ut avgiften helt eller delvis om överträdelsen är ringa eller ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften.

Skälen för förslaget: När sanktionsavgiftens storlek ska bestämmas i det enskilda fallet bör hänsyn tas till alla relevanta omständigheter. Det är inte möjligt att på förhand ange vad som ska beaktas i varje enskilt fall. Av artikel 34.2 framgår vissa vägledande kriterier som ska beaktas vid utdömande av sanktioner.

Överträdelsens art, allvar, omfattning och varaktighet är det första kriteriet. Genom dessa ges ett utrymme för att beakta närmare vad överträdelsen avsett, vad den fått för effekt och hur omfattande den varit både i sig själv och vad gäller varaktighet i tid.

Om en leverantör av dataförmedlingstjänster vidtagit åtgärder för att begränsa de negativa effekterna som en överträdelse haft eller kunnat få, eller att avhjälpa en skada så bör det tala i mildrande riktning vid bestämmande av sanktionsavgiften. Om leverantören av dataförmedlingstjänster tidigare gjort sig skyldig till överträdelser bör det i stället tala i försvårande riktning. Även andra förmildrande och försvårande omständigheter bör kunna beaktas.

En överträdelse av dataförvaltningsförordningens regler kan innebära att leverantören av dataförmedlingstjänster gjort ekonomiska vinster eller undvikit ekonomiska förluster. Sådana ekonomiska vinster och förluster bör direkt påverka storleken på sanktionsavgiften.

Det bör anges i lagen att dessa kriterier ska beaktas särskilt när sanktionsavgiften bestäms. Dessa omständigheter kan i det enskilda

fallet påverka beloppets storlek både i försvårande och förmildrande riktning.

I och med att sanktionsavgiftssystemet bygger på ett strikt ansvar bör det finnas utrymme för att sätta ned sanktionsavgiften eller låta den helt falla bort. Det bör därför framgå av lagen att tillsynsmyndigheten får avstå från att ta ut avgiften helt eller delvis om överträdelsen är ringa eller ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften. Det kan t.ex. vara fråga om en bagatellartad överträdelse som inte har varit till men för något allmänt eller enskilt intresse. En överträdelse kan vara ursäktlig och leda till att avgift inte tas ut eller sätts ned om det har varit närmast omöjligt för den avgiftsskyldige att upptäcka överträdelsen eller om den på annat sätt varit utanför den avgiftsskyldiges kontroll. Avsikten är dock inte att sanktionsavgiften ska sättas ned på grund av bristande kännedom om reglerna, dålig ekonomi, tidsbrist, bristande rutiner eller liknande.

5.8.11 Hinder mot dubbelprövning

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

Skälen för förslaget: Enligt Europakonventionen och EU:s stadga om de grundläggande rättigheterna finns en rätt att inte bli lagförd eller straffas två gånger för samma brott (gärning), det s.k. dubbelprövningsförbudet. Begreppet straff i den mening som avses i Europakonventionen anses även omfatta vite. I regelverk där det är möjligt att utfärda vitesföreläggande och ta ut sanktionsavgift för samma överträdelse införs därför bestämmelser som syftar till att hindra en dubbelprövning. Dessa utformas numera på så sätt att sanktionsavgift inte får beslutas om överträdelsen även omfattas av ett vitesföreläggande och överträdelsen ligger till grund för en ansökan om utdömande av vitet (se t.ex. 12 kap. 3 § LEK, 33 § NIS-lagen och 3 kap. 6 § lagen (2016:1307) om straff för marknadsmissbruk på värdepappersmarknaden och prop.

2021/22:136 s. 363, prop. 2017/18:205 s. 73 och prop. 2016/17:22 s. 228). En motsvarande bestämmelse bör tas in i den nya lagen.

5.8.12 Bestämmelser om förfarandet

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

Sanktionsavgiften ska betalas till tillsynsmyndigheten inom 30 dagar från det att beslutet om att ta ut avgiften fick laga kraft eller inom den längre tid som anges i beslutet. Om sanktionsavgiften inte betalas i tid, ska den obetalda avgiften lämnas för indrivning. Vid indrivning ska verkställighet få ske enligt utsökningsbalken. Sanktionsavgifter ska tillfalla staten.

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

Skälen för förslaget: I och med att tillsynsmyndigheten ska besluta om sanktionsavgift kommer förvaltningslagen (2017:900) att gälla för förfarandet. Det behövs dock vissa ytterligare förfarandebestämmelser.

Beslut om sanktionsavgifter blir ytterligare ett verktyg för tillsynsmyndigheten i dess arbete att kontrollera att reglerna efterlevs.

Ett beslut om sanktionsavgift är en ingripande åtgärd. Det bör därför finnas en bortre tidsgräns för när avgiften får beslutas. En sanktionsavgift bör endast få beslutas om den som avgiften ska tas ut av har fått tillfälle att yttra sig inom två år från det att överträdelsen ägde rum. Bevisbördan för att kommunikation har skett ligger på tillsynsmyndigheten. Tidsfristen räknas från när överträdelsen ägde rum. I fråga om en överträdelse som skett löpande under viss tid är det tillräckligt att kommunikation sker inom två år från det att överträdelsen upphörde för att en sanktionsavgift ska kunna åläggas.

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

En sanktionsavgift bör betalas till tillsynsmyndigheten inom 30 dagar från det att beslutet om avgiften har fått laga kraft eller inom den längre tid som anges i beslutet. Om avgiften inte betalas i tid bör tillsynsmyndigheten vara skyldig att lämna den obetalda avgiften för indrivning. För att sanktionsavgiftssystemet ska bli tillräckligt effektivt bör indrivning kunna ske utan att det krävs något domstolsavgörande. Av 3 kap. 1 § första stycket 6 utsökningsbalken följer att det måste finnas en särskild föreskrift om detta. Sanktionsavgifter bör tillfalla staten.

I likhet med vad som i allmänhet gäller för sanktionsavgifter bör avgiften preskriberas till den del verkställighet inte har skett inom fem år. Bestämmelser som motsvarar det nu anförda bör föras in i den nya lagen.

5.8.13 Överklagande av beslut

Förslag: Tillsynsmyndighetens beslut enligt dataförvaltningsförordningen eller enligt den nya lagen får överklagas till allmän förvaltningsdomstol. När ett beslut överklagas är tillsynsmyndigheten motpart i domstolen.

Skälen för förslaget: Enligt artikel 28.1 i dataförvaltningsförordningen ska berörda fysiska och juridiska personer ha rätt till effektiva rättsmedel avseende rättsligt bindande beslut som avses i artikel 14 och som fattas av den behöriga myndigheten för dataförmedlingstjänster i samband med hantering, övervakning och kontroll av efterlevnaden av anmälningsordningen för leverantörer av dataförmedlingstjänster. Samma sak gäller för rättsligt bindande beslut som avses i artiklarna 19 och 24 som fattas av den behöriga myndigheten för dataaltruismorganisationer i samband med övervakningen av erkända dataaltruismorganisationer. Den behöriga myndighetens yttranden eller rådgivning är inte sådana rättsligt bindande beslut.

Rätten till rättsmedel ska inte påverka administrativa rättsmedel eller andra prövningsförfaranden utanför domstol. Talan mot en

behörig myndighet ska enligt artikel 28.2 väckas vid domstolarna i den medlemsstat där den behöriga myndigheten har sitt säte.

Rätten till ett effektivt rättsmedel mot myndighetsbeslut tillgodoses i svensk rätt normalt genom möjligheten att överklaga beslutet till allmän förvaltningsdomstol, dvs. till en förvaltningsrätt som första instans. När det gäller beslut som fattas enligt en EU-förordning följer rätten att överklaga av allmänna förvaltningsrättsliga principer och rätten att överklaga framgår av förvaltningslagen. Någon särskild överklagandebestämmelse behövs därmed i och för sig inte i nationell lagstiftning när det gäller de beslut som den behöriga myndigheten fattar enligt dataförvaltningsförordningen.

Däremot behövs det särskilda bestämmelser om rätten att överklaga tillsynsmyndighetens beslut enligt den nya lagen, dvs. om att utförda erinran och att ta ut sanktionsavgifter. För att inte skapa otydlighet om hur olika beslut ska kunna överklagas så bör regleringen vara uttömmande i den nya lagen. Således bör även rätten att överklaga tillsynsmyndighetens beslut enligt dataförvaltningsförordningen uttryckligen anges i den nya lagen.

Enligt 42 § FL får ett beslut överklagas av den som beslutet angår, om det har gått honom eller henne emot. Ett beslut får enligt 41 § FL överklagas om beslutet kan antas påverka någons situation på ett inte obetydligt sätt. I 40 § samma lag anges att beslut överklagas till allmän förvaltningsdomstol och att prövningstillstånd krävs vid överklagande till kammarrätten.

Klagorätt tillkommer alltså den som beslutet angår, om beslutet har gått denne emot. Den ordningen överensstämmer enligt utredningens bedömning med kravet på rättsmedel enligt artikel 28.1 i dataskyddförvaltningsförordningen och bör således gälla även för beslut som den behöriga myndigheten fattar enligt förordningen och den kompletterande lagen.[20] I praktiken innebär detta i normalfallet att det är leverantören av en dataförmedlingstjänst eller en dataaltruismorganisation som har rätt att överklaga. Det kan dock inte uteslutas att ett beslut skulle kunna ha rättsligt bindande följder även för andra än den som beslutet riktas mot. Dessa skulle i så fall också ha rätt att överklaga beslutet, enligt förvaltningslagens generella bestämmelse om klagorätt.

[20] Jfr motsvarande bedömning för artikel 78.1 dataskyddsförordningen i prop. 2017/18:105 s. 164.

Särskilt om klagomål

I artikel 27.2 i förordningen anges att de behöriga myndigheterna ska underrätta den som lämnat in ett klagomål om hur arbetet fortskrider och vad resultatet blir, inbegripet möjligheten till rättslig prövning enligt artikel 28. EU-domstolen har angett att motsvarande bestämmelse i artikel 28.3 i det tidigare dataskyddsdirektivet som föregick dataskyddsförordningen innebär att den person som har kommit in med en begäran till tillsynsmyndigheten ska ha tillgång till rättsmedel med vilka han eller hon vid nationella domstolar kan angripa det beslut som gått vederbörande emot (se t.ex. dom Schrems, C-362/14, EU:C:2015:650, punkt 64). Dessa omständigheter talar för att dataförvaltningsförordningen förutsätter att den klagande ska ha en generell rätt att överklaga tillsynsmyndighetens beslut att t.ex. inte vidta någon åtgärd med anledning av ett klagomål.

Det finns emellertid också omständigheter som talar emot en sådan tolkning. Enligt artikel 28.1 är det berörda fysiska och juridiska personer som ska ha rätt till ett effektivt rättsmedel. Dessutom ska beslutet vara rättsligt bindande för denne. Ett beslut om att inte vidta några åtgärder med anledning av ett klagomål medför normalt inte några rättsligt bindande följder för den som har lämnat in klagomålet, även om det inte kan uteslutas att det någon gång skulle kunna förekomma, vilket i så fall skulle medföra överklagbarhet och ge klagorätt enligt förvaltningslagen. Dessutom skulle en ovillkorlig rätt till domstolsprövning av ett sådant beslut kunna underminera tillsynsmyndighetens oberoende ställning, såsom denna kommer till uttryck i artikel 8.3 i EU:s stadga om de grundläggande rättigheterna. Den behöriga myndigheten har inte enligt dataförvaltningsförordningen någon skyldighet att vidta tillsynsåtgärder eller ens att alltid närmare undersöka sakförhållandena i ett klagomål. Tvärtom har den behöriga myndigheten enligt dataförvaltningsförordningen, precis som enligt svensk tillsynstradition, ett tydligt utrymme att själv avgöra vilka tillsynsärenden som ska drivas och på vilket sätt det ska ske. Det framgår inte heller uttryckligen av förordningen att tillsynsmyndigheten måste fatta ett formellt beslut i varje klagomåls- eller tillsynsärende.

Sammanfattningsvis kan konstateras att det är oklart om dataförvaltningsförordningen medför att den som lämnat in ett klagomål har rätt att överklaga tillsynsmyndighetens beslut att inte vidta någon åtgärd med anledning av ett klagomål.

Oavsett hur förordningen ska tolkas i detta avseende, krävs det emellertid inte några författningsåtgärder i svensk rätt. Det bör i stället överlämnas till domstolarna att, genom en tolkning av förvaltningslagens generella bestämmelser om överklagande, ta ställning i frågan om svensk rättspraxis alltjämt är relevant eller om dataförvaltningsförordningen har förändrat rättsläget.

I dataskyddsförordningen finns motsvarande regler om klagomål och rätt till information om hur arbetet fortskrider och information om rättsmedel. Vid införandet av dataskyddsförordningen gjordes samma bedömning som görs här (prop. 2017/18:105 s. 163–165).

Slutsats

Av den nya kompletterande lagen bör det framgå att tillsynsmyndighetens beslut enligt dataförvaltningsförordningen samt dess beslut om erinran och sanktionsavgifter enligt den nya kompletterande lagen får överklagas till allmän förvaltningsdomstol. Vidare bör det anges att prövningstillstånd krävs vid överklagande till kammarrätten. Formerna för överklagande av tillsynsmyndighetens beslut, vilken överklagandefrist som ska gälla, vem som har klagorätt m.m., bör inte avvika från förvaltningslagens bestämmelser. Inga särskilda bestämmelser om detta föreslås därför.

5.9 Sekretess

I dataförvaltningsförordningen finns inga bestämmelser som reglerar sekretess. Sekretess kan dock föreligga hos den behöriga myndigheten enligt befintlig svensk rätt. Det är viktigt att sådan sekretess är ändamålsenlig och att den inte hindrar sådant informationsutbyte som behöver ske mellan olika tillsynsorgan.

Nedan finns en genomgång av vilken sekretess som kan bli aktuell och vilka sekretessbrytande bestämmelser som kan bli tillämpliga. Avsnittet inleds med en beskrivning av vilka uppgifter

den behöriga myndigheten kommer att hantera och vilka behov av att kunna dela information som finns.

5.9.1 Information som den behöriga myndigheten kommer att hantera

Den behöriga myndigheten för dataförmedlingstjänster ska ta emot anmälningar från leverantörer av dataförmedlingstjänster. Sådana anmälningar ska innehålla uppgifter om namn på leverantören och adress till verksamhetsstället, dess rättsliga status, form, ägarstruktur, relevanta dotterföretag och organisationsnummer. Vidare ska anmälan innehålla uppgift om en offentlig webbplats, kontaktperson och kontaktuppgift. Anmälan ska också innehålla en beskrivning av den dataförmedlingstjänst som ska tillhandahållas samt beräknat startdatum för tjänsten. Samtliga dessa uppgifter, förutom uppgift om kontaktperson och kontaktuppgift ska offentliggöras i ett offentligt register som kommissionen ska föra över leverantörer av dataförmedlingstjänster i unionen.

Inom ramen för tillsynsverksamheten ska den behöriga myndigheten också kunna hämta in all information som behövs för att kontrollera uppfyllandet av kraven i kapitel III. Kraven rör bl.a. hur de kommersiella villkoren får se ut, interoperabilitet, säkerhetsåtgärder som ska vidtas och transparens vid behandling av personuppgifter. Leverantören ska också föra logg över dataförmedlingsverksamheten. Information som den behöriga myndigheten kan hämta in för att kunna bedriva tillsyn mot leverantören kan därmed röra olika aspekter av tillhandahållandet av tjänsten så som villkor, format, säkerhetsåtgärder och logg över verksamheten.

Den behöriga myndigheten för dataaltruismorganisationer ska ta emot ansökningar om att registreras som erkänd dataaltruism-organisation. Dessa ansökningar ska innehålla uppgift om namn, adress, rättslig status, organisationsnummer om sådant finns, stadgar, inkomstkällor, en offentlig webbplats med information om organisationen och verksamheten, de mål av allmänt intresse som organisationen ämnar främja när data samlas in och den typ av data som dataaltruismorganisationen avser behandla.

I det offentliga nationella registret som den behöriga myndigheten ska föra ska alla dessa uppgifter förutom uppgift om

stadgar, inkomstkällor och adress till det huvudsakliga verksamhetsstället publiceras av den behöriga myndigheten.

Inom ramen för tillsynsverksamheten över dataaltruismorganisationer ska den behöriga myndigheten kunna hämta in all information som behövs för att kontrollera uppfyllandet av kraven i kapitel IV. Kraven rör bl.a. transparens, säkerhet och information till de registrerade och datainnehavare som delat sina data för altruistiska ändamål. Den regelbok som kommissionen ska ta fram kommer också att innehålla bl.a. säkerhetsmässiga och tekniska krav.

Den erkända dataaltruismorganisationen ska årligen också sammanställa en verksamhetsrapport till den behöriga myndigheten. Denna ska innehålla information om organisationens verksamhet och en beskrivning av hur de mål av allmänt intresse för vilka uppgifter samlats in har främjats. Verksamhetsrapporten ska också innehålla en förteckning över alla fysiska och juridiska personer som tillåtits behandla den data som organisationen innehar tillsammans med en sammanfattande beskrivning av de mål av allmänt intresse som behandlingen är tänkta att uppnå. Den ska också innehålla en beskrivning av de tekniska metoder som använts, inklusive vilka metoder som använts för skydd av den personliga integriteten och dataskydd. Resultat som kan ha uppnåtts av de databehandlingar som tillåtits ska också finnas med i rapporten. Slutligen ska organisationen i rapporten också redogöra för inkomstkällor, och då i synnerhet intäkter från beviljande av tillgång till data, och utgifter.

Den behöriga myndigheten för dataförmedlingstjänster ska också enligt förslagen i denna promemoria ta emot anmälningar från myndigheter avseende vidareutnyttjare som begått överträdelser mot artikel 5.14. En sådan anmälan ska innehålla uppgifter om den som begått överträdelsen, en beskrivning av de data som lämnats ut, vilka villkor som ställts upp för vidareutnyttjandet och överföringen till tredje land, en redogörelse för den eller de överträdelser som vidareutnyttjaren gjort sig skyldig till samt vilka effekter överträdelsen gett. Därutöver ska olika uppgifter som har betydelse för bedömningen av en eventuell sanktionsavgift finnas med.

5.9.2 Sekretess enligt OSL för de aktuella uppgifterna

Sekretess för den verksamhet som den behöriga myndigheten för dataförmedlingstjänster och för dataaltruismorganisationer bedriver och för den information som hanteras kan föreligga enligt olika bestämmelser i OSL. Nedan följer en kort beskrivning av sådan sekretess som kan föreligga. Genomgången ska inte ses som uttömmande, annan sekretess kan också föreligga.

Sekretess i det internationella samarbetet

Enligt 15 kap. 1 a § andra stycket OSL gäller sekretess för uppgift som en myndighet har inhämtat i syfte att överlämna den till ett utländskt organ bl.a. på grund av en bindande EU-rättsakt. Uppgiftens innehåll, art eller karaktär saknar betydelse för bestämmelsens tillämplighet, till skillnad från vad som gäller i fråga om utrikessekretess enligt 15 kap. 1 § OSL. Bestämmelsen är vidare tillämplig även i fråga om uppgifter om enskilda, om de finns hos myndigheten på grund av ett reglerat internationellt samarbete. Så kan exempelvis vara fallet om uppgiften inkommit från en utländsk myndighet och härrör från en utredning, en upphandling eller ett annat ärende där (prop. 2012/13:192 s. 44). Den behöriga myndigheten ska kunna bistå andra behöriga myndigheter och uppgifter kan därmed hämtas in i syfte att lämna till en behörig myndighet i en annan medlemsstat.

Av första stycket framgår vidare att en förutsättning för att sekretess ska gälla är att ett röjande av uppgiften kan antas försämra Sveriges möjlighet att delta i det internationella samarbete som avses i EU-rättsakten eller avtalet. Termen ”försämras” ska inte uppfattas som att det råder en lägre tröskel för att ett utlämnande ska kunna nekas, jämfört med om termen ”skadas” i stället hade använts i bestämmelsen. Tvärtom indikerar termen ”försämras” att det är en viss typ av skada som ska kunna antas uppstå för att skaderekvisitet ska vara uppfyllt (prop. 2012/13:192 s. 44).

Uttrycket ”möjlighet att delta i” syftar i detta sammanhang främst på möjligheten att få del av information i enlighet med EU-rättsakten eller avtalet, dvs. dra nytta av samarbetet. Bestämmelsen innebär att myndigheten i det enskilda fallet är skyldig att göra en självständig bedömning av vilka konsekvenser ett röjande kan antas

få för det fortsatta samarbetet. Myndigheten måste då beakta om och i så fall på vilket sätt frågan om sekretess regleras i rättsakten eller avtalet (prop. 2012/13:192 s. 44). Frågan om sekretess regleras inte alls i dataförvaltningsförordningen. En bedömning behöver i stället göras i det enskilda fallet av om avsaknaden av sekretess utgör ett sådant hinder som stadgas i paragrafen.

Säkerhets- eller bevakningssekretess

Sekretess gäller enligt 18 kap. 8 § OSL för uppgift som lämnar eller kan bidra till upplysning om säkerhets- eller bevakningsåtgärd, om det kan antas att syftet med åtgärden motverkas om uppgiften röjs och åtgärden avser något av de objekt som räknas upp i paragrafen, t.ex. byggnader, lokaler eller inventarier enligt punkten 1 eller system för automatiserad behandling av information enligt punkten 3.

Med system för automatiserad behandling av information avses system där datorer, telekommunikation eller annan teknisk utrustning samverkar för att insamla, ordna, bearbeta, söka och distribuera information. Med uppgifter som lämnar upplysning om säkerhets- eller bevakningsåtgärd avses enligt denna punkt t.ex. uppgifter om konfigurering av brandväggar. Uppgifter som kan bidra till upplysning om säkerhetsåtgärder kan vara t.ex. uppgifter om vilken typ och version av operativsystem eller annan programvara som används. Beskrivningar av hur ett program fungerar i stora drag och vilka typer av uppgifter som bearbetas i ett program bör alltid kunna lämnas utan att uppgifter som omfattas av bestämmelsen behöver röjas (Se Lenberg, Tansjö & Geijer, Offentlighets- och sekretesslagen En kommentar (2022, version 26, JUNO), under rubriken 8 § Säkerhets- och bevakningsåtgärd).

Sekretess till skydd för enskild

De uppgifter som tillsynsmyndigheten samlar in kan vara känsliga för uppgiftslämnaren. De villkor som tillsynsmyndigheten ska utöva tillsyn över avser bl.a. kommersiella villkor och uppbyggnaden av tjänster, säkerhetsåtgärder och loggar.

Bestämmelser om sekretess i statlig tillsynsverksamhet för bl.a. uppgift om ett företags affärs- eller driftsförhållanden finns i 30 kap. 23 § OSL jämförd med 9 § offentlighets- och sekretessförordningen (2009:641) och bilagan till den förordningen.

Paragrafen innehåller huvudregeln om sekretess i statlig tillsynsverksamhet m.m. Myndighetens tillsynsverksamhet ska avse produktion, handel, transportverksamhet eller näringslivet i övrigt. Sekretessen gäller enligt första punkten uppgift om enskilds affärs- eller driftsförhållande, uppfinningar eller forskningsresultat om det kan antas att den enskilda lider skada om uppgiften röjs. Skaderekvisitet är för denna punkt rakt, dvs att det råder presumtion för offentlighet. Sekretess råder också enligt paragrafens andra punkt för uppgift om andra ekonomiska eller personliga förhållanden än de som avses i punkt 1 för den som har trätt i affärsförbindelse eller liknande förbindelse med den som är föremål för myndighetens verksamhet, och för uppgift om andra ekonomiska eller personliga förhållanden om. Sekretessen enligt andra punkten är absolut.

För att sekretess ska gälla krävs att regeringen meddelar föreskrifter som närmare anger vilka uppgifter som omfattas av sekretessen. Sådana föreskrifter har meddelats i 9 § OSF och i bilagan till förordningen regleras att PTS tillsynsverksamhet omfattas. Om PTS utses till behörig myndighet i enlighet med förslagen i denna promemoria omfattas tillsynsverksamheten för dataförmedlingstjänster och dataaltruismorganisationer också av denna sekretess när den är tillämplig. Detta torde omfatta även uppgifter som inkommer genom begäran om tillsyn eller klagomål.

5.9.3 Informationsutbyte med andra tillsynsmyndigheter i Sverige

Förslag: Den behöriga myndigheten ska kunna utbyta sådan information med andra tillsynsmyndigheter som behövs för att myndigheterna ska kunna utföra sina respektive tillsynsuppgifter.

Skälen för förslaget: Den behöriga myndigheten för dataförmedlingstjänster och dataaltruismorganisationer behöver

kunna dela information med tillsynsmyndigheter på andra områden. Tillsynsområdet för dataförmedlingstjänster gränsar mot befintliga tillsynsuppdrag som IMY har på dataskyddsområdet, Konkurrensverket har på konkurrensrättens område och de myndigheter som är ansvariga för cybersäkerhetsfrågor inom ramen för Nationellt cybersäkerhetscenter. Den behöriga myndigheten behöver kunna samverka med dessa myndigheter och dela information. Samverkan kommer i första hand att avse samordning av tillsyn vid behov, överlämning av ärenden eller enskilda frågor inom ett ärende som rör en annan tillsynsmyndighets område eller samverkan för att kunna avgöra enligt vilket regelverk ett visst förfarande ska bedömas.

Det finns inte i OSL några specifika sekretessbrytande regler för överföring till andra tillsynsmyndigheter i kapitel 15, 18 eller 30 gällande sekretessen enligt 30 kap. 23 §, 18 kap. 8 § eller 15 kap. 1 a §.

I 10 kap OSL finns visa övergripande sekretessbrytande bestämmelser. Enligt generalklausulen i 10 kap. 27 § får en sekretessbelagd uppgift lämnas till en myndighet om det är uppenbart att intresset av att uppgiften lämnas har företräde framför det intresse som sekretessen ska skydda.

För att generalklausulen ska vara tillämplig krävs att det är uppenbart att intresset av att uppgifterna lämnas ut har företräde framför det intresse som sekretessen ska skydda. Begreppet uppenbart signalerar att generalklausulen bara ska användas i fall där det står klart att intresset av ett utlämnande har företräde framför det intresse som sekretessen ska skydda. I tveksamma fall bör paragrafen således inte komma till användning.

JO har i flera ärenden understrukit vikten av att utlämnanden med stöd av generalklausulen inte sker slentrianmässigt. Uppgiftslämnandet inte får ske rutinmässigt utan måste föregås av en sådan verklig intresseavvägning i det enskilda fallet som generalklausulen förutsätter (JO 2013/14 s. 230).

I vissa undantagsfall kan utlämnanden ske regelmässigt med generalklausulen som stöd (prop. 1979/80:2 Del A s. 327). Intresseavvägningen ska då göras på förhand.

Av 10 kap. 28 § framgår att sekretess inte hindrar att en uppgift lämnas till en annan myndighet om uppgiftsskyldigheten följer av lag eller förordning. En sådan uppgiftsskyldighet kan avse utlämnande av uppgifter av ett visst slag eller en skyldighet för en

viss myndighet att lämna andra myndigheter information. En allmän reglering som föreskriver samarbete mellan myndigheter som t.ex. den i 6 § förvaltningslagen är inte tillräcklig för att sådan uppgiftsskyldighet som avses i paragrafen ska föreligga (Se Lenberg, Tansjö & Geijer, Offentlighets- och sekretesslagen En kommentar, 2022, version 26, JUNO, kommentar till 10 kap. 28 §). Den samverkansreglering som finns i dataförvaltningsförordningen kan därför heller inte anses vara en sådan uppgiftsskyldighet som krävs för att 10 kap. 28 § ska bli tillämplig.

Vidare måste man skilja föreskrifter om uppgiftsskyldighet från sådana bestämmelser enligt vilka en myndighet får lämna uppgifter till en annan. Bestämmelser som är av det senare slaget har inte den verkan att sekretessen viker enligt nu aktuell paragraf.

Om uppgifter ändå får lämnas till en annan myndighet, får i stället bedömas för varje särskilt fall med tillämpning av bl.a. sekretessbestämmelsernas skaderekvisit och generalklausulen i 10 kap. 27 § OSL. Blir resultatet av denna bedömning att sekretess inte hindrar att en uppgift lämnas ut, kan 6 kap. 5 § OSL bli tillämplig (Se Lenberg, Tansjö & Geijer, Offentlighets- och sekretesslagen En kommentar, 2022, version 26, JUNO, kommentar till 10 kap. 28 §).

Generalklausulen hindrar alltså inte att ett utbyte av uppgifter mellan myndigheter sker rutinmässigt även utan en särskild författningsreglering men regelverket bygger ändå på att rutinmässigt uppgiftsutbyte i regel ska vara författningsreglerat. I de undantagsfall när rutinmässigt uppgiftslämnande inte är författningsreglerat men ändå kan anses tillräckligt motiverat måste den intresseavvägning som ska göras enligt generalklausulen ske i förväg. Vid prövningen av en utlämnandefråga får då den mottagande myndighetens behov av uppgifterna vägas mot det intresse som sekretesskyddet typiskt sett tillgodoser.

Många myndigheter anser att generalklausulen är svår att tillämpa och inte ger den effektivitet i arbetet som är nödvändig då ett löpande informationsutbyte förutsätter en sekretessprövning på förhand. Olika myndigheter gör också olika bedömningar av om förutsättningarna i bestämmelsen är uppfyllda

För att säkerställa att tillsynsmyndigheterna på ett effektivt sätt kan dela den information med varandra som behövs för deras tillsyn bör en uppgiftsskyldighet införas.

En slutsats är att det är svårt att på förhand avgöra vilka uppgifter som kan behöva utbytas och vilken sekretess som kan föreligga. Uppgiftsskyldigheten bör därför utformas så att den bara avser sådana uppgifter som den andra myndigheten behöver för sitt tillsynsuppdrag. På så sätt kommer bestämmelsen bara att omfatta sådana uppgifter som omfattas av sekretess som är nödvändig att bryta.

5.9.4 Informationsutbyte med behöriga myndigheter i andra medlemsstater

Bedömning: För informationsutbyte med behöriga myndigheter i andra medlemsstater finns en uppgiftsskyldighet och en sekretessbrytande bestämmelse som möjliggör ett sådant utbyte. Någon ytterligare reglering behövs inte.

Skälen för bedömningen: Den behöriga myndigheten för dataförmedlingstjänster ska samarbeta med och bistå motsvarande behöriga myndigheter i andra medlemsstater enligt artikel 14.7. Om en leverantör av en dataförmedlingstjänst har sitt huvudsakliga verksamhetsställe eller sin rättsliga företrädare i en medlemsstat men tillhandahåller tjänster i andra medlemsstater ska den behöriga myndigheten i de båda medlemsstaterna samarbeta och bistå varandra. Om en behörig myndighet ska begära bistånd från en annan behörig myndighet så ska den lämna en motiverad begäran, och svar på en sådan begäran ska lämnas utan dröjsmål. Detta bistånd och samarbete får omfatta informationsutbyte och all information som utbyts får användas bara för att hantera det ärende som det begärdes för.

Motsvarande reglering finns för behöriga myndigheter för dataaltruismorganisationer i artikel 24.6. Denna är formulerad på samma sätt och innehåller samma ramar.

Av 8 kap. 3 § 1 OSL framgår att sekretess inte hindrar att uppgifter röjs för en utländsk myndighet, om utlämnandet sker i enlighet med särskild föreskrift i lag eller förordning. En sådan uppgiftsskyldighet finns avseende tillsynsmyndigheter för dataförmedlartjänster i artikel 14.7 dataförvaltningsförordningen och avseende dataaltruismorganisationer i artikel 24.6.

Den sekretess som kan föreligga för olika uppgifter enligt 15 kap. 1 a §, 30 kap. 23 § och 18 kap. 8 § OSL hindrar därför inte informationsutbyte i enlighet med dessa artiklar.

6 Europeiska datainnovationsstyrelsen

Genom dataförvaltningsförordningen inrättas en europeisk datainnovationsstyrelse. I det här kapitlet finns en beskrivning av regleringen av datainnovationsstyrelsen i förordningen samt en analys av vilka överväganingar det innebär för svensk del med förslag på deltagande i styrelsens arbete.

6.1 Europeiska datainnovationsstyrelsen i dataförvaltningsförordningen

I kapitel VI dataförvaltningsförordningen finns bestämmelser om att kommissionen ska inrätta en europeisk datainnovationsstyrelse i form av en expertgrupp. Kommissionen ska vara ordförande för styrelsen och tillhandahålla ett sekretariat som ska bistå styrelsen, artikel 29.3 och 4. Inrättande av den här typen av expertgrupper är reglerat inom EU genom Commission decision establishing horizontal rules on the creation and operation of Commission expert groups, C(2016)3301 .

6.1.1 Deltagare och undergrupper

Datainnovationsstyrelsen ska enligt artikel 29.1 bestå av vissa specifikt utpekade aktörer utöver kommissionen. Dels ska företrädare för de behöriga myndigheterna för dataförmedlingstjänster och för dataaltruismorganisationer i alla medlemsstater ingå. Dels ska representanter från andra organ så som Europeiska dataskyddsstyrelsen, Europeiska datatillsynsmannen, EU:s cybersäkerhetsbyrå Enisa och EU-företrädaren för små och

medelstora företag ingå. I datainnovationsstyrelsen kan också andra företrädare för relevanta organ inom enskilda sektorer samt organ med specifik sakkunskap ingå.

Datainnovationen ska bestå av undergrupper. Tre av dessa är specificerade i artikel 29.2. Dessa är

- Undergrupp bestående av behöriga myndigheter för dataförmedlingstjänster och dataaltruismorganisationer
- Undergrupp för tekniska diskussioner om standardisering, portabilitet och interoperabilitet
- Undergrupp för berörda parter bestående av relevanta företrädare från näringslivet, forskningsverksamhet, akademi, civilsamhället, standardiseringsorganisationer, berörda gemensamma europeiska dataområden och andra berörda intressenter.

6.1.2 Uppgifter

Den europeiska datainnovationsstyrelsen ska ha ett stort antal uppgifter vilka beskrivs i artikel 30 i punkterna a-m. En central uppgift är att rådge och bistå kommissionen inom ett antal olika frågor och områden. Därutöver ska styrelsen föreslå vissa riktlinjer och underlätta samarbetet mellan medlemsstater och behöriga myndigheter. Den europeiska datainnovationsstyrelsen har inte något beslutsmandat enligt förordningen.

Merparten av uppgifterna är fördelade på de olika undergrupper som ska skapas enligt vad som beskrivs i avsnitt 6.1.1. Uppgifter som rör råd och bistånd avseende utveckling av enhetlig praxis för dataaltruism i unionen (punkt c), utarbeta ett formulär för samtycke (punkt l) och förbättra det internationella regelverket för icke-personuppgifter (punkt m) är inte fördelade till någon av undergrupperna. Inte heller frågan om att underlätta samarbetet mellan medlemsstaterna om fastställandet av harmoniserade villkor som möjliggör vidareutnyttjande av skyddade data enligt kapitel II förordningen är fördelad till någon av undergrupperna.

6.1.3 Uppgifter för undergrupperna

Undergrupp för behöriga myndigheter

Undergruppen som består av företrädare för behöriga myndigheter för dataförmedlingstjänster och dataaltruismorganisationer ska bistå och rådge kommissionen när det gäller utarbetandet av en konsekvent praxis för offentliga myndigheter och behöriga organ vid behandlingen av ansökningar om vidareutnyttjande av skyddade data enligt kapitel II (punkt a) och för de behöriga myndigheterna vad gäller tillämpningen av krav för leverantörer av dataförmedlingstjänster och erkända dataaltruismorganisationer (punkt c). Undergruppen ska också ha till uppgift att underlätta samarbetet mellan behöriga myndigheter för dataförmedlingstjänster och behöriga myndigheter för dataaltruismorganisationer, i synnerhet genom att fastställa metoder för ett effektivt utbyte av information som rör anmälan av leverantörer av dataförmedlingstjänster och registreringen och övervakningen av erkända dataaltruismorganisationer (punkt j). Denna uppgift omfattar också samordning i frågor om avgifter och sanktioner. Undergruppen ska slutligen rådge och bistå kommissionen när det gäller utvärderingen av huruvida genomförandeakter gällande överföring av icke-personuppgifter till tredjeland ska antas (punkt k).

Undergrupp för tekniska diskussioner

Undergruppen för tekniska diskussioner om standardisering, portabilitet och interoperabilitet ska rådge kommissionen i olika frågor som rör upprättande av dataområden, standardisering och interoperabilitet (punkterna f och g). I beskrivningen av uppgifterna anges att uppgiften ska ske särskilt i samverkan med standardiseringsorganisationer.

Undergrupp för berörda parter

Undergruppen för berörda parter ska delta i arbetet med de frågor som undergruppen för tekniska diskussioner ska delta i (punkterna f och g). De berörda parterna ska därutöver också rådge och bistå kommissionen när det gäller utarbetandet av konsekventa riktlinjer

för hur man inom ramen förordningen bäst ska skydda kommersiellt känsliga data som inte är personuppgifter, särskilt företagshemligheter, men även icke-personuppgifter med immaterialrättsligt skyddat innehåll, mot olaglig åtkomst med risker för stöld av immateriella rättigheter eller industrispionage (punkt d). Vidare ska gruppen rådge och bistå kommissionen när det gäller utarbetandet av konsekventa riktlinjer för cybersäkerhetskrav vid utbyte och lagring av data (punkt e). Undergruppen ska också föreslå riktlinjer för gemensamma europeiska dataområden (punkt h).

6.2 Representant från Sverige i den europeiska datainnovationsstyrelsen

Som beskriv i avsnitt 6.1 så finns det i artikel 29 ramar för sammansättningen av datainnovationsstyrelsen ramar. Vissa aktörer ska ingå i datainnovationsstyrelsen. Därutöver finns det utrymme för kommissionen att låta andra företrädare för relevanta organ inom enskilda sektorer samt organ med specifik sakkunskap ingå.

Nedan beskrivs vilka som ska ingå enligt förordningens regler. Det följs av förslag på hur den svenska representanten kan få hjälp från ytterligare andra aktörer i sitt uppdrag.

6.2.1 Företrädare för PTS ska delta

Förslag: En företrädare för PTS som behörig myndighet för dataförmedlingstjänster och dataaltruismorganisationer ska delta i datainnovationsstyrelsen.

PTS ska inhämta synpunkter från Digg i arbetet med den europeiska datainnovationsstyrelsen.

Skälen för förslaget: Företrädare för behöriga myndigheter för dataförmedlingstjänster och dataaltruismorganisationer ska ingå i datainnovationsstyrelsen.

En och samma myndighet föreslås i denna promemoria för båda dessa uppgifter, och att den myndigheten ska vara PTS. En företrädare för PTS ska därför ingå i datainnovationsstyrelsen.

Den företrädare för PTS som deltar i styrelsen kommer att ingå i den undergrupp som består av företrädare för de behöriga

myndigheterna för dataaltruismorganisationer och dataförmedlingstjänster. Undergruppens uppgifter består i att rådge och bistå kommissionen i frågor som rör tillämpningen av dataförvaltningsförordningens regler om dataförmedlingstjänster och dataaltruismorganisationer och att underlätta samarbetet mellan behöriga myndigheter i olika medlemsstater och samordna frågor om bl.a. avgifter och sanktioner (artikel 30 punkterna c och j). Dessa frågor kommer PTS som behörig myndighet att ha god kunskap om och deltagandet i styrelsen kommer att ge PTS möjlighet att påverka utvecklingen av praxis på området och ett forum för samarbete med andra motsvarande myndigheter.

Undergruppen för behöriga myndigheter ska också hantera vissa frågor som är kopplade till dataförvaltningsförordningens ramverk för vidareutnyttjande av skyddade data från offentliga myndigheter enligt kapitel II (artikel 30 punkterna a och k). PTS föreslås inte utses till behörigt organ enligt artikel 7 och är inte heller själva en myndighet som förväntas använda ramverket i kapitel II i någon större utsträckning. Dessa frågor har Digg genom samordningsansvaret för behöriga organ enligt artikel 7.1 bättre kunskap om än PTS i rollen som behörig myndighet för dataförmedlingstjänster och dataaltruismorganisationer. PTS ska inhämta synpunkter från Digg när dessa frågor hanteras.

I andra undergrupper där PTS inte automatiskt kommer att ingå ska frågor som rör upprättande av dataområden, standardisering och interoperabilitet hanteras. Frågor om standardisering och interoperabilitet är frågor som ryms inom Diggs ansvar och kompetens. PTS ska därför inhämta synpunkter från Digg också gällande dessa frågor om de hanteras av PTS i arbetet med den europeiska datainnovationsstyrelsen.

6.3 Datainnovationsstyrelsen och kommande lagstiftning från EU

Genom dataförvaltningsförordningen inrättas den europeiska datainnovationsstyrelsen och dess uppgifter beskrivs i artikel 30.

Datainnovationsstyrelsen kommer också att kunna ges uppgifter i kommande lagstiftningsprodukter från EU som utgår ifrån EU:s datastrategi. I utkastet till datarättsförordning finns data-

innovationsstyrelsen med, likaså i utkastet till den kommande AI-förordningen och till den kommande förordningen om ett europeiskt hälsodataområde.

Styrelsens uppgifter liksom frågan om hur många undergrupper som kommer att skapas kan därför komma att förändras framöver. I de förslag som nu lämnas har inte hänsyn tagits till behov utifrån sådan framtida utveckling. Det är dock viktigt att fortsatt löpande bevaka vilka frågor styrelsen hanterar och hur Sverige ska kunna bidra med den kompetens och de resurser som behövs.

7 Ikraftträdande

Förslag: Lagändringarna och lagförslagen ska träda i kraft den 1 januari 2024.

Skälen för förslaget: Dataförvaltningsförordningen ska börja tillämpas den 24 september 2023. De föreslagna lagändringarna och den nya lagen ska komplettera förordningen och det är därför angeläget att de kan träda i kraft så snart som möjligt. Den tidigaste tidpunkten bedöms vara den 1 januari 2024. Lagändringarna och lagförslagen bör därför träda i kraft den 1 januari 2024.

Lagändringarna bedöms inte vara sådana att de motiverar särskilda övergångsbestämmelser.

8 Konsekvensanalys

I detta avsnitt redogörs för förslagens effekter i den omfattning som bedöms lämpligt och med beaktande av förordningen (2007:1244) om konsekvensutredning vid regelgivning.

De största konsekvenserna av tillämpningen av dataförvaltningsförordningen i Sverige för alla berörda är i huvudsak en följd av förordningen i sig och de skyldigheter som följer av den, inte av förslagen i denna promemoria.

De konsekvenser som EU-kommissionen bedömt att dataförvaltningsförordningen får redogörs för kort i avsnitt 8.5.

De kostnader som uppstår av tillämpningen kan vägas mot de potentiella vinster som förutses i form av utökad tillgång till data för samhällsnyttiga ändamål samt utvecklad förmåga till styrning av verksamhet med stöd av data.

För att EU-förordningen ska vara genomförd i svensk rätt krävs att medlemsstaterna utser myndigheter till behöriga organ för att bistå andra myndigheter som innehar skyddade data som någon vill vidareutnyttja och behöriga myndigheter för dataförmedlingstjänster och dataaltruismorganisationer. Medlemsstaterna ska också utse en myndighet som ska tillhandahålla en gemensam informationspunkt. Dessa uppgifter är nya permanenta myndighetsuppgifter.

Utöver detta finns det ett antal krav på införande av regler i nationell rätt. Medlemsstaterna ska införa kriterier och en metod för beräkning av avgifter för att tillåta vidareutnyttjande av skyddade data, och införa en effektiv rätt till överprövning av beslut om tillgång till skyddade data för vidareutnyttjande. Medlemsstaterna får också införa en avgift för anmälan av dataförmedlingstjänster. Vidare ska medlemsstaterna införa en möjlighet att överklaga beslut som den behöriga myndigheten fattar och sanktioner för vissa

överträdelser. Förordningen har ett horisontellt omfång och kan ses som ett relativt nytt författningsmässigt inslag.

I denna promemoria finns förslag på hur detta ska genomföras i Sverige.

8.1 Konsekvenser av nya myndighetsuppgifter

8.1.1 Konsekvenser för behöriga organ för vidareutnyttjande av skyddade data

Bedömning: Förslagen i promemorian om att Myndigheten för digital förvaltning och Statistiska centralbyrån ska utses till behöriga organ för vidareutnyttjande av skyddade data kan uppskattningsvis initialt kräva sammanlagt 2 miljoner kronor per år tills vidare, i huvudsak för framtagande av vägledning, ramverk och annat skriftligt material till stöd för andra myndigheter.

Myndigheternas resursbehov kan tillgodoses genom ökade anslag.

Skälen för bedömningen: Medlemsstaterna ska enligt artikel 7 utse ett eller flera behöriga organ som ska bistå de offentliga myndigheter som beviljar eller vägrar tillgång för vidareutnyttjande av skyddade data. Digg och SCB föreslås utses till behöriga organ enligt artikel 7. Detta är nya permanenta uppgifter för myndigheterna. Digg föreslås bli huvudansvarig och få en samordnande roll i förhållande till andra myndigheter. Myndighetens uppgift ska utöver bistånd till andra myndigheter också bestå i att främja delning av skyddade data. Uppgiften att främja delning av skyddade data följer inte av förordningen utan är ett förslag som går utöver vad som krävs av Sverige som medlemsstat.

Ett flertal myndigheter har fått frågor om i vilken utsträckning de har data som de tillgängliggör för vidareutnyttjande som träffas av förordningens bestämmelser och svaret har varit att det inte finns alls eller annars i väldigt liten utsträckning. Bolagsverket, Digg, Konkurrensverket, Lantmäteriet och Socialstyrelsen bedömer alla att de inte kommer att tillämpa regelverket i kapitel II. SKR bedömer att regelverket, eftersom det inte innefattar krav på att tillgängliggöra skyddade data för vidareutnyttjande, inte kommer att

påverka kommuner och regioner i någon större utsträckning. SCB tillgängliggör vissa skyddade data för forskningsändamål i sin säkra behandlingsmiljö och detta tillgängliggörande skulle i vissa fall kunna omfattas av kapitel II i förordningen. Detta tillgängliggörande är redan väl reglerat och dataförvaltningsförordningen förväntas inte påverka detta tillhandahållande nämnvärt. SCB föreslås också att utses till behörigt organ.

Uppgiften som behörigt organ enligt artikel 7 bedöms utifrån att den avser att ge stöd till andra myndigheter bli mycket begränsad under en överskådlig framtid. På sikt kan den dock förväntas öka i omfattning, särskilt om nya skyldigheter att tillgängliggöra skyddade data införs eller vid utvecklingen av olika dataområden inom EU.

Även om uppgiften inte bedöms bli omfattande inledningsvis så är det en förutsättning för Sveriges genomförande av förordningen att Digg och SCB tilldelas tillräckliga resurser för att kunna utföra uppgiften. Enligt förordningen ska behöriga organ ha tillräckliga juridiska, ekonomiska och tekniska resurser för att utföra uppgifterna, artikel 7.3.

Digg föreslås vara huvudansvariga för funktionen och ha en uppgift att också främja tillgängliggörandet av skyddade data, varför uppgiften hos dem kan förväntas bli mer omfattande än hos SCB. Uppgiften ligger dock väl i linje med befintliga uppgifter hos Digg vilket kan innebära att den inte kräver lika mycket resurser för uppbyggnad. Uppbyggnad av stödet och framtagande av vägledningar kommer dock att kräva vissa resurser särskilt hos Digg som både ha huvudansvar och till uppgift att främja tillgängliggörande av skyddade data.

Hos Digg kan uppgiften bedömas uppgå till en till två årsarbetskrafter, för SCB bedöms uppgiften vara mindre och uppgå till högst en årsarbetskraft. Sammantaget bedöms kostnaderna för behöriga organ uppgå till 2 miljoner kronor per år inledningsvis.

Digg och SCB:s nya permanenta uppgifter kan finansieras genom ett ökat anslag. Över tid kan tillämpningen av regelverket i kapitel II förväntas öka. Finansieringen kan därför behöva öka över tid. På sikt kan uppgiften också innebära att Digg t.ex. behöver tillhandahålla förvaltningsgemensamma tekniska förmågor eller tjänster. Finansieringen kan därför behöva öka till det dubbla efter tre år.

8.1.2 Konsekvenser för myndigheten som tillhandahåller den gemensamma informationspunkten

Bedömning: Förslagen i promemorian om att Myndigheten för digital förvaltning ska tillhandahålla den gemensamma informationspunkten kan uppskattningsvis initialt kräva 3 miljoner kronor per år, i huvudsak för teknisk utveckling för tillhandahållande av den gemensamma informationspunkten och förvaltning av denna samt för vägledning kring metadata. Behoven väntas efter hand öka till 6 miljoner kronor per år.

Myndighetens resursbehov kan tillgodoses genom ökade anslag.

Skälen för bedömningen: Den gemensamma informationspunkten enligt artikel 8 föreslås tillhandahållas av Digg. I den gemensamma informationspunkten ska viss information om dataförvaltningsförordningens artikel 5 och 6 publiceras. Den gemensamma informationspunkten ska tillhandahålla en sökbar tillgångsförteckning som innehåller en översikt över alla tillgängliga datakällor. Kommissionen ska inrätta en europeisk gemensam åtkomstpunkt. De nationella informationspunkterna ska vara anslutna till denna. Därutöver ska Digg genom den gemensamma informationspunkten portalen kunna ta emot förfrågningar och ansökningar om vidareutnyttjande av vissa typer av skyddade data hos andra myndigheter, och vidarebefordra dessa till aktuella myndigheter.

Ansvaret för förteckningen kommer att innebära att Digg behöver utveckla teknisk funktionalitet samt vägleda offentliga myndigheter i hur metadata lämnas. Kostnader kommer att uppkomma för utveckling av funktionaliteten för förteckningen och ansökningshantering. Kostnader kommer också att uppkomma för att hålla informationspunkten uppdaterad med information och att förvalta förteckningen.

Uppgiften som ansvarig för den gemensamma informationspunkten kommer att medföra betydande arbetsinsatser och därmed också kostnader.

Digg tillhandahåller redan idag Dataportalen som skulle kunna vara en lämplig placering för den gemensamma informationspunkten. Oavsett var den gemensamma informationspunkten

tekniskt placeras så krävs dock teknisk utveckling för ny funktionalitet både för förteckningen, anslutning till kommissionens förteckning och för mottagande och vidareförmedling av förfrågningar. Behovet av finansiering är detsamma oavsett hur många myndigheter i Sverige som faktiskt kommer att tillämpa kapitel II i dataförvaltningsförordningen, eftersom de tekniska förmågorna och vägledning avseende metadata måste tas fram oavsett hur många som ska använda dem.

Den gemensamma informationspunkten kan finansieras genom ett ökat anslag till Digg. Detta anslag beräknas till 3 miljoner per år inledningsvis. På sikt kan arbetet med den gemensamma informationspunkten förväntas öka i takt med ett ökat tillgängliggörande av skyddade data. Finansieringen kan därför behöva öka efterhand.

8.1.3 Konsekvenser för behörig myndighet för dataförmedlingstjänster och dataaltruismorganisationer

Bedömning: Förslagen i promemorian om att Post- och telestyrelsen ska utses till behörig myndighet för dataförmedlingstjänster och för dataaltruismorganisationer kan uppskattningsvis initialt kräva 3 miljoner kronor per år, i huvudsak för teknisk utveckling för e-tjänster och för tillhandahållande av anmälnings- och ansökningsförfaranden samt tillsynsverksamhet.

Myndighetens resursbehov kan tillgodoses genom ökade anslag.

Skälen för bedömningen: PTS föreslås bli behörig myndighet för dataförmedlingstjänster och dataaltruismorganisationer. Myndigheten ska enligt artikel 26.5 ha tillräckliga ekonomiska resurser och personalresurser till sitt förfogande för att utföra de uppgifter som de anförtros, inbegripet nödvändiga tekniska kunskaper och resurser.

Antal leverantörer av dataförmedlingstjänster och dataaltruismorganisationer under svensk jurisdiktion

En viktig faktor för att avgöra konsekvenserna för PTS som behörig myndighet är att bedöma hur många leverantörer av dataförmedlingstjänster och dataaltruismorganisationer som kan vilja anmäla sig för att bli erkända sådana som finns i Sverige. När det gäller underlag för att göra en ungefärlig uppskattning av antalet företag under svenskt tillsynsansvar kan konstatera att inga sådana har kunnat identifieras. Detta trots kontakt med branschorganisationer, aktörer som idag handlar med data och myndigheter som tillhandahåller mycket data. Bedömningen är därför att det inte i dagsläget finns några eller bara ett fåtal företag som tillhandahåller en sådan tjänst som är en dataförmedlingstjänst. Detsamma gäller för dataaltruismorganisationer. Flertalet andra medlemsstater gör samma bedömning. Bara i enstaka medlemsstater bedöms det finnas en befintlig marknad med aktörer.

Företag som är etablerade utanför unionen men som verkar här ska utse en rättslig företrädare i någon av medlemsstaterna. Denna skyldighet har ännu inte trätt i kraft, så det kan inte förutses vilka företag som kommer att ange en rättslig företrädare i Sverige eller på annan plats i unionen och inte heller hur stor grupp av leverantörer av dataförmedlingstjänster och dataaltruismorganisationer som samtliga medlemsstater kommer att ha jurisdiktion över. Efter ikraftträdandet av alla skyldigheter finns bättre förutsättningar att få en överblick över vilka utländska aktörer som kommer falla under svensk jurisdiktion. Hittills finns dock inga indikationer på att det kommer att vara något större antal.

Antalet leverantörer av dataförmedlingstjänster påverkar hur många anmälningar som den behöriga myndigheten ska hantera. När det gäller dataaltruismorganisationer så är det frivilligt att ansöka om att registrera sig som en sådan. I det fallet är därmed osäkerhetsfaktorn än större.

Behörig myndighet dataförmedlingstjänster

En behörig myndighet ska utses för att hantera anmälningar från leverantörer av dataförmedlingstjänster och för att utöva tillsyn över

dessa. PTS föreslås utses till behörig myndighet och det är en ny permanent uppgift.

PTS kommer att behöva ta fram en ny e-tjänst som uppfyller kraven i SDG-förordningen för anmälningsförfarandet. PTS måste också säkerställa att de kan underrätta kommissionen elektroniskt om anmälningar. PTS ska också utöva tillsyn över leverantörerna av dataförmedlingstjänst, främst på eget initiativ men det kan också ske både efter begäran och efter klagomål från enskild. Den som lämnat in ett klagomål ska hållas underrättad om hur ärendet fortlöper. Någon skyldighet att inleda tillsyn baserat på en anmälan eller ett klagomål finns dock inte i förordningen. Tillsynsskyldigheten i förordningen omfattar primärt de som anmält sig som leverantörer av dataförmedlingstjänster och någon allmän plikt att identifiera och utreda ej anmälda aktörer är inte nödvändig enligt förordningen. PTS ska kunna utfärda erinran och sanktionsavgifter mot leverantörer av dataförmedlingstjänster. Sanktionsavgift ska också kunna beslutas för vidareutnyttjare efter anmälan från utlämnande myndigheter. Förelägganden mot leverantörer av dataförmedlingstjänster ska också kunna förenas med vite. Sanktionerna ska kunna beslutas av den behöriga myndigheten och överklagas till förvaltningsdomstol.

Kostnader för att utse PTS till behörig myndighet kommer att bestå i vissa inledande kostnader för uppbyggnad av uppgiften med tillhörande rutiner, processer och utveckling av ny e-tjänst. Kostnader kommer också att uppstå över tid för vidareutveckling och förvaltning av e-tjänst och andra tekniska lösningar för ärendehantering samt för personalresurser för hantering och granskning av anmälningar och för att utöva tillsyn. Oavsett hur många ärende som ska hanteras så måste det på myndigheten byggas upp och upprätthållas en kunskap om regelverket för att kunna hantera ärenden och frågor när dessa kommer. Eftersom det finns tekniska lösningar, processer och rutiner att utgå ifrån och eftersom antalet ärenden inte förväntas bli många bedöms uppgiften bli begränsad och den bör inte överstiga två årsarbetskrafter under de första åren.

Anmälningsförfarandet kan enligt förordningen avgiftsbeläggas. I denna promemoria föreslås att avgifts ska kunna tas ut, men att den inte ska ha full kostnadstäckning som mål. Denna avgift påverkar därför inte att uppgiften kan behöva finansieras med utökade anslag.

Införandet av bemyndigandena att få meddela föreskrifter om kompletterande informationskrav respektive avgiftsuttag medför i sig inte några konsekvenser. Om föreskrifter meddelas innebär det en engångskostnad när föreskrifter tas fram och en eventuell kostnad för utökad tillsyn.

Behörig myndighet dataaltruismorganisationer

En behörig myndighet ska utses för att hantera registreringar från dataaltruismorganisationer och för att utöva tillsyn över dessa. PTS föreslås utses till behörig myndighet och det är en ny permanent uppgift.

PTS kommer att behöva ta fram en ny e-tjänst som uppfyller kraven i SDG-förordningen för registreringsförfarandet. PTS ska också tillhandahålla ett publikt register över dataaltruism-organisationer. PTS ska därutöver utöva tillsyn över registrerade dataaltruismorganisationer, både på eget initiativ och efter begäran eller klagomål från enskild. Den som lämnat in ett klagomål ska hållas underrättad om hur ärendet fortlöper. Någon skyldighet att inleda tillsyn baserat på en anmälan eller ett klagomål finns dock inte i förordningen. Tillsyn ska bara utövas över de som ansökt om registrering som dataaltruismorganisation. Eftersom det är ett frivilligt registreringsförfarande faller andra organisationer utanför regelverket i förordningen Någon utredande verksamhet för ej anmälda aktörer finns inte. PTS ska inom ramen för tillsynen kunna utfärda erinran mot dataaltruismorganisationer.

Kostnader för att utse PTS till behörig myndighet kommer att bestå i utveckling av ny e-tjänst och ett offentligt register, förvaltning av dessa över tid samt personalresurser för granskning av ansökningar, årsrapporter och tillsynsarbete. Oavsett hur många ärende som ska hanteras så måste det på myndigheten byggas upp och upprätthållas en kunskap om regelverket för att kunna hantera ärenden och frågor när dessa kommer. Uppgiften förväntas inte bli omfattande och den bör inte överstiga en årsarbetskraft under de första åren.

Sammanfattning

PTS är redan i dag nationell tillsynsmyndighet för flera andra regelverk, såväl nationella som EU-förordningar. Myndigheten ansvarar också för olika anmälningsförfaranden och offentliga register.

Förslaget innebär nya uppgifter för myndigheten, men befintliga e-tjänster, verksamhetssystem, processer och rutiner kan användas som utgångspunkt vid utvecklingen av den nya uppgiften. Det begränsar kostnaden jämfört med om en annan myndighet som inte har samma befintliga kompetens skulle utses. Den sammantagna kostnaden per år för uppgiften beräknas till 3 miljoner kronor. Uppgiften kan finansieras genom ett ökat anslag till PTS.

Över tid kommer sannolikt en marknad med både dataförmedlingstjänster och dataaltruismorganisationer etableras. En sådan utveckling kan påverkas av ökade behov av dataförmedlingstjänster efter genomförandet av datarättsförordningen som för närvarande är under förhandling. Finansieringen kan därför behöva öka till det dubbla efter tre år.

8.1.4 Deltagande i europeiska datainnovationsstyrelsen

Bedömning: Förslagen i promemorian om att företrädare för Post- och telestyrelsen ska ingå i den europeiska datainnovationsstyrelsen och att de ska inhämta synpunkter från Myndigheten för digital förvaltning kan uppskattningsvis initialt kräva 2 miljoner kronor per år, i huvudsak för personalresurser.

Myndigheternas resursbehov kan tillgodoses genom ökade anslag.

Skälen för bedömningen: En representant för den behöriga myndigheten för dataförmedlingstjänster och dataaltruismorganisationer, PTS, ska ingå i den europeiska datainnovationsstyrelse som ska inrättas. PTS ska inhämta synpunkter från Digg i arbetet.

I förordningen finns styrelsens arbetsuppgifter och de undergrupper som ska skapas beskrivna. Det finns dock inga mer detaljerade uppgifter om hur arbetet kommer att bedrivas och hur omfattande deltagandet kommer att bli.

Av förordningen framgår att den europeiska datainnovationsstyrelsen ska få en central roll i långsiktig styrning och förvaltning, t.ex. gällande framtagande av standarder, för att uppnå interoperabilitet som förutses i denna samt andra rättsakter, dvs. det kan ses som en långsiktigt strategisk fråga att Sverige har en adekvat resurssättning för sitt deltagande i styrelsen.

Deltagandet i den europeiska datainnovationsstyrelsen förväntas inte bli en omfattande uppgift inledningsvis. Styrelsen ska dock hantera ett stort antal olika frågor, och hanteringen av dem kommer att behöva involvera fler resurser på respektive myndighet än den representant som deltar direkt i styrelsen. Arbetet i styrelsen kan också förväntas öka över tid, särskilt utifrån hur styrelsen ska samverka med andra utifrån föreslagna kommande lagstiftningsakter så som datarättsförordningen, AI-förordningen och förordning om det europeiska hälsodataområdet.

Deltagandet bedöms med försiktighet uppgå till upp till en årsarbetskraft på PTS och en halv årsarbetskraft på Digg. Deltagande i den europeiska datainnovationsstyrelsen kan finansieras genom ett ökat anslag till PTS och Digg. Detta anslag beräknas utifrån ovanstående till sammanlagt 2 miljoner per år inledningsvis. Finansiering kan på sikt också behöva finnas för deltagande av andra aktörer, antingen som deltagare i styrelsen eller inom arbetsgrupper på nationell nivå och den kan därför behöva fördubblas till år 3.

8.2 Konsekvenser för andra myndigheter och domstolar

8.2.1 Vidareutnyttjande av skyddade data från myndigheter och domstolar

Bedömning: Förslagen får inte ekonomiska konsekvenser för myndigheter som ska hantera begäran om tillgång till skyddade data för vidareutnyttjande. Myndigheternas behandling av sådana begäran bör hanteras inom befintliga budgetramar.

Förslagen förväntas inte leda till att antalet mål i de allmänna förvaltningsdomstolarna ökar i någon större omfattning och eventuella kostnadsökningar bör kunna rymmas inom befintliga ekonomiska ramar.

Skälen för bedömningen: I denna promemoria finns förslag gällande vidareutnyttjande av skyddade data från myndigheter avseende hur avgifter för att tillgängliggöra data ska beräknas, vilka myndigheter som ska utses som behöriga organ enligt artikel 7, vilken myndighet som ska tillhandahålla den gemensamma informationspunkten enligt artikel 8, redovisning av tillgängliga datamängder till den gemensamma informationspunkten, överprövning av beslut och sanktioner för vidareutnyttjares överträdelse av villkor för överföringar till tredje land. Vidare finns förslag om att vissa beslut ska kunna överklagas till allmän förvaltningsdomstol.

Dessa regler får konsekvenser för de myndigheter som innehar skyddade data som någon kan begära tillgång till för vidareutnyttjande och för domstolar som ska hantera överklagade beslut från dessa myndigheter och från den behöriga myndigheten för dataförmedlingstjänster och dataaltruismorganisationer.

Myndigheter

De myndigheter som innehar skyddade data kan få en begäran om att tillgängliggöra sådana data för vidareutnyttjande. Regelverket träffar såväl statliga som kommunala myndigheter. Myndigheter behöver först bedöma om de kan ge tillgång till den aktuella informationen och, först om det är möjligt, avgöra om det är möjligt och lämpligt att ge tillgång för vidareutnyttjande med hjälp av det ramverk som dataförvaltningsförordningen sätter upp. Medlemsstaterna ska säkerställa att offentliga myndigheter är försedda med nödvändiga resurser för att efterleva artikel 5 som reglerar de villkor som ska ställas upp vid tillgängliggörande av skyddade data för vidareutnyttjande.

De myndigheter som föreslås bli behöriga organ och som ska stötta myndigheter besitter en bred kunskap om datahantering och tillgängliggörande av data. Myndigheterna kommer därmed kunna få ett bra och kvalitativt stöd i handläggningen av en begäran.

Myndigheterna omfattas redan idag av datalagen. Den föreslagna handläggningen av ärenden enligt dataförvaltningsförordningen ska i huvudsak ske på samma sätt som befintliga ärenden avseende öppna

data. Utvecklingen av nya arbetsrutiner och informationsinsatser bör därför bli mycket begränsade.

Många myndigheter bedömer som beskrivs i avsnitt 8.1.1 att förordningens ramverk i kapitel II får liten eller ingen påverkan på dem. Utifrån detta bedöms att de myndigheter som ska tillämpa reglerna bör kunna göra det inom ramen på sin befintliga finansiering.

En myndighet får överföra konfidentiella data som en vidareutnyttjare avser överföra till tredjeland bara i enlighet med kraven i artikel 5.10. Om en myndighet gör det och får kännedom om att vidareutnyttjaren överträder de villkor som ställts upp eller genomförandeakter som kommissionen antagit avseende tredjelandsöverföringar ska myndigheten anmäla överträdelsen till den behöriga myndigheten för dataförmedlingstjänster. Anmälningsskyldigheten gällande överträdelser av artikel 5.14 till den behöriga myndigheten för dataförmedlingstjänster bedöms inte heller bli omfattande. Detta eftersom det bara kan bli aktuellt först i de fall en myndighet medgett tillgång till konfidentiella data för överföring till tredjeland i enlighet med artikel 5.10. Eftersom antalet ärenden där en vidareutnyttjare beviljas tillgång till skyddade data alls förväntas bli låg kan antalet ärenden där tillgång medges till denna typ av data för överföring till tredjeland förväntas bli än lägre. Myndigheterna ska också bara anmäla sådana överträdelser som de får kännedom om. Skyldigheten bedöms därför inte få sådana konsekvenser att de inte kan hanteras inom befintliga anslag.

Domstolar

När det gäller möjligheten att överklaga beslut till domstol så innehåller promemorian förslag på att det ska kunna ske avseende beslut som en myndighet fattar om att bevilja eller vägra tillgång till skyddade data för vidareutnyttjande samt för beslut som fattas av den behöriga myndigheten för dataförmedlingstjänster och dataaltruismorganisationer. Antalet ärenden hos såväl myndigheter som hos tillsynsmyndigheter förväntas bli låg. Ärendetyperna är förvisso nya, men de har nära samband med befintliga ärenden i domstol. Överklagande av myndigheters beslut avseende tillgängliggörande av data är en utveckling av motsvarande

överklagandemöjlighet för ärenden som rör öppna data. Överklagandemöjligheten av tillsynsmyndighetens beslut ligger i linje med motsvarande överklaganderätt för andra tillsynsbeslut.

Förslagen bedöms inte medföra att antalet mål på förvaltningsdomstolarna ökar i en omfattning som inte ryms inom Sveriges Domstolars befintliga anslag.

8.3 Konsekvenser för företagen

8.3.1 Leverantörer av dataförmedlingstjänster

Bedömning: Förslagen bedöms inte ha några konsekvenser för företagen. Förslagen bedöms inte heller ha konkurrenspåverkande effekter.

Skälen för bedömningen: Dataförvaltningsförordningen innehåller skyldigheter för leverantörer av dataförmedlingstjänster och kan därför väntas ge ekonomiska konsekvenser för sådana leverantörer. Förordningens innehåll och konsekvenser bedöms dock inte här.

De förslag som lämnas i denna promemoria om behörig myndighet, avgifter och sanktioner antas i sig inte ge några direkta ekonomiska konsekvenser för leverantörer av dataförmedlingstjänster.

Förslaget att utse PTS till behörig myndighet väntas bidra till sakkunnig tillsyn och efterlevnadskontroll, effektivitet och förutsebarhet för både leverantörer av dataförmedlingstjänster och de näringsidkare som har avtal med leverantörerna. Myndigheten väntas på effektivt sätt upprätthålla reglerna på marknaden och därmed bidra till ett sunt affärsklimat och fungerande konkurrens för alla aktörer.

Anmälningsförfarandet bör på sikt kunna avgiftsbeläggas med en avgift som syftar till full kostnadstäckning. I nuläget föreslås dock avgifter bara en mindre fast handläggningsavgift få införas. Avgifter med full kostnadstäckning för både handläggning och tillsyn föreslås inte då sådana avgifter på en marknad med få aktörer riskerar att bli oproportionerligt stora vilket skulle kunna få hämmande effekter på marknaden.

Om avgifter framöver ska ha full kostnadstäckning som målsättning kommer leverantörerna att betala en högre avgift, vilket medför en kostnad för dem. Utöver kostnaden innebär detta en administrativ börda för företagen. Det finns i förordningen möjligheter att införa en lägre eller avgift eller att avgiftsbefria mikroföretag samt små och medelstora företag om det bedöms som lämpligt.

Förslagen väntas inte påverka företag i andra avseenden.

8.3.2 Dataaltruismorganisationer

Bedömning: Förslagen bedöms inte ha några konsekvenser för företagen. Förslagen bedöms inte heller ha konkurrenspåverkande effekter.

Skälen för bedömningen: Dataförvaltningsförordningen innehåller möjligheter för dataaltruismorganisationer att ansöka om registrering som en erkänd dataaltruismorganisation. Detta ramverk kan väntas ge ekonomiska konsekvenser för sådana organisationer. Förordningens innehåll och konsekvenser bedöms dock inte här.

De förslag som lämnas i denna promemoria om behörig myndighet och sanktioner antas i sig inte ge några direkta ekonomiska konsekvenser för dataaltruismorganisationer.

Förslaget att utse PTS till behörig myndighet väntas bidra till sakkunnig tillsyn och efterlevnadskontroll, effektivitet och förutsebarhet för både dataaltruismorganisationer och de fysiska och juridiska personer som delar med sig av sina data till organisationen. Myndigheten väntas på effektivt sätt upprätthålla reglerna på marknaden och därmed bidra till ett sunt affärsklimat och fungerande konkurrens för alla aktörer och att dataaltruismorganisationer kan utföra sina uppgifter för mål av allmänt intresse i enlighet med förordningen.

Förslagen väntas inte påverka företag i andra avseenden.

8.4 Övriga konsekvenser

Bedömning: Förslagen syftar till att uppnå en effektiv, enhetlig och ändamålsenlig tillämpning av EU-förordningen.

Förslagen bedöms förenligt med EU-rätten och förväntas inte få några konsekvenser för brottsligheten, för jämställdheten mellan kvinnor och män eller för de nationella klimat- och miljömålen.

Skälen för bedömningen: Förslaget påverkar inte det materiella innehållet i EU-förordningen och bedöms i övrigt vara förenligt med EU-rätten.

Förslagen bedöms inte påverka den kommunala självstyrelsen eller sysselsättningen. Förslaget väntas inte få några konsekvenser för brottsligheten och det brottsförebyggande arbetet, för jämställdheten mellan kvinnor och män, för de nationella klimat- och miljömålen eller för de integrationspolitiska målen.

8.5 Konsekvenser av dataförvaltningsförordningen

Dataförvaltningsförordningen är direkt tillämplig som lag i Sverige. De bestämmelser som finns direkt i förordningen kommer att leda till konsekvenser för såväl myndigheter, företag, organisationer och privatpersoner i Sverige.

EU-kommissionen tog i samband med att det första förslaget till förordningen togs fram också fram en konsekvensanalys avseende förordningen, Commission staff working document impact assessment report Accompanying the document Proposal for a regulation of the European parliament and of the Council on European data governance (Data Governance Act), hädanefter konsekvensanalys. I konsekvensanalysen finns en närmare genomgång av förordningens ekonomiska konsekvenser, sociala och miljömässiga påverkan samt konsekvenser för små och medelstora företag. Detta då det är på dessa områden som förordningen förväntas få störst påverkan enligt en bredare s.k. multikriterieanalys som genomfördes innan konsekvensutredningen (konsekvensanalys s. 85).

Beskrivningen och beräkningen av konsekvenserna tar sitt avstamp i de förväntade konsekvenserna för EU:s datastrategi eftersom förordningen är en del av genomförandet av strategin.

Kommissionen konstaterar i sin konsekvensanalys att införandet av förordningen skulle leda till påvisbara fördelar jämfört nollalternativet att inte införa den föreslagna förordningen (konsekvensanalys s. 93). Genom förordningen säkerställs att datadelning kan ske mellan sektorer och mellan medlemsstater inom unionen. De positiva effekterna uppnås bara genom harmoniserande EU-initiativ som når hela den inre marknadens omfattning med dess potential och stordriftsfördelar.

Insatserna som införs genom förordningen kommer enligt konsekvensanalysen att förbättra den inre marknaden för data, och därmed den inre marknaden som helhet. I framtiden menar kommissionen att produkter och tjänster kommer till nytta i olika skeden, från big data-analyser, användning av sensordata (IoT) och maskininlärning (konsekvensanalys s. 93). Säkra produkter och tjänster med tillgång till stora datamängder är centralt för denna utveckling. En sådan utveckling är svår att genomföra genom nationella regelverk i olika medlemsstater, och då särskilt för små och medelstora länder. Genom en EU-förordning som är direkt tillämpbar i alla medlemsstater så blir det lättare för företag att anpassa sina produkter eller tjänster som utvecklats i en medlemsstat till marknaden för andra medlemsstater.

Ett mer harmoniserat regelverk för att på ett kontrollerat sätt dela uppgifter mellan medlemsstater och sektorer innebär fördelar för industrisektorer och aktörer i hela värdekedjan. Detta oavsett deras skillnader i storlek eller olika medlemsstater. Ett mer likformigt och samordnat europeiskt tillvägagångssätt kan utgöra ett alternativ till de nuvarande affärsmodellerna kring data och datadelning som domineras av Big Tech-plattformar. Förordningen ska enligt kommissionens konsekvensanalys minska fragmenteringen i de rättsliga och politiska ramverken för data (inklusive frånvaron av dem), som för närvarande står i vägen för att skapa gemensamma europeiska dataområden och en dataekonomi som är transparent, effektiv och betrodd (konsekvensanalys s. 93).

9 Författningskommentar

9.1 Förslaget till lag med kompletterande bestämmelser till EU:s dataförvaltningsförordning

Inledande bestämmelse

1 § Denna lag kompletterar Europaparlamentets och rådets förordning (EU) 2022/868 av den 30 maj 2022 om europeisk dataförvaltning och om ändring av förordning (EU) 2018/1724 (dataförvaltningsakten), nedan EU:s dataförvaltningsförordning.

Termer och uttryck i lagen har samma betydelse som i EU:s dataförvaltningsförordning.

I paragrafen anges bl.a. att lagen kompletterar Europaparlamentets och rådets förordning (EU) 2022/868. Övervägandena finns i avsnitt 5.3.2 och 5.3.3.

I *första stycket* anges att lagen innehåller kompletterande bestämmelser till dataskyddsförordningen. Detta innebär att lagen inte kan tillämpas fristående, utan endast tillsammans med dataförvaltningsförordningen. Hänvisningen till EU-förordningen i första stycket, liksom hänvisningarna i lagen i övrigt till EU-förordningen, är utformad så att den avser förordningen i den vid varje tidpunkt gällande lydelsen, s.k. dynamisk hänvisning. När det hänvisas till dataförvaltningsförordningen i lagen är det alltså dess gällande lydelse som avses.

Av *andra stycket* framgår att de termer och uttryck som används i lagen, exempelvis behörig myndighet, dataförmedlingstjänst och dataaltruism, ska förstås på samma sätt som i dataförvaltningsförordningen. Det innebär att definitionerna i artikel 2 i dataförvaltningsförordningen även gäller vid tillämpningen av lagen. Också sådana termer och uttryck som används i dataförvaltnings-

förordningen utan att definieras där, ska tolkas och tillämpas på samma sätt när de förekommer i lagen. Som exempel kan nämnas uttrycket vidareutnyttjare (6 §).

Tillsynsmyndighet

2 § Den myndighet som regeringen bestämmer ska vara tillsynsmyndighet enligt denna lag. Den myndighet som är tillsynsmyndighet enligt denna lag är behörig myndighet för dataförmedlingstjänster enligt artikel 13 EU:s dataförvaltningsförordning och behörig myndighet för registrering av dataaltruismorganisationer enligt artikel 23 EU:s dataförvaltningsförordning.

I paragrafen ges regeringen mandat att bestämma vilken myndighet som ska vara tillsynsmyndighet och därmed behörig myndighet för dataförmedlingstjänster och dataaltruismorganisationer. Övervägandena finns i avsnitt 5.4, 5.5, 5.6 och 5.7.

Dataförvaltningsförordning förutsätter att medlemsstaterna utser behöriga myndigheter som också ska vara tillsynsmyndigheter för både leverantörer av dataförmedlingstjänster och för erkända dataaltruismorganisationer. Genom paragrafen regleras att en och samma myndighet ska utses till behörig myndighet för dataförmedlingstjänster och till behörig myndighet för registrering av dataaltruismorganisationer.

Uppgifterna för den behöriga myndigheten för dataförmedlingstjänster framgår av artiklarna 11, 13, 14, 27 och 28 dataförvaltningsförordningen. Den behöriga myndigheten ska ta emot anmälningar från leverantörer av dataförmedlingstjänster i enlighet med artikel 11. Myndigheten ska också övervaka och utöva tillsyn över leverantörernas efterlevnad av kraven i dataförvaltningsförordningen. I 13 § finns ett bemyndigande för att avgiftsbelägga anmälningsförfarandet. Den behöriga myndighetens tillsynsuppgift regleras närmare i artikel 14. Där framgår att tillsyn får ske både på tillsynsmyndighetens eget initiativ, på begäran från en fysisk eller juridisk person eller efter klagomål enligt artikel 27.1. Den behöriga myndigheten har befogenhet att begära in nödvändig information från leverantören av dataförmedlingstjänster, artikel 14.2. Om myndigheten finner att en leverantör inte uppfyller ett eller flera krav ska den meddela leverantören detta och ge den möjlighet att yttra sig inom 30 dagar, artikel 14.3. Den behöriga myndigheten har

också befogenhet att förelägga en leverantör av en dataförmedlingstjänst att upphöra med en överträdelse och vidta åtgärder för att säkerställa efterlevnad. Sådana åtgärder kan t.ex. vara att förena förelägganden med vite (5 §), att besluta om en erinran (4 §) eller en sanktionsavgift (6–11 §§). Den behöriga myndigheten kan också kräva att tillhandahållandet av tjänsten skjuts upp eller upphör, artikel 14.4.

Uppgifterna för den behöriga myndigheten för dataaltruismorganisationer framgår av artiklarna 17, 19, 20, 23, 24, 27 och 28 dataförvaltningsförordningen. Den behöriga myndigheten ska ta emot ansökningar om att registreras som erkänd dataaltruismorganisation och tillhandahålla ett offentligt register över dessa enligt artikel 17 och 19. Myndighetens tillsynsansvar regleras i artikel 24 och det innefattar utöva tillsyn över dataaltruismorganisationernas efterlevnad av kraven i dataförvaltningsförordningen. I artikel 24 framgår att tillsyn kan ske både på tillsynsmyndighetens eget initiativ, på begäran från en fysisk eller juridisk person eller efter klagomål enligt artikel 27.1. Den behöriga myndigheten för dataaltruismorganisationer har befogenhet att begära in nödvändig information från leverantören av dataförmedlingstjänster, artikel 24.2. Om myndigheten finner att en erkänd dataaltruismorganisation inte uppfyller ett eller flera krav ska den meddela organisationen detta och ge den möjlighet att yttra sig inom 30 dagar, artikel 24.3. Den behöriga myndigheten för dataaltruismorganisationer har befogenhet att kräva att en överträdelse upphör, artikel 24.4, och den kan besluta att en erkänd dataaltruismorganisation förlorar sin rätt att använda beteckningen ”dataaltruismorganisation som är erkänd i unionen”, artikel 24.5. Den behöriga myndigheten kan också utfärda erinran mot dataaltruismorganisationer vid överträdelser (4 §)

En representant för tillsynsmyndigheten ska vidare delta i den europeiska datainnovationsstyrelsen som inrättas genom dataförvaltningsförordningen.

Informationsutbyte

3 § De myndigheter regeringen bestämmer ska på begäran lämna tillsynsmyndigheten de uppgifter som den behöver för att kunna utföra sitt tillsynsuppdrag enligt EU:s dataförvaltningsförordning.

Tillsynsmyndigheten ska på begäran lämna de uppgifter som andra myndigheter som regeringen bestämmer behöver för att kunna utföra tillsynsuppdrag enligt annan författning.

Paragrafen innehåller ett bemyndigande för att införa en uppgiftsskyldighet mellan tillsynsmyndigheten enligt lagen och andra tillsynsmyndigheter. Övervägandena finns i avsnitt 5.9.3.

Den behöriga myndigheten för dataförmedlingstjänster och dataaltruismorganisationer behöver enligt dataförvaltningsförordningen kunna samverka med tillsynsmyndigheter på andra områden. Tillsynsområdet för dataförmedlingstjänster gränsar framför allt mot befintliga tillsynsuppdrag som IMY har på dataskyddsområdet och som Konkurrensverket har på konkurrensrättens område Den behöriga myndigheten behöver kunna samverka med dessa myndigheter och dela information. Samverkan kommer i första hand att avse samordning av tillsyn vid behov, överlämning av ärenden eller enskilda frågor inom ett ärende som rör en annan tillsynsmyndighets område eller samverkan för att kunna avgöra enligt vilket regelverk ett visst förfarande ska bedömas.

Genom paragrafen möjliggörs en uppgiftsskyldighet mellan tillsyns-myndigheten enligt lagen och andra tillsynsmyndigheter. Genom denna uppgiftsskyldighet blir den sekretessbrytande bestämmelsen i 10 kap. 28 § OSL tillämplig. Uppgiftsskyldigheten avser bara sådana uppgifter som respektive myndighet behöver för att kunna genomföra sina tillsynsuppdrag enligt olika regelverk.

Vilka myndigheter som tillsynsmyndigheten ska kunna utbyta information med och vilka övriga tillsynsregelverk som ska beaktas framgår i förordningen till lagen.

Erinran

4 § Tillsynsmyndigheten får meddela en erinran till en leverantör av dataförmedlingstjänster som bryter mot anmälningsskyldigheten enligt artikel 11, villkoren för tillhandahållande av dataförmedlingstjänster enligt artikel 12 eller villkoren för överföring av andra uppgifter än personuppgifter till tredjeland enligt artikel 31 EU:s dataförvaltningsförordning.

Tillsynsmyndigheten får meddela en erinran till en erkänd dataaltruismorganisation som bryter mot villkoren för registrering som erkänd dataaltruismorganisation i artiklarna 18, 20, 21 och 22 eller villkoren för överföring

av andra uppgifter än personuppgifter till tredjeland enligt artikel 31 EU:s dataförvaltningsförordning.

Paragrafen innehåller en möjlighet för den behöriga myndigheten att meddela en erinran för vissa överträdelser av dataförvaltningsförordningen. Övervägandena finns i avsnitt 5.8.1 och 5.8.5.

Medlemsländerna ska enligt artikel 34 dataförvaltningsförordningen fastställa sanktioner för överträdelser av vissa bestämmelser iförordningen. Sanktionerna ska vara effektiva, proportionella och avskräckande. Erinran är en av de sanktioner som ska kunna utfärdas.

Innan ett ingripande görs kan det i vissa fall vara aktuellt med påpekanden och rekommendationer för att få till stånd en frivillig rättelse.

I dataförvaltningsförordningen finns möjligheter för den behöriga myndigheten att inom ramen för tillsynen meddela en leverantör av en dataförmedlingstjänst eller dataaltruismorganisation som inte uppfyller tillämpliga krav om de iakttagelser som gjorts och ge dem möjlighet att yttra sig inom 30 dagar, artikel 14.3 respektive 24.3.

Det finns vidare en möjlighet för den behöriga myndigheten att besluta att en leverantörs tillhandahållande av en dataförmedlingstjänst ska skjutas upp, avbrytas eller upphöra, artikel 14.4. Den behöriga myndigheten får också besluta att återkalla rätten att använda beteckningen ”dataaltruismorganisation som är erkänd i unionen”, artikel 24.5. Ett sådant avbrott i tillhandahållande av en tjänst eller återkallande av rätten att använda beteckningen är de allvarligaste ingripandeåtgärderna som tillsynsmyndigheten har.

Om leverantören av dataförmedlingstjänsten eller dataaltruismorganisationen vidtar åtgärder för att säkerställa att de efterlever förordningen och överträdelse av förordningen inte är så allvarlig att avbrytande av tillhandahållandet av tjänsten eller en återkallelse av rätten att använda beteckningen inte är aktuell kan en annan mildare sanktion vara lämplig. Den behöriga myndigheten kan då i stället besluta om en erinran.

För överträdelser som leverantörer av dataförmedlingstjänster gör sig skyldiga till kan i stället sanktionsavgifter enligt 6 § vara en lämplig sanktion vid allvarligare överträdelser.

Vite

5 § Tillsynsmyndigheten får förena förelägganden enligt artikel 14 EU:s dataförvaltningsförordning med vite.

Paragrafen stadgar att förelägganden mot leverantörer av dataförmedlingstjänster ska kunna förenas med vite. Övervägandena finns i avsnitt 5.8.4.

Tillsynsmyndigheten är enligt 2 § behörig myndighet för dataförmedlingstjänster. Av artikel 14.4 i dataförvaltningsförordningen framgår att den behöriga myndigheten för dataförmedlingstjänster genom administrativa förfaranden får ålägga leverantörerna avskräckande ekonomiska sanktioner. Dessa får inbegripa löpande viten.

Att ha möjlighet att hämta in uppgifter från tillsynsobjekt är ett viktigt redskap i all slags tillsynsverksamhet. De inhämtade uppgifterna ingår i underlaget för tillsynsorganets granskning och beslut. En sådan möjlighet finns gentemot leverantörer av dataförmedlingstjänster i artikel 14.2. Om den som uppgiftsskyldigheten åvilar motsätter sig att lämna ut uppgifter ska denne vid vite kunna föreläggas att uppfylla sin skyldighet. I dataförvaltningsförordningen finns vidare möjligheter att utfärda åtgärdsförelägganden till leverantörer av dataförmedlingstjänster och kräva att en identifierad överträdelse upphör, artikel 14.4. Ett sådant åtgärdsföreläggande kan förenas med vite. Föreläggandet avser pågående överträdelser och tillsynsmyndigheten ska ge leverantören en rimlig tid att vidta åtgärder och det inte avser allvarliga överträdelser då överträdelsen ska upphöra omedelbart.

Om den behöriga myndigheten finner att en leverantör av en dataförmedlingstjänst inte uppfyller ett eller flera krav ska den meddela leverantören detta och ge den möjlighet att yttra sig, artikel 14.3. Ett sådant meddelande är inte ett föreläggande och kan därför inte förenas med vite.

Dubbelprövningsförbudet kan aktualiseras då vite utdöms för överträdelser som också kan leda till sanktionsavgifter. Detta regleras i 8 §.

Föreläggande av vite ska ske i enlighet med lag (1985:206) om viten, vilken bl.a. stadgar att vitesförelägganden ska delges (2 §) och att utdömande av viten prövas av förvaltningsrätt på ansökan av den myndighet som utfärdat vitesföreläggandet (6 §).

Sanktionsavgifter

6 § Tillsynsmyndigheten får ta ut en sanktionsavgift av en leverantör av en dataförmedlingstjänst vid överträdelser av

- anmälningsskyldigheten för leverantören av dataförmedlingstjänster enligt artikel 11,
- villkoren för tillhandahållande av dataförmedlingstjänster enligt artikel 12, eller
- villkoren för överföring av andra uppgifter än personuppgifter till tredjeland enligt artikel 31 EU:s dataförvaltningsförordning.

Tillsynsmyndigheten får ta ut en sanktionsavgift av en vidareutnyttjare för överträdelser av artikel 5.14 i EU:s dataförvaltningsförordning.

Paragrafen reglerar att en sanktionsavgift får tas ut av tillsynsmyndigheten i vissa fall. Övervägandena finns i avsnitt 5.8.6 och 5.8.8.

En sanktionsavgift riktar sig mot en konstaterad överträdelse av en författningsbestämmelse. Sanktionsavgifterna bygger på strikt ansvar. Det krävs alltså varken uppsåt eller oaktsamhet för att sanktionsavgift ska kunna åläggas, utan det är tillräckligt att en överträdelse har skett.

En sanktionsavgift får enligt *första stycket* tas ut från leverantörer av dataförmedlingstjänster vid vissa överträdelser av dataförvaltningsförordningen. Sanktionsavgifter ska kunna komma i fråga för leverantörer av dataförmedlingstjänster för överträdelser mot anmälningsskyldigheten enligt artikel 11, villkoren för tillhandahållande enligt artikel 12 dataförvaltningsförordningen samt för villkoren för överföring av andra uppgifter än personuppgifter till tredjeland enligt artikel 31.

En sanktionsavgift får enligt *andra stycket* också tas ut från en vidareutnyttjare för överträdelser mot artikel 5.14. En myndighet som överför s.k. konfidentiella data till en vidareutnyttjande för överföring till tredjeland får bara göra det i enlighet med vissa krav i artikel 5. Med konfidentiella data avses enligt artikel 5.8 data som skyddas som affärshemligheter eller av statistiksekretess. Om en vidareutnyttjare som får tillgång till konfidentiella data för överföring till tredje land bryter mot artikel 5.14, som i sin tur hänvisar tillbaka till artikel 5.10, 5.12 och 5.13, ska den kunna träffas av en sanktion enligt artikel 34. Genom andra stycket regleras att sanktionen ska kunna vara en sanktionsavgift och att det är tillsynsmyndigheten som kan besluta om den.

Tillsynsmyndigheten har inte tillsynsansvar över regelverket i kapitel II i förordningen där artikel 5 återfinns. Tillsynsmyndigheten ska ta ställning till frågan om sanktionsavgift först om den får en anmälan från den myndighet som tillgängliggjort konfidentiella data för vidareutnyttjande. Den utlämnande myndigheten har enligt 2 kap. 5 a § andra stycket lagen om den offentliga sektorns tillgänglig-görande av data en skyldighet att göra en sådan anmälan om den får kännedom om att vidareutnyttjaren gjort sig skyldig till överträdelser.

Bedömningen av om en sanktionsavgift ska utgå och hur stor den i så fall ska vara ska göras på det underlag som den anmälande myndigheten lämnat. Tillsynsmyndigheten har inte någon vidare utredningsskyldighet utöver förvaltningslagens krav och ärendet ska handläggas på handlingarna. Tillsynsmyndigheten kan begära kompletterande uppgifter från både den anmälande myndigheten och vidareutnyttjaren. Inför beslut ska tillsynsmyndigheten kommunicera underlaget med vidareutnyttjaren i enlighet med förvaltningslagen.

Tillsynsmyndigheten har enligt 7 § tredje stycket möjlighet att i vissa fall helt eller delvis efterge sanktionsavgiften. Enligt 8 § får tillsynsmyndigheten inte besluta om sanktionsavgift om överträdelsen omfattas av ett föreläggande som har förenats med vite och den ligger till grund för en ansökan om utdömande av vitet.

7 § En sanktionsavgift ska bestämmas till lägst 5 000 kronor och högst 10 000 000 kronor.

När avgiftens storlek bestäms ska särskild hänsyn tas till

1. överträdelsens art, allvar, omfattning och varaktighet,
2. eventuella åtgärder som leverantören av dataförmedlingstjänster eller vidareutnyttjaren vidtagit för att begränsa eller avhjälpa den skada som överträdelsen har orsakat,
3. tidigare överträdelser som leverantören av dataförmedlingstjänster eller vidareutnyttjaren har gjort sig skyldig till,
4. de ekonomiska vinster som leverantören av dataförmedlingstjänster eller vidareutnyttjaren gjort eller de förluster som de undvikit till följd av överträdelsen, och
5. andra försvårande eller förmildrande omständigheter.

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

Paragrafen reglerar hur sanktionsavgiften ska bestämmas. Övervägandena finns i avsnitt 5.8.9 och 5.8.10.

I *första stycket* fastställs det lägsta och det högsta beloppet för en sanktionsavgift. Beloppsintervallet är förhållandevis stort. Detta för att ge tillsynsmyndigheten möjlighet att göra en nyanserad bedömning i det enskilda fallet när avgiftens storlek ska bestämmas. På så sätt kan sanktionsavgiften vara både effektiv och avskräckande men ändå i det enskilda fallet beslutas på ett proportionerligt sätt. De högsta beloppen ska vara reserverade för de mest allvarliga överträdelserna.

Av *andra stycket* framgår de omständigheter som särskilt ska beaktas när en sanktionsavgift bestäms i det enskilda fallet. Det är inte möjligt att på förhand ange precis vad som ska beaktas i varje enskilt fall. De kriterier som ska beaktas enligt andra stycket grundar sig på uppräkningen av vägledande kriterier för sanktioner i artikel 34.2 dataförvaltningsförordningen.

Enligt *punkten 1* ska tillsynsmyndigheten särskilt beakta överträdelsens art, allvar, omfattning och varaktighet. Genom detta ges ett utrymme för att beakta närmare vad överträdelsen avsett, vad den fått för effekt och hur omfattande den varit både i sig själv och vad gäller varaktighet i tid.

Enligt *punkten 2* ska åtgärder som leverantören vidtagit för att begränsa eller avhjälpa den skada som överträdelsen kan ha orsakats beaktas. Sådana skademinimerande åtgärder kan tala i mildrande riktning vid bestämmande av en sanktionsavgift.

Eventuella tidigare överträdelser ska enligt *punkten 3* beaktas. Tidigare överträdelser kan vara tidigare överträdelser av samma sort som är aktuell vid bedömningen eller andra överträdelser som samma aktör gjort sig skyldig till. Tidigare överträdelser talar i försvårande riktning.

Enligt *punkten 4* ska ekonomiska vinster eller undvikta förluster också påverka storleken på sanktionsavgiften. En överträdelse av dataförvaltningsförordningens regler kan innebära att leverantören av dataförmedlingstjänster gjort ekonomiska vinster eller undvikit ekonomiska förluster. Detsamma kan gälla för vidareutnyttjare som inte följt kraven i artikel 5 vid överföring av konfidentiella data till tredje land. Sådana ekonomiska vinster och förluster ska direkt påverka storleken på sanktionsavgiften.

I *punkten 5* finns en övrig punkt som tydliggör att uppräkningen inte är uttömmande utan att också andra omständigheter kan påverka bestämmandet av sanktionsavgift i såväl försvårande som förmildrande riktning. Genom detta ges tillsynsmyndigheten ett brett mandat att göra självständiga och ändamålsenliga bedömningar vid bestämmandet av storleken på sanktionsavgifter. Det kan t.ex. vara relevant att beakta tillhandahållarens finansiella ställning eller att tillsynsobjektet samarbetat med tillsynsmyndigheten för att komma till rätta med överträdelsen.

Enligt *tredje stycket* får tillsynsmyndigheten i undantagsfall avstå från att ta ut en sanktionsavgift helt eller delvis. Det kan t.ex. vara fråga om en bagatellartad överträdelse som inte har varit till men för något allmänt eller enskilt intresse. En överträdelse kan vara ursäktlig och leda till att avgift inte tas ut eller sätts ned om det har varit närmast omöjligt för den avgiftsskyldige att upptäcka överträdelsen eller om den på annat sätt varit utanför den avgiftsskyldiges kontroll. Avsikten är dock inte att sanktionsavgiften ska sättas ned på grund av bristande kännedom om reglerna, dålig ekonomi, tidsbrist, bristande rutiner eller liknande.

8 § En sanktionsavgift får inte beslutas om överträdelsen omfattas av ett föreläggande som har förenats med vite och överträdelsen ligger till grund för en ansökan om utdömande av vitet.

Paragrafen syftar till att hindra dubbla prövningar och sanktioner av samma överträdelse. Övervägandena finns i avsnitt 5.8.11.

Om ett vitesföreläggande inte följs, kan tillsynsmyndigheten välja att ansöka om utdömande av vitet eller att besluta om en sanktionsavgift om förutsättningarna för det är uppfyllda. När en domstolsprocess om utdömande av vite har inletts är dock tillsynsmyndigheten förhindrad att besluta om sanktionsavgift för samma överträdelse.

9 § En sanktionsavgift får inte beslutas om den som avgiften ska tas ut av inte har fått tillfälle att yttra sig inom två år från den dag då överträdelsen ägde rum.

Ett beslut om sanktionsavgift ska delges.

Paragrafen reglerar bl.a. preskriptionstiden för sanktionsavgifter. Övervägandena finns i avsnitt 5.8.12.

Första stycket innebär att kommunikation enligt 25 § förvaltningslagen (2017:900) måste ske inom två år för att en sanktionsavgift ska få beslutas. Bevisbördan för att kommunikation har skett ligger på tillsynsmyndigheten. Tidsfristen räknas från när överträdelsen ägde rum. I fråga om en överträdelse som skett löpande under viss tid är det tillräckligt att kommunikation sker inom två år från det att överträdelsen upphörde för att en sanktionsavgift ska kunna åläggas.

Andra stycket innebär att ett beslut om sanktionsavgift ska delges den avgiftsskyldige med hjälp av något av de förfaranden för delgivning som regleras i delgivningslagen (2010:1932).

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

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

En sanktionsavgift tillfaller staten.

Paragrafen reglerar betalning och indrivning av sanktionsavgifter. Övervägandena finns i avsnitt 5.8.12.

Om avgiften inte betalas inom den angivna tiden, är tillsynsmyndigheten skyldig att lämna den obetalda avgiften för indrivning enligt lagen om indrivning av statliga fordringar m.m. För att sanktionssystemet ska bli tillräckligt effektivt ska en sanktionsavgift som inte betalats inom angiven tid få verkställas enligt utsökningsbalken. Det innebär att den kan drivas in utan att det krävs något domstolsavgörande.

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

Paragrafen anger en bortre tidsgräns för när en beslutad sanktionsavgift kan drivas in. Övervägandena finns i avsnitt 5.8.11.

En beslutad sanktionsavgift preskriberas i den utsträckning verkställighet inte har skett inom fem år från det att beslutet fick laga kraft.

Avgifter

12 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om skyldighet för den som omfattas av anmälningsskyldigheten enligt artikel 11 EU:s dataförvaltningsförordning att betala avgift för tillsynsmyndighetens verksamhet enligt EU:s dataförvaltningsförordning och denna lag.

Paragrafen innehåller ett bemyndigande gällande avgifter. Övervägandena finns i avsnitt 5.3.1.

Enligt bestämmelsen bemyndigas regeringen eller den myndighet som regeringen bestämmer att meddela föreskrifter om avgifter. Paragrafen är utformad på motsvarande sätt som andra avgiftsregleringar inom PTS verksamhetsområde, bl.a. 4 kap. 21 § postlagen och 9 § lagen (2019:181) med kompletterande bestämmelser till EU:s förordning om gränsöverskridande paketleveranstjänster.

Bestämmelsen gör det möjligt att införa ett avgiftsuttag i enlighet med artikel 11 dataförvaltningsförordningen för att finansiera den nationella tillsynsmyndighetens verksamhet enligt artikel 14. Avgifter ska kunna tas ut från leverantörer av dataförmedlingstjänster.

Överklagande

13 § Tillsynsmyndighetens beslut enligt artikel 14, 19 och 24 EU:s dataförvaltningsförordning eller enligt denna lag får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

I paragrafen regleras rätten att överklaga tillsynsmyndighetens beslut. Övervägandena finns i avsnitt 5.8.13.

För beslut som fattas enligt en EU-förordning följer rätten att överklaga av allmänna förvaltningsrättsliga principer och rätten att överklaga framgår av förvaltningslagen. Någon särskild överklagandebestämmelse behövs därmed i och för sig inte i nationell lagstiftning när det gäller de beslut som den behöriga myndigheten fattar enligt dataförvaltningsförordningen. Däremot behövs det särskilda bestämmelser om rätten att överklaga tillsynsmyndighetens beslut enligt den nya lagen, dvs. om att utfärda erinran och att ta ut sanktionsavgifter.

Hur beslut ska kunna överklagas är uttömmande reglerat i 13 § och omfattar också rätten att överklaga tillsynsmyndighetens beslut enligt dataförvaltningsförordningen.

Enligt 42 § förvaltningslagen får ett beslut överklagas av den som beslutet angår, om det har gått honom eller henne emot. Ett beslut får enligt 41 § förvaltningslagen överklagas om beslutet kan antas påverka någons situation på ett inte obetydligt sätt. I 40 § samma lag anges att beslut överklagas till allmän förvaltningsdomstol och att prövningstillstånd krävs vid överklagande till kammarrätten.

Klagorätt tillkommer alltså den som beslutet angår, om beslutet har gått denne emot. I praktiken innebär detta i normalfallet att det är leverantören av en dataförmedlingstjänst eller en dataaltruism-organisation som har rätt att överklaga. Det kan dock inte uteslutas att ett beslut skulle kunna ha rättsligt bindande följder även för andra än den som beslutet riktas mot. Dessa skulle i så fall också ha rätt att överklaga beslutet, enligt förvaltningslagens generella bestämmelse om klagorätt.

9.2 Förslaget till lag om ändring i lagen (2022:818) om den offentliga sektorns tillgängliggörande av data

1 kap. Inledande bestämmelser

1 a § Denna lag kompletterar Europaparlamentets och rådets förordning (EU) 2022/868 av den 30 maj 2022 om europeisk dataförvaltning och om ändring av förordning (EU) 2018/1724 (dataförvaltningsakten), nedan EU:s dataförvaltnings-förordning.

Paragrafen är ny och anger att datalagen innehåller bestämmelser som kompletterar dataförvaltningsförordningen. Övervägandena finns i avsnitt 4.4.1.

Lagen reglerar den offentliga sektorns tillgängliggörande av data för vidareutnyttjande. I dataförvaltningsförordnings kapitel II regleras vidareutnyttjande av vissa kategorier av skyddade data som innehas av offentliga myndigheter. I förordningen finns ett ramverk med villkor för hur sådana data kan tillgängliggöras när det är möjligt. Förordningen är direkt tillämplig i medlemsländerna. Lagen

kompletterar ramverket i förordningen bl.a. gällande hur ärenden ska hanteras, hur avgifter får beräknas och hur beslut kan överklagas.

I paragrafen ges också förordningen en egen benämning, EU:s dataförvaltningsförordning, som också används i 1 kap. 1 a, 4 och 10 §§, 2 kap. 5 a §, 3 kap. 1 a § och 4 kap. 2 a §.

2 § Denna lag påverkar inte tillämpningen av bestämmelser i någon annan lag eller förordning som ger någon rätt att få tillgång till data *eller skyddade data* eller som begränsar en sådan rätt.

Paragrafen anger hur lagen förhåller sig till författningar som reglerar tillgång till data. Övervägandena finns i avsnitt 4.5.1.

Dataförvaltningsförordningens regler om tillgängliggörande av skyddade data för vidareutnyttjande ger inte någon rätt till tillgång till information, utan regelverket avser frågan om *hur* information kan och ska tillhandahållas, dvs. frågor om avgifter och andra villkor för tillgängliggörande. De kompletterande bestämmelserna i lagen reglerar på motsvarande sätt inte frågan om tillgång till skyddade data.

Med skyddade data menas sådana skyddade data som avses i artikel 3.1 i dataförvaltningsförordningen. Uttrycket förklaras närmare i 4 §.

3 § Om det i någon annan lag eller i en förordning finns mer långtgående krav i fråga om tillgängliggörande av data *eller skyddade data* än i denna lag, ska de kraven tillämpas.

Paragrafen anger hur lagen förhåller sig till författningar som reglerar hur data ska göras tillgängliga. Genom ett tillägg av uttrycket *skyddade data* tydliggörs att lagen inte heller påverkar tillgången till sådana data. Med skyddade data menas sådana skyddade data som avses i artikel 3.1 i dataförvaltningsförordningen. Uttrycket förklaras närmare i 4 §.

Ord och uttryck i lagen

4 § I lagen avses med

begäran om tillgängliggörande av data för vidareutnyttjande: en begäran om att data *eller skyddade data* ska göras tillgängliga för vidareutnyttjande i enlighet med denna lag *eller kapitel II EU:s dataförvaltningsförordning*,

bulknedladdning: nedladdning av en avgränsad datamängd,

data: information i digitalt format oberoende av medium,

dynamiska data: data som uppdateras ofta eller i realtid för att vara aktuella och relevanta att vidareutnyttja,

forskningsdata: data som till någon del är offentligt finansierade, som samlas in eller framställs inom ramen för vetenskaplig forskningsverksamhet och som görs direkt tillgängliga för vidareutnyttjande genom en dataplattform som är allmänt åtkomlig,

gränssnitt: en regeluppsättning för dynamiskt datautbyte mellan programvaror,

maskinläsbart format: ett filformat som är strukturerat på ett sådant sätt att det enkelt kan läsas av ett datorprogram,

offentligt företag: ett företag som en eller flera myndigheter har ett bestämmande inflytande över och som är verksamt

- inom de sektorer som framgår av 2 kap. 1 § och 5-8 §§ lagen (2016:1146) om upphandling inom försörjningssektorerna,
- som ett kollektivtrafikföretag enligt Europaparlamentets och rådets förordning (EG) nr 1370/2007 av den 23 oktober 2007 om kollektivtrafik på järnväg och väg och om upphävande av rådets förordning (EEG) nr 1191/69 och (EEG) nr 1107/70,
- som ett lufttrafikföretag som har allmän trafikplikt enligt artikel 16 i Europaparlamentets och rådets förordning (EG) nr 1008/2008 av den 24 september 2008 om gemensamma regler för tillhandahållande av lufttrafik i gemenskapen, eller
- som ett rederi inom gemenskapen som uppfyller förpliktelser vid allmän trafik enligt artikel 4 i rådets förordning (EEG) nr 3577/92 av den 7 december 1992 om tillämpning av principen om frihet att tillhandahålla tjänster på sjötransportområdet inom medlemsstaterna (cabotage),

offentligt styrt organ: ett sådant organ som avses i 1 kap. 18 § lagen (2016:1145) om offentlig upphandling eller en sammanslutning av sådana organ,

skyddade data: sådana kategorier av skyddade data som avses i artikel 3.1 EU:s dataförvaltningsförordning,

vidareutnyttjande: bearbetning av data från den offentliga sektorn för valfritt ändamål,

värdefull datamängd: data som förtecknas i en genomförandeakt som har meddelats med stöd av artikel 14.1 i öppna data-direktivet,

öppna data-direktivet: Europaparlamentets och rådets direktiv (EU) 2019/1024 av den 20 juni 2019 om öppna data och vidareutnyttjande av information från den offentliga sektorn.

Paragrafen redogör för innebörden av vissa ord och uttryck. Övervägandena finns i avsnitt 4.4.2.

Genom ändringen av paragrafen ändras ett uttryck och ett nytt uttryck införs.

Med begäran om tillgängliggörande av data för vidareutnyttjande avses efter ändringen såväl begäran enligt lagen som enligt dataförvaltningsförordningen. De grundläggande ramarna för en sådan begäran som avser skyddade data återfinns i förordningens

kapitel II. Detta ramverk kompletteras av reglerna om handläggning av en sådan begäran enligt lagen. Begreppet används i lagen i 1 kap. 8 §, i rubriken till kapitel 5 samt i 5 kap. 1 och 3 §§. Genom ändringen av definitionen av uttrycket omfattar dessa delar också en begäran om tillgängliggörande av skyddade data.

Med skyddade data avses data som enligt artikel 3.1 dataförvaltningsförordningenen är skyddade på grund av insynsskydd för kommersiella rättigheter inbegripet affärs-, yrkes- och företagshemligheter, insynsskydd för statistiska uppgifter, skydd för tredje parts immateriella rättigheter, eller skydd för personuppgifter i den mån sådana uppgifter faller utanför tillämpningsområdet för öppna data-direktivet. Dessa datamängder är sådana som inte omfattades av öppna data-direktivet och som därmed heller inte omfattats av lagen.

Uppgifter som är skyddade på grund av insynsskydd för kommersiella rättigheter är olika typer av konfidentiell information i näringslivet. Affärshemligheter kan ses som ett samlingsbegrepp för företagshemligheter och yrkeshemligheter. Regler som rör affärshemligheter finns i flera olika författningar, exempelvis i lag (2018:558) om företagshemligheter (FHL), rättegångsbalken (1942:740) (RB), konkurrenslagen (2008:579) och arbetsmiljölagen (1977:1160).

Uppgift med insynsskydd för statistiska uppgifter är uppgifter som omfattas av statistiksekretess enligt 24 kap. 8 § offentlighets- och sekretesslagen (2009:400).

Med skydd för tredje parts immateriella rättigheter avses data som omfattas av någon av de immateriella rättigheterna, t.ex. upphovsrätt, patenträtt eller varumärkesrätt. De olika immateriella rättigheterna regleras i olika lagar. Upphovsrätt regleras i upphovsrättslagen (1960:729), patent i patentlagen (1967:837), varumärkesskydd i varumärkeslagen (2010:1877) och mönsterskydd i mönsterskyddslagen (1970:485). Den immateriella rättighet som oftast kan förekomma i myndigheters data är upphovsrätt. Upphovsrätt gäller som huvudregel för litterära och konstnärliga verk oavsett i vilken form dessa har kommit till. För att upphovsrätt ska föreligga krävs att det har en viss grad av självständighet och originalitet, s.k. verkshöjd. I myndigheternas verksamheter förekommer ett stort antal verk och andra alster som kan vara föremål för upphovsrätt eller närstående rättigheter. Rätten för

enskilda att ta del av allmänna handlingar gäller även för handlingar som är upphovsrättsligt skyddade, 2 kap. 26 b § URL

Personuppgifter är all slags information som direkt eller indirekt kan knytas till en person som är i livet. Det kan röra sig om t.ex. namn, adress och personnummer. Begreppet definieras i dataskyddsförordningen artikel 4.1. Behandling av personuppgifter ska ske i enlighet med dataskyddsreglerna, framför allt dataskyddsförordningen.

Skyddade data omfattar data som innehåller personuppgifter bara om sådana data inte omfattas av tillämpningsområdet för öppna data-direktivet som genomförts genom införandet av denna lag. Begränsningen i lagen gällande personuppgifter finns i 2 kap. 1 § där det framgår att data som innehåller personuppgifter bara kan göras tillgängliga för vidareutnyttjande om skyddet för personuppgifter kan upprätthållas.

En datamängd som innehåller personuppgifter omfattas alltså bara av begreppet skyddade data om den inte kan göras tillgänglig enligt de regler som genomförde öppna data-direktivet. Om en datamängd som innehåller personuppgifter omfattas av öppna data-direktivet eller dataförvaltningsförordningen får avgöras i det enskilda fallet. Vid prövningen ska en bedömning först göras av om uppgifterna ryms inom tillämpningsområdet för öppna data-direktivet. Bara om de inte gör det ska datamängden anses innehålla skyddade data.

7 a § Bestämmelserna om vidareutnyttjande av skyddade data ska endast tillämpas av myndigheter, dock inte av kulturinstitutioner och utbildningsinstitutioner.

Paragrafen är ny och anger att de bestämmelser som ska tillämpas för skyddade data bara ska tillämpas av myndigheter. Övervägandena finns i avsnitt 4.4.3.

Paragrafen införs för att tydliggöra att de bestämmelser som också omfattar skyddade data, bara ska tillämpas av myndigheter eftersom regelverket i kapitel II dataförvaltningsförordningen där vidareutnyttjande av skyddade data regleras bara ska tillämpas av myndigheter.

Bestämmelserna ska inte tillämpas av offentliga företag, kulturinstitutioner eller utbildningsinstitutioner eftersom dessa är undantagna från tillämpningsområdet för kapitel II i dataförvaltningsförordningen.

Kulturinstitutioner är institutioner så som bibliotek, arkiv och museer samt orkestrar, operor, baletter och teatrar. Anledningen till att dessa är undantagna från tillämpningsområdet i dataförvaltningsförordningen är att de verk och handlingar som dessa innehar till övervägande del omfattas av tredje parts immateriella rättigheter.

Utbildningsinstitutioner definieras inte särskilt i dataförvaltningsförordningen. Vissa institutioner bedriver både utbildning och annan verksamhet, såsom exempelvis forskning. Av skäl 12 till förordningen framgår att forskning kan bedrivas av offentliga myndigheter och att förordningen då bara ska tillämpas på dem enbart i deras egenskap av organisation som bedriver forskning. Forskning och undervisning bedrivs ofta samlat på svenska universitet och högskolor. I dessa fall ska reglerna i kapitel II i dataförvaltningsförordningen och de kompletterande reglerna i lagen bara tillämpas på forskningsverksamheten.

Det förtydligande av vad som avses med myndighet som finns i 1 kap. 5 § andra stycket gäller också för den nya paragrafen.

När lagen ska tillämpas

8 § Lagen ska tillämpas

1. när någon som har rätt att få tillgång till data *eller skyddade data* enligt någon annan lag eller förordning framställer en begäran om tillgängliggörande av data för vidareutnyttjande,

2. när en myndighet eller ett offentligt företag på eget initiativ tillgängliggör data som omfattas av lagen i syfte att de ska kunna vidareutnyttjas,

3. när en myndighet på eget initiativ tillgängliggör skyddade data som omfattas av lagen i syfte att de ska kunna vidareutnyttjas, eller

4. när data lämnas till en statlig eller kommunal myndighet som ska använda dem i en konkurrensutsatt verksamhet som avser tillhandahållande av data.

Trots första stycket ska lagen inte tillämpas

1. när data, i andra fall än som avses i första stycket 3, lämnas

a) mellan statliga och kommunala myndigheter,

b) från ett organ som enligt 1 kap. 5 § andra stycket jämställs med en myndighet eller ett offentligt företag till en statlig eller kommunal myndighet, eller

2. när en statlig eller kommunal myndighet tillhandahåller data i en konkurrensutsatt verksamhet.

Paragrafen klargör när lagen ska tillämpas. Övervägandena finns i avsnitt 4.5.3.

Lagen kan inte åberopas som en grund för att få tillgång till skyddade data. För att lagen ska vara tillämplig krävs att en

vidareutnyttjare enligt en annan författning eller på någon annan grund har rätt att få tillgång till skyddade data.

Enligt *första stycket första punkten* ska lagen tillämpas när någon som enligt någon annan lag eller förordning har rätt att få tillgång till data, begär att de ska göras tillgängliga för vidareutnyttjande. Det förutsätter att vidareutnyttjaren begär dels att få tillgång till data enligt någon annan författning, dels att de ska tillgängliggöras för vidareutnyttjande enligt förevarande lag. Denna lag ska alltså tillämpas först när det har konstaterats att det finns en författningsreglerad rätt till tillgång och att det inte finns några hinder mot att ge tillgång till de data som efterfrågas (jfr 2 §).

Enligt *första stycket tredje punkten* ska lagen också tillämpas när en myndighet på eget initiativ ger tillgång till skyddade data som omfattas av lagen, i syfte att de ska kunna vidareutnyttjas. Sådant tillgängliggörande kan ske på helt frivillig grund. Skyddade data kan dock inte göras tillgängliga på internet fritt utan kan bara tillgängliggöras i enlighet med de villkor som myndigheten ställer upp. Myndigheten kan dock utan att ha fått någon begäran ta fram villkor för vidareutnyttjande och publicera dessa för ett enklare tillgängliggörande.

Genom ett tillägg av uttrycket skyddade data i punkten 1 och tillägget av en ny punkt 3 som omfattar frivilligt tillgängliggörande av skyddade data tydliggörs att lagen också omfattar sådana data som avses i artikel 3.1 dataförvaltningsförordningen och en begäran om tillgängliggörande av sådana data enligt dataförvaltningsförordningen.

10 § Lagen gäller inte för data som

1. omfattas av en sådan ensamrätt som följer av patentlagen (1967:837), mönsterskyddslagen (1970:485), lagen (1992:1685) om skydd för kretsmönster för halvledarprodukter, växtförädlarrättslagen (1997:306), varumärkeslagen (2010:1877) eller lagen (2018:1653) om företagsnamn,
2. tredje man innehar rätt till enligt lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk,
3. utgörs av datorprogram, eller
4. utgörs av logotyper, heraldiska vapen eller insignier.

Första stycket ska inte tillämpas avseende sådana kategorier av skyddade data som framgår av artikel 3.1 c i EU:s dataförvaltningsförordning.

Paragrafen innehåller undantag för vissa data. Övervägandena för ändringen finns i avsnitt 4.4.4.

Genom införandet av det nya stycket i paragrafen stadgas att data som omfattas av tredje mans immateriella rättigheter omfattas vid tillämpningen för skyddade data. Skyddade data är enligt 1 kap. 4 § sådana kategorier av skyddade data som avses i artikel 3.1 dataförvaltningsförordningen. En av de särskilda kategorier av skyddade data som anges i denna artikel är data som skyddas av tredje parts immateriella rättigheter. Immaterialrättsligt skyddade data ska därför omfattas av lagen, men bara vid tillämpning av den som ett komplement till dataförvaltningsförordningen.

2 kap. Tillgängliggörande av data för vidareutnyttjande

5 a § *En myndighet som tillgängliggör skyddade data för vidareutnyttjande ska ställa upp villkor för vidareutnyttjandet i enlighet med artikel 5 i EU:s dataförvaltningsförordning.*

En myndighet som tillgängliggör konfidentiella data till en vidareutnyttjare som avser att överföra dem till tredje land i enlighet med artikel 5.10 i EU:s dataförvaltningsförordning är skyldig att anmäla de överträdelser av artikel 5.14 som myndigheten får kännedom om till tillsynsmyndigheten enligt lag (2023:000) med kompletterande bestämmelser till EU:s dataförvaltningsförordning.

Paragrafen är ny och anger att myndigheten vid tillgängliggörande av skyddade data ska ställa villkor i enlighet med artikel 5 i dataförvaltningsförordningen samt att de ska anmäla vissa överträdelser till tillsynsmyndigheten enligt lag med kompletterande bestämmelser till dataförvaltningsförordningen. Övervägandena finns i avsnitt 4.5.5 och 5.8.8.

Första stycket införs som en upplysning om att villkor för vidareutnyttjande av skyddade data ska följa kraven i artikel 5 i dataförvaltningsförordningen och inte regleringen i 2 kap. 5 §. I artikel 5 stadgas bl.a. att de villkor som myndigheten ställer upp ska vara icke-diskriminerande, transparenta, proportionerliga och objektivt motiverade med hänsyn till den data som vidareutnyttjandet gäller.

Myndigheter ska, om de tillgängliggör skyddade data för vidareutnyttjande, säkerställa att den skyddade karaktären för aktuella data bevaras. Med detta avses att tillgängliggörande för vidareutnyttjandet bara får ske om skyddet kan bevaras genom skyddsåtgärder och villkor i enlighet med artikeln. Det är

myndigheten som innehar skyddade data som är ansvarig för att säkerställa att vidareutnyttjande bara medges när det är möjligt.

Myndigheter som ska hantera en begäran om tillgängliggörande av skyddade data för vidareutnyttjande kan bistås av andra myndigheter som utsetts till så kallade behöriga organ enligt artikel 7.1. Överväganden om vilka som ska utses som behöriga organ finns i avsnitt 4.5.6.

Myndigheterna ska offentliggöra villkoren för att tillåta vidareutnyttjande genom en gemensam informationspunkt som inrättas enligt artikel 8 i förordningen. Överväganden avseende den gemensamma informationspunkten finns i avsnitt 4.6.

Genom *andra stycket* införs en anmälningsskyldighet för utlämnande myndigheter. En överträdelse av artikel 5.14 ska kunna leda till en sanktion. Det är tillsynsmyndigheten enligt lag (2023:000) med kompletterande bestämmelser till EU:s dataförvaltningsförordning som ska kunna besluta om sanktioner i enlighet med 6 § andra stycket den lagen. För att tillsynsmyndigheten ska kunna besluta om sanktioner behöver de få kännedom om överträdelser av artikel 5.14. Den myndighet som lämnat ut data är den som kan ha kännedom om överträdelser. Myndigheten har därför skyldighet att anmäla de överträdelser som den får kännedom om till tillsynsmyndigheten som får besluta om sanktionsavgift.

För att anmälningsskyldigheten ska bli aktuell krävs att myndigheten tillgängliggjort vissa typer av konfidentiella data för överföring till tredje land i enlighet med vad som stadgas i artikel 5.10 i dataförvaltningsförordningen. Med konfidentiella data menas i artikel 5.10 data som skyddas av unionsrätt eller nationell rätt om affärshemligheter eller insynsskydd för statistiska uppgifter. En myndighet som tillåter vidareutnyttjare att överföra sådana data till tredje land ska ställa upp avtalsmässiga villkor enligt artikel 5.10.

För att myndigheten ska ha en skyldighet att anmäla överträdelser mot reglerna om tredjelandsöverföringar krävs att myndigheten efter tillgängliggörandet fått kännedom om att vidareutnyttjaren har gjort sig skyldiga till överträdelser av artikel 5.14.

De överträdelser som ska anmälas är överträdelser av artikel 5.14. Artikel 5.14 hänvisar tillbaka till artikel 5.10, 5.12 och 5.13 vilket innebär att överträdelser av också dessa punkter omfattas av

anmälningsskyldigheten. Artikel 5.12 ger kommissionen rätt att anta genomförandeakter i vilka det intygas att ett visst tredjelands rättsliga, tillsynsmässiga och verkställighetsmässiga arrangemang säkerställer skydd för immateriella rättigheter och företagshemligheter, tillämpas och verkställs på ett effektivt sätt och omfattar effektiva rättsmedel. Har sådana genomförandeakter antagits ska myndigheten anmäla om den får kännedom om att vidareutnyttjaren gjort sig skyldig till överträdelser av dessa. I artikel 5.13 stadgas att kommissionen ska anta delegerade akter som kompletterar dataförvaltningsförordningen genom att fastställa särskilda villkor som ska tillämpas på överföring av vissa kategorier av icke-personuppgifter som anses vara mycket känsliga till tredjeländer. Om sådana delegerade akter har antagits av kommissionen och en myndighet får kännedom om att en vidareutnyttjare gjort sig skyldig till överträdelser av dessa så ska det anmälas.

En anmälan ska innehålla de uppgifter om överträdelsen som tillsynsmyndigheten behöver för att kunna besluta om sanktioner. Uppgifter om vidareutnyttjaren ska framgå av anmälan. Vidare ska den innefatta en beskrivning av de data som lämnats ut, vilka villkor som ställts upp för vidareutnyttjandet och överföringen till tredje land, en redogörelse för den eller de överträdelser som vidareutnyttjaren gjort sig skyldig till samt, när det är möjligt, vilka effekter överträdelsen fått. Uppgifter om hur överträdelsen upptäcktes och hur allvarlig den är, vilken omfattning den har och under hur lång tid överträdelsen pågått ska finnas med i anmälan när det är aktuellt. Om myndigheten har kännedom om tidigare överträdelser som viderutnyttjaren gjort sig skyldig till ska det framgå av anmälan. Likaså uppgifter om ekonomiska vinster eller förluster som undvikits som överträdelsen kan ha inneburit för vidareutnyttjaren. Myndigheten ska därutöver i anmälan inkludera andra försvårande eller förmildrande omständigheter som kan ha betydelse för bedömningen av en sanktionsavgift.

Förteckning över skyddade data som görs tillgängliga

6 a § *Den myndighet som regeringen bestämmer ska tillhandahålla en gemensam informationspunkt enligt artikel 8 i EU:s dataförvaltningsförordning.*

En myndighet som tillgängliggör skyddade data för vidareutnyttjande ska informera den myndighet som tillhandahåller den gemensamma informationspunkten om sådana data och villkoren för vidareutnyttjande av dessa.

Rubriken och paragrafen är nya och uppställer ett krav på att det ska finnas en förteckning över data som finns tillgängliga för vidareutnyttjande. Övervägandena finns i avsnitt 4.7.2 och 4.7.3.

Genom *första stycket* ges regeringen befogenhet att utse den myndighet som ska tillhandahålla den gemensamma informationspunkten enligt artikel 8 i dataförvaltningsförordningen. Förteckningen ska enligt artikel 8.2 på elektronisk väg tillhandahålla en sökbar innehållsförteckning med en översikt över alla tillgängliga datakällor, tillsammans med relevant information som beskriver tillgängliga data, inbegripet åtminstone dataformatet och datastorleken samt villkoren för vidareutnyttjandet av dessa data.

Den gemensamma informationspunkten ska också kunna ta emot förfrågningar eller ansökningar om vidareutnyttjande av skyddade data och vidareförmedla dessa till de myndigheter som innehar aktuella data, artikel 8.2.

I *andra stycket* införs en skyldighet för myndigheter som gör skyddade data tillgängliga för vidareutnyttjande att informera den myndighet som ska föra förteckningen. Informationen ska bestå av vilken data som avses och de villkor som ställs upp för vidareutnyttjande.

Med tillgängliggöra avses att en myndighet ger tillgång till information, oavsett om det görs frivilligt eller på grund av en skyldighet i annan författning. Ett tillgängliggörande förutsätter inte att det sker på viss rättlig grund. För att skyddade data ska kunna göras tillgängliga för vidareutnyttjande behöver den offentliga myndigheten vidta vissa skyddsåtgärder och i normalfallet ställa upp vissa villkor för vidareutnyttjandet. Sådana skyddade data kan därför inte tillhandahållas utan en begäran. Den myndighet som innehar skyddade data ska underrätta den gemensamma informationspunkten som sådana data som gjorts tillgängliga för vidareutnyttjande på begäran eller sådana data som myndigheten på eget initiativ identifierat och satt upp villkor för vidareutnyttjande för.

Paragrafen är en del av genomförandet av inrättande av en gemensam informationspunkt i artikel 8 dataförvaltningsförordningen.

3 kap. Exklusiv rätt att utnyttja data

1 a § En myndighet som innehar skyddade data får bara ge någon en exklusiv rätt att vidareutnyttja dessa data i den mån det är tillåtet enligt artikel 4 i EU:s dataförvaltningsförordning.

Paragrafen är ny och anger begränsningarna för exklusiva avtal för skyddade data finns i förordningen. Övervägandena finns i avsnitt 4.4.6.

Bestämmelsen införs som en upplysning om att begränsningarna av exklusiva avtal för vidareutnyttjande av de kategorier av skyddade data som finns i artikel 3.1 dataförvaltningsförordningen ska följa kraven i artikel 4.

4 kap. Avgifter

Rätten att ta ut en avgift

1 § En myndighet eller ett offentligt företag som har rätt att ta ut en avgift för att tillgängliggöra data *eller skyddade data* för vidareutnyttjande får inte beräkna den till ett högre belopp än vad som följer av 2–6 §§.

Paragrafen innehåller en generell princip om att avgifter som tas ut vid tillgängliggörande av data måste hålla sig inom de begränsningar som lagen ställer upp. Övervägandena finns i avsnitt 4.5.7.

Rätten att ta ut en avgift för tillgängliggörande av skyddade data följer direkt av artikel 6.1 dataförvaltningsförordningen. Medlemsstaterna ska i nationell rätt fastställa kriterier och metod för beräkning av avgifter enligt artikel 6.6. Tillägget av uttrycket skyddade data är en del av genomförandet av artikel 6.6.

Paragrafen träffar både myndigheter och offentliga företag. Det är dock bara myndigheter som träffas av reglerna i dataförvaltningsförordningens kapitel II och som har rätt att ta ut en avgift för tillgängliggörande av skyddade uppgifter enligt artikel 6.1. Tillägget i paragrafen träffar enligt 1 kap. 7 a § endast myndigheter.

Avgiftsuttag vid tillgängliggörande av data

2 a § *Vid tillgängliggörande av skyddade data får en avgift, utöver vad som följer av 2 § första stycket första meningen, också täcka sådana kostnader som framgår av artikel 6.5 i EU:s dataförvaltningsförordning.*

Paragrafen anger de yttre ramarna för uttag av avgifter vid tillgängliggörande av skyddade data. Tillägget genomför artikel 6.6 i dataförvaltningsförordningen. Övervägandena finns i avsnitt 4.5.8 och 4.5.9.

Genom hänvisningen till 4 kap. 2 § första stycket första meningen regleras att en avgift för att tillgängliggöra skyddade data i enlighet med kapitel II dataförvaltningsförordningen ska kunna omfatta reproduktion, tillhandahållande och spridning av data och för att avidentifiera personuppgifter.

Paragrafen hänvisar vidare till artikel 6.5 dataförvaltningsförordningen och att de kostnader som framgår där får ingå i avgiften. I artikel 6.5 finns en uppräkning av nödvändiga kostnader i samband med:

- reproduktion, tillhandahållande och spridning av data,
- klarering av upphovsrätt,
- anonymisering eller andra former av framställning av personuppgifter och affärshemligheter,
- underhåll av säkra behandlingsmiljöer,
- förvärvande av rättigheter från tredje part och
- visst bistånd till vidareutnyttjare

Kostnader för reproduktion, tillhandahållande och spridning av data innefattar kostnader för att bearbeta, sammanställa och distribuera data. Även kostnader för att formatera eller verifiera data får räknas in, liksom kostnader för material och programmering. Avgiftsunderlaget får även avse kostnader för utveckling och drift av en tjänst som möjliggör att data tillgängliggörs, t.ex. via internet eller genom en säker behandlingsmiljö på distans eller i fysiska lokaler. Kostnader för att samla in data eller förvalta system får dock inte omfattas med stöd av denna skrivning.

Kostnader för klarering av upphovsrätt får ingå i kostnadsunderlaget. Med detta avses att alla som har rättigheter ger sitt tillstånd till användningen, t.ex. genom en licens eller ett avtal. Detta kan innebära kostnader både för själva upphovsrätten och för

den arbetsinsats som klareringen innebär för myndigheten. Samtliga sådana kostnader ska kunna omfattas av avgiften.

Kostnader för anonymisering eller andra formera av framställning av personuppgifter och affärshemligheter får ingå i kostnadsunderlaget. Med detta avses sådan bearbetning av data som myndigheterna kan vidta för att bevara integritet för data i enlighet med artikel 5.3 dataskyddsförordningen. Det rör sig om olika metoder för att ändra data på ett sådant sätt att ingen konfidentiell information lämnas.

Kostnader för underhåll av en säker behandlingsmiljö i vilken data tillhandahålls ska också kunna ingå i underlaget. Sådana kostnader kan bestå i exempelvis supportavtal för hårdvara, nyinköp för att ersätta befintlig hårdvara när garantin gått ut, uppgraderings- och supportavtal för programvarulicenser och personalkostnader för säkerhetspatchningar, backuper, uppgraderingar och annat underhåll.

Kostnader för förvärvande av rätt att tillåta vidareutnyttjande från tredje part från också omfattas av kostnadsunderlaget för avgiften. Detta omfattar både sådana faktiska kostnader för förvärvande av rätten som personalkostnader för detta.

Kostnader för att bistå vidareutnyttjare som begär de registrerades samtycke och tillstånd från datainnehavara får ingå i kostnadsunderlaget. En sådan kostnads skulle typiskt sätt primärt bestå i kostnader för nedlagt arbete. Det är dock viktigt att poängtera att utrymmet för en myndighet att bistå en vidareutnyttjare med dessa uppgifter i normalfallet är små.

5 kap. Handläggning av en begäran om tillgängliggörande av data för vidareutnyttjande

1 § En myndighet ska inom fyra veckor avgöra ett ärende till följd av en begäran om tillgängliggörande av data för vidareutnyttjande.

Om en sådan begäran avser skyddade data ska ärendet avgöras inom åtta veckor.

Tidsfristen får förlängas med ytterligare fyra veckor, om en begäran är omfattande eller komplicerad. Myndigheten ska underrätta sökanden om förlängningen och redovisa skälen för den senast tre veckor från den dag då begäran kom in.

Paragrafen anger vilka tidsfrister som gäller vid handläggning av ett ärende om tillgängliggörande av data. Övervägandena finns i avsnitt 4.5.4 och 4.5.11.

I paragrafen föreslås ett nytt stycke som reglerar vilka tidsfrister som ska gälla för ett ärende om tillgängliggörande av sådana data som avses i artikel 3.1 dataförvaltningsförordningen. I artikel 9.1 dataförvaltningsförordningen regleras att ett sådant ärende ska avgöras inom två månader från dagen för mottagen begäran, såvida inte kortare tidsfrister fastställs i nationell rätt.

En begäran om vidareutnyttjande av skyddade data är till sin natur mer komplex än en begäran om vidareutnyttjande av andra data. Det är därför lämpligt att tiden för hantering av ärendet är längre för ärenden som avser skyddade data enligt dataförvaltningsförordningen. Den svenska regleringen av handläggningstiden bör därför i princip motsvara den längsta tiden i förordningen. I datalagen är dock handläggningstiden beskriven i veckor, inte månader. För att inte i samma lagrum ha olika tidsmått är den tid inom vilken ett ärende ska hanteras åtta veckor.

Exceptionellt omfattande eller komplicerade begäran om vidareutnyttjande tar längre tid att handlägga. Handläggningen av ett sådant ärende får därför enligt dataförvaltningsförordningen artikel 9.1 andra stycket förlängas med högst 30 dagar. I datalagen är tidsfristerna uttryckta i veckor och inte i dagar och förlängning tillåten med som mest fyra veckor. Denna tid motsvarar i princip de 30 dagar som dataförvaltningsförordningen tillåter. För en tydlig och effektiv reglering av tidsfrister ska samma tid gälla för förlängning av handläggningstiden för ärenden om vidare-utnyttjande av skyddade data enligt dataförvaltnings-förordningen som för data i andra fall.

De beslut som en myndighet fattar i ett ärende kan överklagas till allmän förvaltningsdomstol enligt 4 §. Av artikel 9.2 i data-förvaltningsförordningen följer att fysiska eller juridiska personer som direkt påverkas av ett beslut efter en begäran om vidareutnyttjande av skyddade data ska ha effektiv rätt till överprövning. 4 § motsvarar de krav på överprövning som ställs i artikel 9.2.

Enligt artikel 9.2 framgår att fysiska och juridiska personer som direkt eller indirekt påverkas av ett beslut om att medge eller vägra

tillgång till skyddade data för vidareutnyttjande ska kunna överklaga ett sådant beslut.

Enligt 42 § förvaltningslagen får ett beslut överklagas av den som beslutet angår, om det har gått honom eller henne emot. Ett beslut får enligt 41 § förvaltningslagen överklagas om beslutet kan antas påverka någons situation på ett inte obetydligt sätt. I 40 § samma lag anges att beslut överklagas till allmän förvaltningsdomstol och att prövningstillstånd krävs vid överklagande till kammarrätten. Klagorätt enligt förvaltningslagen tillkommer alltså den som beslutet angår, om beslutet har gått denne emot.

Den som direkt påverkas av ett beslut om tillgång till skyddade data för vidareutnyttjande kan vara den som begär tillgång till sådana data. Den har också möjlighet att klaga på ett beslut om att medge eller vägra tillgång till informationen enligt 2 kap. TF. För sådana beslut anses inte den som sekretessen avser vara en som beslutet angår, och denne har inte rätt att klaga på ett sådant beslut om tillgång till information.

Den som skyddet för den aktuella datamängden avser skulle dock kunna påverkas direkt av ett beslut om att tillgängliggöra dessa data för vidareutnyttjande, t.ex. om den vars affärshemligheter ingår eller den som innehar upphovsrätt till data anser att dennes affärshemlighet eller upphovsrätt inte blivit tillräckligt skyddad vid tillgängliggörandet. I sådana fall bör denna ha rätt att överklaga beslutet enligt artikel 9.2. Den som påverkas direkt av beslutet bör också anses vara en som beslutet angår i förvaltningslagens mening vid tillämpningen av 4 § för ärenden om tillgängliggörande av skyddade data.

3.6.2022 SV Europeiska unionens officiella tidning L 152/1

I

(Lagstiftningsakter)

FÖRORDNINGAR

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2022/868

av den 30 maj 2022

om europeisk dataförvaltning och om ändring av förordning (EU) 2018/1724 (dataförvaltningsakten)

(Text av betydelse för EES)

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 114,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande ([1]),

efter att ha hört Regionkommittén,

i enlighet med det ordinarie lagstiftningsförfarandet ([2]), och

av följande skäl:

(1) I enlighet med fördraget om Europeiska unionens funktionssätt (EUF-fördraget) ska en inre marknad inrättas och en ordning skapas som säkerställer att konkurrensen på den inre marknaden inte snedvrids. Fastställande av gemensamma regler och gemensam praxis i medlemsstaterna för utformning av en ram för dataförvaltning bör bidra till att dessa mål uppnås, samtidigt som grundläggande rättigheter respekteras fullt ut. Förstärkningen av unionens öppna strategiska oberoende bör också garanteras och ett internationellt fritt dataflöde samtidigt främjas.

(2) Under det senaste årtiondet har den digitala tekniken förändrat ekonomin och samhället genom sin inverkan på alla verksamhetssektorer och det dagliga livet. I centrum för den omvandlingen står data: datadriven innovation kommer att medföra enorma fördelar för både unionsmedborgare och ekonomin, till exempel genom förbättrad medicin och precisionsmedicin, genom tillhandahållande av ny mobilitet och genom dess bidrag till kommissionens meddelande av den 11 december 2019 om den europeiska gröna given. För att göra den datadrivna ekonomin inkluderande för alla unionsmedborgare måste särskild uppmärksamhet ägnas åt att minska den digitala klyftan, stimulera kvinnors deltagande i dataekonomin och främja europeisk spetskompetens inom tekniksektorn. Dataekonomin måste byggas på ett sätt som möjliggör välmående företag, särskilt mikroföretag och små och medelstora företag enligt definitionen i bilagan till kommissionens rekommendation 2003/361/EG ([3]) samt nystartade företag, där neutral dataåtkomst, dataportabilitet och interoperabilitet säkerställs och inlåsningseffekter undviks. I sitt meddelande av den 19 februari 2020 om en EU-strategi för data (*EU-strategin för data*) beskrev kommissionen visionen om ett gemensamt europeiskt dataområde, som innebär en inre marknad för data, där data kan användas i enlighet med gällande lagstiftning oavsett var i unionen de fysiskt lagras, vilket bland annat skulle kunna vara avgörande för den snabba utvecklingen av teknik för artificiell intelligens.

([1]) EUT C 286, 16.7.2021, s. 38.
([2]) Europaparlamentets ståndpunkt av den 6 april 2022 (ännu inte offentliggjord i EUT) och rådets beslut av den 16 maj 2022.
([3]) Kommissionens rekommendation 2003/361/EG av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag (EUT L 124, 20.5.2003, s. 36).

Kommissionen efterlyste också ett fritt och säkert dataflöde med tredjeländer, med undantag och inskränkningar som rör allmän säkerhet, allmän ordning och andra legitima mål för unionens offentliga politik, i enlighet med internationella åtaganden, inbegripet om grundläggande rättigheter. För att förverkliga denna vision föreslog kommissionen att det inrättas domänspecifika gemensamma europeiska dataområden för datadelning och datapoolning. I EU-strategin för data föreslås att sådana gemensamma europeiska dataområden skulle kunna omfatta områden såsom hälsa, mobilitet, tillverkning, finansiella tjänster, energi eller jordbruk, eller en kombination av sådana områden, till exempel energi och klimat, samt tematiska områden såsom den europeiska gröna given eller europeiska dataområden för offentlig förvaltning eller kompetens. Gemensamma europeiska dataområden bör göra data sökbara, tillgängliga, interoperabla och möjliga att vidareutnyttja (*Fairdataprinciperna*) och samtidigt säkerställa en hög nivå på cybersäkerheten. När det råder likvärdiga förutsättningar i dataekonomin konkurrerar företagen om tjänsternas kvalitet, inte om mängden data som de kontrollerar. I syfte att utforma, skapa och behålla likvärdiga förutsättningar i dataekonomin behövs sund styrning där de berörda parterna i ett gemensamt europeiskt dataområde behöver samarbeta och vara representerade.

(3) Det är nödvändigt att förbättra villkoren för datadelning på den inre marknaden genom att skapa en harmoniserad ram för utbyte av data och föreskriva vissa grundläggande krav på dataförvaltning, med särskild omsorg om att underlätta samarbetet mellan medlemsstaterna. Denna förordning bör syfta till att vidareutveckla den gränslösa digitala inre marknaden samt ett datasamhälle och en dataekonomi som ställer människan i centrum och präglas av förtroende och säkerhet. Genom sektorsspecifik unionsrätt kan, beroende på sektorns särdrag, nya och kompletterande delar utvecklas, anpassas och föreslås, såsom den planerade unionsrätten om det europeiska hälsodataområdet och om tillgång till fordonsdata. Dessutom regleras vissa sektorer av ekonomin redan av sektorsspecifik unionsrätt som omfattar regler om den gränsöverskridande eller unionsomfattande delningen av eller tillgången till data, till exempel Europaparlamentets och rådets direktiv 2011/24/EU ([4]) inom ramen för det europeiska hälsodataområdet, och relevanta lagstiftningsakter på transportområdet, till exempel Europaparlamentets och rådets förordningar (EU) 2019/1239 ([5]) och (EU) 2020/1056 ([6]) samt Europaparlamentets och rådets direktiv 2010/40/EU ([7]) inom ramen för det europeiska dataområdet för rörlighet.

([4]) Europaparlamentets och rådets direktiv 2011/24/EU av den 9 mars 2011 om tillämpningen av patienträttigheter vid gränsöverskridande hälso- och sjukvård (EUT L 88, 4.4.2011, s. 45).

([5]) Europaparlamentets och rådets förordning (EU) 2019/1239 av den 20 juni 2019 om inrättande av en europeisk kontaktpunkt för sjöfart och om upphävande av direktiv 2010/65/EU (EUT L 198, 25.7.2019, s. 64).

([6]) Europaparlamentets och rådets förordning (EU) 2020/1056 av den 15 juli 2020 om elektronisk godstransportinformation (EUT L 249, 31.7.2020, s. 33).

([7]) Europaparlamentets och rådets direktiv 2010/40/EU av den 7 juli 2010 om ett ramverk för införande av intelligenta transportsystem på vägtransportområdet och för gränssnitt mot andra transportslag (EUT L 207, 6.8.2010, s. 1).

Denna förordning bör därför inte påverka Europaparlamentets och rådets förordningar (EG) nr 223/2009 ([8]), (EU) 2018/858 ([9]) och (EU) 2018/1807 ([10]) samt direktiv 2000/31/EG ([11]), 2001/29/EG ([12]), 2004/48/EG ([13]), 2007/2/EG ([14]), 2010/40/EU, (EU) 2015/849 ([15]), (EU) 2016/943 ([16]), (EU) 2017/1132 ([17]), (EU) 2019/790 ([18]) och (EU) 2019/1024 ([19]) samt annan sektorsspecifik unionsrätt som reglerar tillgång till och vidareutnyttjande av data. Denna förordning bör inte påverka unionsrätten och nationell rätt om tillgången till och användningen av data för förebyggande, förhindrande, utredning, avslöjande eller lagföring av brott eller verkställande av straffrättsliga påföljder och inte heller det internationella samarbetet i det sammanhanget.

Denna förordning bör inte påverka medlemsstaternas befogenheter när det gäller deras verksamhet som rör allmän säkerhet, försvar och nationell säkerhet. Vidareutnyttjandet av data som är skyddade av sådana skäl och innehas av offentliga myndigheter, inbegripet data från upphandlingsförfaranden som omfattas av tillämpningsområdet för Europaparlamentets och rådets direktiv 2009/81/EG ([20]), bör inte omfattas av denna förordning. Ett övergripande system för vidareutnyttjande av vissa kategorier av skyddade data som innehas av offentliga myndigheter och tillhandahållande av dataförmedlingstjänster och tjänster baserade på dataaltruism i unionen bör inrättas. De olika sektorernas särdrag kan göra att det behöver skapas sektorsspecifika databaserade system, som samtidigt ska bygga på kraven i denna förordning. Leverantörer av dataförmedlingstjänster som uppfyller kraven i denna förordning bör kunna använda beteckningen "leverantör av dataförmedlingstjänster som är erkända i unionen". Juridiska personer som vill stödja mål av allmänt intresse genom att tillhandahålla relevanta data baserat på dataaltruism i större skala och som uppfyller de krav som fastställs i denna förordning, bör kunna registrera sig som och använda beteckningen "dataaltruismorganisation som är erkänd i unionen". Om sektorsspecifik unionsrätt eller nationell rätt kräver att offentliga myndigheter, sådana leverantörer av dataförmedlingstjänster eller sådana juridiska personer (erkända dataaltruismorganisationer) uppfyller specifika ytterligare tekniska, administrativa eller organisatoriska krav, däribland genom ett auktorisations- eller certifieringssystem, bör de bestämmelserna i den sektorsspecifika unionsrätten eller nationella rätten också gälla.

([8]) Europaparlamentets och rådets förordning (EG) nr 223/2009 av den 11 mars 2009 om europeisk statistik och om upphävande av Europaparlamentets och rådets förordning (EG, Euratom) nr 1101/2008 om utlämnande av insynsskyddade statistiska uppgifter till Europeiska gemenskapernas statistikkontor, rådets förordning (EG) nr 322/97 om gemenskapsstatistik och rådets beslut 89/382/EEG, Euratom om inrättande av en kommitté för Europeiska gemenskapernas statistiska program (EUT L 87, 31.3.2009, s. 164).

([9]) Europaparlamentets och rådets förordning (EU) 2018/858 av den 30 maj 2018 om godkännande av och marknadskontroll över motorfordon och släpfordon till dessa fordon samt av system, komponenter och separata tekniska enheter som är avsedda för sådana fordon, om ändring av förordningarna (EG) nr 715/2007 och (EG) nr 595/2009 samt om upphävande av direktiv 2007/46/EG (EUT L 151, 14.6.2018, s. 1).

([10]) Europaparlamentets och rådets förordning (EU) 2018/1807 av den 14 november 2018 om en ram för det fria flödet av andra data än personuppgifter i Europeiska unionen (EUT L 303, 28.11.2018, s. 59).

([11]) Europaparlamentets och rådets direktiv 2000/31/EG av den 8 juni 2000 om vissa rättsliga aspekter på informationssamhällets tjänster, särskilt elektronisk handel, på den inre marknaden ("Direktiv om elektronisk handel") (EGT L 178, 17.7.2000, s. 1).

([12]) Europaparlamentets och rådets direktiv 2001/29/EG av den 22 maj 2001 om harmonisering av vissa aspekter av upphovsrätt och närstående rättigheter i informationssamhället (EGT L 167, 22.6.2001, s. 10).

([13]) Europaparlamentets och rådets direktiv 2004/48/EG av den 29 april 2004 om säkerställande av skyddet för immateriella rättigheter (EUT L 157, 30.4.2004, s. 45).

([14]) Europaparlamentets och rådets direktiv 2007/2/EG av den 14 mars 2007 om upprättande av en infrastruktur för rumslig information i Europeiska gemenskapen (Inspire) (EUT L 108, 25.4.2007, s. 1).

([15]) Europaparlamentets och rådets direktiv (EU) 2015/849 av den 20 maj 2015 om åtgärder för att förhindra att det finansiella systemet används för penningtvätt eller finansiering av terrorism, om ändring av Europaparlamentets och rådets förordning (EU) nr 648/2012 och om upphävande av Europaparlamentets och rådets direktiv 2005/60/EG och kommissionens direktiv 2006/70/EG (EUT L 141, 5.6.2015, s. 73).

([16]) Europaparlamentets och rådets direktiv (EU) 2016/943 av den 8 juni 2016 om skydd mot att icke röjd know-how och företagsinformation (företagshemligheter) olagligen anskaffas, utnyttjas och röjs (EUT L 157, 15.6.2016, s. 1).

([17]) Europaparlamentets och rådets direktiv (EU) 2017/1132 av den 14 juni 2017 om vissa aspekter av bolagsrätt (EUT L 169, 30.6.2017, s. 46).

([18]) Europaparlamentets och rådets direktiv (EU) 2019/790 av den 17 april 2019 om upphovsrätt och närstående rättigheter på den digitala inre marknaden och om ändring av direktiven 96/9/EG och 2001/29/EG (EUT L 130, 17.5.2019, s. 92).

([19]) Europaparlamentets och rådets direktiv (EU) 2019/1024 av den 20 juni 2019 om öppna data och vidareutnyttjande av information från den offentliga sektorn (EUT L 172, 26.6.2019, s. 56).

([20]) Europaparlamentets och rådets direktiv 2009/81/EG av den 13 juli 2009 om samordning av förfarandena vid tilldelning av vissa kontrakt för byggentreprenader, varor och tjänster av upphandlande myndigheter och enheter på försvars- och säkerhetsområdet och om ändring av direktiven 2004/17/EG och 2004/18/EG (EUT L 216, 20.8.2009, s. 76).

(4) Denna förordning bör inte påverka tillämpningen av Europaparlamentets och rådets förordningar (EU) 2016/679 ([21]) och (EU) 2018/1725 ([22]) och av Europaparlamentets och rådets direktiv 2002/58/EG ([23]) och (EU) 2016/680 ([24]) samt motsvarande bestämmelser i nationell rätt, inbegripet då personuppgifter och andra data än personuppgifter i en datamängd är oupplösligt sammanlänkade. Den här förordningen bör i synnerhet inte tolkas som att den skapar en ny rättslig grund för behandling av personuppgifter för någon av de reglerade verksamheterna, eller ändrar de informationskrav som fastställs i förordning (EU) 2016/679. Genomförandet av den här förordningen bör inte förhindra gränsöverskridande överföringar av data i enlighet med kapitel V i förordning (EU) 2016/679. Om den här förordningen står i strid med unionsrätten om skydd av personuppgifter eller nationell rätt som antagits i enlighet med sådan unionsrätt bör relevant unionsrätt eller nationell rätt om skydd av personuppgifter ha företräde. Det bör vara möjligt att betrakta dataskyddsmyndigheter som behöriga myndigheter inom ramen för den här förordningen. Om andra myndigheter fungerar som behöriga myndigheter enligt den här förordningen bör de göra detta på ett sätt som inte påverkar dataskyddsmyndigheternas tillsynsbefogenheter och behörigheter enligt förordning (EU) 2016/679.

(5) Åtgärder på unionsnivå är nödvändiga för att öka förtroendet för datadelning genom att inrätta lämpliga mekanismer för de registrerades och datainnehavares kontroll över data som avser dem och för att ta itu med andra hinder för en väl fungerande och konkurrenskraftig datadriven ekonomi. Dessa åtgärder bör inte påverka tillämpningen av skyldigheter och åtaganden enligt internationella handelsavtal som ingås av unionen. En unionsomfattande styrningsram bör syfta till att skapa förtroende bland enskilda personer och företag när det gäller tillgång till samt kontroll, delning, användning och vidareutnyttjande av data, särskilt genom att fastställa lämpliga mekanismer för att de registrerade ska känna till sina rättigheter och kunna utöva dem på ett meningsfullt sätt, och när det gäller vidareutnyttjande av vissa typer av data som innehas av offentliga myndigheter, tillhandahållande av tjänster från leverantörer av dataförmedlingstjänster till registrerade, datainnehavare och dataanvändare samt insamling och behandling av data som fysiska och juridiska personer gör tillgängliga för altruistiska ändamål. I synnerhet kan större öppenhet om vad syftet med dataanvändningen är och under vilka villkor företag lagrar data bidra till att stärka förtroendet.

(6) Tanken att data som har tagits fram eller samlats in av offentliga myndigheter eller andra enheter på offentliga budgetars bekostnad bör gynna samhället har länge varit en del av unionens politik. Genom direktiv (EU) 2019/1024 och sektorsspecifik unionsrätt säkerställs att de offentliga myndigheterna gör en större del av de data de producerar lättillgängliga för användning och vidareutnyttjande. Vissa kategorier av data, såsom data som rör affärshemligheter, insynsskyddade statistiska data och data som skyddas av tredje parts immateriella rättigheter, inbegripet företagshemligheter och personuppgifter, i offentliga databaser görs dock ofta inte tillgängliga, inte ens för forskning eller innovativ verksamhet i allmänhetens intresse, trots att sådan tillgänglighet är möjligt i enlighet med tillämplig unionsrätt, särskilt förordning (EU) 2016/679 och direktiven 2002/58/EG och (EU) 2016/680. På grund av sådana datas känslighet måste vissa tekniska och rättsliga förfarandekrav uppfyllas innan de görs tillgängliga, inte minst för att säkerställa att andra personers rättigheter till sådana data iakttas eller för att begränsa den negativa effekten på de grundläggande rättigheterna, principen om icke-diskriminering och dataskyddet. Det är vanligen tidsödande och kunskapsintensiva att uppfylla sådana krav. Detta har lett till ett otillräckligt nyttjande av sådana data. Vissa medlemsstater håller på att inrätta strukturer, processer eller lagstiftning för att underlätta den typen av vidareutnyttjande, men detta är inte fallet i hela unionen. För att underlätta privata och offentliga enheters användning av data för europeisk forskning och innovation behövs tydliga villkor över hela unionen för tillgång till och användning av sådana data.

([21]) Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1).

([22]) Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (EUT L 295, 21.11.2018, s. 39).

([23]) Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation) (EGT L 201, 31.7.2002, s. 37).

([24]) 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 (EUT L 119, 4.5.2016, s. 89).

(7) Det finns teknik som möjliggör analyser för databaser som innehåller personuppgifter, såsom anonymisering, differentiell integritet, generalisering, undertryckande och randomisering, användningen av syntetiska data eller liknande metoder och andra toppmoderna integritetsbevarande metoder som kan bidra till en mer integritetsvänlig databehandling. Medlemsstaterna bör ge stöd till offentliga myndigheter så att de kan optimera användningen av sådan teknik och därigenom göra en så stor mängd data som möjligt tillgänglig för delning. Tillämpningen av sådan teknik, tillsammans med övergripande konsekvensbedömningar avseende dataskydd och andra skyddsåtgärder, kan bidra till större säkerhet i användningen och vidareutnyttjandet av personuppgifter och bör kunna säkerställa att företagsdata som rör affärshemligheter kan vidareutnyttjas för forsknings-, innovations- och statistikändamål på ett säkert sätt. I många fall innebär tillämpningen av sådan teknik, sådana konsekvensbedömningar och sådana andra skyddsåtgärder att data endast kan användas och vidareutnyttjas i en säker behandlingsmiljö som tillhandahålls eller kontrolleras av den offentliga myndigheten. Det finns erfarenheter på unionsnivå från sådana säkra behandlingsmiljöer som används för forskning om statistiska mikrodata på grundval av kommissionens förordning (EU) nr 557/2013 ([25]). När det gäller personuppgifter bör behandlingen av dessa i allmänhet baseras på en eller flera av de rättsliga grunder för behandling som anges i artiklarna 6 och 9 i förordning (EU) 2016/679.

(8) I enlighet med förordning (EU) 2016/679 bör principerna för dataskyddet inte gälla för anonym information, nämligen information som inte hänför sig till en identifierad eller identifierbar fysisk person, eller för personuppgifter som anonymiserats på ett sådant sätt att den registrerade inte eller inte längre är identifierbar. Återidentifiering av registrerade på grundval av anonymiserade dataset bör vara förbjuden. Detta bör inte påverka möjligheten att bedriva forskning om anonymiseringsteknik, i synnerhet för att säkerställa informationssäkerhet, förbättra befintlig anonymiseringsteknik och bidra till anonymiseringens övergripande robusta karaktär, som genomförs i enlighet med förordning (EU) 2016/679.

(9) För att underlätta skyddet av personuppgifter och konfidentiella uppgifter och för att påskynda förfarandet med att göra sådana uppgifter tillgängliga för vidareutnyttjande inom ramen för denna förordning bör medlemsstaterna uppmuntra de offentliga myndigheterna att ta fram och tillgängliggöra data i enlighet med den princip om *inbyggd öppenhet och öppenhet som standard* som avses i artikel 5.2 i direktiv (EU) 2019/1024 och att främja framställning och upphandling av data i format och strukturer som möjliggör snabb anonymisering.

(10) De kategorier av data som innehas av offentliga myndigheter och som bör vidareutnyttjas enligt denna förordning faller utanför tillämpningsområdet för direktiv (EU) 2019/1024, som utesluter uppgifter som inte är tillgängliga på grund av insynsskydd för statistiska och kommersiella uppgifter och data som ingår i verk eller andra alster till vilka tredje man innehar immateriella rättigheter. Data som rör affärshemligheter inbegriper data som skyddas av företagshemligheter, skyddad know-how och annan information vars otillbörliga röjande skulle påverka företagets marknadsställning eller finansiella sundhet. Denna förordning bör tillämpas på personuppgifter som faller utanför tillämpningsområdet för direktiv (EU) 2019/1024 i den mån som bestämmelserna om tillgång till handlingar utesluter eller begränsar tillgången till sådana data av skäl som rör dataskydd, privatlivet och den enskilda personens integritet, särskilt i enlighet med dataskyddsbestämmelserna. Vidareutnyttjande av uppgifter som kan innehålla företagshemligheter bör ske utan att det påverkar tillämpningen av direktiv (EU) 2016/943, som fastställer ramen för tillåtet anskaffande, användande eller röjande av företagshemligheter.

(11) Denna förordning bör inte göra det obligatoriskt att tillåta vidareutnyttjande av data som innehas av offentliga myndigheter. Mer specifikt, bör varje medlemsstat därför kunna besluta om data ska göras tillgängliga för vidareutnyttjande, även i fråga om syftena med och tillämpningsområdet för denna åtkomst. Denna förordning bör komplettera och inte påverka tillämpningen av mer specifika skyldigheter för offentliga myndigheter att tillåta vidareutnyttjande av data som fastställs i sektorsspecifik unionsrätt eller nationell rätt. Allmänhetens rätt att få tillgång till officiella handlingar kan betraktas som ett allmänt intresse. Med hänsyn till den roll som allmänhetens rätt att få tillgång till officiella handlingar och öppenheten spelar i ett demokratiskt samhälle bör denna förordning inte heller påverka tillämpningen av nationell rätt om beviljande av tillgång till och utlämnande av officiella handlingar. Tillgång till officiella handlingar kan i synnerhet beviljas i enlighet med nationell rätt utan att föreskriva särskilda villkor eller genom att föreskriva särskilda krav som inte föreskrivs i denna förordning.

([25]) Kommissionens förordning (EU) nr 557/2013 av den 17 juni 2013 om tillämpning av Europaparlamentets och rådets förordning (EG) nr 223/2009 om europeisk statistik vad gäller tillgång till konfidentiella uppgifter för vetenskapliga syften och om upphävande av kommissionens förordning (EG) nr 831/2002 (EUT L 164, 18.6.2013, s. 16).

(12) Det system för vidareutnyttjande som föreskrivs i denna förordning bör tillämpas på sådana data vars tillhandahållande ingår i den offentliga verksamhet som bedrivs av de berörda offentliga myndigheterna, enligt lag eller andra bindande regler i medlemsstaterna. Om sådana regler saknas bör den offentliga verksamheten fastställas i enlighet med gängse administrativ praxis i medlemsstaterna, förutsatt att den offentliga verksamheten är tydligt avgränsad och föremål för översyn. Den offentliga verksamheten kan fastställas generellt eller från fall till fall för enskilda offentliga myndigheter. Eftersom offentliga företag inte omfattas av definitionen av offentlig myndighet bör de data som innehas av offentliga företag inte omfattas av denna förordning. Data som innehas av kulturinstitutioner, såsom bibliotek, arkiv och museer samt orkestrar, operor, baletter och teatrar, och av utbildningsanstalter bör inte omfattas av denna förordning eftersom de verk och andra handlingar som de innehar till övervägande del omfattas av tredje parts immateriella rättigheter. Organisationer som bedriver forskning och organisationer som finansierar forskning kan också organiseras som offentliga myndigheter eller offentligrättsliga organ.

Denna förordning bör tillämpas på sådana hybridorganisationer endast i deras egenskap av organisationer som bedriver forskning. Om en organisation som bedriver forskning innehar data som en del av en specifik offentlig–privat sammanslutning med organisationer från den privata sektorn eller andra offentliga myndigheter, offentligrättsliga organ eller hybridorganisationer som bedriver forskning, dvs. som är organiserade som antingen offentliga myndigheter eller offentliga företag, med bedrivande av forskning som huvudsakligt syfte, bör inte heller dessa data omfattas av denna förordning. I relevanta fall bör medlemsstaterna kunna tillämpa denna förordning på offentliga företag eller privata företag som utför uppdrag inom offentlig sektor eller tillhandahåller tjänster av allmänt intresse. Utbytet av data, helt och hållet inom ramen för fullgörandet av deras offentliga uppdrag, mellan offentliga myndigheter i unionen eller mellan offentliga myndigheter i unionen och offentliga myndigheter i tredjeländer eller internationella organisationer, samt utbytet av data mellan forskare för icke-kommersiella vetenskapliga forskningsändamål, bör inte omfattas av bestämmelserna i denna förordning om vidareutnyttjande av vissa kategorier av skyddade data som innehas av offentliga myndigheter.

(13) Offentliga myndigheter bör följa konkurrensrätten när de fastställer principerna för vidareutnyttjande av data som de innehar, och undvika att ingå avtal vars syfte eller verkan kan vara att skapa exklusiva rättigheter för vidareutnyttjande av vissa data. Sådana avtal bör endast vara möjliga om det är motiverat och nödvändigt för tillhandahållandet av en tjänst eller tillhandahållandet av en produkt av allmänt intresse. Detta kan vara fallet om den exklusiva användningen av data är det enda sättet att maximera de samhälleliga fördelarna av berörda data, till exempel om det bara finns en enda enhet (som har specialiserat sig på behandling av en viss datamängd) som kan tillhandahålla den tjänst eller produkt som gör det möjligt för den offentliga myndigheten att tillhandahålla en tjänst eller tillhandahålla en produkt av allmänt intresse. Sådana arrangemang bör dock ingås i enlighet med tillämplig unionsrätt eller nationell rätt och bli föremål för regelbunden översyn baserad på en marknadsanalys för att fastställa om en sådan exklusivitet fortfarande är nödvändig. Dessutom bör sådana arrangemang, beroende på vad som är lämpligt, vara förenliga med relevanta regler för statligt stöd och bör ingås för en begränsad period som inte bör överstiga tolv månader. För att säkerställa öppenhet bör sådana exklusiva avtal offentliggöras online i en form som är förenlig med relevant unionsrätt om offentlig upphandling. Om en exklusiv rätt till vidareutnyttjande av data inte är förenlig med denna förordning bör den exklusiva rätten vara ogiltig.

(14) Förbjudna exklusiva avtal och andra metoder eller arrangemang som rör vidareutnyttjande av data som innehas av offentliga myndigheter och som inte uttryckligen beviljar exklusiva rättigheter men som rimligen kan förväntas begränsa tillgången till data för vidareutnyttjande och som har ingåtts eller redan var införda innan den dag då denna förordning träder i kraft, bör inte förnyas efter det att deras giltighetstid har löpt ut. När det gäller avtal på obestämd tid eller med lång löptid bör de upphöra att gälla inom 30 månader från den dag då denna förordning träder i kraft.

(15) I denna förordning bör det fastställas villkor för vidareutnyttjande av skyddade data som ska gälla för offentliga myndigheter utsedda till behöriga enligt nationell rätt att bevilja eller vägra tillgång för vidareutnyttjande, och som inte ska påverka rättigheter eller skyldigheter avseende tillgång till sådana data. Dessa villkor bör vara icke-diskriminerande, transparenta, proportionella och objektivt motiverade utan att begränsa konkurrensen, med särskilt fokus på att främja små och medelstora företags och nystartade företags tillgång till sådana data. Villkoren för vidareutnyttjande bör utformas på ett sätt som främjar vetenskaplig forskning så att det, till exempel, som regel bör anses vara icke-diskriminerande att privilegiera vetenskaplig forskning. Offentliga myndigheter som tillåter vidareutnyttjande bör förfoga över de tekniska medel som krävs för att säkerställa skyddet av tredje parts rättigheter och intressen och bör ges befogenhet att begära nödvändig information från vidareutnyttjaren. Villkoren för vidareutnyttjande av data bör begränsas till vad som är nödvändigt för att skydda tredje parts rättigheter och intressen i data och integriteten hos de offentliga myndigheternas it- och kommunikationssystem. Offentliga myndigheter bör tillämpa sådana villkor som bäst gagnar vidareutnyttjarens intressen utan att detta leder till en oproportionerlig börda för de offentliga myndigheterna. Villkoren för vidareutnyttjande av data bör utformas på ett sätt som säkerställer effektiva skyddsåtgärder för personuppgifter. Före överföring bör personuppgifter vara

anonymiserade så att de registrerade inte kan identifieras, och data som innehåller affärshemligheter bör ändras på ett sådant sätt att ingen konfidentiell information lämnas ut. Om tillhandahållandet av anonymiserade eller ändrade data inte skulle tillgodose vidareutnyttjarens behov, förutsatt att eventuella krav på att genomföra en konsekvensbedömning avseende dataskydd och samråda med tillsynsmyndigheten enligt artiklarna 35 och 36 i förordning (EU) 2016/679 uppfylls och om riskerna för de registrerades rättigheter och deras intressen är minimala, kan det tillåtas att vidareutnyttja uppgifterna på plats eller på distans inom en säker behandlingsmiljö.

Detta skulle kunna vara ett lämpligt arrangemang för vidareutnyttjande av pseudonymiserade data. Dataanalyser i sådana säkra behandlingsmiljöer bör övervakas av den offentliga myndigheten för att skydda tredje parts rättigheter och intressen. I synnerhet bör personuppgifter överföras till en tredje part för vidareutnyttjande endast om en rättslig grund inom ramen för dataskyddslagstiftningen tillåter en sådan överföring. Icke-personuppgifter bör endast överföras om det saknas skäl att tro att en kombination av dataset som inte består av personuppgifter kan leda till identifiering av de registrerade. Detta bör även gälla pseudonymiserade data som behåller sin status som personuppgifter. Vid återidentifiering av registrerade bör en skyldighet att anmäla en sådan uppgiftsincident till den offentliga myndigheten gälla utöver en skyldighet att anmäla en sådan uppgiftsincident till en tillsynsmyndighet och den registrerade i enlighet med förordning (EU) 2016/679. I tillämpliga fall bör de offentliga myndigheterna underlätta vidareutnyttjande av data efter att de registrerade samtyckt eller datainnehavare med lämpliga tekniska metoder gett sitt tillstånd till vidareutnyttjande av data som rör dem. I det avseendet bör den offentliga myndigheten göra sitt bästa för att bistå potentiella vidareutnyttjare som behöver sådant samtycke eller tillstånd genom att inrätta tekniska mekanismer som gör det möjligt att vidarebefordra begäranden om samtycke eller tillstånd från vidareutnyttjare, när detta är praktiskt genomförbart. Ingen kontaktinformation bör lämnas som gör det möjligt för vidareutnyttjare att kontakta registrerade eller datainnehavare direkt. Om den offentliga myndigheten översänder en begäran om samtycke eller tillstånd bör den säkerställa att den registrerade eller datainnehavaren tydligt informeras om möjligheten att vägra samtycke eller tillstånd.

(16) För att underlätta och främja användningen av data som innehas av offentliga myndigheter för vetenskaplig forskning uppmuntras offentliga myndigheter att utarbeta en harmoniserad strategi och harmoniserade förfaranden för att göra dessa data enkelt tillgängliga för vetenskaplig forskning i allmänhetens intresse. Det skulle bland annat kunna innebära att man skapar rationaliserade administrativa förfaranden, standardiserade dataformat, informativa metadata om metod- och datainsamlingsvalen samt standardiserade datafält som möjliggör enkel sammanslagning av dataset från olika källor till data från den offentliga sektorn om detta är relevant för analysen. Målet för dessa metoder bör vara att främja offentligt finansierade och framtagna data för vetenskaplig forskning i enlighet med principen *så öppen som möjligt, så begränsad som nödvändigt*.

(17) Immateriella rättigheter som innehas av tredje part bör inte påverkas av denna förordning. Denna förordning bör inte påverka vare sig förekomsten av immateriella rättigheter hos offentliga myndigheter eller deras äganderätt av desamma, eller begränsa utövandet av dessa rättigheter på något sätt. De skyldigheter som införs i enlighet med denna förordning bör endast tillämpas i den mån de är förenliga med internationella avtal om skydd av immateriella rättigheter, i synnerhet Bernkonventionen för skydd av litterära och konstnärliga verk (Bernkonventionen), avtalet om handelsrelaterade aspekter av immaterialrätter (Trips-avtalet) och Världsorganisationen för den intellektuella äganderättens fördrag om upphovsrätt (WCT) samt unionsrätt eller nationell rätt om immateriella rättigheter. Offentliga myndigheter bör emellertid använda sin upphovsrätt på ett sätt som underlättar vidareutnyttjande.

(18) Data som omfattas av immateriella rättigheter och företagshemligheter bör endast överföras till en tredje part om överföringen är laglig enligt unionsrätten eller nationell rätt eller med rättsinnehavarens samtycke. Om offentliga myndigheter är innehavare av en databasproducents rätt som föreskrivs i artikel 7.1 i Europaparlamentets och rådets direktiv 96/9/EG ([26]), bör de inte utöva denna rätt för att förhindra vidareutnyttjande av data eller begränsa vidareutnyttjande utöver de gränser som fastställs i denna förordning.

([26]) Europaparlamentets och rådets direktiv 96/9/EG av den 11 mars 1996 om rättsligt skydd för databaser (EGT L 77, 27.3.1996, s. 20).

(19) Företagen och de registrerade bör kunna förlita sig på att vidareutnyttjandet av vissa kategorier av skyddade data som innehas av de offentliga myndigheterna kommer att ske på ett sätt som är i enlighet med deras rättigheter och intressen. Ytterligare skyddsåtgärder bör därför införas för situationer där vidareutnyttjande av sådana data från den offentliga sektorn sker på grundval av behandling av data utanför den offentliga sektorn, såsom ett krav på att offentliga myndigheter säkerställer att fysiska och juridiska personers rättigheter och intressen är fullt skyddade, särskilt med avseende på personuppgifter, kommersiellt känsliga data och immateriella rättigheter, i alla situationer, inklusive om sådana uppgifter överförs till tredjeländer. Offentliga myndigheter bör inte tillåta vidareutnyttjandet av information som lagras av försäkringsföretag eller andra tjänsteleverantörer i e-hälsotillämpningar i syfte att diskriminera vid prissättning, eftersom detta skulle strida mot den grundläggande rätten till tillgång till hälso- och sjukvård.

(20) För att upprätthålla rättvis konkurrens och den öppna marknadsekonomin är det dessutom av största vikt att skyddade data av icke-personuppgiftskaraktär skyddas, särskilt företagshemligheter, men även icke-personuppgifter som avser innehåll som skyddas av immateriella rättigheter, från olaglig tillgång som kan leda till stöld av immateriella rättigheter eller industrispionage. För att säkerställa skyddet av datainnehavarnas rättigheter eller intressen bör det vara möjligt att överföra icke-personuppgifter som ska skyddas från olaglig eller otillåten åtkomst i enlighet med unionsrätten eller nationell rätt och som innehas av offentliga myndigheter till tredjeländer, men endast om lämpliga skyddsåtgärder för användningen av data tillhandahålls. Sådana lämpliga skyddsåtgärder bör inbegripa ett krav att den offentliga myndigheten överför skyddade data till en vidareutnyttjare endast om den vidareutnyttjaren avtalsmässigt åtar sig att skydda dessa data. En vidareutnyttjare som avser att överföra skyddade data till ett tredjeland bör fullgöra de skyldigheter som fastställs i denna förordning även efter det att berörda data har överförts till tredjelandet. För att säkerställa att sådana skyldigheter fullgörs korrekt bör vidareutnyttjaren också godta att den medlemsstat där den offentliga myndighet är belägen som tillät vidareutnyttjandet är behörig vid rättslig tvistlösning.

(21) Lämpliga skyddsåtgärder bör även anses ha vidtagits om det i tredjelandet till vilket icke-personuppgifter har överförts, finns likvärdiga åtgärder som säkerställer att uppgifterna omfattas av en skyddsnivå liknande den som tillämpas enligt unionsrätten, särskilt vad gäller skyddet av företagshemligheter och immateriella rättigheter. När så motiveras på grund av betydande antal begäranden i hela unionen om vidareutnyttjandet av icke-personuppgifter i specifika tredjeländer bör kommissionen för detta ändamål kunna intyga, genom genomförandeakter, att ett tredjeland tillhandahåller en skyddsnivå som i allt väsentligt är likvärdig med den som föreskrivs i unionsrätten. Kommissionen bör bedöma om sådana genomförandeakter är nödvändiga på grundval av informationen från medlemsstaterna via Europeiska datainnovationsstyrelsen. Sådana genomförandeakter skulle försäkra de offentliga myndigheterna om att vidareutnyttjande av data som innehas av offentliga myndigheter i det berörda tredjelandet inte skulle hota dessa datas skyddade karaktär. Bedömningen av skyddsnivån i det berörda tredjelandet bör i synnerhet ta hänsyn till relevant allmän rätt och sektorsspecifik rätt, inklusive om allmän säkerhet, försvar, nationell säkerhet och straffrätt när det gäller tillgång till och skydd av data som inte är personuppgifter, eventuell åtkomst för de offentliga myndigheterna i det tredjelandet till de uppgifter som överförs, huruvida det finns en eller flera effektivt fungerande oberoende tillsynsmyndigheter med ansvar för att säkerställa och kontrollera efterlevnaden av den rättsliga ordning som säkerställer tillgång till sådana data, tredjelandets internationella åtaganden i fråga om dataskydd, eller andra skyldigheter som följer av rättsligt bindande konventioner eller instrument samt av dess deltagande i multilaterala eller regionala system.

Det är särskilt viktigt att det finns effektiva rättsmedel för datainnehavare, offentliga myndigheter eller leverantörer av dataförmedlingstjänster i det berörda tredjelandet i samband med överföring av icke-personuppgifter till det tredjelandet. Sådana skyddsåtgärder bör därför inbegripa tillgång till verkställbara rättigheter och effektiva rättsmedel. Sådana genomförandeakter bör inte påverka rättsliga skyldigheter eller kontraktsmässiga arrangemang som en vidareutnyttjare redan har fullgjort för att skydda icke-personuppgifter, särskilt industridata, och offentliga myndigheters rätt att ålägga vidareutnyttjare att uppfylla villkoren för vidareutnyttjande, i enlighet med denna förordning.

(22) Vissa tredjeländer antar lagar, förordningar och andra rättsakter som syftar till att direkt överföra eller ge statlig tillgång till icke-personuppgifter som finns i unionen och som fysiska och juridiska personer som står under medlemsstaternas jurisdiktion har kontroll över. Beslut och domar av domstolar i tredjeländer eller beslut av förvaltningsmyndigheter i tredjeländer som innehåller krav på sådan överföring eller tillgång till icke-personuppgifter ska vara verkställbara, om de grundar sig på ett gällande internationellt avtal, såsom ett fördrag om ömsesidig rättshjälp, mellan det begärande tredjelandet och unionen eller en medlemsstat. I vissa fall kan det uppstå situationer där skyldigheten att överföra eller ge tillgång till icke-personuppgifter som härrör från ett tredjelands rätt står i strid med en skyldighet att skydda sådana data enligt unionsrätten eller nationell rätt, särskilt när det gäller skyddet av den enskilda personens grundläggande rättigheter eller en medlemsstats grundläggande intressen med

avseende på nationell säkerhet eller försvar samt skyddet av kommersiellt känsliga uppgifter och skyddet av immateriella rättigheter, inbegripet avtalsskyldigheter i fråga om konfidentiell behandling i enlighet med sådan rätt. I avsaknad av internationella avtal som reglerar sådana frågor bör överföring av eller tillgång till icke-personuppgifter endast tillåtas om det, i synnerhet, har kontrollerats att tredjelandets rättssystem omfattar krav på att beslutets eller domens skäl och proportionalitet anges, att beslutet eller domen är specifik till sin karaktär och att den motiverade invändningen från mottagaren är föremål för prövning av en behörig domstol i tredjelandet, som har befogenhet att vederbörligen beakta de relevanta rättsliga intressena för den som tillhandahåller sådana uppgifter.

Offentliga myndigheter, fysiska eller juridiska personer som beviljats rätten att vidareutnyttja data, leverantörer av dataförmedlingstjänster och erkända dataaltruismorganisationer bör dessutom, om de undertecknar avtal med andra privata partner, säkerställa att icke-personuppgifter som innehas i unionen görs tillgängliga i eller överförs till tredjeländer endast i enlighet med unionsrätten eller den berörda medlemsstatens nationella rätt.

(23) I syfte att ytterligare främja förtroendet för unionens dataekonomi är det avgörande att de skyddsåtgärder för unionsmedborgare, den offentliga sektorn och företag som säkerställer kontroll över dessas strategiska och känsliga uppgifter genomförts och att unionsrätt, värden och standarder upprätthålls inom bland annat, men inte enbart, områdena säkerhet, dataskydd och konsumentskydd. För att förhindra olaglig åtkomst till icke-personuppgifter bör de offentliga myndigheterna, de fysiska eller juridiska personer som beviljats rätten att vidareutnyttja data, leverantörerna av dataförmedlingstjänster och erkända dataaltruismorganisationer, vidta alla rimliga åtgärder för att förhindra åtkomst till de system där icke-personuppgifter lagras, inbegripet kryptering av data eller företagspolicyer. För det ändamålet bör det säkerställas att offentliga myndigheter, fysiska eller juridiska personer som beviljats rätten att vidareutnyttja data, leverantörer av dataförmedlingstjänster och erkända dataaltruismorganisationer uppfyller samtliga relevanta tekniska standarder, uppförandekoder och certifieringar på unionsnivå.

(24) För att bygga upp förtroendet för mekanismer för vidareutnyttjande kan det vara nödvändigt att införa strängare villkor för vissa typer av icke-personuppgifter som kan komma att identifieras som mycket känsliga i framtida särskilda unionslagstiftningsakter, när det gäller överföring till tredjeländer, om en sådan överföring skulle kunna äventyra unionens offentligpolitiska mål, i linje med internationella åtaganden. Till exempel på hälsoområdet kan vissa dataset som innehas av aktörer i det allmänna hälso- och sjukvårdssystemet, t.ex. offentliga sjukhus, fastställas som mycket känsliga hälsodata. Andra relevanta sektorer är transport, energi, miljö och finans. För att säkerställa en harmoniserad praxis i hela unionen bör sådana typer av mycket känsliga offentliga icke-personuppgifter definieras i unionsrätten, till exempel inom ramen för det europeiska hälsodataområdet eller annan sektorspecifik rätt. Dessa villkor för överföring av sådana uppgifter till tredjeländer bör fastställas i delegerade akter. Villkoren bör vara proportionella, icke-diskriminerande och nödvändiga för att upprätthålla de legitima offentligpolitiska mål för unionen som fastställts, såsom skydd av folkhälsan, säkerhet, miljö, allmän moral, konsumentskydd, integritet och skydd av personuppgifter. Villkoren bör motsvara de risker som identifierats i förhållande till känsligheten hos sådana data, bland annat när det gäller risken för återidentifiering av enskilda personer. Sådana villkor kan omfatta villkor för överföringen eller tekniska arrangemang, såsom krav på användning av en säker behandlingsmiljö, begränsningar när det gäller vidareutnyttjande av data i tredjeländer eller kategorier av personer som har rätt att överföra sådana data till tredjeland eller har tillgång till dem i tredjelandet. I undantagsfall kan sådana villkor också omfatta begränsningar av överföringen av data till tredjeländer för att skydda allmänintresset.

(25) Offentliga myndigheter bör kunna ta ut avgifter för vidareutnyttjande av data, men bör också kunna tillåta vidareutnyttjande till en nedsatt avgift eller kostnadsfritt, till exempel för vissa kategorier av vidareutnyttjande såsom icke-kommersiellt vidareutnyttjande eller vidareutnyttjande för forskningsändamål, eller små och medelstora företags, nystartade företags, civilsamhällets och utbildningsanstalters vidareutnyttjande, för att ge incitament för sådant vidareutnyttjande i syfte att stimulera forskning och innovation och stödja företag som är en viktig källa till innovation och vanligtvis har svårare att själva samla in relevanta data, i enlighet med reglerna för statligt stöd. I det specifika sammanhanget bör forskningsändamål anses inbegripa alla forskningsrelaterade ändamål oaktat den berörda forskningsinstitutionens organisatoriska eller finansiella struktur, med undantag för forskning som bedrivs

av ett företag och som syftar till att utveckla, förbättra eller optimera produkter eller tjänster. Sådana avgifter bör, vara transparenta, icke-diskriminerande och begränsade till de nödvändiga kostnaderna och bör inte begränsa konkurrensen. En förteckning över kategorier av vidareutnyttjare som betalar lägre avgift eller helt slipper avgift bör offentliggöras tillsammans med de kriterier som använts för upprättandet av förteckningen.

(26) För att ge incitament till vidareutnyttjande av särskilda kategorier av data som innehas av offentliga myndigheter bör medlemsstaterna inrätta en gemensam informationspunkt som ska fungera som ett gränssnitt för vidareutnyttjare som vill vidareutnyttja dessa data. Denna informationspunkt bör ha ett sektorsövergripande uppdrag och vid behov komplettera arrangemang på sektorsnivå. Den gemensamma informationspunkten bör kunna förlita sig på automatiska metoder när den överför förfrågningar eller ansökningar om vidareutnyttjande. En tillräcklig mänsklig tillsyn i överföringsprocessen bör säkerställas. Befintliga praktiska arrangemang som till exempel portaler för öppna data skulle kunna användas för detta syfte. Den enda informationspunkten bör ha en förteckning över resurser som innehåller en översikt över alla tillgängliga datakällor, däribland de datakällor som finns tillgängliga vid sektorsspecifika, regionala eller lokala informationspunkter, tillsammans med relevant information som beskriver tillgängliga data. Dessutom bör medlemsstaterna utse, inrätta eller underlätta inrättandet av behöriga organ för att stödja verksamheten inom offentliga myndigheter som tillåter vidareutnyttjande av vissa kategorier av skyddade data. Deras uppgifter kan inbegripa att bevilja tillgång till data, om detta föreskrivs enligt sektorsspecifik unionsrätt eller nationell rätt. Dessa behöriga organ bör ge bistånd till offentliga myndigheter med hjälp av den senaste tekniken, bland annat avseende hur data bäst struktureras och lagras för att göra dem lättillgängliga, i synnerhet genom applikationsprogrammeringsgränssnitt, samt göra data interoperabla, överförbara och sökbara, med beaktande av bästa praxis för databehandling samt eventuella befintliga tillsynsstandarder och tekniska standarder och säkra databehandlingsmiljöer, som möjliggör dataanalys med bevarande av informationens integritet.

De behöriga organen bör agera i enlighet med den offentliga myndighetens instruktioner. En sådan biståndsstruktur skulle kunna bistå de registrerade och datainnehavarna att hantera samtycke eller tillstånd för vidareutnyttjande, inbegripet samtycke och tillstånd till vissa områden av vetenskaplig forskning, om vedertagna etiska standarder för vetenskaplig forskning iakttas. De behöriga myndigheterna bör inte ha någon tillsynsfunktion, då denna uteslutande ska utövas av tillsynsmyndigheter enligt förordning (EU) 2016/679. Databehandlingen bör, utan att det påverkar dataskyddsmyndigheternas tillsynsbefogenheter, utföras under ansvar av den offentliga myndighet som ansvarar för det register som innehåller dessa data, och som förblir personuppgiftsansvarig enligt definitionen i förordning (EU) 2016/679 i den mån personuppgifter berörs. Medlemsstaterna bör kunna ha ett eller flera behöriga organ, som kan vara verksamma inom olika sektorer. De offentliga myndigheternas interna avdelningar skulle även kunna fungera som behöriga organ. Ett behörigt organ skulle kunna vara en offentlig myndighet som bistår andra offentliga myndigheter när det gäller att tillåta vidareutnyttjande av data, om så är relevant, eller en offentlig myndighet som själv ger tillstånd till vidareutnyttjande. Biståndet till andra offentliga myndigheter bör omfatta att på begäran informera dem om bästa praxis när det gäller att uppfylla de krav som fastställs i den här förordningen, bland annat de tekniska medlen för tillhandahållande av en säker behandlingsmiljö eller de tekniska metoderna för att säkerställa integritet och konfidentiell behandling när tillgång ges till vidareutnyttjande av data som omfattas av tillämpningsområdet för den här förordningen.

(27) Dataförmedlingstjänster förväntas spela en nyckelroll i dataekonomin, i synnerhet när det gäller att stödja och främja metoder för frivillig datadelning mellan företag eller att underlätta datadelning när det gäller skyldigheter som fastställs i unionsrätten eller nationell rätt. De skulle kunna bli ett verktyg för att underlätta utbyte av stora mängder relevanta data. Leverantörer av dataförmedlingstjänster, vilka även kan omfatta offentliga myndigheter, som erbjuder tjänster som kopplar samman de olika aktörerna kan bidra till en effektiv samkörning av data och till att underlätta bilateral datadelning. Specialiserade dataförmedlingstjänster som är oberoende av registrerade, datainnehavare och dataanvändare skulle kunna underlätta framväxten av nya datadrivna ekosystem som är oberoende av aktörer med betydande marknadsinflytande, samtidigt som de möjliggör icke-diskriminerande tillgång till dataekonomin för aktörer av alla storlekar, särskilt små och medelstora företag och nystartade företag med begränsade ekonomiska, rättsliga eller administrativa resurser. Detta kommer att vara av särskild vikt i samband med inrättandet av gemensamma europeiska dataområden, nämligen ändamåls- eller sektorsspecifika eller sektorsöverskridande interoperabla ramar med gemensamma standarder och praxisformer för delning eller gemensam behandling av data bl.a. för utvecklingen av nya produkter och tjänster, vetenskaplig forskning eller civilsamhällsinitiativ. Dataförmedlingstjänsterna skulle kunna innefatta bilateral eller multilateral delning av data eller inrättandet av plattformar eller databaser som möjliggör datadelning eller gemensamt utnyttjande av data, liksom inrättandet av en särskild infrastruktur för sammankoppling av registrerade och datainnehavare med dataanvändare.

(28) Denna förordning bör omfatta tjänster som syftar till att med tekniska, rättsliga eller andra medel upprätta affärsförbindelser för datadelning mellan ett obestämt antal registrerade och datainnehavare, å ena sidan, och dataanvändare, å andra sidan, inbegripet för utövande av de registrerades rättigheter avseende personuppgifter. Om företag eller andra enheter erbjuder flera datarelaterade tjänster bör endast sådan verksamhet som direkt berör tillhandahållandet av dataförmedlingstjänster omfattas av denna förordning. Tillhandahållande av molnlagring, analys, programvara för datadelning, webbläsare, insticksprogram för webbläsare eller e-posttjänster bör inte anses vara dataförmedlingstjänster i den mening som avses i denna förordning, under förutsättning att sådana tjänster endast tillhandahåller tekniska verktyg för registrerade eller datainnehavare för delning av data med andra, men tillhandahållandet av sådana verktyg varken syftar till att upprätta en affärsförbindelse mellan datainnehavare och dataanvändare eller ger leverantören av dataförmedlingstjänster möjlighet att erhålla information om upprättandet av affärsförbindelser som syftar till datadelning. Exempel på dataförmedlingstjänster inkluderar datamarknader där företag kan göra data tillgängliga för andra, organisatörer av ekosystem för datadelning som är öppna för alla intresserade parter, till exempel inom ramen för gemensamma europeiska dataområden, samt datapooler som inrättas gemensamt av flera juridiska eller fysiska personer i avsikten att licensiera användningen av sådana datapooler till alla intresserade parter på ett sätt som innebär att alla deltagare som bidrar till datapooler belönas för sitt bidrag.

Detta skulle exkludera tjänster som erhåller data från datainnehavare och aggregerar, berikar eller omvandlar data i syfte att avsevärt öka deras värde och licensierar användningen av resulterande data till dataanvändare, utan att upprätta en affärsförbindelse mellan datainnehavare och dataanvändare. Dessutom skulle det exkludera tjänster som uteslutande används av en datainnehavare för att möjliggöra användning av de data som den datainnehavaren innehar, eller som används av flera juridiska personer i en sluten grupp, inbegripet leverantörs- eller kundrelationer eller samarbeten som grundar sig på avtal, särskilt sådana som har som huvudsakligt syfte att säkerställa funktioner för föremål och enheter som är anslutna till sakernas internet.

(29) Tjänster som är inriktade på förmedling av upphovsrättsligt skyddat innehåll, däribland onlineleverantör av delningstjänster för innehåll enligt definitionen i artikel 2.6 i direktiv (EU) 2019/790, bör inte omfattas av den här förordningen. Tillhandahållare av konsoliderad handelsinformation enligt definitionen i artikel 2.1.35 i Europaparlamentets och rådets förordning (EU) nr 600/2014 ([27]) och leverantörer av kontoinformationstjänster enligt definitionen i artikel 4.19 i Europaparlamentets och rådets direktiv (EU) 2015/2366 ([28]) bör inte anses vara leverantörer av dataförmedlingstjänster vid tillämpning av den här förordningen. Den här förordningen bör inte tillämpas på tjänster som erbjuds av offentliga myndigheter för att underlätta antingen vidareutnyttjande av skyddade data som innehas av offentliga myndigheter i enlighet med den här förordningen eller användning av andra data, i den mån dessa tjänster inte syftar till att upprätta affärsförbindelser. Dataaltruismorganisationer som regleras i denna förordning bör inte anses erbjuda dataförmedlingstjänster förutsatt att dessa tjänster inte upprättar en affärsförbindelse mellan potentiella dataanvändare, å ena sidan, och registrerade och datainnehavare som tillgängliggör data utifrån altruistiska ändamål, å andra sidan. Andra tjänster som inte syftar till att upprätta affärsförbindelser, till exempel databaser som syftar till att möjliggöra vidareutnyttjande av vetenskapliga forskningsdata i enlighet med principerna om öppen tillgång bör inte anses vara dataförmedlingstjänster i den mening som avses i den här förordningen.

(30) En särskild kategori av dataförmedlingstjänster omfattar leverantörer av tjänster som erbjuder sina tjänster till registrerade. Sådana leverantörer av dataförmedlingstjänster strävar efter att stärka de registrerades handlingsförmåga och särskilt enskilda personers kontroll över de uppgifter som avser dem. Sådana leverantörer hjälper enskilda personer att utöva sina rättigheter enligt förordning (EU) 2016/679, särskilt att hantera deras givande och återkallande av samtycke till databehandling, rätten att få tillgång till sina egna personuppgifter, rätten till rättelse av felaktiga personuppgifter, rätten till radering eller rätten ”att bli bortglömd”, rätten att begränsa behandlingen och rätten till dataportabilitet, som gör det möjligt för registrerade att flytta sina personuppgifter från en personuppgiftsansvarig till en annan. I det sammanhanget är det viktigt att sådana leverantörers affärsmodell säkerställer att det inte finns några dåligt anpassade incitament som uppmuntrar enskilda personer att använda sådana tjänster för att tillgängliggöra mer data som avser dem för behandling än vad som skulle ligga i deras intresse. Detta skulle kunna inbegripa rådgivning till enskilda personer om möjlig användning av deras data och hur de gör due diligence-kontroller av dataanvändare innan de tillåts kontakta registrerade, i syfte att undvika bedrägerier. I vissa situationer kan det vara önskvärt att samla faktiska data inom ett personligt dataområde, så att

([27]) Europaparlamentets och rådets förordning (EU) nr 600/2014 av den 15 maj 2014 om marknader för finansiella instrument och om ändring av förordning (EU) nr 648/2012 (EUT L 173, 12.6.2014, s. 84).

([28]) Europaparlamentets och rådets direktiv (EU) 2015/2366 av den 25 november 2015 om betaltjänster på den inre marknaden, om ändring av direktiven 2002/65/EG, 2009/110/EG och 2013/36/EU samt förordning (EU) nr 1093/2010 och om upphävande av direktiv 2007/64/EG (EUT L 337, 23.12.2015, s. 35).

behandlingen kan ske inom det området utan att personuppgifter överförs till tredje part, för att maximera skyddet av personuppgifter och integritet. Sådana personliga dataområden skulle kunna innehålla statiska personuppgifter, däribland namn, adress och födelsedatum, samt dynamiska data som genereras av en enskild person, genom till exempel användning av en onlinetjänst eller ett föremål anslutet till sakernas internet. De skulle också kunna användas för att lagra verifierade identitetsuppgifter, såsom passnummer eller socialförsäkringsuppgifter samt behörighetsuppgifter, såsom körkort, examensbevis eller uppgifter om bankkonton.

(31) Datakooperativ strävar efter att uppnå ett antal mål, särskilt att stärka enskilda personers ställning när det gäller att fatta välgrundade beslut innan de samtycker till dataanvändning, påverka dataanvändarorganisationers villkor och bestämmelser knutna till dataanvändning på ett sätt som ger gruppens enskilda medlemmar bättre valmöjligheter, eller eventuellt finna lösningar på meningsmotsättningar mellan enskilda medlemmar i en grupp om hur data kan användas om dessa data är relaterade till flera registrerade inom den gruppen. I det sammanhanget är det viktigt att slå fast att rättigheterna enligt förordning (EU) 2016/679 är personliga rättigheter som tillhör den registrerade och att registrerade inte kan avsäga sig sådana rättigheter. Datakooperativ skulle också kunna vara ett användbart verktyg för enmansföretag samt små och medelstora företag som ofta är jämförbara med enskilda personer när det gäller kunskap om datadelning.

(32) För att öka förtroendet för sådana dataförmedlingstjänster, i synnerhet när det gäller användningen av data och uppfyllandet av de villkor som de registrerade och datainnehavarna sätter upp, är det nödvändigt att upprätta ett regelverk på unionsnivå som fastställer krav med hög harmoniseringsgrad avseende ett tillförlitligt tillhandahållande av sådana dataförmedlingstjänster och som genomförs av de behöriga myndigheterna. Det regelverket kommer att bidra till att säkerställa att de registrerade och datainnehavarna samt dataanvändarna får bättre kontroll över tillgången till och användningen av deras data, i enlighet med unionsrätten. Kommissionen skulle även kunna uppmuntra och underlätta utarbetandet av uppförandekoder på unionsnivå med deltagande av berörda parter, särskilt vad avser interoperabilitet. Både i situationer där datadelning sker i samband med företagstjänster och när datadelning sker i samband med konsumenttjänster bör leverantörer av dataförmedlingstjänster erbjuda en ny ”europeisk” dataförvaltning genom att i säkra en åtskillnad i dataekonomin mellan tillhandahållandet, förmedlingen och användningen av data. Leverantörer av dataförmedlingstjänster skulle också kunna göra särskild teknisk infrastruktur tillgänglig för sammankoppling av registrerade och datainnehavare med dataanvändare. I detta avseende är det särskilt viktigt att utforma denna infrastruktur på ett sådant sätt att små och medelstora företag och nystartade företag inte stöter på några tekniska eller andra hinder för sitt deltagande i dataekonomin.

Leverantörer av dataförmedlingstjänster bör tillåtas att erbjuda ytterligare särskilda verktyg till datainnehavare eller de registrerade för det särskilda syftet att underlätta utbytet av data, exempelvis i form av tillfällig lagring, kuratering, konvertering, anonymisering och pseudonymisering. Dessa verktyg och tjänster bör användas endast på uttrycklig begäran eller efter uttryckligt godkännande av datainnehavaren eller den registrerade, och tredjepartsverktyg som erbjuds i detta sammanhang bör inte använda data för andra ändamål. Samtidigt bör leverantörer av dataförmedlingstjänster tillåtas anpassa de data som utbyts, för att göra dem mer användbara för dataanvändaren om dataanvändaren så önskar, eller att förbättra interoperabiliteten genom, till exempel, att konvertera dessa data till specifika format.

(33) Det är viktigt att möjliggöra en konkurrensutsatt miljö för datadelning. En viktig faktor för att ökaförtroendet och datainnehavarnas, de registrerades och dataanvändarnas kontroll över dataförmedlingstjänster är att leverantörerna av dataförmedlingstjänster är neutrala när det gäller de data som utbyts mellan datainnehavare eller de registrerade och dataanvändare. Leverantörerna av dataförmedlingstjänster bör därför endast fungera som förmedlare i transaktionerna och inte använda de data som utbyts för några andra ändamål. De kommersiella villkoren, inklusive prissättning, för tillhandahållandet av dataförmedlingstjänster bör inte vara beroende av huruvida en potentiell datainnehavare eller dataanvändare använder andra tjänster, däribland lagring, analys, artificiell intelligens eller andra databaserade tillämpningar, som tillhandahålls av samma leverantör av dataförmedlingstjänster eller en närstående enhet, och i så fall i vilken utsträckning datainnehavaren eller data användaren använder sådana andra tjänster. Detta kommer också förutsätta en strukturell åtskillnad mellan dataförmedlingstjänsten och alla andra tjänster som erbjuds, så att intressekonflikter undviks. Därmed bör dataförmedlingstjänsten erbjudas via en juridisk person som är separat från all övrig verksamhet som bedrivs av leverantören av dataförmedlingstjänster. Emellertid bör leverantörer av dataförmedlingstjänster kunna använda de data som tillhandahålls av datainnehavaren för att förbättra sina dataförmedlingstjänster.

Leverantörer av dataförmedlingstjänster bör endast kunna ställa sina egna eller tredje parts verktyg till datainnehavares, de registrerades eller dataanvändares förfogande för att underlätta utbytet av data, exempelvis verktyg för konvertering eller kuratering av data, efter den registrerades eller datainnehavarens uttryckliga begäran eller godkännande. De tredjepartsverktyg som erbjuds i detta sammanhang bör inte använda data för andra ändamål än de som är relaterade till dataförmedlingstjänster. Leverantörer av dataförmedlingstjänster som

förmedlar ett utbyte av data mellan enskilda personer som registrerade och juridiska personer som dataanvändare bör, utöver att axla sitt förvaltaruppdrag gentemot de enskilda personerna, säkerställa att de agerar i de registrerades intresse. Frågor om ansvar för alla materiella och immateriella skador och brister som uppstår till följd av agerandet av leverantören av dataförmedlingstjänster bör tas upp i det berörda avtalet, på grundval av nationella ansvarsordningar.

(34) Leverantörer av dataförmedlingstjänster bör vidta rimliga åtgärder för att säkerställa interoperabilitet inom en sektor och mellan olika sektorer i syfte att säkerställa en korrekt fungerande inre marknad. Rimliga åtgärder skulle bland annat kunna inbegripa att man följer de befintliga standarder som allmänt används i den sektor inom vilken leverantören av dataförmedlingstjänster är verksam. Europeiska datainnovationsstyrelsen bör underlätta framtagningen av ytterligare branschstandarder där det är nödvändigt. Leverantörer av dataförmedlingstjänster bör i god tid genomföra de åtgärder för interoperabilitet mellan dataförmedlingstjänster som antagits av Europeiska datainnovationsstyrelsen.

(35) Denna förordning bör inte påverka skyldigheten för leverantörer av dataförmedlingstjänster att uppfylla kraven i förordning (EU) 2016/679 och tillsynsmyndigheternas skyldighet att säkerställa efterlevnaden av den förordningen. Den här förordningen bör inte påverka skyddet av personuppgifter i de fall då leverantörer av dataförmedlingstjänster behandlar personuppgifter. I de fall då leverantörer av dataförmedlingstjänster är personuppgiftsansvariga eller personuppgiftsbiträden enligt definitionerna i förordning (EU) 2016/679 är de bundna av bestämmelserna i den förordningen.

(36) Leverantörer av dataförmedlingstjänster förväntas ha infört förfaranden och åtgärder för att ålägga sanktioner för bedrägliga eller otillbörliga metoder i samband med parter som söker åtkomst via deras dataförmedlingstjänster, inbegripet genom åtgärder såsom uteslutning av dataanvändare som bryter mot tjänstevillkoren eller mot befintlig rätt.

(37) Leverantörer av dataförmedlingstjänster bör också vidta åtgärder för att säkerställa att konkurrensrätten följs och inrätta förfaranden för det ändamålet. Detta gäller i synnerhet sådana situationer där datadelning gör det möjligt för företag att få kännedom om faktiska eller potentiella konkurrenters marknadsstrategier. Typisk information som är känslig i konkurrenshänseende är till exempel information om kunduppgifter, framtida priser, produktionskostnader, kvantiteter, omsättning, försäljning eller kapacitet.

(38) Ett anmälningsförfarande för dataförmedlingstjänster bör inrättas för att säkerställa att dataförvaltning inom unionen är baserad på ett tillförlitligt utbyte av data. Vinsterna av en tillförlitlig miljö kan bäst uppnås genom ett införande av ett antal krav för tillhandahållandet av dataförmedlingstjänster, men utan något krav på ett uttryckligt beslut eller en uttrycklig administrativ åtgärd av den behöriga myndigheten för dataförmedlingstjänster för tillhandahållandet av sådana tjänster. Anmälningsförfarandet bör inte medföra otillbörliga hinder för små och medelstora företag, nystartade företag och civilsamhällesorganisationer och bör vara förenlig med principen om icke-diskriminering.

(39) För att stödja ett effektivt gränsöverskridande tillhandahållande av tjänster bör leverantören av dataförmedlingstjänster åläggas att sända en anmälan endast till den behöriga myndigheten för dataförmedlingstjänster från den medlemsstat där leverantörens huvudsakliga verksamhetsställe är beläget eller där leverantörens rättsliga ombud finns. En sådan anmälan bör inte innefatta mer än en ren förklaring om avsikten att tillhandahålla sådana tjänster och bör endast kompletteras genom tillhandahållande av den information som anges i denna förordning. Efter relevant anmälan bör leverantören av dataförmedlingstjänster kunna inleda sin verksamhet i varje medlemsstat utan ytterligare anmälningsskyldigheter.

(40) Det anmälningsförfarande som fastställs i denna förordning bör inte påverka tillämpningen av särskilda kompletterande bestämmelser för tillhandahållandet av dataförmedlingstjänster som är tillämpliga genom sektorsspecifik rätt.

(41) Det huvudsakliga verksamhetsstället för en leverantör av dataförmedlingstjänster i unionen bör vara platsen för dess centrala förvaltning i unionen. Det huvudsakliga verksamhetsstället för en leverantör av dataförmedlingstjänster i unionen bör fastställas i enlighet med objektiva kriterier och bör avse det faktiska och reella utövandet av ledningsverksamheten. Den verksamhet som bedrivs av en leverantör av dataförmedlingstjänster bör överensstämma med den nationella rätten i den medlemsstat där denne har sitt huvudsakliga verksamhetsställe.

(42) För att säkerställa att leverantörerna av dataförmedlingstjänster uppfyller de villkor som fastställs i denna förordning bör de ha sitt huvudsakliga verksamhetsställe i unionen. Om en leverantör av dataförmedlingstjänster som inte är etablerad i unionen erbjuder tjänster inom unionen bör leverantören utse en rättslig företrädare. Det är nödvändigt att utse en rättslig företrädare i sådana fall med tanke på att sådana leverantörer av dataförmedlingstjänster hanterar både personuppgifter och data som rör affärshemligheter och det därmed är nödvändigt att övervaka att leverantörerna av dataförmedlingstjänster efterlever denna förordning. I syfte att fastställa om en sådan leverantör av dataförmedlingstjänster erbjuder tjänster inom unionen bör det kontrolleras om det är uppenbart att leverantören av dataförmedlingstjänster planerar att erbjuda tjänster till personer i en eller flera medlemsstater. Enbart det faktum att en webbplats är tillgänglig i unionen eller att det finns en e-postadress eller andra kontaktuppgifter för leverantören av dataförmedlingstjänster eller att man använder ett språk som används i det tredjeland där leverantören av dataförmedlingstjänster är etablerad, bör inte anses räcka för att fastställa en sådan avsikt. Emellertid kan sådana faktorer som användning av ett visst språk eller en viss valuta som allmänt används i en eller flera medlemsstater, och möjlighet att beställa tjänster på detta språk, eller att användare i unionen omnämns, göra det uppenbart att leverantören av dataförmedlingstjänster planerar att erbjuda tjänster inom unionen.

En utsedd rättslig företrädare bör agera på uppdrag av leverantören av dataförmedlingstjänster och det bör vara möjligt för behöriga myndigheter för dataförmedlingstjänster att vända sig till den rättsliga företrädaren utöver eller i stället för leverantören av dataförmedlingstjänster, även i händelse av en överträdelse, i syfte att inleda verkställighetsförfaranden mot en leverantör av dataförmedlingstjänster som inte uppfyller kraven och som inte är etablerad i unionen. Den rättsliga företrädaren bör utses genom en skriftlig fullmakt från leverantören av dataförmedlingstjänster att agera på dess vägnar med avseende på leverantörens skyldigheter enligt denna förordning.

(43) För att hjälpa de registrerade och datainnehavare att enkelt identifiera, och därigenom öka sitt förtroende för leverantörer av dataförmedlingstjänster som är erkända i unionen bör det inrättas en gemensam logotyp som är igenkännlig i hela unionen, utöver beteckningen ”leverantörer av dataförmedlingstjänster som är erkända i unionen”.

(44) De behöriga myndigheterna för dataförmedlingstjänster som utses för att övervaka leverantörer av dataförmedlingstjänsters uppfyllande av kraven i denna förordning bör väljas på grundval av sin kapacitet och sakkunskap avseende horisontellt eller sektorsbaserat datautbyte. De bör vara oberoende av alla leverantörer av dataförmedlingstjänster samt transparenta och opartiska i utförandet av sina arbetsuppgifter. Medlemsstaterna bör meddela kommissionen dessa behöriga myndigheter för dataförmedlingstjänsters identitet. De behöriga myndigheterna för dataförmedlingstjänsters behörighet och befogenheter bör inte påverka dataskyddsmyndigheternas befogenheter. I synnerhet i alla frågor som rör en bedömning av efterlevnaden av förordning (EU) 2016/679 bör den behöriga myndigheten för dataförmedlingstjänster, i tillämpliga fall, efterfråga ett yttrande eller beslut av den behöriga tillsynsmyndighet som inrättats i enlighet med den förordningen.

(45) Det finns en stor potential för mål av allmänt intresse vid användningen av data som tillhandahålls frivilligt av de registrerade på grundval av deras informerade samtycke eller, när det gäller icke-personuppgifter som tillhandahålls av datainnehavare. Sådana mål skulle kunna inkludera hälso- och sjukvård, bekämpande av klimatförändringar, förbättring av mobiliteten, främjande av utveckling, framställning och spridning av officiell statistik, förbättrat tillhandahållande av offentliga tjänster eller politiskt beslutsfattande. Stöd till vetenskaplig forskning bör också anses vara ett mål av allmänt intresse. Denna förordning bör syfta till att bidra till framväxten av tillräckligt stora datapooler som görs tillgängliga baserat på dataaltruism för att möjliggöra dataanalys och maskininlärning, i hela unionen. För att uppnå det målet bör medlemsstaterna kunna inrätta organisatoriska eller tekniska arrangemang, eller båda, som underlättar dataaltruism. Sådana arrangemang skulle kunna innefatta tillgång till lättanvända verktyg för registrerade eller datainnehavare för givande av samtycke eller tillstånd till altruistisk användning av deras data, anordnande av informationskampanjer eller ett strukturerat utbyte mellan behöriga myndigheter avseende hur offentlig politik, såsom förbättring av trafik och folkhälsa och bekämpning av klimatförändringar, kan gynnas av dataaltruism. För det ändamålet bör medlemsstaterna kunna fastställa nationella strategier för dataaltruism. Registrerade bör endast kunna erhålla ersättning för de kostnader som deådrar sig när de gör sina data tillgängliga för mål av allmänt intresse.

(46) Registreringen av erkända dataaltruismorganisationer och användningen av beteckningen ”dataaltruismorganisation som är erkänd i unionen” förväntas leda till upprättandet av centrallager för databaser. En registrering i en medlemsstat skulle gälla i hela unionen, och förväntas främja en gränsöverskridande användning av data inom unionen och framväxten av datapooler som täcker flera medlemsstater. Datainnehavare skulle kunna ge tillstånd till behandling av deras icke-personuppgifter för ett antal ändamål som inte är fastställda vid den tidpunkt då de ger sitt

tillstånd. Sådana erkända dataaltruismorganisationers uppfyllande av ett antal krav som fastställs i denna förordning bör skapa förtroende för att de data som tillhandahålls för altruistiska ändamål faktiskt tjänar ett mål av allmänt intresse. Sådant förtroende bör i synnerhet uppnås genom att ha en etableringsort eller en rättslig företrädare inom unionen, samt från kravet att erkända dataaltruismorganisationer är icke-vinstdrivande organisationer, från transparenskrav och från särskilda skyddsmekanismer för att skydda de registrerades och företagens rättigheter och intressen.

Ytterligare skyddsmekanismer bör inkludera att göra det möjligt att behandla relevanta data inom en säker behandlingsmiljö som drivs av de erkända dataaltruismorganisationerna, tillsynsmekanismer som etiska råd eller styrelser, inbegripet företrädare från det civila samhället för att säkerställa att de personuppgiftsansvariga upprätthåller höga standarder när det gäller forskningsetik och skydd av grundläggande rättigheter, effektiva och tydligt förmedlade tekniska metoder för att när som helst dra tillbaka eller ändra sitt samtycke, på grundval av personuppgiftsbiträdenas informationsskyldighet enligt förordning (EU) 2016/679, samt möjligheter för de registrerade att hålla sig underrättade om användningen av de data som de tillhandahållit. Registrering som en erkänd dataaltruismorganisation bör inte vara en förutsättning för att bedriva dataaltruismverksamhet. Kommissionen bör genom delegerade akter utarbeta en regelbok i nära samarbete med dataaltruismorganisationer och berörda parter. Efterlevnad av den regelboken bör vara ett krav för registrering som en erkänd dataaltruismorganisation.

(47) För att hjälpa de registrerade och datainnehavare att enkelt identifiera, och därigenom öka sitt förtroende för, erkända dataaltruismorganisationer bör det inrättas en gemensam logotyp som är igenkännlig i hela unionen. Den gemensamma logotypen bör åtföljas av en QR-kod med en länk till det offentliga unionsregistret över erkända dataaltruismorganisationer.

(48) Denna förordning bör inte påverka inrättandet av, organisationen av eller funktionssättet för enheter som önskar bedriva dataaltruism i enlighet med nationell rätt och bygger på krav i nationell rätt för bedrivande av laglig verksamhet i en medlemsstat som icke-vinstdrivande organisation.

(49) Denna förordning bör inte påverka inrättandet av, organisationen av eller funktionssättet för andra enheter än offentliga myndigheter som bedriver delning av data och innehåll på grundval av öppna licenser och därmed bidrar till att skapa gemensamma resurser som är tillgängliga för alla. Detta bör inbegripa öppna samarbetsplattformar för kunskapsdelning, vetenskapliga och akademiska databaser med öppen åtkomst, plattformar för programvaruutveckling med öppen källkod och plattformar för sammanställning av innehåll med öppen åtkomst.

(50) Erkända dataaltruismorganisationer bör kunna samla in relevanta data direkt från fysiska och juridiska personer eller behandla data som samlats in av andra. Dataaltruismorganisationer skulle kunna behandla insamlade data för ändamål som de själva fastställer, eller så skulle de, i förekommande fall, kunna tillåta tredjeparter att utföra behandlingen för dessa ändamål. I de fall då erkända dataaltruismorganisationer är personuppgiftsansvariga eller personuppgiftsbiträden enligt definitionerna i förordning (EU) 2016/679 är de bundna av bestämmelserna i den förordningen. Generellt skulle dataaltruism bygga på de registrerades samtycke i den mening som avses i artiklarna 6.1 a och 9.2 a i förordning (EU) 2016/679 vilket bör uppfylla kraven för lagligt samtycke i enlighet med artiklarna 7 och 8 i den förordningen. I enlighet med förordning (EU) 2016/679 skulle ändamål som rör vetenskaplig forskning kunna stödjas genom samtycke till vissa forskningsområden så länge som de är förenliga med allmänt erkända etiska normer för vetenskaplig forskning eller till vissa forskningsområden eller delar av forskningsprojekt. I artikel 5.1 b i förordning (EU) 2016/679 fastställs att ytterligare behandling för vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1 i förordning (EU) 2016/679 inte ska anses vara oförenlig med de ursprungliga ändamålen. Nyttjandebegränsningarna för icke-personuppgifter bör återfinnas i det tillstånd som ges av datainnehavaren.

(51) De behöriga myndigheter för registrering av dataaltruismorganisationer som utses för att övervaka erkända dataaltruismorganisationers uppfyllande av kraven i denna förordning bör väljas på grundval av sin kapacitet och sakkunskap. De bör vara oberoende av alla dataaltruismorganisationer samt transparenta och opartiska i utförandet av sina arbetsuppgifter. Medlemsstaterna bör meddela kommissionen dessa behöriga myndigheter för registrering av dataaltruismorganisationers identitet. De behöriga myndigheterna för registrering av dataaltruismorganisationers behörighet och befogenheter bör inte påverka dataskyddsmyndigheternas befogenheter. I synnerhet i alla frågor som rör en bedömning av efterlevnaden av förordning (EU) 2016/679 bör den behöriga myndigheten för registrering av dataaltruismorganisationer, i tillämpliga fall, efterfråga ett yttrande eller beslut av den behöriga tillsynsmyndighet som inrättats i enlighet med den förordningen.

(52) För att främja förtroendet och få till stånd ökad rättssäkerhet och användarvänlighet vad gäller förfarandet för beviljande och tillbakadragande av samtycke, i synnerhet i samband med vetenskaplig forskning och statistisk användning av data som tillhandahålls baserat på altruism, bör ett europeiskt formulär för dataaltruism utarbetas och användas i samband med altruistisk datadelning. Ett sådant formulär bör för de registrerade bidra till ytterligare transparens om att tillgången till och användningen av deras data kommer att ske i enlighet med deras samtycke och även i full överensstämmelse med dataskyddsbestämmelserna. Formuläret bör också göra det lättare att bevilja och dra tillbaka samtycke och kunna användas för att rationalisera företagens dataaltruism och tillhandahålla en mekanism som tillåter sådana företag att dra tillbaka sitt samtycke till användningen av data. För att ta hänsyn till de enskilda sektorernas särdrag, även ur ett dataskyddsperspektiv, bör det europeiska formuläret för samtycke till dataaltruism baseras på moduler, så att det kan anpassas till enskilda sektorer och olika syften.

(53) För att genomförandet av dataförvaltningsramen ska bli framgångsrikt bör en europeisk datainnovationsstyrelse inrättas, i form av en expertgrupp. Europeiska datainnovationsstyrelsen bör bestå av företrädare för alla medlemsstaters behöriga myndigheter för dataförmedlingstjänster och behöriga myndigheter för registrering av dataaltruismorganisationer, Europeiska dataskyddsstyrelsen, Europeiska datatillsynsmannen, Europeiska unionens cybersäkerhetsbyrå (Enisa), kommissionen, EU-företrädaren för små och medelstora företag eller en företrädare utsedd av nätverket av företrädare för små och medelstora företag och andra företrädare för relevanta organ inom enskilda sektorer samt organ med specifik sakkunskap. Europeiska datainnovationsstyrelsen bör bestå av ett antal undergrupper, inbegripet en undergrupp för deltagande av berörda parter bestående av relevanta företrädare för näringslivet, såsom hälsa, miljö, jordbruk, transport, energi, industriell tillverkning, medier, kulturella och kreativa sektorer och statistik, samt för forskningsvärlden, den akademiska världen, civilsamhället, standardiseringsorganisationer, berörda gemensamma europeiska dataområden och andra berörda intressenter och tredje parter, bland annat organ med specifik sakkunskap såsom nationella statistikbyråer.

(54) Europeiska datainnovationsstyrelsen bör bistå kommissionen i samordningen av nationella arbetsmetoder och strategier på de områden som omfattas av denna förordning och stödjandet av sektorsövergripande dataanvändning genom iakttagande av principerna i den europeiska interoperabilitetsramen och genom användning av europeiska och internationella standarder och specifikationer (inklusive genom EU:s flerpartsforum för IKT-standardisering, basvokabulären och byggstenarna inom Fonden för ett sammanlänkat Europa), och bör beakta det standardiseringsarbete som bedrivs inom enskilda sektorer eller områden. Arbetet med teknisk standardisering skulle kunna innefatta fastställandet av prioriteringar för utvecklingen av standarder och fastställandet och upprätthållandet av ett antal tekniska och rättsliga standarder för överföring av data mellan två behandlingsmiljöer som gör det möjligt att organisera dataområden, framför allt för att klarlägga och särskilja vilka standarder och praxisformer som är sektorsöverskridande och vilka som är sektorsspecifika. Europeiska datainnovationsstyrelsen bör samarbeta med sektorsorgan, nätverk eller expertgrupper och andra sektorsövergripande organisationer som hanterar vidareutnyttjandet av data. När det gäller dataaltruism bör Europeiska datainnovationsstyrelsen bistå kommissionen i utarbetandet av formuläret för dataaltruism, efter samråd med Europeiska dataskyddsstyrelsen. Genom att föreslå riktlinjer för gemensamma europeiska dataområden bör Europeiska datainnovationsstyrelsen stödja utvecklingen av en fungerande europeisk dataekonomi på grundval av dessa dataområden, i enlighet med den europeiska datastrategin.

(55) Medlemsstaterna bör fastställa regler om tillämpliga sanktioner vid överträdelse av denna förordning och bör vidta alla nödvändiga åtgärder för att säkerställa att de tillämpas. De sanktioner som föreskrivs bör vara effektiva, proportionella och avskräckande. Stora skillnader mellan sanktionsreglerna skulle kunna snedvrida konkurrensen på den digitala inre marknaden. I det avseendet skulle det vara fördelaktigt med en harmonisering av dessa regler.

(56) För att säkerställa en effektiv efterlevnad av denna förordning och se till att leverantörer av dataförmedlingstjänster och enheter som vill registrera sig som erkända dataaltruismorganisationer kan få tillgång till och genomföra förfarandena för anmälan och registrering helt online och över gränserna, bör sådana förfaranden erbjudas genom den gemensamma digitala ingång som inrättas i enlighet med Europaparlamentets och rådets förordning (EU) 2018/1724 ([29]). Dessa förfaranden bör läggas till i förteckningen över förfaranden i bilaga II till förordning (EU) 2018/1724.

(57) Förordning (EU) 2018/1724 bör därför ändras i enlighet med detta.

([29]) Europaparlamentets och rådets förordning (EU) 2018/1724 av den 2 oktober 2018 om inrättande av en gemensam digital ingång för tillhandahållande av information, förfaranden samt hjälp- och problemlösningstjänster och om ändring av förordning (EU) nr 1024/2012 (EUT L 295, 21.11.2018, s. 1).

(58) I syfte att säkerställa denna förordnings ändamålsenlighet, bör befogenheten att anta akter i enlighet med artikel 290 i EUF-fördraget delegeras till kommissionen med avseende på att komplettera denna förordning genom att fastställa särskilda villkor som är tillämpliga på överföring till tredjeländer av vissa kategorier av icke-personuppgifter som anses vara mycket känsliga i särskilda unionslagstiftningsakter och genom att ta fram en regelbok för erkända dataaltruismorganisationer, som dessa organisationer ska följa och som föreskriver informationskrav, tekniska krav och säkerhetskrav samt färdplaner för kommunikation och interoperabilitetsstandarder. Det är särskilt viktigt att kommissionen genomför lämpliga samråd under sitt förberedande arbete, inklusive på expertnivå, och att dessa samråd genomförs i enlighet med principerna i det interinstitutionella avtalet av den 13 april 2016 om bättre lagstiftning ([30]). För att säkerställa lika stor delaktighet i förberedelsen av delegerade akter erhåller Europaparlamentet och rådet alla handlingar samtidigt som medlemsstaternas experter, och deras experter ges systematiskt tillträde till möten i kommissionens expertgrupper som arbetar med förberedelse av delegerade akter.

(59) För att säkerställa enhetliga villkor för tillämpningen av denna förordning bör kommissionen tilldelas genomförandebefogenheter för att bistå offentliga myndigheter och vidareutnyttjare med deras efterlevnad av de villkor för vidareutnyttjande som fastställs i denna förordning genom att fastställa standardavtalsklausuler för vidareutnyttjares överföring av icke-personuppgifter till ett tredjeland, intyga att ett tredjelands rättsliga, tillsynsmässiga och verkställighetsmässiga arrangemang är likvärdiga med det skydd som säkerställs genom unionsrätten, utforma den gemensamma logotypen för leverantörer av dataförmedlingstjänster och den gemensamma logotypen för erkända dataaltruismorganisationer samt utarbeta och utveckla det europeiska formuläret för samtycke till dataaltruism. Dessa befogenheter bör utövas i enlighet med Europaparlamentets och rådets förordning (EU) nr 182/2011 ([31]).

(60) Denna förordning bör inte påverka tillämpningen av konkurrensreglerna, särskilt artiklarna 101 och 102 i EUF-fördraget. De åtgärder som föreskrivs i denna förordning bör inte användas för att begränsa konkurrensen på ett sätt som strider mot EUF-fördraget. Detta gäller i synnerhet reglerna om utbyte av information som är känslig i konkurrenshänseende mellan faktiska och potentiella konkurrenter via dataförmedlingstjänster.

(61) Samråd har skett med Europeiska datatillsynsmannen och Europeiska dataskyddsstyrelsen i enlighet med artikel 42.1 i förordning (EU) 2018/1725 som avgav sitt yttrande den 10 mars 2021.

(62) De vägledande principerna för denna förordning är respekten för de grundläggande rättigheterna och de principer som erkänns främst genom Europeiska unionens stadga om de grundläggande rättigheterna, inklusive rätten till privatliv, skyddet av personuppgifter, näringsfriheten, rätten till egendom och integreringen av personer med funktionsnedsättning. När det gäller det sistnämnda bör offentliga myndigheter och tjänster inom ramen för denna förordning, i förekommande fall, uppfylla kraven i Europaparlamentets och rådets direktiv (EU) 2016/2102 ([32]) och (EU) 2019/882 ([33]). Vidare bör hänsyn tas till design för alla i samband med informations- och kommunikationsteknik, som är ett medvetet och systematiskt försök att aktivt tillämpa principer, metoder och verktyg för att främja universell design inom datorrelaterad teknik, däribland internetbaserad teknik, och därigenom undvika behovet av anpassningar i efterhand eller specialiserad design.

(63) Eftersom målen för denna förordning, nämligen vidareutnyttjande inom unionen av vissa kategorier av data som innehas av offentliga myndigheter samt inrättandet av en ram för anmälan av och tillsyn över tillhandahållandet av datadelningstjänster, en ram för frivillig registrering av enheter som samlar in och behandlar data som tillhandahålls för altruistiska ändamål och en ram för inrättandet av en europeisk datainnovationsstyrelse, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna utan snarare, på grund av deras omfattning och verkningar, kan uppnås bättre på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen. I enlighet med proportionalitetsprincipen i samma artikel går denna förordning inte utöver vad som är nödvändigt för att uppnå dessa mål.

([30]) EUT L 123, 12.5.2016, s. 1.

([31]) Europaparlamentets och rådets förordning (EU) nr 182/2011 av den 16 februari 2011 om fastställande av allmänna regler och principer för medlemsstaternas kontroll av kommissionens utövande av sina genomförandebefogenheter (EUT L 55, 28.2.2011, s. 13).

([32]) Europaparlamentets och rådets direktiv (EU) 2016/2102 av den 26 oktober 2016 om tillgänglighet avseende offentliga myndigheters webbplatser och mobila applikationer (EUT L 327, 2.12.2016, s. 1).

([33]) Europaparlamentets och rådets direktiv (EU) 2019/882 av den 17 april 2019 om tillgänglighetskrav för produkter och tjänster (EUT L 151, 7.6.2019, s. 70).

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I

Allmänna bestämmelser

Artikel 1

Innehåll och tillämpningsområde

1. I denna förordning fastställs följande:

a) Villkoren för vidareutnyttjande inom unionen av vissa kategorier av data som innehas av offentliga myndigheter.

b) En ram för anmälan av och tillsyn över tillhandahållandet av dataförmedlingstjänster.

c) En ram för frivillig registrering av enheter som samlar in och behandlar data som tillhandahålls för altruistiska ändamål.

d) En ram för inrättandet av en europeisk datainnovationsstyrelse.

2. Denna förordning medför inte någon skyldighet för offentliga myndigheter att tillåta vidareutnyttjande av data och befriar inte heller offentliga myndigheter från deras skyldigheter i fråga om konfidentiell behandling enligt unionsrätten eller nationell rätt.

Denna förordning ska inte påverka

a) tillämpningen av särskilda bestämmelser i unionsrätten eller nationell rätt om tillgång till eller vidareutnyttjande av vissa kategorier av data, särskilt när det gäller beviljandet av tillgång till och utlämnandet av officiella handlingar, och

b) offentliga myndigheters skyldigheter enligt unionsrätten eller nationell rätt att tillåta vidareutnyttjande av data eller krav som rör behandling av icke-personuppgifter.

I de fall då en sektorsspecifik unionsrätt eller nationell rätt föreskriver att offentliga myndigheter, leverantörer av dataförmedlingstjänster eller erkända dataaltruismorganisationer ska uppfylla särskilda ytterligare tekniska, administrativa eller organisatoriska krav, däribland genom ett auktorisations- eller certifieringssystem, ska de bestämmelserna i den sektorsspecifika unionsrätten eller den nationella rätten också tillämpas. Eventuella sådana särskilda ytterligare krav ska vara icke-diskriminerande, proportionella och objektivt motiverade.

3. Unionsrätt och nationell rätt om skydd av personuppgifter ska tillämpas på alla personuppgifter som behandlas i samband med denna förordning. Denna förordning påverkar i synnerhet inte tillämpningen av förordningarna (EU) 2016/679 och (EU) 2018/1725 och direktiven 2002/58/EG och (EU) 2016/680, inklusive vad gäller tillsynsmyndigheternas befogenheter och behörighet. Om den här förordningen står i strid med unionsrätten om skydd av personuppgifter eller nationell rätt som antagits i enlighet med sådan unionsrätt, bör den relevanta unionsrätten eller nationella rätten om skydd av personuppgifter ha företräde. Den här förordningen skapar inte någon rättslig grund för behandling av personuppgifter och påverkar inte heller några av de skyldigheter och rättigheter som anges i förordningarna (EU) 2016/679 eller (EU) 2018/1725 eller direktiven 2002/58/EG eller (EU) 2016/680.

4. Denna förordning påverkar inte tillämpningen av konkurrensrätten.

5. Denna förordning påverkar inte medlemsstaternas befogenheter när det gäller deras verksamhet som rör allmän säkerhet, försvar och nationell säkerhet.

Artikel 2

Definitioner

I denna förordning gäller följande definitioner:

1. *data*: varje digital återgivning av handlingar, fakta eller information och varje sammanställning av sådana handlingar, sådana fakta eller sådan information, däribland i form av ljudinspelningar, bildinspelningar eller audiovisuella inspelningar).

2. *vidareutnyttjande*: fysiska eller juridiska personers användning av data som innehas av offentliga myndigheter för andra kommersiella eller icke-kommersiella ändamål än det ursprungliga ändamål inom den offentliga verksamheten för vilket de framställdes, med undantag för utbyte av data mellan offentliga myndigheter som enbart sker i samband med deras offentliga verksamhet.

3. *personuppgifter*: personuppgifter enligt definitionen i artikel 4.1 i förordning (EU) 2016/679.

4. *icke-personuppgifter*: andra data än personuppgifter.

5. *samtycke*: samtycke enligt definitionen i artikel 4.11 i förordning (EU) 2016/679.

6. *tillstånd*: att ge dataanvändare rätt att behandla icke-personuppgifter.

7. *registrerad*: registrerad som avses i artikel 4.1 i förordning (EU) 2016/679.

8. *datainnehavare*: en juridisk person, inklusive en offentlig myndighet och internationella organisationer, eller en fysisk person som inte är en registrerad i förhållande till de specifika uppgifterna i fråga, som i enlighet med tillämplig unionsrätt eller nationell rätt har rätt att bevilja tillgång till eller dela vissa personuppgifter eller icke-personuppgifter.

9. *dataanvändare*: fysisk eller juridisk person som har laglig tillgång till vissa personuppgifter eller icke-personuppgifter och som har rätt att, även enligt förordning (EU) 2016/679 när det gäller personuppgifter, använda dessa data för kommersiella eller icke-kommersiella ändamål.

10. *datadelning*: en registrerads eller datainnehavares tillhandahållande av data till en dataanvändare för gemensam eller individuell användning av dessa delade data, baserat på frivilliga avtal, unionsrätt eller nationell rätt, direkt eller via en förmedlare, till exempel inom ramen för öppna eller kommersiella licenser mot en avgift eller kostnadsfritt.

11. *dataförmedlingstjänst*: en tjänst som syftar till att med tekniska, rättsliga eller andra medel upprätta affärsförbindelser för datadelning mellan ett obestämt antal registrerade och datainnehavare, å ena sidan, och dataanvändare, å andra sidan, inbegripet för att utöva de registrerades rättigheter avseende personuppgifter, med uteslutande av åtminstone följande:

    a) Tjänster som erhåller data från datainnehavare och aggregerar, berikar eller omvandlar data i syfte att avsevärt öka deras värde och licensierar användningen av resulterande data till dataanvändare, utan att upprätta en affärsförbindelse mellan datainnehavare och dataanvändare.

    b) Tjänster som är inriktade på förmedling av upphovsrättsligt skyddat innehåll.

    c) Tjänster som uteslutande används av en datainnehavare för att möjliggöra användning av de data som den datainnehavaren innehar, eller som används av flera juridiska personer en sluten grupp, inbegripet leverantörs- eller kundrelationer eller samarbeten som grundar sig på avtal, särskilt sådana som har som huvudsakligt syfte att säkerställa funktionerna för föremål och enheter som är anslutna till sakernas internet.

    d) Datadelningstjänster som erbjuds av offentliga myndigheter som inte syftar till att upprätta affärsförbindelser.

12. *behandling*: behandling enligt definitionen i artikel 4.2 i förordning (EU) 2016/679 när det gäller personuppgifter eller artikel 3.2 i förordning (EU) 2018/1807 när det gäller icke-personuppgifter.

13. *tillgång*: dataanvändning i enlighet med särskilda tekniska, rättsliga eller organisatoriska krav, utan att det nödvändigtvis innefattar överföring eller nedladdning av data.

14. *huvudsakligt verksamhetsställe* för en juridisk person: platsen för dess centrala förvaltning i unionen.

15. *datakooperativs tjänster*: dataförmedlingstjänster som tillhandahålls av en organisationsstruktur i vilken registrerade, enmansföretag eller små och medelstora företag är medlemmar, och vars huvudsakliga syften är att hjälpa medlemmarna att utöva sina rättigheter avseende vissa data, så att de bland annat kan fatta välgrundade beslut innan de samtycker till databehandling, att utbyta synpunkter om de ändamål och villkor för databehandling som bäst företräder sina medlemmars intressen när det gäller deras data och att förhandla om villkoren för databehandling för sina medlemmar innan de ger tillstånd till behandling av icke-personuppgifter eller lämnar sitt samtycke till behandling av personuppgifter.

16. *dataaltruism*: den frivilliga delningen av data på grundval av de registrerades samtycke till behandling av personuppgifter som rör dem, eller tillstånd från datainnehavare att tillåta användning av deras icke-personuppgifter utan något krav på eller mottagande av ersättning utöver ersättning för de kostnader som de ådragit sig när de gör uppgifterna tillgängliga för mål av allmänintresse, som det föreskrivs i nationell rätt i förekommande fall, såsom hälso- och sjukvård, bekämpande av klimatförändringar, förbättring av mobiliteten, främjande av utveckling, framställning och spridning av officiell statistik, förbättrat tillhandahållande av offentliga tjänster, politiskt beslutsfattande eller vetenskaplig forskning av allmänt intresse.

17. *offentliga myndigheter*: statliga, regionala eller lokala myndigheter och offentligrättsliga organ, eller sammanslutningar av en eller flera sådana myndigheter eller av ett eller flera sådana offentligrättsliga organ.

18. *offentligrättsliga organ*: organ som har följande egenskaper:

    a) De har särskilt inrättats för att tillgodose behov av allmänt intresse, och är inte av industriell eller kommersiell art.

    b) De är juridiska personer.

    c) De finansieras till största delen av statliga, regionala eller lokala myndigheter, eller andra offentligrättsliga organ, står under administrativ tillsyn av sådana myndigheter eller organ, eller har ett förvaltnings-, lednings- eller kontrollorgan där mer än hälften av ledamöterna utses av staten, av regionala eller lokala myndigheter eller av andra offentligrättsliga organ.

19. *offentligt företag*: varje företag över vilket de offentliga myndigheterna har ett direkt eller indirekt bestämmande inflytande till följd av ägarförhållande, finansiellt deltagande eller gällande regler; inom ramen för denna definition ska offentliga myndigheter anses utöva bestämmande inflytande när dessa myndigheter, direkt eller indirekt,

    a) äger större delen av det tecknade kapitalet i företaget,

    b) kontrollerar majoriteten av de rösträtter som är knutna till företagets emitterade aktier,

    c) kan utse fler än hälften av ledamöterna i företagets förvaltningsorgan, styrelseorgan eller övervakande organ.

20. *säker behandlingsmiljö*: fysisk eller virtuell miljö och organisatoriska metoder för att säkerställa överensstämmelse med unionsrätten, såsom förordning (EU) 2016/679, särskilt vad gäller de registrerades rättigheter, immateriella rättigheter samt insynsskydd, integritet och tillgänglighet för kommersiella och statistiska uppgifter, samt med tillämplig nationell rätt, och göra det möjligt för den enhet som tillhandahåller den säkra behandlingsmiljön att fastställa och övervaka alla databehandlingsåtgärder, inbegripet förevisandet, lagringen, nedladdningen och exporten av data och beräkningen av härledda data med hjälp av dataalgoritmer.

21. *rättslig företrädare*: en fysisk eller juridisk person etablerad i unionen som uttryckligen utsetts för att agera på uppdrag av en i unionen ej etablerad leverantör av dataförmedlingstjänster eller i unionen ej etablerad enhet som för syften av allmänt intresse samlar in data som tillhandahålls av fysiska eller juridiska personer baserat på dataaltruism, till vilken de behöriga myndigheterna för dataförmedlingstjänster och de behöriga myndigheterna för registrering av dataaltruismorganisationer kan vända sig till utöver eller i stället för leverantören av dataförmedlingstjänster eller enheten när det gäller skyldigheterna enligt denna förordning, inklusive när det gäller att inleda verkställighetsförfaranden mot en leverantör av dataförmedlingstjänster eller enhet som inte uppfyller kraven och som inte är etablerad i unionen.

KAPITEL II

Vidareutnyttjande av vissa kategorier av skyddade data som innehas av offentliga myndigheter

Artikel 3

Kategorier av data

1. Detta kapitel ska tillämpas på data som innehas av offentliga myndigheter och som är skyddade på grund av

a) insynsskydd för kommersiella uppgifter, inklusive affärs-, yrkes- och företagshemligheter,

b) insynsskydd för statistiska uppgifter,

c) skydd av tredje parts immateriella rättigheter, eller

d) skydd av personuppgifter, i den mån sådana uppgifter faller utanför tillämpningsområdet för direktiv (EU) 2019/1024.

2. Detta kapitel ska inte tillämpas på

a) data som innehas av offentliga företag,

b) data som innehas av public service-bolag och deras dotterbolag och av andra organ eller deras dotterbolag för fullgörandet av ett uppdrag att verka i allmänhetens tjänst på radio- eller tv-området,

c) data som innehas av kulturinstitutioner och utbildningsinstitutioner,

d) data som innehas av offentliga myndigheter och är skyddade av skäl som rör allmän säkerhet, försvar eller nationell säkerhet, eller

e) data vars tillhandahållande inte omfattas av den offentliga verksamhet som bedrivs av de berörda offentliga myndigheterna, såsom den definieras i lagstiftning eller andra bindande regler i den berörda medlemsstaten eller, om sådana regler saknas, såsom den definieras i enlighet med gängse administrativ praxis i denna, förutsatt att den offentliga verksamheten är tydligt avgränsad och föremål för översyn.

3. Detta kapitel påverkar inte tillämpningen av

a) unionsrätten, nationell rätt och internationella avtal som unionen eller medlemsstaterna är parter i och som avser skydd av de kategorier av data som avses i punkt 1, och

b) unionsrätt och nationell rätt om tillgång till handlingar.

Artikel 4

Förbud mot exklusiva avtal

1. Det ska vara förbjudet med avtal eller annan praxis som rör vidareutnyttjande av data som innehas av offentliga myndigheter och som omfattar kategorier av data som avses i artikel 3.1, vilka omfattar beviljande av exklusiva rättigheter eller vars syfte eller verkan omfattar beviljande av sådana exklusiva rättigheter eller begränsning av tillgången till data för vidareutnyttjande av andra enheter än parterna i sådana avtal eller sådan annan praxis.

2. Med avvikelse från punkt 1 får en exklusiv rättighet beviljas för vidareutnyttjande av data som avses i den punkten i den mån som det är nödvändigt för tillhandahållande av en tjänst eller tillhandahållande av en produkt av allmänt intresse som annars inte skulle vara möjligt.

3. En exklusiv rättighet som avses i punkt 2 ska beviljas genom en administrativ åtgärd eller ett kontraktsmässigt arrangemang i enlighet med tillämplig unionsrätt eller nationell rätt och i enlighet med principerna om transparens, likabehandling och icke-diskriminering.

4. Perioden för en exklusiv rättighet till vidareutnyttjande av data får inte överstiga tolv månader. När ett avtal har ingåtts ska avtalets löptid vara samma som perioden för den exklusiva rättigheten.

5. Beviljandet av en exklusiv rättighet i enlighet med punkterna 2, 3 och 4, inklusive skälen till varför detta beviljande är nödvändigt, ska vara transparenta och göras allmänt tillgängliga online i en form som är förenlig med relevant unionslagsrätt om offentlig upphandling.

6. Avtal eller andra metoder som omfattas av tillämpningsområdet för det förbud som avses i punkt 1, som inte uppfyller de villkor som fastställs i punkterna 2 och 3 och som ingicks före den 23 juni 2022 ska upphöra att gälla när det tillämpliga avtalet löper ut och i vilket fall senast den 24 december 2024.

Artikel 5

Villkor för vidareutnyttjande

1. Offentliga myndigheter som enligt nationell rätt är behöriga att bevilja eller vägra tillgång till vidareutnyttjandet av en eller flera kategorier av data som avses i artikel 3.1 ska offentliggöra villkoren för att tillåta sådant vidareutnyttjande samt förfarandet för att begära vidareutnyttjandet via den gemensamma informationspunkt som avses i artikel 8. När de beviljar eller vägrar tillgång till vidareutnyttjande får de bistås av de behöriga organ som avses i artikel 7.1.

Medlemsstaterna ska säkerställa att offentliga myndigheter är försedda med nödvändiga resurser för att efterleva denna artikel.

2. Villkoren för vidareutnyttjande ska vara icke-diskriminerande, transparenta, proportionerliga och objektivt motiverade med hänsyn till kategorierna av data, vidareutnyttjandets syfte och typerna av data för vilka vidareutnyttjande tillåts. Dessa villkor får inte användas för att begränsa konkurrensen.

3. Offentliga myndigheter ska i enlighet med unionsrätt och nationell rätt säkerställa att uppgifternas skyddade karaktär bevaras. De kan föreskriva följande krav:

a) Att tillgång till vidareutnyttjande av data beviljas endast om den offentliga myndigheten eller det behöriga organet efter begäran om vidareutnyttjande har säkerställt att data har

   i) anonymiserats, när det gäller personuppgifter, och

   ii) ändrats, aggregerats eller behandlats med någon annan metod för kontroll av utlämnande, när det gäller affärshemligheter, inbegripet företagshemligheter eller innehåll som skyddas av immateriella rättigheter.

b) Att tillgång till och vidareutnyttjande av data på distans sker inom en säker behandlingsmiljö som tillhandahålls eller kontrolleras av den offentliga myndigheten.

c) Att tillgång till och vidareutnyttjande av data säkerställs i de fysiska lokaler där den säkra behandlingsmiljön är belägen i enlighet med höga säkerhetsnormer, förutsatt att fjärråtkomst inte kan tillåtas utan att tredje parters rättigheter och intressen hotas.

4. Om vidareutnyttjande har tillåtits i enlighet med punkt 3 b och c, ska offentliga myndigheter införa villkor som bevarar integriteten för de tekniska systemens funktionssätt i den säkra behandlingsmiljön. Offentliga myndigheter ska förbehålla sig rätten att verifiera processen, metoderna och alla resultat från den behandling av data som görs av vidareutnyttjaren för att bevara integriteten i dataskyddet och förbehålla sig rätten att förbjuda användningen av resultat som innehåller information som hotar tredje parters rättigheter och intressen. Beslutet att förbjuda användningen av resultat ska vara lättbegripligt och tydligt för vidareutnyttjaren.

5. Såvida det i den nationella rätten inte föreskrivs särskilda skyddsåtgärder för tillämpliga skyldigheter i fråga om konfidentiell behandling avseende det vidareutnyttjande av data som avses i artikel 3.1, ska den offentliga myndigheten ställa som villkor för vidareutnyttjandet av data som tillhandahålls i enlighet med punkt 3 i den här artikeln att vidareutnyttjaren uppfyller en skyldighet i fråga om konfidentiell behandling som förbjuder utlämnande av information som äventyrar tredje parts rättigheter och intressen som vidareutnyttjaren kan ha erhållit trots de skyddsåtgärder som införts. Det ska vara förbjudet för vidareutnyttjare att återidentifiera de registrerade som uppgifterna gäller, och vidareutnyttjarna ska vidta tekniska och operativa åtgärder för att förhindra återidentifiering och underrätta den offentliga myndigheten om alla uppgiftsincidenter som leder till att berörda registrerade återidentifieras. Vid otillåtet vidareutnyttjande av icke-personuppgifter ska vidareutnyttjaren utan dröjsmål, och när så är lämpligt med bistånd från den offentliga myndigheten, underrätta de juridiska personer vars rättigheter och intressen kan påverkas.

6. I de fall då vidareutnyttjande av data inte kan tillåtas i enlighet med de skyldigheter som fastställs i punkterna 3 och 4 i denna artikel, och det inte finns någon rättslig grund för överföring av data inom ramen för förordning (EU) 2016/679, ska den offentliga myndigheten, i den utsträckning det är tillåtet i enlighet med unionsrätten och nationell rätt, göra sitt yttersta för att bistå potentiella vidareutnyttjare som begär de registrerades samtycke eller tillstånd från datainnehavare vars rättigheter och intressen kan påverkas av ett sådant vidareutnyttjande, om detta är möjligt utan en oproportionell börda för den offentliga myndigheten. När den tillhandahåller sådant bistånd får den offentliga myndigheten bistås av de behöriga organ som avses i artikel 7.1.

7. Vidareutnyttjande av data ska endast tillåtas i enlighet med immateriella rättigheter. En databasproducents rätt som föreskrivs i artikel 7.1 i direktiv 96/9/EG får inte utövas av offentliga myndigheter för att förhindra vidareutnyttjande av data eller begränsa vidareutnyttjandet i högre grad än vad som anges i den här förordningen.

8. Om data som begärs anses vara konfidentiella i enlighet med unionsrätten eller nationell rätt om affärshemligheter eller insynsskydd för statistiska uppgifter, ska de offentliga myndigheterna säkerställa att dessa konfidentiella data inte röjs till följd av att vidareutnyttjande tillåts, såvida inte sådant vidareutnyttjande är tillåtet i enlighet med punkt 6.

9. I de fall då en vidareutnyttjare avser att överföra icke-personuppgifter som är skyddade på grund av de skäl som anges i artikel 3.1 till ett tredjeland, ska vidareutnyttjaren underrätta den offentliga myndigheten om sin avsikt att överföra sådana uppgifter och om syftet med en sådan överföring vid tidpunkten för begäran om vidareutnyttjande av dessa data. Vid vidareutnyttjande i enlighet med punkt 6 i den här artikeln, ska vidareutnyttjaren, när så är lämpligt med bistånd från den offentliga myndigheten, underrätta den juridiska person vars rättigheter och intressen kan påverkas av denna avsikt, om detta syfte och de lämpliga skyddsåtgärderna. Den offentliga myndigheten får inte tillåta vidareutnyttjandet om inte den juridiska personen ger sitt tillstånd till överföringen.

10. Offentliga myndigheter får överföra konfidentiella data som inte är personuppgifter eller data som skyddas av immateriella rättigheter till en vidareutnyttjare som avser att överföra dessa data till ett annat tredjeland än ett land som utsetts i enlighet med punkt 12 endast om vidareutnyttjaren avtalsmässigt åtar sig att

a) fullgöra de skyldigheter som införts i enlighet med punkterna 7 och 8 även efter att data överförts till det berörda tredjelandet, och

b) godta jurisdiktionen för domstolarna i den överförande offentliga myndighetens medlemsstat när det gäller eventuella tvister som rör efterlevnaden av punkterna 7 och 8.

11. Offentliga myndigheter ska, när så är lämpligt och i den utsträckning de kan, ge vidareutnyttjare vägledning och bistånd i fullgörandet av de skyldigheter som avses i punkt 10 i denna artikel.

För att bistå de offentliga myndigheterna och vidareutnyttjarna får kommissionen anta genomförandeakter som fastställer standardavtalsklausuler för fullgörande av de skyldigheter som avses i punkt 10 i denna artikel. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 33.3.

12. När så motiveras på grund av ett betydande antal begäranden i hela unionen om vidareutnyttjandet av icke-personuppgifter i specifika tredjeländer får kommissionen anta genomförandeakter i vilka det intygas att ett tredjelands rättsliga, tillsynsmässiga och verkställighetsmässiga arrangemang

a) säkerställer ett skydd för immateriella rättigheter och företagshemligheter som i allt väsentligt är likvärdigt med det skydd som säkerställs genom unionsrätten,

b) tillämpas och verkställs på ett effektivt sätt, och

c) omfattar effektiva rättsmedel.

Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 33.3.

13. Enligt särskilda unionslagstiftningsakter kan vissa kategorier av icke-personuppgifter som innehas av offentliga myndigheter anses vara mycket känsliga vid tillämpningen av denna artikel, när överföringen av dem till tredjeländer kan äventyra unionens offentligpolitiska mål, exempelvis säkerhet och folkhälsa, eller leda till risk för återidentifiering av anonymiserade data som inte är personuppgifter. Om en sådan akt antas ska kommissionen anta delegerade akter i enlighet med artikel 32 som kompletterar denna förordning genom att fastställa särskilda villkor som ska tillämpas på överföring av sådana uppgifter till tredjeländer.

Dessa särskilda villkor ska baseras på typen av de kategorier av icke-personuppgifter som anges i den särskilda unionslagstiftningsakten och skälen för att anse dessa kategorier vara mycket känsliga, med beaktande av riskerna för återidentifiering av anonymiserade data som inte är personuppgifter. De ska vara icke-diskriminerande och begränsade till vad som är nödvändigt för att uppnå de unionens offentligpolitiska mål som anges i den akten, i enlighet med unionens internationella skyldigheter.

Om så krävs enligt de särskilda unionslagstiftningsakter som avses i första stycket, kan sådana särskilda villkor innefatta villkor som är tillämpliga på överföring eller tekniska avtal i detta hänseende, begränsningar vad gäller vidareutnyttjande av data i tredjeländer eller kategorier av personer som har rätt att överföra sådana data till tredjeländer eller, i exceptionella fall, begränsningar vad gäller överföring till tredjeländer.

14. De fysiska eller juridiska personer som beviljades rätten att vidareutnyttja icke-personuppgifter får endast överföra dessa data till de tredjeländer för vilka kraven i punkterna 10, 12 och 13 uppfylls.

Artikel 6

Avgifter

1. Offentliga myndigheter som tillåter vidareutnyttjande av de kategorier av data som avses i artikel 3.1 får ta ut en avgift för att tillåta vidareutnyttjandet av sådana data.

2. Avgifter som tas ut i enlighet med punkt 1 ska vara transparenta, icke-diskriminerande, proportionella och objektivt motiverade och får inte begränsa konkurrensen.

3. Offentliga myndigheter ska säkerställa att alla avgifter också kan betalas online med hjälp av allmänt tillgängliga gränsöverskridande betalningstjänster, utan diskriminering på grund av betaltjänstleverantörens etableringsort, betalningsinstrumentets utfärdandeort eller den plats där betalkontot finns inom unionen.

4. När offentliga myndigheter tar ut avgifter ska de vidta åtgärder för att ge incitament till vidareutnyttjande av de kategorier av data som avses i artikel 3.1 för icke-kommersiella ändamål, såsom vetenskaplig forskning, och av små och medelstora företag och uppstartsföretag i enlighet med reglerna för statligt stöd. I detta avseende får de offentliga myndigheterna också göra dessa data tillgängliga till en nedsatt avgift eller kostnadsfritt, särskilt för små och medelstora företag och uppstartsföretag, det civila samhället och utbildningsanstalter. Offentliga myndigheter får därför upprätta en förteckning över kategorier av vidareutnyttjare för vilka data för vidareutnyttjande ska göras tillgängliga till en nedsatt avgift eller kostnadsfritt. Förteckningen och kriterierna för upprättande av den ska offentliggöras.

5. Avgifterna ska härledas från kostnaderna för att genomföra förfarandet för begäran om vidareutnyttjande av de kategorier av data som avses i artikel 3.1, och vara begränsade till nödvändiga kostnader i samband med

a) reproduktion, tillhandahållande och spridning av data,

b) klarering av upphovsrätt,

c) anonymisering eller andra former av framställning av personuppgifter och affärshemligheter som föreskrivs i artikel 5.3,

d) underhåll av den säkra behandlingsmiljön,

e) förvärvande av rätten att tillåta vidareutnyttjande i enlighet med detta kapitel av tredje parter utanför den offentliga sektorn, och

f) bistånd till vidareutnyttjare som begär de registrerades samtycke och tillstånd från datainnehavare vars rättigheter och intressen kan påverkas av ett sådant vidareutnyttjande.

6. Kriterierna och metoden för beräkning av avgifter ska fastställas av medlemsstaterna och offentliggöras. Offentliga myndigheter ska offentliggöra en beskrivning av huvudkategorierna av kostnader och reglerna för fördelning av kostnader.

Artikel 7

Behöriga organ

1. För utförandet av de uppgifter som avses i denna artikel ska varje medlemsstat utse ett eller flera behöriga organ, som får vara behöriga för särskilda sektorer, för att bistå de offentliga myndigheter som beviljar eller vägrar tillgång för vidareutnyttjande av de kategorier av data som avses i artikel 3.1. Medlemsstaterna får antingen inrätta ett eller flera nya behöriga organ eller förlita sig på befintliga offentliga myndigheter eller interna avdelningar inom offentliga myndigheter som uppfyller de villkor som fastställs i denna förordning.

2. De behöriga organen får ges befogenhet att bevilja tillgång till vidareutnyttjande av de kategorier av data som avses i artikel 3.1, i enlighet med unionsrätten eller nationell rätt som medger att sådan tillgång beviljas. När de beviljar eller vägrar tillgång för vidareutnyttjande ska artiklarna 4, 5, 6 och 9 tillämpas på dessa behöriga organ.

3. Behöriga organ ska ha tillräckliga juridiska, ekonomiska och tekniska resurser och personalresurser för att utföra de uppgifter som de anförtrotts, inbegripet de nödvändiga tekniska kunskaperna för att kunna följa relevant unionsrätt eller nationell rätt om systemen för tillgång till de kategorier av data som avses i artikel 3.1.

4. Det bistånd som föreskrivs i punkt 1 ska, när så är nödvändigt, innefatta följande:

a) Tekniskt stöd för att tillhandahålla en säker behandlingsmiljö för att ge tillgång till vidareutnyttjande av data.

b) Vägledning och tekniskt stöd om hur data bäst kan struktureras och lagras så att dessa data är lättillgängliga.

c) Tekniskt stöd för pseudonymisering och för att säkerställa databehandling på ett sätt som effektivt bevarar integriteten, konfidentialiteten, dataintegriteten och tillgängligheten för den information som finns i de data för vilka vidareutnyttjande tillåts, däribland teknik för anonymisering, generalisering, undertryckande och randomisering av personuppgifter eller andra toppmoderna integritetsbevarande metoder och radering av kommersiellt känslig information, däribland affärshemligheter eller innehåll som är skyddat av immateriella rättigheter.

d) Bistånd till offentliga myndigheter, i förekommande fall, för att stödja vidareutnyttjare när de begär registrerades samtycke till vidareutnyttjande eller datainnehavares tillstånd i linje med deras särskilda beslut, däribland om den jurisdiktion där databehandlingen är avsedd att utföras, och bistånd till offentliga myndigheter när de behöver inrätta tekniska mekanismer som gör det möjligt att vidarebefordra begäranden om samtycke eller tillstånd från vidareutnyttjare, när detta är praktiskt genomförbart.

e) Bistånd till offentliga myndigheter vid bedömningen av tillräckligheten i de avtalsmässiga åtaganden som görs av en vidareutnyttjare i enlighet med artikel 5.10.

5. Varje medlemsstat ska senast den 24 september 2023 meddela kommissionen vilka behöriga organ som utsetts i enlighet med punkt 1. Varje medlemsstat ska också meddela kommissionen alla senare ändringar av dessa behöriga organs identitet.

Artikel 8

Gemensamma informationspunkter

1. Medlemsstaterna ska säkerställa att all relevant information om tillämpningen av artiklarna 5 och 6 finns tillgänglig och lätt åtkomlig via en gemensam informationspunkt. Medlemsstaterna ska inrätta ett nytt organ eller utse ett befintligt organ som gemensam informationspunkt. Den gemensamma informationspunkten kan vara länkad till sektoriella, regionala eller lokala informationspunkter. En gemensam informationspunkts funktioner får vara automatiserade förutsatt att den offentliga myndigheten säkerställer tillräckligt stöd.

2. Den gemensamma informationspunkten ska vara behörig att ta emot förfrågningar eller ansökningar om vidareutnyttjande av de kategorier av data som avses i artikel 3.1 och ska när så är möjligt och lämpligt automatiskt överföra dessa till de behöriga offentliga myndigheter som avses i artikel 7.1, i förekommande fall. Den gemensamma informationspunkten ska på elektronisk väg tillhandahålla en sökbar tillgångsförteckning som innehåller en översikt över alla tillgängliga datakällor, däribland, i relevanta fall, de datakällor som finns tillgängliga vid sektorsspecifika, regionala och lokala informationspunkter, tillsammans med relevant information som beskriver tillgängliga data, inbegripet åtminstone dataformatet och datastorleken samt villkoren för vidareutnyttjandet av dessa data.

3. Den gemensamma informationspunkten får inrätta en separat, förenklad och väldokumenterad informationskanal för små och medelstora företag och nystartade företag som möter deras behov och förmågor i samband med begäran av vidareutnyttjande av de kategorier av data som avses i artikel 3.1.

4. Kommissionen ska inrätta en europeisk gemensam åtkomstspunkt som erbjuder ett sökbart elektroniskt register över tillgängliga data i nationella gemensamma informationspunkter och ytterligare information om hur man begär data via dessa nationella gemensamma informationspunkter.

Artikel 9

Behandling av begäranden om vidareutnyttjande

1. Såvida inte kortare tidsfrister har fastställts i enlighet med nationell rätt ska de behöriga offentliga myndigheterna eller de behöriga organ som avses i artikel 7.1 anta ett beslut om begäran om vidareutnyttjande av de kategorier av data som avses i artikel 3.1 inom två månader från dagen för mottagandet av begäran.

Vid exceptionellt omfattande och komplicerade begäranden om vidareutnyttjande får denna tvåmånadersperiod förlängas med högst 30 dagar. I sådana fall ska de behöriga offentliga myndigheterna eller de behöriga organ som avses i artikel 7.1 underrätta den sökande så snart som möjligt om att mer tid krävs för att genomföra förfarandet, tillsammans med skälen till dröjsmålet.

2. Fysiska eller juridiska personer som direkt påverkas av ett beslut såsom avses i punkt 1 ska ha effektiv rätt till överprövning i den medlemsstat där det relevanta organet är lokaliserat. Denna rätt till överprövning ska föreskrivas i nationell rätt och inbegripa möjlighet till omprövning av en opartisk myndighet som besitter lämplig sakkunskap, såsom den nationella konkurrensmyndigheten, den berörda myndigheten för tillgång till handlingar, den tillsynsmyndighet som inrättats i enlighet med förordning (EU) 2016/679 eller en nationell rättslig myndighet, vars beslut är bindande för den berörda offentliga myndigheten eller det berörda behöriga organet.

KAPITEL III

Krav som är tillämpliga på dataförmedlingstjänster

Artikel 10

Dataförmedlingstjänster

Tillhandahållandet av följande dataförmedlingstjänster ska uppfylla artikel 12 och ska omfattas av ett anmälningsförfarande:

a) Förmedlingstjänster mellan datainnehavare och potentiella dataanvändare, däribland tillhandahållandet av tekniska eller andra metoder för att möjliggöra sådana tjänster; dessa tjänster kan innefatta bilaterala eller multilaterala utbyten av data eller inrättandet av plattformar eller databaser som möjliggör utbyte eller gemensam användning av data, liksom inrättandet av annan särskild infrastruktur för sammankoppling av datainnehavare med dataanvändare.

b) Förmedlingstjänster mellan de registrerade som önskar göra sina personuppgifter tillgängliga eller fysiska personer som önskar göra icke-personuppgifter tillgängliga, och potentiella dataanvändare, däribland tillhandahållandet av tekniska eller andra metoder för att möjliggöra sådana tjänster, och i synnerhet som möjliggör utövandet av de registrerades rättigheter som föreskrivs i förordning (EU) 2016/679.

c) Datakooperativs tjänster.

Artikel 11

Anmälning från leverantörer av dataförmedlingstjänster

1. Varje leverantör av dataförmedlingstjänster som avser att tillhandahålla de dataförmedlingstjänster som avses i artikel 10 ska lämna en anmälan till den behöriga myndigheten för dataförmedlingstjänster.

2. Vid tillämpning av denna förordning ska en leverantör av dataförmedlingstjänster med verksamhetsställen i mer än en medlemsstat anses omfattas av jurisdiktionen i den medlemsstat där den har sitt huvudsakliga verksamhetsställe, utan att det påverkar unionslagsrätten som reglerar gränsöverskridande skadeståndstalan och tillhörande förfaranden.

3. En leverantör av dataförmedlingstjänster som inte är etablerad i unionen men som i unionen erbjuder de dataförmedlingstjänster som avses i artikel 10 ska utse en rättslig företrädare i en av de medlemsstater där dessa tjänster erbjuds.

För att säkerställa efterlevnaden av denna förordning ska leverantören av dataförmedlingstjänster ge den rättslige företrädaren uppdraget att utöver eller i stället för denna kunna kontaktas av behöriga myndigheter för dataförmedlingstjänster eller registrerade och datainnehavare i alla frågor som rör de tillhandahållna dataförmedlingstjänsterna. Den rättslige företrädaren ska samarbeta med de behöriga myndigheterna för dataförmedlingstjänster och, på begäran, för dessa på ett övergripande sätt påvisa de åtgärder som vidtagits och de bestämmelser som införts av leverantören av dataförmedlingstjänster för att säkerställa överensstämmelse med denna förordning.

Leverantören av dataförmedlingstjänster ska anses omfattas av jurisdiktionen i den medlemsstat där den rättsliga företrädaren finns. Att en leverantör av dataförmedlingstjänster utser en rättslig företrädare ska inte påverka eventuella rättsliga åtgärder som kan vidtas mot leverantören av dataförmedlingstjänster.

4. Efter att ha lämnat en anmälan i enlighet med punkt 1 får leverantören av dataförmedlingstjänster inleda verksamheten i enlighet med de villkor som fastställs i detta kapitel.

5. Den anmälan som avses i punkt 1 ska ge leverantören av dataförmedlingstjänster rätt att tillhandahålla dataförmedlingstjänster i alla medlemsstater.

6. Den anmälan som avses i punkt 1 ska innehålla följande uppgifter:

a) Namnet på leverantören av dataförmedlingstjänster.

b) Dataförmedlingstjänsteleverantörens rättsliga status, form, ägarstruktur, relevanta dotterföretag och, om leverantören av dataförmedlingstjänster är registrerad i ett handelsregister eller annat liknande offentligt nationellt register, registreringsnummer

c) Adressen till dataförmedlingstjänsteleverantörens huvudsakliga verksamhetsställe i unionen, i förekommande fall, och, om tillämpligt, eventuella underordnade filialer i en annan medlemsstat, eller till den rättsliga företrädaren.

d) En offentlig webbplats med fullständig och uppdaterad information om leverantören av dataförmedlingstjänster och verksamheten, inbegripet åtminstone den information som avses i leden a, b, c och f.

e) Dataförmedlingstjänsteleverantörens kontaktpersoner och kontaktuppgifter.

f) En beskrivning av den dataförmedlingstjänst som leverantören av dataförmedlingstjänster avser att tillhandahålla och en uppgift om de kategorier som förtecknas i artikel 10 som dessa dataförmedlingstjänster omfattas av.

g) Beräknat startdatum för verksamheten, om ett annat än anmälningsdatumet.

7. Den behöriga myndigheten för dataförmedlingstjänster ska säkerställa att anmälningsförfarandet är icke-diskriminerande och inte snedvrider konkurrensen.

8. På begäran av leverantören av dataförmedlingstjänster ska den behöriga myndigheten för dataförmedlingstjänster inom en vecka från och med en vederbörligen och fullständigt genomförd anmälan utfärda en standardiserad förklaring som bekräftar att leverantören av dataförmedlingstjänster har inkommit med den anmälan som avses i punkt 1 och att anmälan innehåller de uppgifter som avses i punkt 6.

9. På begäran av leverantören av dataförmedlingstjänster ska den behöriga myndigheten för dataförmedlingstjänster bekräfta att leverantören av dataförmedlingstjänster uppfyller denna artikel och i artikel 12. När leverantören av dataförmedlingstjänster har mottagit en sådan bekräftelse får den i sin skriftliga och muntliga kommunikation använda beteckningen "leverantör av dataförmedlingstjänster som är erkänd i unionen" samt en gemensam logotyp.

För att säkerställa att leverantörer av dataförmedlingstjänster som är erkända i unionen lätt kan identifieras i hela unionen ska kommissionen genom genomförandeakter fastställa den gemensamma logotypens utformning. Leverantörer av dataförmedlingstjänster som är erkända i unionen ska tydligt visa den gemensamma logotypen på alla online- och offline-publikationer som anknyter till deras dataförmedlingsverksamhet.

Dessa genomförandeakter ska antas i enlighet med det rådgivande förfarande som avses i artikel 33.2.

10. Den behöriga myndigheten för dataförmedlingstjänster ska på elektronisk väg och utan dröjsmål underrätta kommissionen om varje ny anmälan. Kommissionen ska föra och regelbundet uppdatera ett offentligt register över alla leverantörer av dataförmedlingstjänster som tillhandahåller sina tjänster i unionen. De uppgifter som avses i punkt 6 a, b, c, d, f och g ska offentliggöras i det offentliga registret.

11. Den behöriga myndigheten för dataförmedlingstjänster får ta ut avgifter för anmälan i enlighet med nationell rätt. Sådana avgifter ska vara proportionella och objektiva och baseras på de administrativa kostnaderna för de behöriga myndigheterna för dataförmedlingstjänsters övervakning av efterlevnaden och andra marknadskontrollåtgärder avseende anmälningar av leverantörer av dataförmedlingstjänster. För små och medelstora företag samt nystartade företag får den behöriga myndigheten ta ut en nedsatt avgift eller avstå från avgiften.

12. Leverantörer av dataförmedlingstjänster ska underrätta den behöriga myndigheten för dataförmedlingstjänster om alla ändringar av den information som tillhandahållits i enlighet med punkt 6 inom 14 dagar från dagen för ändringen.

13. När en leverantör av dataförmedlingstjänster upphör med sin verksamhet ska den inom 15 dagar underrätta den berörda behöriga myndighet för dataförmedlingstjänster som fastställts i enlighet med punkterna 1, 2 och 3.

14. Den behöriga myndigheten för dataförmedlingstjänster ska på elektronisk väg och utan dröjsmål underrätta kommissionen om varje underrättelse som avses i punkterna 12 och 13. Kommissionen ska uppdatera det offentliga registret över leverantörer av dataförmedlingstjänster i unionen i enlighet med detta.

Artikel 12

Villkor för tillhandahållande av dataförmedlingstjänster

Tillhandahållandet av de dataförmedlingstjänster som avses i artikel 10 ska omfattas av följande villkor:

a) Leverantören av dataförmedlingstjänster får inte använda de data för vilka dataförmedlingstjänsterna tillhandahålls för andra ändamål än att ställa dem till dataanvändarnas förfogande och ska tillhandahålla dataförmedlingstjänsterna via en separat juridisk person.

b) De kommersiella villkoren, inklusive prissättningen, för tillhandahållandet av dataförmedlingstjänster till en datainnehavare eller dataanvändare får inte knytas till huruvida datainnehavaren eller dataanvändaren använder andra tjänster från samma leverantör av dataförmedlingstjänster eller en närstående enhet, och i så fall i vilken utsträckning datainnehavaren eller dataanvändaren använder sådana andra tjänster.

c) De data som samlas in om en fysisk eller juridisk persons aktivitet för tillhandahållandet av dataförmedlingstjänsten, däribland datum, tid, geolokaliseringsdata, aktivitetens varaktighet och kopplingar till andra fysiska eller juridiska personer som har inrättats av den person som använder dataförmedlingstjänsten får endast användas för utvecklingen av denna dataförmedlingstjänst, vilket kan innebära användning av data för att upptäcka bedrägerier eller för cybersäkerhet, och ska på begäran göras tillgängliga för datainnehavare.

d) Leverantören av dataförmedlingstjänster ska främja ett utbyte av data i det format som den erhåller dessa data från en registrerad eller en datainnehavare, ska endast konvertera data till särskilda format för att öka interoperabiliteten inom och mellan sektorer, eller om datainnehavaren så begär eller detta föreskrivs i unionsrätten, eller för att säkerställa harmonisering med internationella eller europeiska datastandarder och ska erbjuda registrerade och datainnehavare en möjlighet till undantag avseende dessa konverteringar, såvida inte konverteringen föreskrivs i unionsrätten.

e) Dataförmedlingstjänster får omfatta erbjudande av ytterligare särskilda verktyg och tjänster till datainnehavare eller de registrerade för det särskilda syftet att underlätta utbytet av data, exempelvis i form av tillfällig lagring, kuratering, konvertering, anonymisering och pseudonymisering, varvid sådana verktyg endast får användas på uttrycklig begäran eller efter uttryckligt godkännande av datainnehavaren eller den registrerade, och tredjepartsverktyg som erbjuds i sammanhanget inte får användas för andra ändamål.

f) Leverantören av dataförmedlingstjänster ska säkerställa att förfarandet för tillgång till dess tjänster är rättvist, transparent och icke-diskriminerande för både registrerade och datainnehavare samt för dataanvändare, även när det gäller prissättning och villkor för tjänsten.

g) Leverantören av dataförmedlingstjänster ska ha infört förfaranden för att förhindra bedrägerier eller otillbörliga metoder i samband med parter som önskar sådan tillgång via dess dataförmedlingstjänster.

h) Leverantören av dataförmedlingstjänster ska, vid sin insolvens, säkerställa en rimlig kontinuitet i tillhandahållandet av sina dataförmedlingstjänster och, när sådana dataförmedlingstjänster säkerställer lagring av data, ha mekanismer på plats för att möjliggöra att datainnehavarna och dataanvändarna kan få tillgång till, överföra eller hämta sina data, och om sådana dataförmedlingstjänster tillhandahålls mellan registrerade och dataanvändare, göra det möjligt för registrerade att utöva sina rättigheter.

i) Leverantören av dataförmedlingstjänster ska vidta lämpliga åtgärder för att säkerställa interoperabiliteten med andra dataförmedlingstjänster genom bland annat allmänt använda öppna standarder inom den sektor i vilken leverantören av dataförmedlingstjänster är verksam.

j) Leverantören av dataförmedlingstjänster ska vidta tillräckliga tekniska, rättsliga och organisatoriska åtgärder för att förhindra sådan överföring av eller tillgång till icke-personuppgifter som strider mot unionsrätten eller den nationella rätten i den berörda medlemsstaten.

k) Leverantören av dataförmedlingstjänster ska utan dröjsmål informera datainnehavarna vid otillåten överföring av, tillgång till eller användning av icke-personuppgifter som den har delat.

l) Leverantören av dataförmedlingstjänster ska vidta nödvändiga åtgärder för att säkerställa en lämplig säkerhetsnivå för lagringen, behandlingen och överföringen av icke-personuppgifter, och leverantören av dataförmedlingstjänster ska vidare säkerställa högsta säkerhet för lagringen och överföringen av information som är känslig i konkurrenshänseende.

m) Leverantören av dataförmedlingstjänster som erbjuder tjänster åt de registrerade ska handla i deras bästa intresse när den främjar deras utövande av sina rättigheter, i synnerhet genom att informera och, i lämpliga fall, ge de registrerade råd på ett koncist, transparent, begripligt och lättåtkomligt sätt om dataanvändarnas avsedda dataanvändningar och de standardvillkor som är förbundna med sådan användning, innan de registrerade ger sitt samtycke.

n) Om en leverantör av dataförmedlingstjänster tillhandahåller verktyg för att erhålla de registrerades samtycke eller erhålla tillstånd att behandla data som tillhandhålls av datainnehavare, ska den i relevanta fall ange inom vilken tredjelandsjurisdiktion som dataanvändningen är avsedd att äga rum och förse de registrerade med verktyg för att både ge och återkalla sitt samtycke och datainnehavarna med verktyg för att både ge och återkalla tillstånd för behandling av data.

o) Leverantören av dataförmedlingstjänster ska föra ett loggregister över dataförmedlingsverksamheten.

Artikel 13

Behöriga myndigheter för dataförmedlingstjänster

1. Varje medlemsstat ska utse en eller flera behöriga myndigheter för att utföra uppgifter i samband med anmälningsförfarandet för dataförmedlingstjänster och ska meddela kommissionen dessa behöriga myndigheters identitet senast den 24 september 2023. Varje medlemsstat ska även meddela kommissionen alla eventuella senare ändringar av dessa behöriga myndigheters identitet.

2. De behöriga myndigheterna för dataförmedlingstjänster ska uppfylla de krav som anges i artikel 26.

3. Befogenheterna för de utsedda behöriga myndigheterna för dataförmedlingstjänsters ska inte påverka befogenheterna för dataskyddsmyndigheterna, de nationella konkurrensmyndigheterna, de myndigheter som ansvarar för cybersäkerhet och andra relevanta sektorsmyndigheter. Dessa myndigheter ska i enlighet med sina respektive befogenheter enligt unionsrätten och nationell rätt etablera ett starkt samarbete och utbyta den information som behövs för att de ska kunna utföra sina uppgifter i förhållande till leverantörerna av dataförmedlingstjänster, och ska eftersträva att de beslut som fattas vid tillämpningen av denna förordning är konsekventa.

Artikel 14

Övervakning av efterlevnaden

1. De behöriga myndigheterna för dataförmedlingstjänster ska övervaka och utöva tillsyn över leverantörer av dataförmedlingstjänsters efterlevnad av kraven i detta kapitel. De behöriga myndigheterna för dataförmedlingstjänster får även övervaka och utöva tillsyn över leverantörer av dataförmedlingstjänsters efterlevnad på grundval av en begäran från en fysisk eller juridisk person.

2. De behöriga myndigheterna för dataförmedlingstjänster ska ha befogenhet att från leverantörer av dataförmedlingstjänster eller deras rättsliga företrädare begära all information som är nödvändig för att kontrollera uppfyllandet av kraven i detta kapitel. Varje begäran om information ska stå i proportion till uppgiftens utförande och innehålla en motivering.

3. I de fall då den behöriga myndigheten för dataförmedlingstjänster finner att en leverantör av dataförmedlingstjänster inte uppfyller ett eller flera av kraven i detta kapitel ska den meddela leverantören av dataförmedlingstjänster dessa iakttagelser och ge den möjlighet att yttra sig, inom 30 dagar från mottagandet av meddelandet.

4. Den behöriga myndigheten för dataförmedlingstjänster ska ha befogenhet att kräva att den överträdelse som avses i punkt 3 upphör, inom en rimlig tidsperiod eller omedelbart vid allvarlig överträdelse, och ska vidta ändamålsenliga och proportionella åtgärder för att säkerställa efterlevnaden. I det hänseendet ska den behöriga myndigheten för dataförmedlingstjänster, när så är lämpligt, ha befogenhet att

a) genom administrativa förfaranden ålägga avskräckande ekonomiska sanktioner, som får inbegripa löpande viten och sanktioner med retroaktiv verkan, inleda rättsliga förfaranden för åläggande av sanktionsavgifter, eller bådadera,

b) kräva att inledandet eller avbrytandet av tillhandahållandet av dataförmedlingstjänsten skjuts upp tills villkoren, enligt den behöriga myndigheten för dataförmedlingstjänsters begäran, har ändrats, eller

c) kräva att tillhandahållandet av dataförmedlingstjänsten upphör om allvarliga eller upprepade överträdelser inte har åtgärdats trots utfärdat meddelande enligt punkt 3.

Den behöriga myndigheten för dataförmedlingstjänster ska begära att kommissionen avlägsnar leverantören av dataförmedlingstjänster från registret över leverantörer av dataförmedlingstjänster när den har utfärdat föreläggande om att tillhandahållandet av dataförmedlingstjänsten ska upphöra i enlighet med första stycket c.

Om en leverantör av dataförmedlingstjänster åtgärdar överträdelserna, ska den leverantören av dataförmedlingstjänster på nytt anmäla detta till den behöriga myndigheten för dataförmedlingstjänster. Den behöriga myndigheten för dataförmedlingstjänster ska underrätta kommissionen om varje förnyad anmälan.

5. Om en leverantör av dataförmedlingstjänster som inte är etablerad i unionen inte utser en rättslig företrädare, eller om den rättsliga företrädaren inte på begäran av den behöriga myndigheten för dataförmedlingstjänster lämnar de nödvändiga upplysningar som på ett övergripande sätt visar efterlevnad av denna förordning, ska den behöriga myndigheten för dataförmedlingstjänster ha befogenhet att skjuta upp inledandet av eller att avbryta tillhandahållandet av dataförmedlingstjänsten tills en rättslig företrädare utses eller nödvändig information lämnas.

6. De behöriga myndigheterna för dataförmedlingstjänster ska utan dröjsmål underrätta den berörda leverantören av dataförmedlingstjänster om de åtgärder som vidtas i enlighet med punkterna 4 och 5, och de skäl som de baseras på samt de nödvändiga åtgärder som ska vidtas för att åtgärda bristerna i fråga, och ska fastställa en rimlig tidsperiod, vilken ska vara högst 30 dagar, för leverantören av dataförmedlingstjänsters uppfyllande av dessa krav.

7. Om en leverantör av dataförmedlingstjänster har sitt huvudsakliga verksamhetsställe eller sin rättsliga företrädare i en medlemsstat, men tillhandahåller tjänster i andra medlemsstater, ska den behöriga myndigheten för dataförmedlingstjänster i den medlemsstat där det huvudsakliga verksamhetsstället är belägen eller där den rättsliga företrädaren är lokaliserad och de behöriga myndigheterna för dataförmedlingstjänster i dessa andra medlemsstater samarbeta och bistå varandra. Detta bistånd och samarbete får omfatta informationsutbyte mellan de berörda behöriga myndigheterna för dataförmedlingstjänster för utförande av deras uppgifter inom ramen för denna förordning och motiverade begäranden om att de tillsynsåtgärder som avses i denna artikel ska vidtas.

Om en behörig myndighet för dataförmedlingstjänster i en medlemsstat begär bistånd från en myndighet för dataförmedlingstjänster i annan medlemsstat ska den lämna en motiverad begäran. Den behöriga myndigheten för dataförmedlingstjänster ska, i fall av en sådan begäran, lämna ett svar utan dröjsmål och inom en tidsram som står i proportion till hur brådskande begäran är.

All information som utbyts inom ramen för assistans som begärs och tillhandahålls enligt denna punkt får användas endast med avseende på det ärende för vilket den har begärts.

Artikel 15

Undantag

Detta kapitel ska inte tillämpas på erkända dataaltruismorganisationer eller andra icke-vinstdrivande enheter i den mån som deras verksamhet består i att samla in data för ändamål av allmänt intresse som tillhandahålls av fysiska eller juridiska personer baserat på dataaltruism, såvida inte dessa organisationer och enheter syftar till att upprätta affärsförbindelser mellan, å ena sidan, ett obestämt antal registrerade och datainnehavare och, å andra sidan, dataanvändare.

KAPITEL IV

Dataaltruism

Artikel 16

Nationella arrangemang för dataaltruism

Medlemsstaterna får införa organisatoriska eller tekniska arrangemang, eller bådadera, för att underlätta dataaltruism. För det ändamålet får medlemsstaterna fastställa nationella strategier för dataaltruism. Dessa nationella strategier får framför allt bistå registrerade, när dessa frivilligt gör data som avser dem och som innehas av offentliga myndigheter tillgängliga för dataaltruism, och ange den nödvändiga information som ska tillhandahållas de registrerade om vidareutnyttjandet av deras data i allmänt intresse.

Om en medlemsstat utarbetar sådana nationella strategier ska den underrätta kommissionen om detta.

Artikel 17

Offentliga register över erkända dataaltruismorganisationer

1. Varje behörig myndighet för registrering av dataaltruismorganisationer ska föra och regelbundet uppdatera ett offentligt nationellt register över erkända dataaltruismorganisationer.

2. Kommissionen ska i informationssyfte hålla ett offentligt unionsregister över erkända dataaltruismorganisationer. Förutsatt att en enhet är registrerad i det offentliga nationella registret över erkända dataaltruismorganisationer i enlighet med artikel 18 får den använda beteckningen "dataaltruismorganisation som är erkänd i unionen" i sin skriftliga och muntliga kommunikation samt en gemensam logotyp.

För att säkerställa att erkända dataaltruismorganisationer lätt kan identifieras i hela unionen ska kommissionen genom genomförandeakter fastställa utformningen för den gemensamma logotypen. Erkända dataaltruismorganisationer ska tydligt visa den gemensamma logotypen på alla publikationer online och offline som anknyter till deras dataaltruismverksamhet. Den gemensamma logotypen ska åtföljas av en QR-kod med en länk till det offentliga unionsregistret över erkända dataaltruismorganisationer.

Dessa genomförandeakter ska antas i enlighet med det rådgivande förfarande som avses i artikel 33.2.

Artikel 18

Allmänna krav för registrering

För att kvalificera sig för registrering i ett offentligt nationellt register över erkända dataaltruismorganisationer ska en enhet

a) utföra dataaltruismåtgärder,

b) vara en juridisk person som bildats i enlighet med nationell rätt för att uppfylla mål av allmänt intresse, som det föreskrivs i nationell rätt i förekommande fall,

c) bedriva verksamhet på icke-vinstdrivande grund och vara rättsligt fristående från alla enheter som bedriver verksamhet på vinstdrivande grund,

d) utföra sina dataaltruismåtgärder via en struktur som är funktionellt fristående från dess övriga åtgärder.

e) följa den regelbok som avses i artikel 22.1 senast 18 månader efter dagen för ikraftträdandet av de delegerade akter som avses i den punkten.

Artikel 19

Registrering av erkända dataaltruismorganisationer

1. En enhet som uppfyller kraven i artikel 18 får lämna in en ansökan om registrering i det offentliga nationella registret över erkända dataaltruismorganisationer i den medlemsstat där den är etablerad.

2. En enhet som uppfyller kraven i artikel 18 och har verksamhetsställen i fler än en medlemsstat får inlämna en ansökan om registrering i det offentliga nationella registret över erkända dataaltruismorganisationer i den medlemsstat där den har sitt huvudsakliga verksamhetsställe.

3. En enhet som uppfyller kraven i artikel 18 men som inte är etablerad i unionen ska utse en rättslig företrädare i en av de medlemsstater i vilka dataaltruismtjänsterna erbjuds.

För att säkerställa efterlevnaden av denna förordning ska enheten ge den rättslige företrädaren uppdraget att utöver eller i stället för denna kunna kontaktas av behöriga myndigheter för registrering av dataaltruismorganisationer eller registrerade och datainnehavare i alla frågor som rör den enheten. Den rättslige företrädaren ska samarbeta med de behöriga myndigheterna för registrering av dataaltruismorganisationer och, på begäran, för dessa på ett övergripande sätt påvisa de åtgärder som vidtagits och bestämmelser som införts av enheten för att säkerställa överensstämmelse med denna förordning.

Enheten ska anses omfattas av jurisdiktionen i den medlemsstat där den rättsliga företrädaren finns. En sådan enhet får lämna in en ansökan om r registrering i det offentliga nationella registret över erkända dataaltruismorganisationer i den medlemsstaten. Att enheten utser en rättslig företrädare ska inte påverka rättsliga åtgärder som kan vidtas mot enheten.

4. De ansökningar om registrering som avses i punkterna 1, 2 och 3 ska innehålla följande uppgifter:

a) Enhetens namn.

b) Enhetens rättsliga status, form och, om enheten är registrerad i ett offentligt nationellt register, registreringsnummer.

c) Enhetens stadgar, i förekommande fall.

d) Enhetens inkomstkällor.

e) Adressen till enhetens huvudsakliga verksamhetsställe i unionen, i förekommande fall, och, om tillämpligt, eventuella underordnade filialer i en annan medlemsstat, eller till den rättsliga företrädaren.

f) En offentlig webbplats med fullständig och uppdaterad information om enheten och verksamheten, inbegripet åtminstone den information som avses i leden a, b, d, e och h.

g) Enhetens kontaktpersoner och kontaktuppgifter.

h) De mål av allmänt intresse som enheten avser att främja när den samlar in data.

i) Den typ av data som enheten avser att kontrollera eller behandla och, när det gäller personuppgifter, en angivelse av kategorierna av personuppgifter.

j) Alla andra handlingar som visar att kraven i artikel 18 uppfylls.

5. När enheten har lämnat all nödvändig information i enlighet med punkt 4, och efter det att den behöriga myndigheten för registrering av dataaltruismorganisationer har utvärderat ansökan om registrering och konstaterat att enheten uppfyller kraven i artikel 18, ska den registrera enheten i det offentliga nationella registret över erkända dataaltruismorganisationer inom tolv veckor efter mottagandet av ansökan om registrering. Registreringen ska gälla i alla medlemsstater.

Den behöriga myndigheten för registrering av dataaltruismorganisationer ska underrätta kommissionen om alla registreringar. Kommissionen ska föra in registreringarna i det offentliga unionsregistret över erkända dataaltruismorganisationer.

6. De uppgifter som avses i punkt 4 a, b, f, g och h ska offentliggöras i det relevanta offentliga nationella registret över erkända dataaltruismorganisationer.

7. En erkänd dataaltruismorganisation ska underrätta den relevanta behöriga myndigheten för registrering av dataaltruismorganisationer om alla ändringar av de uppgifter som tillhandahållits i enlighet med punkt 4 inom 14 dagar från dagen för ändringen.

Den behöriga myndigheten för registrering av dataaltruismorganisationer ska utan dröjsmål underrätta kommissionen om varje sådan underrättelse på elektronisk väg. På grundval av en sådan underrättelse ska kommissionen utan dröjsmål uppdatera det offentliga unionsregistret över erkända dataaltruismorganisationer.

Artikel 20

Transparenskrav

1. En erkänd dataaltruismorganisation ska föra fullständiga och noggranna register över

a) alla fysiska eller juridiska personer som getts möjlighet att behandla data som innehas av den erkända dataaltruismorganisationen, och deras kontaktuppgifter,

b) datum eller varaktighet för behandlingen av personuppgifter eller användning av icke-personuppgifter,

c) behandlingens ändamål som det angetts av den fysiska eller juridiska person som getts möjlighet till behandling,

d) avgifter som betalas av fysiska eller juridiska personer som behandlar data, i förekommande fall.

2. En erkänd dataaltruismorganisation ska utarbeta och till den relevanta behöriga myndigheten för registrering av dataaltruismorganisationer sända en årlig verksamhetsrapport som ska innehålla minst följande:

a) Information om den erkända dataaltruismorganisationens verksamhet.

b) En beskrivning av hur de mål av allmänt intresse som föranledde insamlingen av data har främjats under det aktuella budgetåret.

c) En förteckning över alla fysiska och juridiska personer som tillåtits att behandla de data som enheten innehar, inbegripet en sammanfattande beskrivning av de mål av allmänt intresse som är tänkta att uppnås genom sådan databehandling och en beskrivning av de tekniska metoder som använts, inbegripet en beskrivning av de tekniker som använts för skyddet av personlig integritet och dataskydd.

d) En sammanfattning av resultaten av de databehandlingar som tillåtits av den erkända dataaltruismorganisationen, i förekommande fall.

e) Information om den erkända dataaltruismorganisationens inkomstkällor, i synnerhet alla intäkter från beviljandet av tillgång till data, och om utgifter.

Artikel 21

Särskilda krav för att skydda de registrerades och datainnehavarnas rättigheter och intressen när det gäller deras data

1. En erkänd dataaltruismorganisation ska på ett klart och lättbegripligt sätt underrätta registrerade eller datainnehavare innan deras data behandlas

a) om de mål av allmänt intresse och, om tillämpligt, de särskilda, uttryckligt angivna och berättigade ändamål för vilka personuppgifter ska behandlas, och för vilka den tillåter att deras data behandlas av dataanvändare, och

b) om lokaliseringen och målen av allmänt intresse i fråga om vilka den tillåter behandling som utförs i ett tredjeland, om behandlingen utförs av den erkända dataaltruismorganisationen.

2. Den erkända dataaltruismorganisationen får inte använda data för några andra mål än de mål av allmänt intresse för vilka den registrerade eller datainnehavaren tillåter behandling. Den erkända dataaltruismorganisationen får inte använda vilseledande marknadsföringsmetoder i samband med förfrågan om tillhandahållande av data.

3. Den erkända dataaltruismorganisationen ska tillhandahålla verktyg för inhämtande av samtycke från registrerade eller tillstånd att behandla data som datainnehavare har gjort tillgängliga. Den erkända dataaltruismorganisationen ska också tillhandahålla verktyg för enkelt återkallande av sådant samtycke eller tillstånd.

4. Den erkända dataaltruismorganisationen ska vidta åtgärder för att säkerställa en lämplig säkerhetsnivå för lagringen och behandlingen av icke-personuppgifter som den har samlat in på grundval av dataaltruism.

5. Den erkända dataaltruismorganisationen ska utan dröjsmål informera datainnehavarna vid otillåten överföring av, tillgång till eller användning av icke-personuppgifter som den har delat.

6. Om den erkända dataaltruismorganisationen underlättar tredjeparters behandling av data, bland annat genom att tillhandahålla verktyg för att erhålla de registrerades samtycke eller erhålla tillstånd att behandla data som tillhandhålls av datainnehavare, ska den i relevanta fall, ange inom vilken tredjelandsjurisdiktion som dataanvändningen är avsedd att äga rum.

Artikel 22

Regelbok

1. Kommissionen ska anta delegerade akter i enlighet med artikel 32 med avseende på att komplettera denna förordning genom skapandet av en regelbok som fastställer

a) lämpliga informationskrav som säkerställer att registrerade och datainnehavare, innan ett samtycke eller tillstånd för dataaltruism ges, tillhandahålls tillräckligt utförlig, tydlig och transparent information om användningen av data, verktygen för givande och återkallande av samtycke eller tillstånd och de åtgärder som vidtagits för att undvika missbruk av de data som delas med dataaltruismorganisationen,

b) lämpliga tekniska och säkerhetsmässiga krav för att säkerställa en lämplig nivå av säkerhet för lagringen och behandlingen av data samt för verktygen för givande och återkallande av samtycke eller tillstånd,

c) kommunikationsfärdplaner med multidisciplinär ansats för att öka medvetenheten om dataaltruism, om erhållen status som ”dataaltruismorganisation som är erkänd i unionen” och om regelboken bland berörda parter, särskilt datainnehavare och registrerade som kan tänka sig att dela med sig av sina data,

d) rekommendationer om relevanta interoperabilitetsstandarder.

2. Den regelbok som avses i punkt 1 ska utarbetas i nära samarbete med dataaltruismorganisationer och berörda parter.

Artikel 23

Behöriga myndigheter för registrering av dataaltruismorganisationer

1. Varje medlemsstat ska utse en eller flera behöriga myndigheter som ansvarar för dess offentliga nationella register av erkända dataaltruismorganisationer.

De behöriga myndigheterna för registrering av dataaltruismorganisationer ska uppfylla de krav som anges i artikel 26.

2. Varje medlemsstat ska underrätta kommissionen om identiteten på sina behöriga myndigheter för registrering av dataaltruismorganisationers identitet senast den 24 september 2023. Varje medlemsstat ska även underrätta kommissionen om alla eventuella senare ändringar av dessa behöriga myndigheters identitet

3. Den behöriga myndigheten för registrering av dataaltruismorganisationer i en medlemsstat ska utföra sina uppgifter i samarbete med den relevanta dataskyddsmyndigheten, när dessa uppgifter rör behandlingen av personuppgifter, och med relevanta sektorsmyndigheterna i den medlemsstaten.

Artikel 24

Övervakning av efterlevnaden

1. De behöriga myndigheterna för registrering av dataaltruismorganisationer ska övervaka och utöva tillsyn över att erkända dataaltruismorganisationer uppfyller de krav som fastställs i detta kapitel. Den behöriga myndigheten för registrering av dataaltruismorganisationer får även övervaka och utöva tillsyn över sådana erkända dataaltruismorganisationers efterlevnad på grundval av en begäran från en fysisk eller juridisk person.

2. De behöriga myndigheterna för registrering av dataaltruismorganisationer ska ha befogenhet att från erkända dataaltruismorganisationer begära sådan information som är nödvändig för att kontrollera att kraven i detta kapitel följs. Varje begäran om information ska stå i proportion till uppgiftens utförande och innehålla en motivering.

3. I de fall då den behöriga myndigheten för registrering av dataaltruismorganisationer finner att en erkänd dataaltruismorganisation inte uppfyller ett eller flera av kraven i detta kapitel ska den meddela den erkända dataaltruismorganisationen dessa iakttagelser och ge den möjlighet att yttra sig, inom 30 dagar efter mottagandet av meddelandet.

4. Den behöriga myndigheten för registrering av dataaltruismorganisationer ska ha befogenhet att kräva att den överträdelse som avses i punkt 3 upphör, antingen omedelbart eller inom en rimlig tidsperiod, och ska vidta ändamålsenliga och proportionella åtgärder för att säkerställa efterlevnaden.

5. Om en erkänd dataaltruismorganisation inte uppfyller ett eller flera krav i detta kapitel ens efter att den i enlighet med punkt 3 har underrättats av den behöriga myndigheten för registrering av dataaltruismorganisationer, ska den erkända dataaltruismorganisationen

a) förlora sin rätt att använda beteckningen ”dataaltruismorganisation som är erkänd i unionen” i sin skriftliga och muntliga kommunikation,

b) avlägsnas från det relevanta offentliga nationella registret över erkända dataaltruismorganisationer och det offentliga unionsregistret över erkända dataaltruismorganisationer.

Ett beslut om att återkalla rätten att använda beteckningen ”dataaltruismorganisation om är erkänd i unionen” enligt första stycket led a ska offentliggöras av den behöriga myndigheten för registrering av dataaltruismorganisationer.

6. Om en enhet som registreras i det offentliga nationella registret över erkända dataaltruismorganisationer har sitt huvudsakliga verksamhetsställe eller sin rättsliga företrädare i en medlemsstat, men är aktiv i andra medlemsstater, ska den behöriga myndigheten för registrering av dataaltruismorganisationer i den medlemsstat där det huvudsakliga verksamhetsstället är beläget eller där den rättsliga företrädaren är lokaliserad och de behöriga myndigheterna för registrering av dataaltruismorganisationer i dessa andra medlemsstater samarbeta och bistå varandra. Detta bistånd och samarbete får omfatta informationsutbyte mellan de berörda behöriga myndigheterna för registrering av dataaltruismorganisationer för utförande av deras uppgifter inom ramen för denna förordning och motiverade begäranden om att de åtgärder som avses denna artikel ska vidtas.

Om en behörig myndighet för registrering av dataaltruismorganisationer i en medlemsstat begär bistånd från en behörig myndighet för registrering av dataaltruismorganisationer i en annan medlemsstat ska den lämna en motiverad begäran. Den behöriga myndigheten för registrering av dataaltruismorganisationer ska i fall av en sådan begäran svara på denna utan dröjsmål och inom en tidsram som står i proportion till hur brådskande begäran är.

All information som utbyts inom ramen för assistans som begärs och tillhandahålls enligt denna punkt får användas endast med avseende på det ärende för vilket den har begärts.

Artikel 25

Europeiskt formulär för samtycke till dataaltruism

1. För att främja insamling av data baserat på dataaltruism ska kommissionen anta genomförandeakter om upprättande och utarbetande av ett europeiskt formulär för samtycke till dataaltruism, efter samråd med Europeiska dataskyddsstyrelsen och med beaktande av rådgivning från Europeiska datainnovationsstyrelsen samt med vederbörligt deltagande av berörda parter. Detta formulär ska göra det möjligt att erhålla samtycke eller tillstånd i alla medlemsstater och i ett enhetligt format. Dessa genomförandeakter ska antas i enlighet med det rådgivande förfarande som avses i artikel 33.2.

2. Det europeiska formuläret för samtycke till dataaltruism ska baseras på moduler, så att det kan anpassas till enskilda sektorer och olika syften.

3. När personuppgifter tillhandahålls ska det europeiska formuläret för samtycke till dataaltruism säkerställa att de registrerade kan ge och dra tillbaka sitt samtycke till en specifik databehandlingsoperation i enlighet med kraven i förordning (EU) 2016/679.

4. Formuläret ska tillhandahållas på ett sådant sätt att det kan tryckas på papper, är lättförståeligt och även finns i elektronisk, maskinläsbar form.

KAPITEL V

Behöriga myndigheter och förfarandebestämmelser

Artikel 26

Krav på behöriga myndigheter

1. De behöriga myndigheterna för dataförmedlingstjänster och de behöriga myndigheterna för registrering av dataaltruismorganisationer ska vara juridiskt åtskilda från, och funktionellt oberoende av, alla leverantörer av dataförmedlingstjänster eller erkända dataaltruismorganisationer. Funktionerna för de behöriga myndigheterna för dataförmedlingstjänster och de behöriga myndigheterna för registrering av dataaltruismorganisationer får utföras av samma myndighet. Medlemsstaterna får antingen inrätta en eller flera nya myndigheter eller förlita sig på befintliga myndigheter.

2. De behöriga myndigheterna för dataförmedlingstjänster och de behöriga myndigheterna för registrering av dataaltruismorganisationer ska utföra sina uppgifter på ett opartiskt, transparent, konsekvent och tillförlitligt sätt och utan dröjsmål. När de utför sina uppgifter ska de skydda rättvis konkurrens och icke-diskriminering.

3. De ledande befattningshavarna och personalen som ansvarar för att utföra de berörda uppgifterna hos de behöriga myndigheterna för dataförmedlingstjänster och de behöriga myndigheterna för registrering av dataaltruismorganisationer får inte vara personer som utformar, tillverkar, tillhandahåller, installerar, köper in, äger, använder eller underhåller de tjänster som de bedömer, och inte heller vara auktoriserade företrädare eller ombud för någon av dessa parter. Detta ska dock inte hindra en användning av bedömda tjänster som är nödvändig för verksamheten vid de behöriga myndigheterna för dataförmedlingstjänster och de behöriga myndigheterna för registrering av dataaltruismorganisationer eller en användning av sådana tjänster för personliga ändamål.

4. De ledande befattningshavarna och personalen vid de behöriga myndigheterna för dataförmedlingstjänster och de behöriga myndigheterna för registrering av dataaltruismorganisationer får inte delta i någon verksamhet som kan påverka deras objektivitet och integritet i samband med de bedömningar av verksamhet som de anförtrotts att göra.

5. De behöriga myndigheterna för dataförmedlingstjänster och de behöriga myndigheterna för registrering av dataaltruismorganisationer ska ha tillräckliga ekonomiska resurser och personalresurser till sitt förfogande för att utföra de uppgifter som de anförtrotts, inbegripet de nödvändiga tekniska kunskaperna och resurserna.

6. De behöriga myndigheterna för dataförmedlingstjänster och de behöriga myndigheterna för registrering av dataaltruismorganisationer i en medlemsstat ska, på motiverad begäran och utan dröjsmål, förse kommissionen och de behöriga myndigheterna för dataförmedlingstjänster och de behöriga myndigheterna för registrering av dataaltruismorganisationer från andra medlemsstater med den information som dessa behöver för att utföra sina uppgifter enligt denna förordning. Om en behörig myndighet för dataförmedlingstjänster eller en behörig myndighet för registrering av dataaltruismorganisationer anser att den begärda informationen är konfidentiell i enlighet med unionsrätten och nationell rätt om affärshemligheter och tystnadsplikt, ska kommissionen och andra berörda behöriga myndigheter för dataförmedlingstjänster eller behöriga myndigheter för registrering av dataaltruismorganisationer säkerställa sådan konfidentiell behandling.

Artikel 27

Rätt att lämna in klagomål

1. Fysiska och juridiska personer ska, avseende frågor som omfattas av tillämpningsområdet för denna förordning, ha rätt att inkomma med klagomål, individuellt eller i relevanta fall kollektivt, till den berörda a behöriga myndigheten för dataförmedlingstjänster mot en leverantör av dataförmedlingstjänster eller till den behöriga myndigheten för registrering av dataaltruismorganisationer mot en erkänd dataaltruismorganisation.

2. Den behöriga myndigheten för dataförmedlingstjänster eller den behöriga myndigheten för registrering av dataaltruismorganisationer till vilket klagomålet har lämnats in ska underrätta den klagande om

a) hur förfarandet fortskrider och vilket beslut som fattats, och

b) rättsmedel enligt artikel 28.

Artikel 28

Rätten till ett effektivt rättsmedel

1. Utan att det påverkar administrativa rättsmedel eller andra prövningsförfaranden utanför domstol, ska berörda fysiska och juridiska personer ha rätt till effektiva rättsmedel avseende rättsligt bindande beslut som avses i artikel 14 och som fattats av de behöriga myndigheterna för dataförmedlingstjänster i samband med hantering, övervakning och kontroll av efterlevnaden av anmälningsordningen för leverantörer av dataförmedlingstjänster och rättsligt bindande beslut som avses i artiklarna 19 och 24 som fattas av de behöriga myndigheterna för registrering av dataaltruismorganisationer i samband med övervakningen av erkända dataaltruismorganisationer.

2. Förfaranden enligt denna artikel ska inledas vid domstolarna i den medlemsstat där den behöriga myndigheten för dataförmedlingstjänster eller den behöriga myndigheten för registrering av dataaltruismorganisationer som rättsmedlen avser är belägen, antingen individuellt eller, i förekommande fall kollektivt, av företrädare för en eller flera fysiska eller juridiska personer.

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

KAPITEL VI

Europeiska datainnovationsstyrelsen

Artikel 29

Europeiska datainnovationsstyrelsen

1. Kommissionen ska inrätta en europeisk datainnovationsstyrelse i form av en expertgrupp som består av företrädare för de behöriga myndigheterna för dataförmedlingstjänster och de behöriga myndigheterna för registrering av dataaltruismorganisationer i alla medlemsstater, Europeiska dataskyddsstyrelsen, Europeiska datatillsynsmannen, Enisa, kommissionen, EU-företrädaren för små och medelstora företag eller en företrädare utsedd av nätverket av företrädare för små och medelstora företag och andra företrädare för relevanta organ inom enskilda sektorer samt organ med specifik sakkunskap. I sin utnämning av enskilda experter ska kommissionen sträva efter att uppnå jämn könsfördelning och geografisk balans bland medlemmarna av expertgruppen.

2. Europeiska datainnovationsstyrelsen ska bestå av minst följande tre undergrupper:

a) en undergrupp bestående av de behöriga myndigheterna för dataförmedlingstjänster och de behöriga myndigheterna för registrering av dataaltruismorganisationer, som är avsedd att utföra uppgifterna enligt artikel 30 a, c, j och k,

b) en undergrupp för tekniska diskussioner om standardisering, portabilitet och interoperabilitet i enlighet med artikel 30 f och g,

c) en undergrupp för deltagande av berörda parter bestående av relevanta företrädare från näringslivet, forskningsvärlden, den akademiska världen, civilsamhället, standardiseringsorganisationer, berörda gemensamma europeiska dataområden och andra berörda intressenter och tredje parter som ger råd till Europeiska datainnovationsstyrelsen om uppgifter i enlighet med artikel 30 d, e, f, g och h.

3. Kommissionen ska vara ordförande vid Europeiska datainnovationsstyrelsens sammanträden.

4. Europeiska datainnovationsstyrelsen ska bistås av ett sekretariat som tillhandahålls av kommissionen.

Artikel 30

Europeiska datainnovationsstyrelsens uppgifter

Europeiska datainnovationsstyrelsen ska ha följande uppgifter:

a) Att rådge och bistå kommissionen när det gäller utarbetandet av en konsekvent praxis för offentliga myndigheter och behöriga organ enligt 7.1 vid behandlingen av ansökningar om vidareutnyttjande av de kategorier av data som avses i artikel 3.1.

b) Att rådge och bistå kommissionen när det gäller utvecklingen av en enhetlig praxis för dataaltruism i hela unionen.

c) Att rådge och bistå kommissionen när det gäller utarbetandet av en konsekvent praxis för de behöriga myndigheterna för dataförmedlingstjänster och de behöriga myndigheterna för registreringen av dataaltruismorganisationer vad gäller tillämpningen av krav för leverantörer av dataförmedlingstjänster och erkända dataaltruismorganisationer.

d) Att rådge och bistå kommissionen när det gäller utarbetandet av konsekventa riktlinjer för hur man inom ramen för denna förordning bäst ska skydda kommersiellt känsliga data som inte är personuppgifter, särskilt företagshemligheter, men även icke-personuppgifter med immaterialrättsligt skyddat innehåll, mot olaglig åtkomst med risker för stöld av immateriella rättigheter eller industrispionage.

e) Att rådge och bistå kommissionen när det gäller utarbetandet av konsekventa riktlinjer för cybersäkerhetskrav vid utbyte och lagring av data.

f) Att rådge kommissionen, särskilt med hänsyn till bidrag från standardiseringsorganisationer, om prioriteringsordningen för sektorsövergripande standarder som ska användas och utvecklas för dataanvändning och sektorsöverskridande datadelning mellan framväxande gemensamma europeiska dataområden, sektorsöverskridande jämförelse och utbyte av bästa praxis när det gäller sektorskrav avseende säkerhet samt förfaranden för tillgång, med beaktande av sektorsspecifik standardiseringsverksamhet, framför allt för att klarlägga och särskilja vilka standarder och praxisformer som är sektorsöverskridande och vilka som är sektorsspecifika.

g) Att bistå kommissionen, särskilt med hänsyn till bidrag från standardiseringsorganisationer, med att ta itu med fragmenteringen av den inre marknaden och av dataekonomin på den inre marknaden genom att förbättra den gränsöverskridande, sektorsövergripande interoperabiliteten för data och datadelningstjänster mellan olika sektorer och områden, baserat på befintliga europeiska, internationella eller nationella standarder, bland annat med syftet att uppmuntra inrättandet av gemensamma europeiska dataområden.

h) Att föreslå riktlinjer för gemensamma europeiska dataområden, nämligen ändamåls- eller sektorsspecifika eller sektoröverskridande interoperabla ramar med allmänna standarder och praxisformer för delning eller gemensam behandling av data bl.a. för utveckling av nya produkter och tjänster, vetenskaplig forskning eller civilsamhällsinitiativ, sådana allmänna standarder och praxisformer tar hänsyn till befintliga standarder, följer konkurrensreglerna och säkerställer icke-diskriminerande tillgång för alla deltagare, för att underlätta datadelning i unionen och utnyttja potentialen i befintliga och framtida dataområden, som bland annat tar upp

   i) sektorsövergripande standarder som ska användas och utvecklas för dataanvändning och sektorsöverskridande datadelning, sektorsöverskridande jämförelse och utbyte av bästa praxis när det gäller sektorskrav avseende säkerhet samt förfaranden för tillgång, med beaktande av sektorsspecifik standardiseringsverksamhet, framför allt för att klarlägga och särskilja vilka standarder och praxisformer som är sektorsöverskridande och vilka som är sektorsspecifika,

   ii) krav för att motverka hinder för marknadstillträde och för att undvika inlåsningseffekter, i syfte att säkerställa rättvis konkurrens och interoperabilitet,

iii) tillräckligt skydd för lagliga dataöverföringar till tredjeländer, däribland skyddsåtgärder mot överföringar som är förbjudna enligt unionsrätten,

iv) tillräcklig och icke-diskriminerande representation av berörda parter i förvaltningen av gemensamma europeiska dataområden,

v) efterlevnad av cybersäkerhetskrav i enlighet med unionsrätten.

i) Att underlätta samarbetet mellan medlemsstaterna om fastställandet av harmoniserade villkor som möjliggör vidareutnyttjande av de kategorier av data som avses i artikel 3.1 och som innehas av offentliga myndigheter överallt på den inre marknaden.

j) Att underlätta samarbetet mellan behöriga myndigheter för dataförmedlingstjänster och behöriga myndigheter för registrering av dataaltruismorganisationer, genom kapacitetsuppbyggnad och informationsutbyte, i synnerhet genom att fastställa metoder för ett effektivt utbyte av information som rör förfarandet för anmälan av leverantörer av dataförmedlingstjänster och registreringen och övervakningen av erkända dataaltruismorganisationer, inbegripet samordning avseende fastställande av avgifter eller sanktioner, samt underlätta samarbetet mellan behöriga myndigheter för dataförmedlingstjänster och behöriga myndigheter för registrering av dataaltruismorganisationer avseende internationell tillgång till och överföring av data.

k) Att rådge och bistå kommissionen när det gäller utvärderingen av huruvida de genomförandeakter som avses i artikel 5.11 och 5.12 ska antas.

l) Att rådge och bistå kommissionen när det gäller utarbetande av det europeiska formuläret för samtycke till dataaltruism i enlighet med artikel 25.1.

m) Att rådge kommissionen om förbättring av det internationella regelverket för icke-personuppgifter, inbegripet standardisering.

KAPITEL VII

internationell tillgång och överföring

Artikel 31

Internationell tillgång och överföring

1. Den offentliga myndighet, den fysiska eller juridiska person som beviljats rätt att vidareutnyttja data i enlighet med kapitel II, leverantören av dataförmedlingstjänster eller den erkända dataaltruismorganisationen ska vidta alla rimliga tekniska, rättsliga och organisatoriska åtgärder, inbegripet kontraktsmässiga arrangemang, för att förhindra internationell överföring av eller statlig tillgång till icke-personuppgifter som innehas i unionen, om en sådan överföring eller tillgång skulle strida mot unionsrätten eller den nationella rätten i den berörda medlemsstaten, utan att detta påverkar punkt 2 eller 3.

2. Beslut eller domar från en domstol i ett tredje land och beslut från förvaltningsmyndigheter i ett tredjeland där det krävs att en offentlig myndighet, en fysisk eller juridisk person som beviljas rätten att vidareutnyttja data i enlighet med kapitel II, en leverantör av dataförmedlingstjänster eller en erkänd dataaltruismorganisation överför icke-personuppgifter som omfattas av tillämpningsområdet för denna förordning från unionen eller ger tillgång till sådana icke-personuppgifter som innehas i unionen får endast erkännas eller genomföras på något som helst sätt om det grundar sig på en internationell överenskommelse, såsom ett fördrag om ömsesidig rättslig hjälp, som gäller mellan det begärande tredjelandet och unionen, eller ett sådant avtal mellan det begärande tredjelandet och en medlemsstat.

3. I de fall då, i avsaknad av en internationell överenskommelse som avses i punkt 2 i denna artikel, en offentlig myndighet, en fysisk eller juridisk person som i enlighet med kapitel II beviljats rättigheten att vidareutnyttja data, en leverantör av dataförmedlingstjänster eller en erkänd dataaltruismorganisation är adressat för ett beslut eller en dom från en domstol i ett tredje land eller ett beslut från en förvaltningsmyndighet i ett tredjeland om att överföra icke-personuppgifter som omfattas av tillämpningsområdet för denna förordning från unionen eller ge tillgång till sådana icke-personuppgifter som innehas i unionen, och efterlevnaden av ett sådant beslut skulle riskera att medföra att adressaten bryter mot unionsrätten eller den nationella rätten i den berörda medlemsstaten, ska tredjelandsmyndighetens överföring av eller tillgång till sådana data endast äga rum om:

a) tredjelandets system kräver att skälen till och proportionaliteten hos sådana beslut eller domar ska fastställas, och föreskriver att sådana beslut eller domar är av specifik art, exempelvis genom att det fastställs en tillräckligt stark koppling till vissa misstänkta personer eller till överträdelser,

b) adressatens motiverade invändning är föremål för en granskning av en behörig domstol i tredjelandet, och

c) den behöriga domstol i tredjelandet som utfärdar beslutet eller domen eller granskar en förvaltningsmyndighets beslut enligt det tredjelandets rätt har befogenhet att ta vederbörlig hänsyn till de relevanta rättsliga intressena för leverantören av de data som skyddas av unionsrätten eller den nationella rätten i den berörda medlemsstaten.

4. Om de villkor som fastställs i punkterna 2 och 3 är uppfyllda ska den offentliga myndigheten, den fysiska eller juridiska person som beviljats rätt att vidareutnyttja data i enlighet med kapitel II, leverantören av dataförmedlingstjänster eller den erkända dataaltruismorganisationen tillhandahålla den minimimängd data som är tillåten till följd av en begäran, baserat på en rimlig tolkning av denna begäran.

5. Den offentliga myndigheten, den fysiska eller juridiska person som i enlighet med kapitel II beviljats rättigheten att vidareutnyttja data, leverantören av dataförmedlingstjänster 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, innan den tillmötesgår den begäran, förutom då denna begäran avser brottsbekämpande ändamål och så länge som detta är nödvändigt för att skydda brottsbekämpningens effektivitet.

KAPITEL VIII

Delegering och kommittéförfarande

Artikel 32

Utövande av delegeringen

1. Befogenheten att anta delegerade akter ges till kommissionen med förbehåll för de villkor som anges i denna artikel.

2. Den befogenhet att anta delegerade akter som avses i artiklarna 5.13 och 22.1 ges till kommissionen tills vidare från och med den 23 juni 2022.

3. Den delegering av befogenhet som avses i artiklarna 5.13 och 22.1 får när som helst återkallas av Europaparlamentet eller rådet. Ett beslut om återkallelse innebär att delegeringen av den befogenhet som anges i beslutet upphör att gälla. Beslutet får verkan dagen efter det att det offentliggörs i *Europeiska unionens officiella tidning*, eller vid ett senare i beslutet angivet datum. Det påverkar inte giltigheten av delegerade akter som redan har trätt i kraft.

4. Innan kommissionen antar en delegerad akt ska den samråda med experter som utsetts av varje medlemsstat i enlighet med principerna i det interinstitutionella avtalet av den 13 april 2016 om bättre lagstiftning.

5. Så snart kommissionen antar en delegerad akt ska den samtidigt delge Europaparlamentet och rådet denna.

6. En delegerad akt som antas enligt artikel 5.13 eller 22.1 ska träda i kraft endast om varken Europaparlamentet eller rådet har gjort invändningar mot den delegerade akten inom en period på tre månader från den dag då akten delgavs Europaparlamentet och rådet, eller om både Europaparlamentet och rådet, före utgången av den perioden, har underrättat kommissionen om att de inte kommer att invända. Denna period ska förlängas med tre månader på Europaparlamentets eller rådets initiativ.

Artikel 33

Kommittéförfarande

1. Kommissionen ska biträdas av en kommitté. Denna kommitté ska vara en kommitté i den mening som avses i förordning (EU) nr 182/2011.

2. När det hänvisas till denna punkt ska artikel 4 i förordning (EU) nr 182/2011 tillämpas.

3. När det hänvisas till denna punkt ska artikel 5 i förordning (EU) nr 182/2011 tillämpas.

KAPITEL IX

Slut- och övergångsbestämmelser

Artikel 34

Sanktioner

1. Medlemsstaterna ska fastställa regler om sanktioner för överträdelse av skyldigheterna om överföring av icke-personuppgifter till tredjeländer enligt artiklarna 5.14 och 31, anmälningsskyldigheten för leverantörer av dataförmedlingstjänster enligt artikel 11, villkoren för tillhandahållande av dataförmedlingstjänster enligt artikel 12 och villkoren för registrering som erkänd dataaltruismorganisation enligt artiklarna 18, 20, 21 och 22 och vidta alla nödvändiga åtgärder för att säkerställa att de tillämpas. Sanktionerna ska vara effektiva, proportionella och avskräckande. Medlemsstaterna ska i sina regler om sanktioner ta hänsyn till Europeiska datainnovationsstyrelsens rekommendationer. Medlemsstaterna ska till kommissionen anmäla dessa regler och åtgärder senast den 24 september 2023 samt utan dröjsmål eventuella ändringar som berör dem.

2. Medlemsstaterna ska i lämpliga fall beakta följande icke-uttömmande och vägledande kriterier för utdömande av sanktioner för leverantörer av dataförmedlingstjänster och erkända dataaltruismorganisationer vid överträdelser av denna förordning:

a) Överträdelsens art, allvar, omfattning och varaktighet.

b) Eventuella åtgärder som leverantören av dataförmedlingstjänster eller den erkända dataaltruismorganisationen vidtagit för att begränsa eller avhjälpa den skada som överträdelsen har orsakat.

c) Eventuella tidigare överträdelser som leverantören av dataförmedlingstjänster eller den erkända dataaltruismorganisationen har gjort sig skyldig till.

d) De ekonomiska vinster som leverantören av dataförmedlingstjänster eller den erkända dataaltruismorganisationen gjort eller de förluster som de undvikit till följd av överträdelsen, i den mån sådana vinster eller förluster på ett tillförlitligt sätt kan fastställas.

e) Eventuella andra försvårande eller förmildrande omständigheter som är tillämpliga på ärendet.

Artikel 35

Utvärdering och översyn

Kommissionen ska senast den 24 september 2025 genomföra en utvärdering av denna förordning och lämna en rapport om de viktigaste resultaten till Europaparlamentet, rådet och Europeiska ekonomiska och sociala kommittén. Rapporten ska vid behov åtföljas av lagstiftningsförslag.

I rapporten ska särskilt följande bedömas:

a) Tillämpningen av och funktionssättet för de regler om sanktioner som medlemsstaterna fastställt i enlighet med artikel 34.

b) I vilken utsträckning de rättsliga företrädarna för leverantörer av dataförmedlingstjänster och erkända dataaltruismorganisationer som inte är etablerade i unionen efterlever denna förordning, och i vilken utsträckning de sanktioner som åläggs är verkställbara på dessa leverantörer och organisationer.

c) Vilken typ av dataaltruismorganisationer som registrerats i enlighet med kapitel IV, samt en översikt av för vilka mål av allmänt intresse datadelning förekommer, för att tydliga kriterier för detta ska kunna fastställas.

Medlemsstaterna ska förse kommissionen med de uppgifter som är nödvändiga för att utarbeta den rapporten.

Artikel 36

Ändring av förordning (EU) 2018/1724

I tabellen i bilaga II till förordning (EU) 2018/1724 ska posten ”Starta företag och bedriva affärsverksamhet” ersättas med följande:

Livshändelser	Förfaranden	Förväntat resultat med förbehåll för den behöriga myndighetens bedömning av ansökan i enlighet med nationell rätt, där så är relevant
Starta företag och bedriva affärsverksamhet	Anmälan av affärsverksamhet, tillstånd för affärsverksamhet, ändring av affärsverksamhet och avslutande av affärsverksamhet utan insolvens- eller likvidationsförfaranden, undantaget inledande registrering av affärsverksamhet i företagsregistret och undantaget förfaranden för bildande eller senare anmälan av bolag i den mening som avses i artikel 54 andra stycket i EUF-fördraget	Bekräftelse på mottagande av anmälan eller ändring av – eller av ansökan om tillstånd för – affärsverksamhet
	Registrera en arbetsgivare (en fysisk person) i ett obligatoriskt pensions- och försäkringssystem	Bekräftelse på registrering eller socialförsäkringsnummer
	Registrera anställda i ett obligatoriskt pensions- och försäkringssystem	Bekräftelse på registrering eller socialförsäkringsnummer
	Lämna in en bolagsskattedeklaration	Bekräftelse på mottagande av deklarationen
	Meddela socialförsäkringssystemet när en anställds kontrakt avslutas, dock ej förfaranden för kollektivt avslutande av anställningskontrakt	Bekräftelse på mottagande av meddelandet
	Betala sociala avgifter för anställda	Kvitto eller annan form av bekräftelse på betalningen av sociala avgifter för anställda
	Anmälan som leverantör av dataförmedlingstjänster	Bekräftelse på mottagande av anmälan
	Registrering som dataaltruismorganisation som är erkänd i unionen	Bekräftelse av registreringen

Artikel 37

Övergångsbestämmelser

Enheter som tillhandahåller de dataförmedlingstjänster som avses i artikel 10 den 23 juni 2022 ska fullgöra de skyldigheter som fastställs i kapitel III senast den 24 september 2025.

Artikel 38

Ikraftträdande och tillämpning

Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

Den ska tillämpas från och med den 24 september 2023.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Bryssel den 30 maj 2022.

På Europaparlamentets vägnar	*På rådets vägnar*
R. METSOLA	B. LE MAIRE
Ordförande	*Ordförande*

Departementsserien 2023

Kronologisk f rteckning

1. Ändringar i regelverket om överlämnande enligt en europeisk och nordisk arresteringsorder. Ju.
2. Näringsförbud till följd av förbud att bedriva näringsverksamhet som har meddelats i en annan stat. KN.
3. Statens ansvar för det svenska flygplatssystemet. För tillgänglighet och beredskap. LI.
4. Frågor om val till Sametinget. Ku.
5. Natura 2000-tillstånd vid ansökan om bearbetningskoncession enligt minerallagen. KN.
6. Genomförande av det nya blåkortsdirektivet. Ju.
7. Tilläggsprotokoll 16 till Europakonventionen – en möjlighet för de högsta domstolarna att begära rådgivande yttrande från Europadomstolen. Ju.
8. Förslag på åtgärder för att skapa bättre förutsättningar för kliniska prövningar – för en bättre välfärd och en starkare life science-sektor. KN.
9. En säkrare tillgång till vattenreningskemikalier. LI.
10. En registerlag för Myndigheten för vård- och omsorgsanalys. S.
11. Skjutvapen och explosiva varor – skärpta straff för de allvarligare brotten. Ju.
12. Kontrollstation 2023. Fö.
13. En registerlag för Inspektionen för socialförsäkringen. S.
14. En översyn av vissa frågor om offentliga biträden. Ju.
15. Fler verktyg i socialtjänsternas arbete för att förebygga brott och stärka skyddet för barn. S.
16. Avtal med Finland om polissamarbete i gränsområdet. Ju.
17. Vistelseförbud på allmän plats och vissa andra platser. Ju.
18. Stärkt hyresrättsligt skydd för våldsutsatta kvinnor. Ju.
19. Allvarstid. Försvarsberedningens säkerhetspolitiska rapport 2023. Fö.
20. Utökade befogenheter på särskilda ungdomshem och LVM-hem. S.
21. En modern lagstiftning för Kriminalvårdens personuppgiftsbehandling. Ju.
22. Sveriges tillträde till vissa Natoavtal. Fö.
23. Uppdrag att möjliggöra bättre tillgång till hälso- och sjukvård i hela landet genom främjande av etablering i glesbygd. S.
24. Genomförande av EU:s dataförvaltningsförordning. Fi.

Departementsserien 2023

Systematisk f rteckning