Yttrande 5/2023 om Europeiska kommissionens utkast till genomförandebeslut om ett adekvat skydd för personuppgifter enligt EU:s och USA:s ram för dataskydd

Antaget den 28 februari 2023

Sammanfattning

Den 13 december 2022 offentliggjorde Europeiska kommissionen ett utkast till beslut om adekvat skyddsnivå (*utkastet till beslut*), vars bilagor utgör en ny ram för transatlantiskt utbyte av personuppgifter, ramen för dataskydd mellan EU och USA (*dataskyddsramen*). Dataskyddsramen är avsedd att ersätta den tidigare gällande skölden för skydd av privatlivet, som ogiltigförklarades av Europeiska unionens domstol (*EU-domstolen*) den 16 juli 2020, i Schrems II-målet. Den viktigaste beståndsdelen i dataskyddsramen är dess principer, inbegripet de kompletterande principerna (nedan tillsammans kallade *ramens principer*).

I enlighet med artikel 70.1 s i Europaparlamentets och rådets förordning (EU) 2016/679[1] (*dataskyddsförordningen*) begärde kommissionen ett yttrande från Europeiska dataskyddsstyrelsen (*dataskyddsstyrelsen*) om utkastet till beslut.

Dataskyddsstyrelsen har, genom att granska utkastet till beslut, gjort en bedömning av huruvida den skyddsnivå som upprätthålls i USA är adekvat. Vid sin bedömning har dataskyddsstyrelsen vägt in såväl kommersiella aspekter som amerikanskamyndigheters tillgång till och användning av personuppgifter som överförts från EU.

Dataskyddsstyrelsen har beaktat den tillämpliga rättsliga ramen för dataskydd i EU, så som denna fastställs i dataskyddsförordningen, liksom den grundläggande rätt till privatliv och dataskydd som stadfästs i artiklarna 7 och 8 i Europeiska unionens stadga om de grundläggande rättigheterna och artikel 8 i den europeiska konventionen om de mänskliga rättigheterna. Dataskyddsstyrelsen har också beaktat den rätt till ett effektivt rättsmedel och till en opartisk domstol som fastställs i artikel 47 i stadgan, samt rättspraxis i fråga om de olika grundläggande rättigheterna.

Därtill har dataskyddsstyrelsen tagit hänsyn till kraven i den referensram för adekvat skyddsnivå som styrelsen antagit[2].

Dataskyddsstyrelsens främsta mål är att lämna ett yttrande till kommissionen om adekvat skyddsnivå för enskilda personer vilkas personuppgifter överförs till Förenta staterna (*USA*). Det är viktigt att notera att dataskyddsstyrelsen inte förväntar sig att den amerikanska ramen för dataskydd ska spegla den europeiska dataskyddslagstiftningen.

Dataskyddsstyrelsen påminner dock om att artikel 45 i dataskyddsförordningen och EU-domstolens rättspraxis kräver att ett tredjelands lagstiftning säkerställer en skyddsnivå för de registrerade som i huvudsak motsvarar EU:s för att landet ska anses erbjuda adekvat skyddsnivå.

1.1 Allmänna dataskyddsaspekter

Enligt dataskyddsramen får ramorganisationers efterlevnad av ramens principer begränsas i vissa fall (exempelvis till vad som krävs för att följa ett domstolsbeslut eller tillgodose allmänintresset). För att bättre kunna avgöra hur dessa undantag påverkar skyddsnivån för de registrerade rekommenderar

[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) (EUT L 119, 4.5.2016, s. 1).

[2] Artikel 29-gruppen, Referensram för adekvat skyddsnivå, WP 254 rev.01, 28 november 2017, senast reviderad och antagen den 6 februari 2018 och godkänd av dataskyddsstyrelsen den 25 maj 2018 (nedan kallad *referensramen för adekvat skyddsnivå*).

dataskyddsstyrelsen att kommissionen i utkastet till beslut medtagit ett förtydligande av undantagens omfattning, däribland tillämpliga skyddsåtgärder enligt amerikansk lag.

Dataskyddsstyrelsen konstaterar att bilagornas struktur och numrering gör det relativt svårt att hitta och hänvisa till informationen. Detta bidrar till en generellt sett komplex presentation av den nya ramen, i vars bilagor handlingar med olika rättsverkan blandas, och ger kanske inte de registrerade, de organisationer som omfattas av ramen och EU:s dataskyddsmyndigheter de bästa förutsättningarna att skapa sig en god förståelse av ramens principer. Dataskyddsstyrelsen betonar även att terminologin bör användas konsekvent i hela ramen. Vidare saknas definitioner av vissa centrala termer[3].

Dataskyddsstyrelsen välkomnar uppdateringarna av ramens principer[4], vilka utgör det bindande rättsliga ramverket för de organisationer som omfattas av ramen. Dataskyddsstyrelsen konstaterar dock att de principer som organisationerna måste följa, trots ett antal ändringar och ytterligare förtydliganden i skälen i utkastet till beslut, förblir i huvudsak oförändrade jämfört med de principer som gällde enligt skölden för skydd av privatlivet (som låg till grund för artikel 29-gruppens och dataskyddsstyrelsens årliga gemensamma översyner). Ramens principer är också i stor utsträckning desamma som principerna i det utkast till sköld för skydd av privatlivet som artikel 29-gruppen kommenterade i sitt yttrande från 2016[5]. När det gäller de av ramens principer som är i stort sett oförändrade ser dataskyddsstyrelsen inget behov av att upprepa alla de synpunkter som tidigare lämnats av artikel 29-gruppen. Dataskyddsstyrelsen har beslutat att fokusera på särskilda aspekter som den uppfattar som än mer relevanta i dag, med tanke på hur den tekniska och rättsliga miljön har utvecklats.

Exempelvis konstaterar dataskyddsstyrelsen att vissa av de problem som tidigare lyfts av artikel 29-gruppen och dataskyddsstyrelsen vad gäller principerna för skölden för skydd av privatlivet kvarstår. Det gäller i synnerhet registrerades rättigheter (t.ex. vissa undantag från rätten till tillgång och tidpunkten och formerna för rätten att göra invändningar), avsaknaden av definitioner av viktiga termer, bristen på tydlighet när det gäller principernas tillämpning på personuppgiftsbiträden samt det breda undantaget för allmänt tillgängliga uppgifter[6].

Dataskyddsstyrelsen vill också upprepa att skyddsnivån för enskilda personer vars uppgifter överförs inte får undergrävas genom vidare överföringar från den ursprungliga mottagaren av de överförda uppgifterna[7]. Dataskyddsstyrelsen uppmanar än en gång kommissionen att klargöra att de skyddsåtgärder som den ursprungliga mottagaren kräver av införaren i tredjelandet måste vara giltiga mot bakgrund av lagstiftningen i tredjelandet, innan en vidare överföring enligt dataskyddsramen kan ske.

Den snabba utvecklingen på området för automatiserat beslutsfattande och profilering – i allt större utsträckning med hjälp av AI-teknik – kräver särskild uppmärksamhet. Dataskyddsstyrelsen gläder sig därför åt att kommissionen tar upp de särskilda skyddsåtgärder som amerikansk lag inom olika

---

[3] Det gäller t.ex. termerna ”agent” (förmedlare) och ”processor” (personuppgiftsbiträde). Det finns också fortfarande ett behov av att diskutera begreppet ”human resources (HR) data” (personaluppgifter) med de amerikanska myndigheterna.

[4] Exempelvis förtydligandet att kodade uppgifter utgör personuppgifter.

[5] Artikel 29-gruppens yttrande 01/2016 om utkastet till beslut om adekvat skydd genom skölden för skydd av privatlivet i EU och USA av den 13 april 2016 (nedan kallat *artikel 29-gruppens yttrande 01/2016*).

[6] *EU-U.S. Privacy Shield - Third Annual Joint Review*, rapport från Europeiska dataskyddsstyrelsen antagen den 12 november 2019, punkt 11.

[7] Referensramen för adekvat skyddsnivå, 3.A.9.

områden föreskriver[8]. Skyddsnivån för enskilda verkar dock variera beroende på vilka branschspecifika regler – om några – som är tillämpliga på den aktuella situationen. Dataskyddsstyrelsen vidhåller att det krävs särskilda regler för automatiserat beslutsfattande för att uppnå tillräckliga skyddsåtgärder, inbegripet rätt för den enskilde att känna till den logik som tillämpas, att bestrida beslutet och att få mänsklig kontakt när beslutet i väsentlig grad påverkar honom eller henne.

Dataskyddsstyrelsen påminner om vikten av effektiv tillsyn och efterlevnad av dataskyddsramen och anser att efterlevnadskontroller avseende de mer väsentliga kraven är avgörande. Dataskyddsstyrelsen kommer att övervaka dessa aspekter noga, även i samband med de regelbundna översynerna. Dataskyddsstyrelsen noterar de förnyade åtaganden avseende verkställandet av dataskyddsramen som görs i skrivelserna från federala konkurrensmyndigheten[9] och transportdepartementet[10], såsom att prioritera utredning av påstådda överträdelser av dataskyddsramen.

Dataskyddsstyrelsen konstaterar att registrerade från EU erbjuds sju olika möjligheter till prövning om deras personuppgifter skulle behandlas i strid med dataskyddsramen. Dessa prövningsmekanismer är desamma som de som ingick i den tidigare skölden för skydd av privatlivet och som redan har kommenterats av artikel 29-gruppen[11]. Dataskyddsstyrelsen kommer att noggrant övervaka dessa prövningsmekanismers effektivitet, bland annat i samband med de regelbundna översynerna.

1.2 Amerikanska myndigheters tillgång till och användning av personuppgifter som överförts från EU

I utkastet till beslut kommer kommissionen till slutsatsen att de eventuella ingrepp i de grundläggande rättigheterna för enskilda vilkas personuppgifter överförs från EU till USA i enlighet med dataskyddsramen som amerikanska myndigheter gör för allmännyttiga ändamål, särskilt i straffrättsliga syften som rör brottsbekämpning och den nationella säkerheten, kommer att begränsas till vad som är absolut nödvändigt för att uppnå det legitima målet i fråga, och att det finns ett effektivt rättsligt skydd mot sådana ingrepp[12].

Europeiska kommissionen kommer fram till sin slutsats efter en omfattande bedömning av presidentdekret 14086 om stärkta skyddsåtgärder för amerikansk signalspaning (*dekret 14086*). Dekret 14086 utfärdades av USA:s president den 7 oktober 2022, efter förhandlingar mellan Europeiska kommissionen och USA:s regering efter EU-domstolens ogiltigförklarande av det tidigare beslutet om adekvat skyddsnivå, skölden för skydd av privatlivet.

Dataskyddsstyrelsen skulle gärna se att inte endast ikraftträdandet utan även antagandet av beslutet gjordes avhängigt att alla amerikanska underrättelsetjänster antar aktualiserade regler och förfaranden för att genomföra dekret 14086. Dataskyddsstyrelsen rekommenderar kommissionen att utvärdera dessa uppdaterade regler och förfaranden och låta dataskyddsstyrelsen ta del av utvärderingen.

Vad gäller myndigheternas tillgång till personuppgifter som överförts till USA har dataskyddsstyrelsen inriktat sin analys på att utvärdera det nya dekretet 14086, eftersom det i praktiken är avsett att

[8] Utkastet till beslut, skäl 35.
[9] Utkastet till beslut, bilaga IV.
[10] Utkastet till beslut, bilaga V.
[11] Se särskilt artikel 29-gruppens yttrande 01/2016, avsnitt 2.2.6 a.
[12] Utkastet till beslut, skäl 195.

åtgärda de brister som EU-domstolen konstaterade i sin dom i Schrems II-målet, där det tidigare beslutet om adekvat skyddsnivå ogiltigförklarades.

Dataskyddsstyrelsen erkänner att USA:s rättsliga ram för signalspaning har ändrats genom antagandet av dekret 14086 och anser att de ytterligare skyddsåtgärder som införs genom dekretet innebär en betydande förbättring. Genom dekret 14086 införs begreppen nödvändighet och proportionalitet i den amerikanska rättsliga ramen för signalspaning, och, förutsatt att EU ges ställning som villkorsuppfyllande regional organisation för ekonomisk integration, också en ny prövningsmekanism för EU-medborgare. Dataskyddsstyrelsen menar att den nya prövningsmekanismen innebär en avsevärd förbättring jämfört med den så kallade ombudsmannamekanismen, som ingick i skölden till skydd för privatlivet. Till skillnad från den tidigare rättsliga ramen, som - vilket EU-domstolen uttryckligen påpekat - inte skapade några rättigheter för EU-medborgare, upprättas genom det nya dekretet 14086 sådana rättigheter. Genom dekretet införs också fler skyddsåtgärder vad avser oberoendet för domstolen för dataskyddsgranskning samt effektivare korrigerande befogenheter i händelse av överträdelser.

Emellertid har dataskyddsstyrelsen ändå, vid en jämförelse mellan de ytterligare skyddsåtgärder som införs genom dekret 14086 och det som dataskyddsstyrelsen angett som de europeiska nödvändiga garantierna (en standard som bygger på rättspraxis från EU-domstolen och Europeiska domstolen för de mänskliga rättigheterna (*Europadomstolen*)), i sin bedömning urskilt ett antal punkter som kräver förtydliganden eller ytterligare uppmärksamhet eller som ger upphov till oro. Dessa punkter återspeglar det faktum att dataskyddsstyrelsens bedömning, trots att dess yttrande bygger på Schrems II-domen, med nödvändighet omfattar överväganden som går utöver de specifika slutsatser som dras i den domen.

Dataskyddsstyrelsen anser att det finns vissa oklarheter i den amerikanska rättsliga ramen, särskilt avseende ”tillfällig bulkinsamling” och vidare lagring och spridning av uppgifter som samlats in (genom bulkinsamling), som behöver redas ut ytterligare.

Eftersom kravet på väsentlig likvärdighet inte innebär att reglerna måste vara identiska och eftersom skyddsåtgärderna i den nya rättsliga ramen för signalspaning faktiskt har stärkts fokuserar dataskyddsstyrelsen främst på att göra en samlad bedömning av skyddsåtgärderna, enligt en övergripande metod som omfattar hela behandlingscykeln, från insamling till spridning av uppgifter, inklusive tillsyns- och prövningsaspekter.

I detta sammanhang betonar dataskyddsstyrelsen följande slutsatser:

Dataskyddsstyrelsen konstaterar att begreppen nödvändighet och proportionalitet genom dekret 14086 införs i den rättsliga ramen för signalspaning, men vill understryka behovet av att noga övervaka vilka effekter dessa ändringar får i praktiken, t.ex. vad gäller översyn av interna riktlinjer och förfaranden i syfte att genomföra dekretets skyddsåtgärder på myndighetsnivå.

Dataskyddsstyrelsen välkomnar också det faktum att dekret 14086 innehåller en förteckning över specifika ändamål för vilka insamling får respektive inte får ske, men noterar också att ytterligare – inte nödvändigtvis offentliga – mål får läggas till om utvecklingen avseende den nationella säkerheten så kräver.

Aspekter som dataskyddsstyrelsen fastställt vara brister i den nuvarande ramen är i synnerhet det faktum att den amerikanska rättsliga ramen, i och med att den medger bulkinsamling av uppgifter i enlighet med presidentdekret 12333, saknar krav på förhandsgodkännande från en oberoende myndighet, vilket krävs enligt senaste rättspraxis från Europadomstolen, samt att den saknar

bestämmelser om systematisk oberoende efterhandsgranskning av domstol eller liknande oberoende organ. När det gäller oberoende förhandsgodkännanden i enlighet med section 702 i lagen om underrättelseverksamhet och övervakning utomlands (*Foreign Intelligence Surveillance Act*, Fisa) beklagar dataskyddsstyrelsen att domstolen för övervakning av utländsk underrättelseinformation (*Foreign Intelligence Surveillance Court*, FISC) vid sin behandling av ansökningar om certifiering av program med inriktning på utländska medborgare inte gör någon bedömning av efterlevnaden av dekret 14086, trots att de underrättelsemyndigheter som ska genomföra programmen är bundna av dekret 14086. Dataskyddsstyrelsen anser att de ytterligare skyddsåtgärder som detta dekret innehåller icke desto mindre bör beaktas, även av FISC. Dataskyddsstyrelsen erinrar om att rapporter från styrelsen för tillsyn av personlig integritet och medborgerliga friheter (*Civil Liberties Oversight Board*, PCLOB) skulle vara ett särskilt användbart verktyg för att bedöma hur skyddsåtgärderna i dekret 14086 genomförs och hur de tillämpas när uppgifter samlas in i enlighet med section 702 i Fisa och med dekret 12333.

När det gäller prövningsmekanismen erkänner dataskyddsstyrelsen att domstolen för dataskyddsgransknings (*Data Protection Review Court*, DPRC) befogenheter och stärkta oberoende innebär betydande förbättringar jämfört med den tidigare ombudsmannamekanismen. Dataskyddsstyrelsen erkänner också de ytterligare skyddsåtgärder som införs genom den nya prövningsmekanismen, t.ex. de särskilda advokaterna som bl.a. ska företräda klagandens intressen och PCLOB:s granskning av prövningsmekanismen. Även med beaktande av nationella säkerhetsaspekter och de skyddsåtgärder som införs genom dekret 14086 anser dataskyddsstyrelsen att den generella användningen av domstolen för dataskyddsgransknings standardsvar, där den klagande meddelas att domstolen antingen inte har konstaterat några överträdelser som omfattas av regelverket eller har utfärdat ett beslut med krav på lämpliga korrigerande åtgärder, i kombination med avsaknaden av möjlighet att överklaga, utgör en källa till oro. Med tanke på prövningsmekanismens betydelse uppmanar dataskyddsstyrelsen kommissionen att noga övervaka hur denna mekanism fungerar i praktiken.

Dataskyddsstyrelsen förväntar sig att kommissionen lever upp till sitt åtagande att dra tillbaka, ändra eller upphäva beslutet om adekvat skyddsnivå vid tvingande skäl till skyndsamhet, särskilt om den verkställande makten i USA skulle besluta om begränsningar av de skyddsåtgärder som ingår i presidentdekretet[13].

Generellt sett noterar dataskyddsstyrelsen med tillfredsställelse de betydande förbättringar som presidentdekretet innebär jämfört med den tidigare rättsliga ramen, i synnerhet införandet av nödvändighets- och proportionalitetsprinciperna och den individuella prövningsmekanismen för registrerade i EU. Med tanke på de farhågor som uttryckts och de förtydliganden som krävs föreslår dataskyddsstyrelsen att farhågorna tas upp till diskussion och att kommissionen gör de förtydliganden som begärts, i syfte att lägga en fastare grund för utkastet till beslut och säkerställa att det praktiska genomförandet av den nya rättsliga ramen, i synnerhet de skyddsåtgärder den omfattar, övervakas noggrant vid kommande gemensamma översyner.

[13] Utkastet till beslut, skäl 212.

Innehållsförteckning

Europeiska dataskyddsstyrelsen

Europeiska dataskyddsstyrelsen har antagit följande yttrande

med beaktande av artikel 70.1 s i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (*dataskyddsförordningen*)[1],

med beaktande av EES-avtalet, särskilt bilaga XI och protokoll 37, ändrat genom gemensamma EES-kommitténs beslut nr 154/2018 av den 6 juli 2018[2], och

med beaktande av artiklarna 12 och 22 i arbetsordningen.

HÄRIGENOM FRAMFÖRS FÖLJANDE.

1 INLEDNING

1.1 USA:s dataskyddsram

1. Förenta staterna (*USA*) och Europeiska unionen (*EU*) närmar sig frågor om skyddet av privatlivet och personuppgifter på olika sätt. Medan skyddet av privatlivet och personuppgifter i EU är grundläggande rättigheter, stadfästa i artiklarna 7 och 8 i den europeiska stadgan om de grundläggande rättigheterna, ses dataskydd i USA i allmänhet som en fråga om konsumentskydd. Till följd av detta tillämpar USA och EU olika regleringsmetoder[3].

2. Till skillnad från EU:s övergripande strategi i form av dataskyddsförordningen har USA ingen övergripande, generell lag om dataskydd på federal nivå. Skyddet av privatlivet sköts i stället branschvis eller på delstatsnivå. Exempelvis omfattas vissa branscher av särskilda lagar, såsom

   - lagen om rätt till sjukförsäkring och ersättning (*Health Insurance Portability and Accountability Act*, HIPAA).[4]

[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) (Text av betydelse för EES) (EUT L 119, 4.5.2016, s. 1).
[2] Hänvisningar till ”medlemsstater” i detta yttrande ska förstås som hänvisningar till ”medlemsstater i EES”.
[3] Se även kommissionens utkast till genomförandebeslut i enlighet med Europaparlamentets och rådets förordning (EU) 2016/679 om ett adekvat skydd för personuppgifter enligt EU:s och USA:s ram för dataskydd, offentliggjort den 13 december 2022 (nedan kallat *utkastet till beslut*), bilaga I, avsnitt I.
[4] Lagen om rätt till sjukförsäkring och ersättning (*Health Insurance Portability and Accountability Act*, HIPAA) från 1996 är en amerikansk federal lag. Den föreskriver nationella standarder som syftar till att skydda patienters känsliga hälsouppgifter. Lagen syftar till att ge ett tillräckligt skydd för enskildas hälsouppgifter och samtidigt tillåta att hälsouppgifter utbyts i syfte att ge och främja vård av hög kvalitet. HIPAA reglerar användning och röjande av hälsouppgifter för enheter som omfattas av Privacy Rule. Lagen innehåller också normer för enskilda personers rätt att förstå och kontrollera hur deras hälsouppgifter används. https://www.hhs.gov/hipaa/for-professionals/privacy/index.html; https://www.justice.gov/opcl/privacy-act-1974.

- lagen om integritetsskydd för barn i samband med direkttjänster (*Children's Online Privacy Protection Act*, COPPA)[5]
- Gramm-Leach-Billey-lagen (*Gramm-Leach-Billey Act*, GLBA)[6]

3. För myndigheternas tillgång till personuppgifter som överförs från EU till USA gäller ett antal olika rättsliga grunder, begränsningar och skyddsåtgärder. De rättsliga förfarandena för tillgång till uppgifter för brottsbekämpande ändamål härrör antingen direkt från den amerikanska konstitutionen (fjärde tillägget), från lagstiftning och rättspraxis eller från regler och riktlinjer från justitiedepartementet på federal eller delstatlig nivå. Tillgången till uppgifter för nationella säkerhetsändamål regleras i flera rättsliga instrument, i synnerhet Fisa, presidentdekret 12333, det nyligen antagna presidentdekret 14086 samt det dekret från justitieministern[7] genom vilket en domstol för dataskyddsgranskning (Data Protection Review Court) inrättas (*domstolen för dataskyddsgranskning* respektive *justitieministerns dekret*).

4. Den 13 december 2022 offentliggjorde kommissionen sitt utkast till genomförandebeslut enligt Europaparlamentets och rådets förordning (EU) 2016/679 om huruvida en adekvat skyddsnivå för personuppgifter säkerställs genom ramen för dataskydd mellan EU och USA (*utkastet till beslut*), i vars bilaga ramen för dataskydd mellan EU och USA (*dataskyddsramen*) återfinns. Av de skäl som förklaras ovan, grundas utkastet till beslut inte på någon specifik övergripande federal rättslig ram, utan på dataskyddsramen.

5. Dataskyddsramen fungerar enligt följande: *"Det amerikanska handelsdepartementet (departementet) utfärdar principerna för ramen för dataskydd mellan EU och USA, inklusive kompletterande principer, (nedan tillsammans kallade principerna) och bilaga I till principerna (bilaga I) i enlighet med sin lagstadgade befogenhet att främja och utveckla internationell handel (15 U.S.C. § 1512)*"[8].

6. Principerna togs fram i samråd med Europeiska kommissionen och företrädare för näringslivet och andra berörda parter i syfte att underlätta handel mellan EU och USA[9] och samtidigt säkerställa att registrerade åtnjuter en skyddsnivå som är väsentligen likvärdig med den som garanteras inom EU.

7. Principerna beskrivs som en central beståndsdel i dataskyddsramen. Å ena sidan erbjuds genom principerna en användningsklar mekanism för överföring av uppgifter från EU till USA. Å andra sidan

---

[5] COPPA syftar främst till att ge föräldrar kontroll över vilka personuppgifter som samlas in från deras barn under 13 år av operatörer som står bakom webbplatser och direkttjänster som riktar sig till barn (inklusive mobilappar och IoT-enheter såsom smarta leksaker) eller till en allmän publik. Enligt COPPA måste dessa operatörer underrätta barnens föräldrar och inhämta verifierbart samtycke från dem. Detta gäller även uppgifter från utländska barn om webbplatserna eller tjänsterna drivs från USA och omfattas av COPPA. Samtidigt gäller bestämmelserna även utländska webbplatser och tjänster om de riktar sig till barn i USA. Se https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#A.%20General%20Questions och utkastet till beslut, bilaga IV, s. 3.

[6] GLBA har som mål bl.a. att skydda konsumenternas integritet inom finanssektorn. Enligt lagen måste finansinstitut förklara sina metoder för informationsutbyte för kunderna samt vidta åtgärder för att skydda kundernas uppgifter (t.ex. för företag som regleras av den federala konkurrensmyndigheten (*Federal Trade Commission*, FTC) enligt dennas standarder för skydd av kunduppgifter). https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act.

[7] *Attorney General Order No. 5517-2022*, genom vilket amerikanska justitiedepartementets förordningar ändras i enlighet med vad som föreskrivs och godkänns i dekret 14086.

[8] Utkastet till beslut, bilaga I, avsnitt I.

[9] *Ibidem*.

omfattar principerna skyddsmekanismer och garantier för personuppgifter som överförs från EU till USA, i enlighet med EU-lagstiftningens krav.

8. Dataskyddsramen är endast tillämplig på amerikanska organisationer som genomfört självcertifiering enligt ramens krav (*organisationer som omfattas av ramen*). För närvarande är detta endast möjligt om de omfattas av den federala konkurrensmyndighetens eller transportdepartementets behörighet. I framtiden kan fler organ – med behörighet att övervaka genomförandet av ramens principer – komma att läggas till i en ny bilaga.

9. Det förklaras i ramens principer att dess villkor är verkställbara i) av den federala konkurrensmyndigheten i enlighet med section 5 i lagen om den federala konkurrensmyndigheten (*Federal Trade Commission Act*) som förbjuder illojala eller bedrägliga handlingar eller metoder i handeln och i verksamhet som påverkar handel[10], ii) av transportdepartementet i enlighet med 49 U.S.C: § 41712 som förbjuder flygbolag och biljettåterförsäljare att tillämpa illojala eller bedrägliga metoder vid lufttransport eller försäljning av lufttransport eller iii) i enlighet med andra lagar och förordningar enligt vilka sådana handlingar är förbjudna.

10. Det påpekas i principerna att inte vare sig tillämpningen av dataskyddsförordningen eller befintliga bestämmelser om respekt som annars tillämpas i enlighet med amerikansk lag begränsas av ramens principer.

1.2 Omfattning av dataskyddsstyrelsens bedömning

11. Utkastet till beslut återspeglar kommissionens bedömning av dataskyddsramen, som är resultatet av diskussioner med den amerikanska regeringen. Enligt artikel 70.1 s i dataskyddsförordningen förväntas dataskyddsstyrelsen avge ett yttrande över kommissionens slutsatser om adekvat skyddsnivå i ett tredjeland och, vid behov, sträva efter att ge förslag till åtgärder som kan avhjälpa eventuella problem.

12. Dataskyddsstyrelsen välkomnar de uppdateringar som gjorts av ramens principer[11], vilka kommer att utgöra den bindande rättsliga ramen för organisationer som omfattas av dataskyddsramen. Dataskyddsstyrelsen konstaterar dock också att principerna i allt väsentligt är de samma som de som gällde enligt skölden för skydd av privatlivet[12] (vilka utgjorde underlag för artikel 29-arbetsgruppens och dataskyddsstyrelsens årliga gemensamma översyner). Ramens principer är också i stor utsträckning desamma som principerna i det utkast till sköld för skydd av privatlivet på vilket artikel 29-gruppen grundade sitt yttrande från 2016[13] (*artikel 29-gruppens yttrande 01/2016*). När det gäller de av ramens principer som är i stort sett oförändrade ser dataskyddsstyrelsen inget behov av att upprepa alla de synpunkter som tidigare lämnats av artikel 29-gruppen. Dataskyddsstyrelsen har beslutat att fokusera på särskilda aspekter som den uppfattar som än mer relevanta i dag, med tanke på hur den tekniska och rättsliga miljön har utvecklats.

[10] 15 U.S.C. § 45 a.

[11] Exempelvis förtydligandet att kodade uppgifter utgör personuppgifter.

[12] Kommissionens genomförandebeslut (EU) 2016/1250 av den 12 juli 2016 enligt Europaparlamentets och rådets direktiv 95/46/EG om huruvida ett adekvat skydd säkerställs genom skölden för skydd av privatlivet i EU och Förenta staterna, EUT L 207, 1.8.2016, s. 1.

[13] Artikel 29-gruppens yttrande 01/2016 om utkastet till beslut om adekvat skydd genom skölden för skydd av privatlivet i EU och Förenta staterna av den 13 april 2016 (nedan kallat *artikel 29-gruppens yttrande 01/2016*).

13. I linje med EU-domstolens rättspraxis[14] handlar också en central del av analysen om det rättsliga regelverket för myndigheters tillgång till personuppgifter som överförs till USA.

14. Vid sin bedömning har dataskyddsstyrelsen beaktat den tillämpliga europeiska ramen för dataskydd, inbegripet artiklarna 7, 8 och 47 i EU:s stadga om de grundläggande rättigheterna (*stadgan*), genom vilka rätten till privatliv och familjeliv, rätten till skydd av personuppgifter respektive rätten till ett effektivt rättsmedel och en opartisk domstol skyddas, och artikel 8 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (*Europakonventionen*) genom vilken rätten till privatliv och familjeliv skyddas. Utöver ovanstående beaktade dataskyddsstyrelsen dataskyddsförordningens krav, relevant rättspraxis och den referensram för adekvat skyddsnivå som dataskyddsstyrelsen antagit (*referensramen för adekvat skyddsnivå*)[15].

15. Målet med detta arbete är att lämna ett yttrande till Europeiska kommissionen om bedömningen av huruvida dataskyddsramen säkerställer en adekvat skyddsnivå. Begreppet ”adekvat skyddsnivå” som fanns med redan i direktiv 95/46 har vidareutvecklats av EU-domstolen. Det är därför viktigt att påminna om den princip som fastställts av EU-domstolen i Schrems I-domen[16] (där Safe Harbor ogiltigförklaras) och Schrems II-domen[17] (där skölden för skydd av privatlivet ogiltigförklaras).

16. I Schrems I-domen fastslår EU-domstolen att medan ”skyddsnivån” i tredjelandet måste vara ”väsentligen likvärdig” med den som garanteras inom EU gäller att ”de medel som detta tredjeland använder för att säkerställa en sådan skyddsnivå kan skilja sig från dem som används inom unionen”[18]. Därför är målet inte att punkt för punkt efterlikna EU-lagstiftningen utan att fastställa de grundläggande och avgörande kraven i den lagstiftning som undersöks. Adekvat skyddsnivå kan uppnås genom en kombination av rättigheter för de registrerade och skyldigheter för de som behandlar personuppgifter, eller som utövar kontroll över sådan behandling, och övervakning av oberoende organ. Bestämmelser om skydd av personuppgifter är dock endast effektiva om de är verkställbara och följs i praktiken. Det är därför nödvändigt att inte bara se till innehållet i bestämmelserna för överföring av personuppgifter till ett tredjeland eller en internationell organisation utan också till de mekanismer som har inrättats för att säkerställa att dessa bestämmelser är verkningsfulla. Effektiva verkställighetsmekanismer är av avgörande betydelse för att få verkningsfulla bestämmelser om skydd av personuppgifter[19].

17. I Schrems II-domen finner EU-domstolen att de lagar som utgör grund för amerikanska underrättelsemyndigheters tillgång till personuppgifter som överförts till USA (section 702 i Fisa/dekret 12333) i oproportionerligt stor utsträckning begränsar de rättigheter som fastställs i artiklarna 7 och 8 i EU:s stadga om de grundläggande rättigheterna (*stadgan*) och att de därmed inte

[14] I synnerhet EU-domstolens dom av den 6 oktober 2015, Maximilian Schrems/Data Protection Commissioner, C-392/14, ECLI:EU:C:2015:650, och EU-domstolens dom av den 16 juli 2020, Data Protection Commissioner/Facebook Ireland Limited och Maximillian Schrems, C-311/18, ECLI:EU:C:2020:559.

[15] Artikel 29-gruppen, Referensram för adekvat skyddsnivå, WP 254 rev.01, 28 november 2017, senast ändrad och antagen den 6 februari 2018 och godkänd av dataskyddsstyrelsen den 25 maj 2018 (nedan kallad *referensramen för adekvat skyddsnivå*).

[16] EU-domstolens dom av den 6 oktober 2015, Maximilian Schrems/Data Protection Commissioner, C-392/14, ECLI:EU:C:2015:650 (nedan kallad *Schrems I-domen*).

[17] EU-domstolens dom av den 16 juli 2020, Data Protection Commissioner/Facebook Ireland Limited och Maximillian Schrems, C-311/18, ECLI:EU:C:2020:559 (nedan kallad *Schrems II-domen*).

[18] Schrems I-domen, punkterna 73–74.

[19] Referensramen för adekvat skyddsnivå s. 2.

är reglerade på ett sådant sätt att de uppfyller krav som är väsentligen likvärdiga med dem som uppställs i unionsrätten enligt artikel 52.1 andra meningen i stadgan[20].

18. Vidare konstaterade EU-domstolen att den tidigare rättsliga ramen inte gav garantier som var väsentligen likvärdiga med de som krävs enligt artikel 47 i stadgan, eftersom ombudsmannamekanismen inte kunde kompensera för det faktum att varken PPD-28 eller dekret 12333 ger utländska medborgare tillgång till ett effektivt rättsmedel[21]. Ombudsmannen var inte helt oberoende från den verkställande makten och saknade behörighet att fatta beslut som var bindande för de amerikanska underrättelsemyndigheterna[22].

19. Genom dekret 14086, som i stort ersätter PPD-28, infördes två nya krav enligt amerikansk lag som bär Schrems II-domens prägel: För det första ska signalspaning bedrivas endast i den utsträckning det är nödvändigt för att främja insamling av uppgifter till förmån för en godkänd underrättelseprioritering och då endast i en omfattning och på ett sätt som står i proportion till den godkända underrättelseprioriteringen. För det andra inrättas en prövningsmekanism.

20. I detta yttrande bedömer dataskyddsstyrelsen särskilt i vilken utsträckning dataskyddsramen och det nyligen antagna dekretet 14086 faktiskt avhjälper de brister som konstateras i EU-domstolens dom.

1.3 Allmänna kommentarer och frågor

1.3.1 Bedömning av den nationella lagstiftningen

21. Dataskyddsstyrelsen är medveten om att bedömningen i utkastet till beslut avser ramens principer. Icke desto mindre skulle dataskyddsstyrelsen välkomna en redogörelse för den amerikanska rättsliga kontext i vilken de organisationer som omfattas av ramen verkar. Detta skulle ge en bättre förståelse för hur ramen samspelar med den amerikanska lagen. Exempelvis fastställs det i bilaga I avsnitt I[23] att ramens principer inte heller ”begränsar […] de bestämmelser om respekt för privatlivet som annars är tillämpliga enligt amerikansk lag”, men det preciseras inte vilka dessa skyldigheter är.

1.3.2 Internationella åtaganden som ingåtts av USA

22. Enligt artikel 45.2 c i dataskyddsförordningen samt referensramen för adekvat skyddsnivå ska kommissionen vid bedömning av adekvat skyddsnivå i ett tredjeland bland annat beakta de internationella åtaganden som tredjelandet har gjort, eller andra skyldigheter som följer av tredjelandets deltagande i multilaterala eller regionala system, särskilt rörande skydd av personuppgifter, samt genomförandet av sådana skyldigheter.

23. USA har anslutit sig till flera internationella avtal som garanterar rätten till integritet, t.ex. den internationella konventionen om medborgerliga och politiska rättigheter (artikel 17), konventionen om rättigheter för personer med funktionsnedsättning (artikel 22) och konventionen om barnets rättigheter (artikel 16). Dessutom omfattas USA i egenskap av OECD-medlem av OECD:s ram för integritetsskydd, i synnerhet riktlinjerna för integritetsskydd och gränsöverskridande flöden av personuppgifter. Den 14 december 2022 antogs OECD:s förklaring om myndigheters tillgång till personuppgifter som lagras av enheter i den privata sektorn (*Declaration on Government Access to Personal Data held by Private Sector Entities*) av ministrar och företrädare på hög nivå från OECD:s

[20] Schrems II-domen, punkterna 184–185.
[21] Schrems II-domen, punkt 192.
[22] Schrems II-domen, punkt 195.
[23] Utkastet till beslut, bilaga I avsnitt I sista meningen.

medlemsländer samt Europeiska unionen. USA är också part i Budapestkonventionen om it-brottslighet.

24. Därutöver är USA medlem i Apecs (Ekonomiska samarbetet i Asien och Stillahavsområdet) system med gränsöverskridande integritetsskyddsregler (*Cross-Border Privacy Rules*, CBPR), som är ett statligt stött certifieringsprogram till vilket företag kan ansluta sig för att visa att de efterlever internationellt erkända regler för integritetsskydd. Dessa regler har godkänts av Apec-ländernas ledare.

25. Dataskyddsstyrelsen noterar också att USA deltar som observatörsstat i den rådgivande kommittén för Europarådets konvention 108.

26. Vidare noterar dataskyddsstyrelsen med glädje att amerikanska organ kontinuerligt deltar i G7:s nyligen inrättade rundabordsmöten för data- och intregritetsskyddsmyndigheter. Vid rundabordsmötena, som började hållas 2021, samlas oberoende dataskydds- och integritetsövervakningsmyndigheter från G7-länderna. I detta sammanhang har USA exempelvis ställt sig bakom den senaste kommunikén från G7:s rundabordssamarbete[24], som antogs den 8 september 2022 i Bonn i Tyskland och hade fokus på konceptet ”fria dataflöden med förtroende”.

1.3.3 Framsteg avseende USA:s dataskyddslagstiftning

27. Dataskyddsstyrelsen noterar särskilt den utveckling som ägt rum när det gäller dataskydds- och integritetslagstiftningen på delstatsnivå i USA. Dataskyddsstyrelsen ser positivt på det faktum att dataskyddslagar har antagits och trätt i kraft eller kommer att träda i kraft senast 2023 i fem delstater (Kalifornien, Colorado, Connecticut, Virginia och Utah)[25]..

28. Dataskyddsstyrelsen noterar också att motsvarande initiativ till ny lagstiftning redan tagits i många andra delstater.

29. Dataskyddsstyrelsen välkomnar också uttryckligen arbetet med tvåpartiinitiativet för en federal dataskyddslag, amerikanska data- och integritetsskyddslagen (*American Data Privacy and Protection Act*, ADPPA).

1.3.4 Omfattningen av utkastet till beslut

30. Enligt artikel 1 i utkastet till beslut drar kommissionen slutsatsen att USA säkerställer en adekvat skyddsnivå för personuppgifter som överförs från EU till de organisationer i USA som finns upptagna i den förteckning för dataskyddsramen (*Data Privacy Framework List*) som upprättas och offentliggörs av det amerikanska handelsdepartementet i enlighet med avsnitt I.3 i bilaga I[26].

---

[24] *Roundtable of G7 Data Protection and Privacy Authorities, Promoting Data Free Flow with Trust and knowledge sharing about the prospects for International Data Spaces*, 8 september 2022, https://www.bfdi.bund.de/SharedDocs/Downloads/EN/G7/Communique-2022.pdf?__blob=publicationFile&v=1.

[25] *California Consumer Privacy Act* (2018, i kraft sedan den 1 januari 2020), *California Privacy Rights Act* (2020, till fullo i kraft sedan den 1 januari 2023), *Colorado Privacy Act* (2021, träder i kraft den 1 juli 2023), *Connecticut Data Privacy Act* (2022, träder i kraft den 1 juli 2023), *Virginia Consumer Data Protection Act* (2021, i kraft sedan den 1 januari 2023), *Utah Consumer Privacy Act* (2022, träder i kraft den 31 december 2023).

[26] Utkastet till beslut, slutliga överväganden, artikel 1, s. 57. Dataskyddsstyrelsen förstår att utkastet till beslut inte omfattar överföringar från enheter som är belägna utanför EU men som ändå omfattas av dataskyddsförordningen i enlighet med dess artikel 3.2 till certifierade enheter i USA.

31. Dataskyddsramen är tillgänglig för företag som omfattas av den federala konkurrensmyndighetens (FTC) eller transportdepartementets (DoT) behörighet. Dataskyddsstyrelsen påpekar att fler lagstadgade organ med liknande befogenheter kan komma att läggas till i framtiden[27].

1.3.5 Begränsningar av skyldigheten att följa ramens principer

32. Enligt bilaga I, avsnitt I.5 kan de berörda organisationernas efterlevnad av ramens principer begränsas i) till vad som är nödvändigt för att uppfylla krav i fråga om allmänintresset, brottsbekämpningen[28] och den nationella säkerheten[29] (inbegripet fall där en lag eller myndighetsföreskrift skapar motstridiga skyldigheter) och ii) i enlighet med en lag, ett domstolsbeslut eller en myndighetsföreskrift som ger explicita befogenheter, förutsatt att den organisation som omfattas av ramen då den utövar dessa befogenheter kan visa att avvikelsen från ramens principer begränsar sig till vad som är nödvändigt för att de övergripande legitima intressen som är beroende av dessa befogenheter ska kunna tillgodoses.

33. Utan fullständiga kunskaper om amerikansk lag på såväl federal som delstatlig nivå är det svårt för dataskyddsstyrelsen att i detalj bedöma omfattningen av de undantag som anges i denna punkt. Därför rekommenderar dataskyddsstyrelsen att kommissionen i utkastet till beslut tar med ett förtydligande av undantagens omfattning, inbegripet tillämpliga skyddsåtgärder enligt amerikansk lag, i syfte att precisera dessa undantags inverkan på skyddsnivån för de registrerade. Dataskyddsstyrelsen understryker också att kommissionen bör hålla sig underrättad om och övervaka tillämpningen och antagandet av lagar eller myndighetsföreskrifter med påverkan på efterlevnaden av ramens principer.

1.3.6 Ändringar i förhållande till skölden för skydd av privatlivet

34. Dataskyddsstyrelsen välkomnar de ansträngningar som gjorts för att uppfylla kraven i Schrems II-domen. Det skulle dock ha varit glädjande om fler av de problem som konstaterats i) i artikel 29-gruppens yttrande 01/2016 och ii) i de tidigare gemensamma översynerna[30] också hade tagits upp vid förhandlingarna om dataskyddsramen.

35. Dataskyddsstyrelsen konstaterar också att principerna som ska följas av de organisationer som omfattas av ramen, trots att ett antal ändringar och ytterligare förtydliganden gjorts i skälen till utkastet till beslut, i allt väsentligt är oförändrade jämfört med principerna i skölden för skydd av privatlivet.

1.3.7 Bristande tydlighet i dataskyddsramens dokumentstruktur

36. Dataskyddsstyrelsen konstaterar att bilagornas struktur och numrering gör det relativt svårt att hitta och hänvisa till informationen. Detta bidrar till en generellt sett komplex presentation av den nya ramen, i vars bilagor handlingar med olika rättsverkan blandas, och ger kanske inte de registrerade, de

[27] Utkastet till beslut, bilaga I avsnitt I.2.

[28] Se avsnitt 3.1 i detta yttrande för ytterligare kommentarer rörande användningen av personuppgifter som omfattas av dataskyddsramen för brottsbekämpande ändamål.

[29] Se avsnitt 3.2 i detta yttrande för ytterligare kommentarer rörande användningen av personuppgifter som omfattas av dataskyddsramen för ändamål som rör den nationella säkerheten.

[30] Årliga översyner: *EU-U.S. Privacy Shield – First Annual Joint Review*, WP 255, artikel 29-arbetsgruppen, antagen den 28 november 2017 (nedan kallad *första gemensamma översynen*), *EU-U.S. Privacy Shield – Second Annual Joint Review*, rapport från Europeiska dataskyddsstyrelsen, antagen den 22 januari 2019 (nedan kallad *andra gemensamma översynen*), *EU-U.S. Privacy Shield – Third Annual Joint Review,* rapport från Europeiska dataskyddsstyrelsen, antagen den 12 november 2019 (nedan kallad *tredje gemensamma översynen*).

organisationer som omfattas av ramen och EU:s dataskyddsmyndigheter de bästa förutsättningarna att skapa sig en god förståelse av ramens principer.

37. Dataskyddsstyrelsen betonar också att terminologin bör användas konsekvent i hela ramen. Så är för närvarande inte fallet, till exempel när det gäller begreppet ”processing” (behandling). I vissa stycken räknar man endast upp ett antal typer av behandlingsåtgärder, i stället för att använda termen ”behandling”. Detta kan leda till rättslig osäkerhet och eventuellt till kryphål i skyddet[31].

38. Dataskyddsstyrelsen välkomnar det faktum att definitioner av vissa av de termer som används har medtagits i dataskyddsramen[32]. Så är dock inte fallet för vissa andra viktiga termer såsom ”agent” (förmedlare) och ”processor” (personuppgiftsbiträde), som enligt dataskyddsstyrelsen behöver definieras tydligt och specifikt i bilaga I, avsnitt I.8 i dataskyddsramen, på ett sätt som EU och USA är eniga om, i syfte att undvika förvirring i ett senare skede för organisationer som omfattas av och förlitar sig på ramen, tillsynsmyndigheter och allmänheten.

39. När det gäller frågan om skilda tolkningar i EU och USA av begreppet ”human resources (HR) data” (personaluppgifter) instämmer dataskyddsstyrelsen i kommissionens uppfattning, så som denna presenteras i kommissionens rapport om den tredje årliga översynen, att man bör eftersträva fortsatta diskussioner med amerikanska myndigheter[33].

2 ALLMÄNNA DATASKYDDSASPEKTER

2.1 Innehållsmässiga principer

2.1.1 Begrepp

40. Baserat på referensramen för adekvat skyddsnivå bör tredjelandets rättsliga ram innefatta grundläggande begrepp och/eller principer för dataskydd. Dessa begrepp behöver inte exakt återspegla terminologin i dataskyddsförordningen, men de bör avspegla och överensstämma med begreppen i EU:s dataskyddslagstiftning. Till exempel innehåller dataskyddsförordningen följande viktiga begrepp: ”personuppgifter”, ”behandling av personuppgifter”, ”personuppgiftsansvarig”, ”personuppgiftsbiträde”, ”mottagare” och ”känsliga uppgifter”. Dataskyddsstyrelsen välkomnar det faktum att termerna ”personuppgifter”, ”behandling” och ”personuppgiftsansvarig” definieras i dataskyddsramen, så som var fallet även med skölden för skydd av privatlivet.

41. Dataskyddsstyrelsen noterar att det fortfarande är oklart i vilken utsträckning ramens principer är tillämpliga på organisationer som omfattas av ramen och som tar emot personuppgifter från EU ”endast för behandling”. (Dessa kallas ”agents” (förmedlare) eller ”processors” (personuppgiftsbiträden)). Det görs i dataskyddsramen ingen skillnad mellan de principer som är

[31] Exempel: i) Enligt formuleringen i utkastet till beslut, bilaga I avsnitt III.6 f skulle ramens principer vara tillämpliga endast när organisationen ”lagrar, använder eller lämnar ut” de mottagna uppgifterna (och alltså inte vid andra åtgärder som omfattas av termen ”behandling”, såsom insamling, registrering, ändring, framtagning, läsning eller radering). ii) Enligt utkastet till beslut, bilaga I avsnitt II.4 a skulle datasäkerhet krävas endast när personuppgifter ”skapas, lagras, används eller sprids”.

[32] Utkastet till beslut, bilaga I avsnitt I.8.

[33] Tredje gemensamma översynen, s. 5, 15–16 och 30. Se även det arbetsdokument från kommissionens avdelningar som åtföljer rapporten om den tredje årliga översynen av skölden för skydd av privatlivet i EU och USA, s. 17–18.

tillämpliga på förmedlare respektive på personuppgiftsansvariga, trots att flera av de skyldigheter som ingår i ramens principer inte är lämpliga för förmedlare/personuppgiftsbiträden. Exempelvis bör en förmedlare/ett personuppgiftsbiträde inte kunna ge enskilda all den information som principen om meddelande kräver (såsom ändamålen för organisationens insamling och användning av deras personuppgifter)[34], eftersom en förmedlare/ett personuppgiftsbiträde inte självständigt kan fastställa behandlingens ändamål eller behandlingsmetoderna[35].

2.1.2 Principen om ändamålsbegränsning

42. Referensramen för adekvat skyddsnivå föreskriver, i enlighet med dataskyddsförordningen, att personuppgifter ska behandlas för ett specifikt ändamål och därefter användas endast i den mån användningen är förenlig med behandlingsändamålet.

43. Enligt principen om dataintegritet och ändamålsbegränsning får en organisation inte behandla personuppgifter på sätt som är oförenliga med de ändamål för vilka uppgifterna samlades in eller som den enskilda personen i ett senare skede har godkänt[36]. Dataskyddsstyrelsen konstaterar att den terminologi som används skiljer sig åt mellan principen om meddelande, principen om valmöjlighet och principen om dataintegritet och ändamålsbegränsning. Som artikel 29-gruppen redan påpekat och trots de relevanta förtydliganden som gjorts i skälen till utkastet till beslut används termer som ”andra ändamål”, ”ändamål som i sak skiljer sig” eller ”användning som inte överensstämmer med” i dataskyddsramen utan att tydliga definitioner anges, vilket kan leda till rättslig osäkerhet.

2.1.3 Rätt till tillgång, rättelse, radering och invändningar

44. I dataskyddsramen beaktas de registrerades rätt till tillgång, rättelse och radering genom tillgångsprincipen[37].

45. Tillgångsprincipen är densamma som i skölden för skydd av privatlivet. Vissa av de problem som fastställdes i artikel 29-gruppens yttrande 01/2016 är kvarstår därför.

46. När det gäller enskildas rätt till tillgång finner dataskyddsstyrelsen det nödvändigt att upprepa att den närmare beskrivningen av skyldigheten att besvara en begäran från en enskild person borde infogas i huvudtexten om principen (den återfinns fortfarande endast i en fotnot[38]).). Det bör också framgå tydligt att tillgång till personuppgifter ska ges i den mån en organisation som omfattas av ramen behandlar sådana uppgifter, och inte endast när den ”lagrar” dem[39]. Enligt dataskyddsstyrelsens mening skulle den nuvarande ordalydelsen kunna leda till en snäv tolkning av rätten till tillgång.

47. När det gäller förteckningen över undantag från rätten till tillgång[40] tenderar vissa av dessa fortfarande att förskjuta balansen till organisationernas fördel. Dataskyddsstyrelsens farhågor avseende det faktum att det i dessa fall inte tycks finnas något krav på att beakta den enskildes rättigheter och intressen kvarstår[41].

---

[34] Utkastet till beslut, bilaga I avsnitt II.1 a.
[35] Se även artikel 29-gruppens yttrande 01/2016, s. 16.
[36] Utkastet till beslut, bilaga I avsnitt II.5.
[37] Utkastet till beslut, bilaga I avsnitten II.6 och III.8 a i.
[38] Utkastet till beslut, bilaga I avsnitt III.8 a i 1 – fotnot 14.
[39] Utkastet till beslut, bilaga I avsnitt III.8 d ii.
[40] Utkast till beslut, bilaga I avsnitt III.8 e.
[41] Artikel 29-gruppens yttrande 01/2016, punkt 2.2.5.

48. Ett annat undantag, som tidigare har varit föremål för oro från artikel 29-gruppens sida[42] och som för dataskyddsstyrelsen framstår som för brett i sin omfattning, är det undantag från rätten till tillgång som gäller uppgifter som är offentligt tillgängliga och uppgifter från offentliga register[43]. Dataskyddsstyrelsen har upprepade gånger påpekat ett att registrerade enligt EU-lagstiftningen alltid har rätt att få tillgång till sina uppgifter, oavsett om personuppgifterna har offentliggjorts eller inte. Om begäranden om tillgång skulle avvisas på grund av att uppgifterna har hämtats från offentligt tillgängliga källor eller offentliga register skulle enskilda förlora sin möjlighet att kontrollera att uppgifterna är korrekta eller att de har offentliggjorts på ett lagenligt sätt i första läget.

49. Dataskyddsstyrelsen påminner om att rätten till tillgång fastställs i artikel 8.2 i stadgan. Denna rättighet är visserligen inte absolut, men den är grundläggande för rätten till skydd av personuppgifter, eftersom den gör det lättare för den registrerade att utöva andra rättigheter, såsom rätten till korrigering, radering och invändningar[44].

50. Utöver rätten till tillgång och radering bör registrerade ha rätt att när som helst, av tvingande berättigade skäl gällande deras specifika situation, invända mot behandling av deras uppgifter som sker baserat på särskilda villkor som anges i tredjelandets rättsliga ram[45].

51. Genom principen om valmöjlighet fastställs i dataskyddsramen en rätt att invända (*opt-out*) mot utlämnande av personuppgifter till en tredje part eller användning av personuppgifter för ett ändamål som i sak skiljer sig från det ursprungliga[46]. Enskilda har dessutom rätt att när som helst undantas (opt-out) från användning av personuppgifter för direktmarknadsföring[47]. Med undantag för direktmarknadsföring saknas närmare bestämmelser om tidpunkten för utövandet av rätten att invända. Dataskyddsstyrelsen uppmanar därför kommissionen att klargöra på vilket sätt enskilda kan utöva sin rätt att invända.

52. Så som anges i artikel 29-gruppens yttrande 01/2016 anser dataskyddsstyrelsen att en enkel hänvisning till denna rätt i integritetspolicyn inte kan vara tillräckligt. En individualiserad möjlighet att utöva denna rätt bör erbjudas inte bara vid utlämnande eller vidareutnyttjande av personuppgifter. Dataskyddsstyrelsen betonar att dataskyddsramen borde innefatta en allmän rätt för den registrerade att invända av tvingande berättigade skäl gällande hans eller hennes specifika situation. Dataskyddsstyrelsen rekommenderar att en sådan rätt att invända ska vara garanterad den registrerade vid varje givet tillfälle och inte bara i relation till användning av uppgifter för direktmarknadsföring[48].

53. När det gäller personaluppgifter uppskattar dataskyddsstyrelsen kommissionens förtydliganden avseende tillämpningen av principerna för meddelande och för valmöjlighet på situationer där certifierade amerikanska organisationer avser använda personaluppgifter för ett annat, icke-anställningsrelaterat, ändamål, såsom marknadsföringskommunikation[49]. Dataskyddsstyrelsen vidhåller dock att ytterligare behandling av personaluppgifter för andra ändamål än

[42] Artikel 29-gruppens yttrande 01/2016, punkt 2.2.9.
[43] Utkastet till beslut, bilaga I, III.15 d–e.
[44] Artikel 29-gruppens yttrande 01/2016, punkt 2.2.5.
[45] Referensramen för adekvat skyddsnivå, kapitel 3.A.8.
[46] Utkastet till beslut, bilaga I avsnitt II.2 a.
[47] Utkastet till beslut, bilaga I avsnitt III.12. a.
[48] Artikel 29-gruppens yttrande 01/2016, punkt 2.2.2.
[49] Utkastet till beslut, bilaga I avsnitt III.9.b i skäl 15 och fotnot 27.

anställningsrelaterade i de flesta fall kommer att anses vara oförenlig med det ursprungliga syftet, och att ett samtycke som lämnas i ett anställningssammanhang sällan är helt fritt.

54. Dataskyddsstyrelsen delar också de farhågor som artikel 29-gruppen uttryckt när det gäller det undantag från principerna för meddelande och valmöjlighet i relation till personaluppgifter som medges ”i den utsträckning och under den period det krävs för att undvika inverkan på organisationens kapacitet till befordringar, tillsättande av tjänster eller liknande anställningsbeslut”[50], vilket dataskyddsstyrelsen uppfattar som brett och vagt[51].

2.1.4 Begränsningar av vidare överföringar

55. Vidare överföring av personuppgifter från mottagaren av den ursprungliga överföringen ska endast tillåtas när nästa mottagare (det vill säga mottagaren av den vidare överföringen) också omfattas av bestämmelser (inklusive avtalsbaserade bestämmelser) som ger en adekvat skyddsnivå och följer relevanta instruktioner vid behandling av uppgifter på den personuppgiftsansvariges uppdrag. Skyddsnivån för de enskilda vars personuppgifter överförs får inte undergrävas av den vidare överföringen. Den första mottagaren av uppgifter som överförs från EU ska vara skyldig att säkerställa att lämpliga skyddsåtgärder vidtas för vidare överföringar av uppgifter i avsaknad av ett beslut om adekvat skyddsnivå. Sådana vidare överföringar av uppgifter ska endast göras för begränsade och specificerade ändamål och bara så länge det finns en rättslig grund för behandlingen[52].

56. Enligt dataskyddsramens princip om ansvar för vidare överföring får vidare överföringar göras endast för begränsade och specificerade ändamål på grundval av ett avtal mellan organisationen som omfattas av ramen och den tredje parten (alternativt ett jämförbart arrangemang inom en företagskoncern) och endast om det avtalet kräver att den tredje parten säkerställer samma skyddsnivå som den som garanteras av ramens principer[53].

57. Dataskyddsstyrelsen vill upprepa de farhågor som uttrycks i artikel 29-arbetsgruppens yttrande 01/2016 gällande undantaget från kravet att ingå avtal vid koncerninterna överföringar mellan personuppgiftsansvariga[54]. Dataskyddsstyrelsen förstår fortfarande inte den logiska grunden till undantaget från kravet att ingå ett avtal med tredjepartens personuppgiftsansvariga i fall där det rör sig om vidare överföring i samband med ”tillfälliga anställningsbehov”[55].

58. Dataskyddsstyrelsen vill också upprepa artikel 29-gruppens begäran[56] om att organisationer som är bundna av dataskyddsramen före en överföring ska göra en bedömning för att säkerställa att de obligatoriska krav i tredjelandets lagstiftning som är tillämpliga på mottagaren inte undergräver kontinuiteten i skyddet av de registrerade vars uppgifter överförs[57].

---

[50] Utkastet till beslut, bilaga I avsnitt III.9.b iv.
[51] Artikel 29-gruppens yttrande 01/2016, punkt 2.2.7.
[52] Referensramen för adekvat skyddsnivå, kapitel 3.A.9.
[53] Utkastet till beslut, bilaga I, II.3.
[54] Utkastet till beslut, bilaga I, III.10.b i, där det hänvisas till ”andra koncerninterna instrument (t.ex. efterlevnads- och kontrollprogram”), vilka uppenbarligen inte behöver vara bindande, som alternativ.
[55] Utkastet till beslut, bilaga I, III.9.e i, där exempel som försäkringstäckning tas upp.
[56] Artikel 29-gruppens yttrande 01/2016, punkt 2.2.3, s. 21.
[57] Mot bakgrund av Schrems II-domen har dataskyddsstyrelsen i ett antal riktlinjer och rekommendationer ytterligare klargjort de skyldigheter som åligger uppgiftsutförare och uppgiftsinförare i samband med vidare överföringar; se dataskyddsstyrelsens Rekommendationer 01/2020 om åtgärder som kompletterar överföringsverktygen för att säkerställa en efterlevnad av EU:s skyddsnivå för personuppgifter (version 2.0, antagna den 18 juni 2021), Rekommendationer 02/2020 om europeiska nödvändiga garantier för

59. Dataskyddsstyrelsen vidhåller att vidare överföringar av personuppgifter till tredjeländer skulle kunna leda till kränkningar av enskildas grundläggande rättigheter och uppmanar kommissionen att klargöra att de skyddsåtgärder som den ursprungliga mottagaren kräver av införaren i tredjelandet måste vara giltiga mot bakgrund av lagstiftningen i tredjelandet, innan en vidare överföring enligt dataskyddsramen kan ske[58].

2.1.5 Automatiserat beslutsfattande och profilering

60. Beslut som enbart baseras på automatisk behandling (automatiserat individuellt beslutsfattande), inklusive profilering, som får rättsliga följder för eller i betydande grad påverkar den registrerade, får endast äga rum under vissa villkor som fastställs i tredjelandets rättsliga ramar. Inom EU:s rättsliga ramar räknas till sådana villkor, exempelvis, behovet att erhålla den registrerades uttryckliga samtycke eller nödvändigheten av ett sådant beslut för att ett avtal ska kunna fullgöras. Om beslutet inte sker i enlighet med de villkor som fastställs i tredjelandets rättsliga ramar, ska den registrerade ha rätt att inte underställas det. Tredjelandets lagstiftning ska under alla förhållanden omfatta nödvändiga skyddsåtgärder, inklusive rätten att informeras om de specifika skälen och logiken bakom beslutet, rätten att korrigera felaktig eller ofullständig information och rätten att bestrida beslutet om det har fattats på felaktigt faktaunderlag[59].

61. Dataskyddsramen ger inga särskilda rättsliga garantier när enskilda personer blir föremål för beslut som har rättsliga följder för dem eller som märkbart påverkar dem och som enbart grundas på automatisk behandling av uppgifter som är avsedda att bedöma vissa personliga egenskaper hos den berörda personen, exempelvis arbetsprestationer, kreditvärdighet, pålitlighet eller uppträdande.

62. Som redan beaktats i artikel 29-gruppens yttrande 01/2016, liksom av dataskyddsstyrelsen i dennas tidigare yttranden om besluten om adekvat skyddsnivå i Japan respektive Sydkorea[60], kräver den snabba utvecklingen på området för automatiserat beslutsfattande och profilering – i allt större utsträckning med hjälp av AI-teknik – särskild uppmärksamhet i detta sammanhang[61].

63. Dataskyddsstyrelsen noterar kommissionens argument, nämligen att skyddsnivån för personuppgifter som samlats in i unionen sannolikt inte kommer att påverkas av frånvaron av särskilda regler för automatiserat beslutsfattande i dataskyddsramen (eftersom eventuella beslut baserade på automatiserad behandling i typfallet skulle fattas av den personuppgiftsansvarige i unionen som har en direkt relation till den berörda registrerade)[62].. Enligt dataskyddsstyrelsens mening kan det dock inte uteslutas att en personuppgiftsansvarig i USA använder automatiserat beslutsfattande med

övervakningsåtgärder (antagna den 10 november 2020), Riktlinjer 04/2021 om uppförandekoder som överföringsverktyg (version 2.0, antagna den 22 februari 2022), *Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules*, antagna den 14 november 2022), *Guidelines 07/2022 on certification as a tool for transfers*, antagna efter offentligt samråd den 14 februari 2023).

[58] Artikel 29-gruppens yttrande 01/2016, punkt 2.2.3, s. 21.

[59] Referensramen för adekvat skyddsnivå, kapitel 3.B.3.

[60] Dataskyddsstyrelsens yttrande 28/2018 om Europeiska kommissionens förslag till genomförandebeslut om adekvat skydd av personuppgifter i Japan, antaget den 5 december 2018, Dataskyddsstyrelsens yttrande 32/2021 om Europeiska kommissionens förslag till genomförandebeslut om adekvat skydd av personuppgifter i Republiken Korea, antaget den 24 september 2021.

[61] Se bl.a. C-634/21, OQ/Land Hessen (SCHUFA Holding m.fl.), begäran om förhandsavgörande (pågående).

[62] Utkastet till beslut, skälen 33 och 34.

uppgifter som överförts inom ramen för utkastet till beslut (dvs. i ett sammanhang som rör bedömning av arbetsprestationer, försäkringstäckning, boende).

64. Dataskyddsstyrelsen ser därför positivt på att kommissionen tar upp de särskilda skyddsåtgärder som amerikansk lag inom olika områden föreskriver[63]. Dataskyddsstyrelsens uppfattning är dock att skyddsnivån för enskilda varierar beroende på vilka branschspecifika regler – om några – som är tillämpliga på den aktuella situationen. Det finns en risk att det uppstår situationer som inte omfattas av skyddsåtgärderna då de ligger utanför tillämpningsområdet för de lagar som det hänvisas till. Beskrivningen av vad den enskildes rättigheter vid automatiserat beslutsfattande innefattar varierar dessutom från en lag till en annan.

65. Mot denna bakgrund anser dataskyddsstyrelsen att det för att uppnå tillräckliga skyddsåtgärder krävs särskilda regler för automatiserat beslutsfattande i dataskyddsramen, inbegripet rätt för den enskilde att känna till den logik som tillämpas, att bestrida beslutet och att få mänsklig kontakt när beslutet i väsentlig grad påverkar honom eller henne[64].

2.2 Förfarande- och verkställandemekanismer

66. Dataskyddsstyrelsen noterar att dataskyddsramen fortsatt bygger på ett system för självcertifiering, även om kommissionen talar om det som ett system för ”certifiering”.

67. Dataskyddsstyrelsen påminner om de förbättringar som uppnåtts under loppet av tidigare gemensamma översyner, exempelvis när det gäller handelsdepartementets roll, processen för (åter-)självcertifiering, övervakningen av företagens efterlevnad av ramens principer (t.ex. genom stickprovskontroller och frågeformulär om efterlevnaden) och insatserna för att fastställa och åtgärda falska påståenden om deltagande (t.ex. via sökningar på nätet).

68. Samtidigt hade artikel 29-arbetsgruppen och dataskyddsstyrelsen uttryckt oro gällande en viss brist på tillsyn av efterlevnaden av kraven i skölden för skydd av privatlivet[65]. I synnerhet instämmer dataskyddsstyrelsen i kommissionens slutsatser efter den tredje årliga översynen av skölden för skydd av privatlivet, nämligen att de stickprov som gjordes av handelsdepartementet inom ramen för skölden tenderade att begränsas till formella krav (t.ex. att kontaktpunkter inte svarade eller att ett företag inte gjort sin integritetspolicy tillgänglig online)[66]. The EDPB considers that . Dataskyddsstyrelsen anser att det är avgörande att efterlevnaden av de krav som är av mer materiell karaktär kontrolleras.

69. Dataskyddsstyrelsen påminner också om vikten av effektiv tillsyn (även av efterlevnaden av materiella krav) och effektivt verkställande av dataskyddsramen. Dataskyddsstyrelsen kommer att övervaka denna aspekt noga, även i samband med de regelbundna översynerna.

70. När det gäller verkställandet noterar dataskyddsstyrelsen att federala konkurrensmyndigheten[67] och transportdepartementet[68] i sina respektive skrivelser förnyar sina åtaganden att prioritera utredningar av påstådda överträdelser av dataskyddsramen, vidta lämpliga verkställighetsåtgärder mot enheter som gör falska eller vilseledande påståenden, övervaka verkställighetsbeslut avseende överträdelser

[63] Utkastet till beslut, skäl 35.
[64] Se även tredje gemensamma översynen, s. 7 6.
[65] Tredje gemensamma översynen, s. 7.
[66] Rapport från kommissionen till Europaparlamentet och rådet om den tredje årliga översynen av skölden för skydd av privatlivet i EU och USA (23.10.2019, COM(2019) 495 final), s. 4.
[67] Utkastet till beslut, bilaga IV.
[68] Utkastet till beslut, bilaga V.

av ramen och samarbeta med EU:s dataskyddsmyndigheter. När det gäller detta är dataskyddsstyrelsen också medveten om att den federala konkurrensmyndigheten har indikerat att man förväntar sig att ytterligare rikta sina verkställandeinsatser mot materiella överträdelser av dataskyddsramen och att myndigheten ämnar göra utredningar (även) på eget initiativ. Dataskyddsstyrelsen kommer att övervaka dessa aspekter noga, även i samband med de regelbundna översynerna.

2.3 Prövningsmekanismer

71. Dataskyddsstyrelsen välkomnar den tydliga presentationen i utkastet till beslut av de sju möjligheter till prövning som registrerade i EU erbjuds för den händelse deras personuppgifter behandlas i strid med dataskyddsramen[69].

72. Dessa olika instanser för handläggning av klagomål har inrättats i enlighet med de krav som ställs genom principen om rättsmedel, genomförande och ansvar och genom kompletterande princip 11 om tvistlösning och efterlevnad som utfärdats av handelsdepartementet och som nämns i bilaga I till utkastet till beslut[70].

73. Som kommissionen understryker i sitt utkast till beslut ”bör den registrerade tillförsäkras effektiv administrativ och rättslig prövning”[71]. Detta återspeglar det krav i dataskyddsförordningens artikel 45.2 a enligt vilket kommissionen vid sin bedömning av huruvida skyddsnivån i ett tredjeland är adekvat i synnerhet ska beakta tillgången till ”effektiv administrativ och rättslig prövning för de registrerade vars personuppgifter överförs”[72]. Även i referensramen för adekvat skyddsnivå tas detta krav upp[73].

74. Dataskyddsstyrelsen konstaterar att dessa prövningsmekanismer är desamma som de som ingick i den tidigare skölden för skydd för privatlivet och som har redan har kommenterats av artikel 29-gruppen[74].

75. När det gäller skiljedomsmekanismen konstaterar dataskyddsstyrelsen att den inte är tillgänglig i samband med undantagen från ramens principer[75] och hänvisar därför till sin kommentar i punkt 33.

76. När det gäller ytterligare möjligheter till rättslig prövning enligt amerikansk lag skulle dataskyddsstyrelsen också välkomna ytterligare detaljer om den lagstiftning som nämns[76] och hänvisar till sin kommentar i punkt 21.

77. Dataskyddsstyrelsen välkomnar också den skrivelse från den federala konkurrensmyndigheten där myndigheten beskriver sin avsikt att bedriva ett nära samarbete med EU:s dataskyddsmyndigheter[77]. Dataskyddsstyrelsen välkomnar också konkurrensmyndighetens avsikt att prioritera klagomål, även om detta kanske inte innebär någon garanti för att alla eventuella klagomål från registrerade kommer att behandlas.

---

[69] Utkastet till beslut, skäl 67.

[70] Utkastet till beslut, bilaga I, avsnitt II.7 och III.11 samt bilaga I till bilaga I.

[71] Utkastet till beslut, skäl 64.

[72] Se även skäl 141 i dataskyddsförordningen, där det hänvisas till artikel 47 i stadgan om de grundläggande rättigheterna, om rätten till ett effektivt rättsmedel i EU.

[73] Referensramen för adekvat skyddsnivå s. 8.

[74] Se särskilt artikel 29-gruppens yttrande 01/2016, avsnitt 2.2.6 a.

[75] Utkastet till beslut, bilaga I till bilaga I, A.

[76] Utkastet till beslut, skäl 85.

[77] Utkastet till beslut, bilaga IV.

78. När det gäller möjligheten för enskilda att lämna in sina klagomål till en dataskyddsmyndighet i EU skulle dataskyddsmyndigheten uppskatta ytterligare information om i) huruvida den möjlighet att ge råd om korrigerande eller kompenserande åtgärder som dataskyddsmyndigheten i EU har skulle kunna innefatta rekommendationer om böter eller användning av utredningsbefogenheter och ii) i vilken utsträckning de åtgärder som vidtas av dataskyddsmyndigheten i EU skulle beaktas som grund för verkställighetsåtgärder av den federala konkurrensmyndigheten eller transportdepartementet[78].

79. Dataskyddsstyrelsen kommer noggrant att övervaka prövningsmekanismernas effektivitet, bland annat i samband med de regelbundna översynerna.

3 AMERIKANSKA MYNDIGHETERS TILLGÅNG TILL OCH ANVÄNDNING AV PERSONUPPGIFTER SOM ÖVERFÖRTS FRÅN EU

3.1 Åtkomst och användning för straffrättsliga ändamål som rör brottsbekämpning

3.1.1 Brottsbekämpande myndigheters tillgång till personuppgifter bör baseras på tydliga, precisa och tillgängliga regler

80. Dataskyddsstyrelsen välkomnar det faktum att den information och de förklaringar som ges i utkastet till beslut när det gäller amerikanska myndigheters tillgång till och användning av personuppgifter för straffrättsliga ändamål som rör brottsbekämpning är mer detaljerade än i det tidigare beslutet om adekvat skyddsnivå. Utkastet till beslut innehåller också, i bilaga VI, en skrivelse från det amerikanska justitiedepartementets straffrättsliga avdelning som ”ger en kortfattad översikt av de främsta utredningsverktyg som används för att erhålla affärsuppgifter och annan information i register från företag i Förenta staterna för ändamål som rör brottsbekämpning och allmänintresset (civilt och lagstadgat), inbegripet de åtkomstbegränsningar som anges av dessa myndigheter”. Enligt skrivelsen används alla de rättsliga förfaranden som beskrivs i skrivelsen för att erhålla information från företag i USA, utan hänsyn till den registrerades nationalitet eller bosättningsort. Samtliga förfaranden uppges härröra antingen direkt från den amerikanska konstitutionen (fjärde tillägget), från lagstiftning och rättspraxis eller från regler och riktlinjer som fastställts av justitiedepartementet. Denna översikt omfattar inte de utredningsverktyg för nationell säkerhet som används av de brottsbekämpande myndigheterna i utredningar om terrorism och i andra utredningar som rör den nationella säkerheten[79].

81. Dataskyddsstyrelsen noterar att det främst är federala brottsbekämpande myndigheter och tillsynsmyndigheter som diskuteras i utkastet till beslut och bilaga VI till beslutet[80]. Det saknas specifika hänvisningar till de lagar på delstatsnivå som reglerar dessa förfaranden för att erhålla information. I bilaga VI nämns också att ”[d]et finns andra rättsliga grunder för företag att bestrida administrativa myndigheters förfrågningar om åtkomst till uppgifter som grundas på den bransch som företaget är verksamt i och vilka typer av uppgifter som de innehar”, vilket följs av flera icke uttömmande exempel, såsom lagen om banksekretess och dess genomförandeföreskrifter[81], lagen om rättvis kreditrapportering[82] och lagen om integritetsskydd för finansiella uppgifter[83]. Dataskyddsstyrelsen

[78] Utkastet till beslut, bilaga I, III.5 b iii.
[79] Utkastet till beslut, fotnot 1 till bilaga VI.
[80] Se utkastet till beslut, skälen 90–93.
[81] 31 U.S.C. § 5318 31 C.F.R. kapitel X.
[82] 15 U.S.C. § 1681b.
[83] 12 U.S.C. §§ 3401–3423.

konstaterar att den tillämpliga rättsliga grunden för en begäran om tillgång beror på vilken typ av uppgifter som begärs ut, vilken typ av företag det rör sig om, vilken typ av rättsliga förfaranden som är aktuella (straffrättsliga, administrativa, kopplade till andra ändamål som rör allmänintresset) och vilken typ av enhet det är som begär tillgång till uppgifterna. Eftersom alla de tillämpliga regler som begränsar de brottsbekämpande myndigheternas tillgång till uppgifter som överförts till USA har sin grund i konstitutionen, lagstiftningen och justitiedepartementets öppna beslut erkänner dataskyddsstyrelsen reglernas tillgänglighet och uppmanar kommissionen att låta detta avspeglas i utkastet till beslut. Det står klart utifrån bilaga VI att dessa lagar och förordningar gäller oavsett den registrerades nationalitet och bostadsort och att de generellt sett införlivar kraven i konstitutionens fjärde tillägg (även om de ofta går längre än så och ger ett mer omfattande skydd).

82. Sammanfattningsvis noterar dataskyddsstyrelsen att utkastet till beslut innehåller en mer detaljerad bedömning gällande de federala brottsbekämpande myndigheternas tillgång till uppgifter än det föregående beslutet om adekvat skyddsnivå. När det gäller delstatliga brottsbekämpande myndigheters tillgång till uppgifter noterar dataskyddsstyrelsen också att enligt bilaga VI måste det delstatliga skyddet åtminstone motsvara det skydd som den amerikanska konstitutionen ger, däribland men inte begränsat till det fjärde tillägget. Dataskyddsstyrelsen uppmanar kommissionen att ytterligare bedöma skyddet på delstatsnivå i kommande översyner.

3.1.2 Nödvändighet och proportionalitet med hänsyn till de legitima mål som eftersträvas måste påvisas

83. Dataskyddsstyrelsen konstaterar att begäranden om tillgång till uppgifter för ändamål som rör brottsbekämpning generellt sett kan anses syfta till ett legitimt mål. Samtidigt är sådana ingrepp endast godtagbara när de är nödvändiga och proportionerliga[84].

84. Enligt EU-domstolens etablerade rättspraxis kräver proportionalitetsprincipen att lagar som inskränker rätten till privatliv och skydd för personuppgifter är ”ägnade att uppnå de legitima mål som eftersträvas med bestämmelserna i fråga och att de inte ska gå utöver vad som är lämpligt och nödvändigt för att uppnå dessa mål”[85]. Bedömningen av nödvändighet och proportionalitet görs därför, i princip, alltid i förhållande till en viss åtgärd som föreskrivs i lagstiftningen.

85. De amerikanska myndigheterna anger i bilaga VI att federala åklagare och federala utredare kan få tillgång till handlingar och annan registerinformation från organisationer genom ”olika typer av obligatoriska rättsprocesser, inklusive förelägganden från åtalsjuryn, administrativa förelägganden och husrannsakningsorder, och kan inhämta andra meddelanden genom federal avlyssning i brottsbekämpande syfte samt befogenheter att utföra ’pen register’”[86]. Dessutom får myndigheter och byråer med civila och lagstadgade ansvarsområden utfärda förelägganden till organisationer om ”företagsregister, elektroniskt lagrad information eller andra materiella ting”[87]. Själva förfarandena

[84] Se EU-domstolens dom av den 6 oktober 2020 i de förenade målen C-511/18, C-512/18 och C-520/18, La Quadrature du Net m.fl., ECLI:EU:C:2020:791 (nedan kallade, *Quadrature du Net-domen*), punkt 140. Se även Europeiska datatillsynsmannen, *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: a toolkit*, 11 april 2017 och Europeiska dataskyddsstyrelsen, *Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*, 19 december 2019.

[85] Se EU-domstolens dom av den 8 april 2014 i de förenade målen C-293/12 och C-594/12, Digital Rights Ireland, ECLI:EU:C:2014:238 (nedan kallad *Digital Rights Ireland-domen*), punkt 46 och där angiven rättspraxis.

[86] Utkastet till beslut, bilaga VI s. 2.

[87] Utkastet till beslut, bilaga VI s. 4.

förklaras också i skälen 90–93 i utkastet till beslut. Dataskyddsstyrelsen noterar den positiva utveckling inom amerikansk rättspraxis på området för elektroniskt lagrad information som nämns i utkastet till beslut[88].

86. I bilaga VI anges vidare att dessa rättsliga förfaranden är icke-diskriminerande och att de används generellt för att erhålla information från ”företag” i USA, oavsett om dessa är certifierade inom dataskyddsramen eller ej och utan hänsyn till den registrerades nationalitet eller bosättningsort.

87. Dessutom innehåller bilaga VI slutsatser om de skyddsåtgärder som fastställs i det fjärde tillägget till den amerikanska konstitutionen, enligt vilka det i princip krävs en husrannsakningsorder från domstol som är grundad på sannolika skäl och som uppfyller preciseringskraven för att brottsbekämpande myndigheter ska få utföra husrannsakningar och göra beslagtaganden, samt en hänvisning till det faktum att den brottsbekämpande åtgärden i de undantagsfall där kravet på husrannsakningsorder inte gäller är föremål för ett skälighetstest enligt det fjärde tillägget[89]. Den som blir föremål för husrannsakan eller vars egendom genomsöks kan vidta åtgärder för att upphäva eventuella bevis som påträffats vid eller till följd av en olaglig husrannsakan om sådana bevis tas upp mot honom eller henne under en brottmålsrättegång[90].

88. Sammanfattningsvis konstaterar dataskyddsstyrelsen att det system av utredningsverktyg som används för att erhålla affärsuppgifter och annan information i register från företag i USA för ändamål som rör brottsbekämpning och allmänintresset, inbegripet åtkomstbegränsningar och skyddsåtgärder, utgör ett omfattande men också komplext åtgärdssystem, som återspeglar, bland annat, den amerikanska statens federala karaktär.

89. Härav följer att det system av utredningsåtgärder för brottsbekämpningsändamål som används i USA allmänt kan anses uppfylla kraven på nödvändighet och proportionalitet i förhållande till den grundläggande rätten till integritet och dataskydd.

3.1.3 Det bör finnas en oberoende tillsynsmekanism

90. Dataskyddsstyrelsen konstaterar att de flesta av de förfaranden som beskrivs i utkastet till beslut och bilaga VI förutsätter ett förhandsbeslut från en domstol för att myndigheterna ska ha rätt att få tillgång till uppgifter (exempelvis domstolsbeslut om användning av ”pen registers” och ”trap and trace”-anordningar[91], domstolsbeslut om övervakning enligt den federala avlyssningslagen[92], husrannsakningsorder – *Federal Rules of Criminal Procedure*, regel 41[93]). Alla förfaranden verkar dock inte kräva att en domstol involveras innan förfarandet inleds. Civila och lagstadgade myndigheter får t.ex. utfärda förelägganden[94]. I dessa fall är det dock möjligt att göra en rättslig kontroll i efterhand av

[88] Se utkastet till beslut, fotnot 146. I en dom från 2018 bekräftar den amerikanska Högsta domstolen att det krävs en husrannsakningsorder eller ett undantag från kravet på husrannsakningsorder även för att brottsbekämpande myndigheter ska få ta del av historiken över de basstationer en mobiltelefon har anslutit till, uppgifter som ger en god översikt över hur användaren förflyttat sig, samt att användare kan förvänta sig en rimlig nivå av integritet när det gäller sådana uppgifter (Timothy Ivory Carpenter/Förenta staterna, nr 16-402, 585 U.S. (2018)).
[89] Se utkastet till beslut, bilaga VI, s. 2.
[90] Se utkastet till beslut, skäl 90.
[91] Se utkastet till beslut, skäl 92.
[92] Se utkastet till beslut, bilaga VI, s. 3.
[93] Se utkastet till beslut, skäl 90 och bilaga VI, s. 3.
[94] Se utkastet till beslut, bilaga VI, s. 4 samt skäl 91.

att föreläggandet var skäligt, eftersom en ”person som mottar ett administrativt föreläggande kan dessutom bestrida verkställandet av detta i domstol”[95].

91. Därutöver beskrivs i utkastet till beslut den tillsyn av de federala brottsbekämpande myndigheterna som utövas av flera olika organ, från den inre kontroll som utövas av tjänstemän med ansvar för integritetsskydd och medborgerliga friheter till den externa kontroll som utövas av generalinspektören och de särskilda utskotten i den amerikanska kongressen[96]. Europeiska kommissionen tillhandahåller nyanserad och detaljerad information och drar generellt sett begripliga slutsatser. Dataskyddsstyrelsen avstår därför från att i detta yttrande upprepa de konstaterade faktauppgifterna och bedömningarna.

92. Utifrån den information som finns tillgänglig konstaterar dataskyddsstyrelsen att det finns en förhållandevis kraftfull tillsynsmekanism när det gäller brottsbekämpande myndigheters tillgång till uppgifter som innehas av företag i USA.

3.1.4 Enskilda personer måste ha tillgång till effektiva rättsmedel

93. Enligt EU-domstolens rättspraxis måste enskilda personer ha tillgång ett effektivt rättsmedel för att tillvarata sina rättigheter när de anser att dessa rättigheter inte respekteras eller inte har respekterats. EU-domstolen förklarar i Schrems I-domen att ”[e]n lagstiftning i vilken det inte föreskrivs någon möjlighet för enskilda att använda rättsmedel för att erhålla tillgång till, rätta eller radera uppgifter som rör dem, respekterar inte det väsentliga innehållet i den grundläggande rätten till effektivt domstolsskydd, vilken är stadfäst i artikel 47 i stadgan. I artikel 47 första stycket i stadgan föreskrivs nämligen att var och en vars unionsrättsligt garanterade fri- och rättigheter har kränkts har rätt till ett effektivt rättsmedel inför en domstol, med beaktande av de villkor som föreskrivs i den artikeln”[97].

94. Utkastet till beslut[98] och dess bilaga VI innehåller mer information om tänkbara rättsmedel med grund i lagstiftningen som skulle vara tillgängliga för en enskild i ett läge där myndigheterna olagligen får tillgång till hans eller hennes uppgifter.

95. I detta avseende fastställs det enligt kommissionen[99] i lagen om administrativa förfaranden (*Administrative Procedure Act*) 5 U.S.C. § 702 att en person som felaktigt drabbats av rättsliga åtgärder till följd av ett organs agerande eller som skadats eller förfördelats till följd av ett organs agerande, har rätt att söka rättslig prövning av detta agerande.

96. Dessutom föreskrivs i lagen om lagrade meddelanden (*Stored Communications Act*) (som utgör avdelning II i lagen om elektronisk brevhemlighet (*Electronic Communications Privacy Act*)) att en person som lider skada till följd av överträdelse av bestämmelserna i det aktuella kapitlet, förutsatt att den handling som utgör överträdelsen begås medvetet eller uppsåtligt, genom civilrättsliga förfaranden kan erhålla lämplig kompensation från personen eller enheten, vilken inte är den amerikanska staten[100]. Därutöver kan den som lider skada genom en uppsåtlig överträdelse av det

[95] Se utkastet till beslut, bilaga VI, s. 4 samt skäl 91.
[96] Se utkastet till beslut, skälen 103–106.
[97] Schrems I-domen, punkt 95.
[98] Se utkastet till beslut, skälen 107–112.
[99] Se utkastet till beslut, skäl 109.
[100] 18 U.S.C. § 2707.

kapitlet eller av kapitel 119 väcka talan mot den amerikanska staten i en federal distriktsdomstol med yrkande om ekonomiskt skadestånd[101].

97. Vidare innehåller utkastet till beslut också uppgifter om rätten att få tillgång till federala myndigheters register i enlighet med *Freedom of Information Act (*(FOIA)[102] och flera andra rättsakter där enskilda tillerkänns rätten att väcka talan mot en amerikansk myndighet eller tjänsteman rörande behandlingen av den enskildes personuppgifter, så som *Wiretap Act*, *Computer Fraud and Abuse Act*, *Federal Torts Claim Act*, *Right to Financial Privacy Act* och *Fair Credit Reporting Act*[103].

98. Dataskyddsstyrelsen välkomnar därför kommissionens förtydliganden avseende antalet möjligheter till prövning som enskilda har tillgång till. Dataskyddsstyrelsen uppmanar också kommissionen att ytterligare klargöra huruvida dessa rättsmedel kan användas av de registrerade för att ”erhålla tillgång till, rätta eller radera uppgifter som rör dem”, så som EU-domstolen kräver.

3.1.5 Vidare användning av de insamlade uppgifterna

3.1.5.1 Vidare användning inom USA av överförda uppgifter som brottsbekämpande myndigheter fått tillgång till

99. Dataskyddsstyrelsen noterar med tillfredsställelse att det i utkastet till beslut görs en bedömning avseende eventuell vidare användning inom USA av uppgifter som brottsbekämpande myndigheter där har fått tillgång till. Dataskyddsstyrelsen beklagar dock att det endast ges ett exempel på de grunder på vilka uppgifterna får spridas vidare[104]. I detta avseende rekommenderar dataskyddsstyrelsen kommissionen att i utkastet till beslut ytterligare förtydliga de principer och skyddsåtgärder som är tillämpliga på vidare användning av uppgifter, så som de som anges i Privacy Act (5 U.S.C. 552a)[105].

3.1.5.2 Vidare överföring utanför USA

100. Dataskyddsstyrelsen noterar också att kommissionen tar upp även vidare överföringar från de brottsbekämpande myndigheterna i USA till myndigheter i tredjeländer, men även detta endast i relation till justitieministerns riktlinjer för inrikes FBI-insatser (*Attorney General Guidelines for Domestic FBI Operations* (AGG-DOM))[106]. Dataskyddsstyrelsen anser att denna information och bedömning är avgörande för att möjliggöra en genomgripande bedömning av den skyddsnivå som säkerställs genom USA:s rättsliga ram och praxis för utlämnande och vidare användning i andra länder. Med tanke på att kommissionen sammantaget har gett endast ett exempel, som dessutom är begränsat till sin karaktär, när det gäller frågan om vidare överföring av uppgifter utanför USA uppmanar dataskyddsstyrelsen kommissionen att ytterligare klargöra de regler och skyddsåtgärder som är tillämpliga på vidare överföring, vidare användning och utlämnande av personuppgifter som samlats in för brottsbekämpande ändamål i USA och sedan överförs till tredjeländer, inbegripet inom ramen för internationella överenskommelser.

---

[101] 18 U.S.C. § 2712.
[102] Se utkastet till beslut, skäl 111.
[103] Se utkastet till beslut, skäl 112.
[104] Se utkastet till beslut, skäl 102.
[105] Se justitieministerns riktlinjer för inrikes FBI-insatser (*Attorney General Guidelines for Domestic FBI Operations* (AGG-DOM)), s. 36, punkt B (1)(g).
[106] Se utkastet till beslut, skäl 102.

3.2 Åtkomst och användning för ändamål som rör den nationella säkerheten

101. Rent allmänt är dataskyddsstyrelsen medveten om att delstaterna har ett stort utrymme för skönsmässig bedömning i frågor som rör den nationella säkerheten, vilket också erkänns av Europadomstolen. Dataskyddsstyrelsen påminner också om att det i artikel 6.3 i fördraget om Europeiska unionen fastställs att de grundläggande rättigheter som stadfästs i Europakonventionen ska ingå i EU-rätten som allmänna principer. (Dataskyddsstyrelsen understryker detta även i sina uppdaterade rekommendationer om europeiska nödvändiga garantier för övervakningsåtgärder[107]). Så länge unionen inte har anslutit sig till Europakonventionen utgör denna dock inte ett rättsligt instrument som formellt införlivats med unionsrätten[108], vilket EU-domstolen påminner om i sin rättspraxis. Alltså måste den skyddsnivå för grundläggande rättigheter som krävs enligt artikel 45 i dataskyddsförordningen fastställas på grundval av bestämmelserna i den förordningen, jämförda med de grundläggande rättigheter som tas upp i stadgan. Enligt artikel 52.3 i stadgan ska dock de rättigheter som ingår i stadgan och som motsvarar rättigheter som garanteras genom Europakonventionen ha samma innebörd och räckvidd som i Europakonventionen. Därmed, vilket EU-domstolen påminner om, måste rättspraxis från Europadomstolen betraktas som lägsta tillåtna skyddsnivå vid tolkningen av motsvarande rättigheter i stadgan[109]. Enligt den sista meningen i artikel 52.3 i stadgan hindrar dock ”[d]enna bestämmelse […] inte unionsrätten från att tillförsäkra ett mer långtgående skydd”.

102. I bedömningen nedan har dataskyddsstyrelsen därför tagit hänsyn till rättspraxis från Europadomstolen, i den mån som stadgan, enligt EU-domstolens tolkning, inte föreskriver en högre skyddsnivå med andra krav än rättspraxis från Europadomstolen.

103. Den amerikanska rättsliga ramen omfattar flera rättsliga instrument som ger amerikanska underrättelsemyndigheter möjlighet att samla in och vidare ta del av och behandla uppgifter.

104. Som kommissionen erinrar om i sitt utkast till beslut kan *amerikanska underrättelsemyndigheter begära åtkomst till personuppgifter som överförts till organisationer i USA för ändamål som rör den nationella säkerheten endast i den mån det medges av lagstiftningen, i synnerhet lagen om underrättelseverksamhet och övervakning utomlands (Foreign Intelligence Surveillance Act, Fisa) och/eller rättsliga bestämmelser som medger åtkomst via nationella säkerhetsskrivelser (National Security Letters, NSL)*[110]. Enligt presidentdekret 12333 (dekret 12333) *har amerikanska underrättelsemyndigheter också möjlighet att samla in personuppgifter utanför USA, vilket kan inbegripa personuppgifter som håller på att överföras mellan unionen och* USA[111].

105. När det gäller regelverket för datainsamling specifikt, i synnerhet section 702 i Fisa samt dekret 12333, införs genom dekret 14086 nu nya regler för att stärka skyddsåtgärderna för USA:s signalspaningsverksamhet. Dessa allmänna regler gäller horisontellt och *måste genomföras vidare via myndigheternas regler och förfaranden för att på så sätt omvandlas till konkreta riktlinjer för den*

[107] Se dataskyddsstyrelsens rekommendationer 02/2020 om europeiska nödvändiga garantier för övervakningsåtgärder.
[108] Se Schrems II-domen, punkt 98.
[109] Se Quadrature du Net-domen, punkt 124.
[110] Se utkastet till beslut, skäl 115.
[111] Se utkastet till beslut, skäl 117.

dagliga verksamheten[112]. Dekret 14086 har i mångt och mycket ersatt det tidigare *Presidential Policy Directive 28* (*PPD-28*)[113].

106. För att få tillgång till den rättsliga ram som är tillämplig på insamling, åtkomst och vidare behandling av uppgifter för ändamål som rör den nationella säkerheten är det alltså viktigt att undersöka den specifika rättsliga ram som reglerar insamling av uppgifter i och utanför USA, dvs. section 702 i Fisa samt dekret 12333, vilka i sig inte har ändrats sedan den senaste översynen av skölden för skydd av privatlivet, med beaktande av det faktum att det nya presidentdekretet 14086 innehåller bestämmelser om skyddsåtgärder som ska genomföras även i samband med uppgiftsinsamling på grundval av specifika texter såsom section 702 i Fisa och dekret 12333.

3.2.1 Garanti A – Behandlingen bör vara förenlig med lagstiftningen och baseras på tydliga, precisa och tillgängliga bestämmelser

107. Avseende dataskyddsstyrelsens bedömning av de allmänna formerna för uppgiftsinsamlingen vill styrelsen påminna om den första av de fyra ”europeiska nödvändiga garantierna”, enligt vilken ”uppgifter bör behandlas utifrån tydliga, precisa och tillgängliga bestämmelser”[114].

108. I enlighet med EU-domstolens fasta rättspraxis ska varje begränsning av rätten till skydd av personuppgifter föreskrivas i lag och den rättsliga grund som möjliggör ett ingrepp i en sådan rättighet måste själv definiera omfattningen av begränsningen av utövandet av den berörda rättigheten[115]. EU-domstolen har också erinrat om att ”lagstiftning ska vara rättsligt bindande enligt nationell rätt”[116]. I detta hänseende klargör i Europadomstolens rättspraxis att begreppet lag ska tolkas i materiell bemärkelse och inte enbart i formell bemärkelse. Det kan omfatta texter med lägre rang än lagstiftning, som regleringsakter som antagits av en yrkessammanslutning, genom delegation från lagstiftaren, inom ramen för dess självständiga normativa befogenhet, och till och med ”oskriven rätt”. För att räknas som ”lag” måste en regel vara tillräckligt tillgänglig och tillräckligt precist formulerad[117].

109. Den grad av precision som krävs ska stå i proportion till omfattningen av begränsningen av rättigheten[118]. När det gäller lagens ”förutsägbarhet” erinrade Europadomstolen i sin dom i målet Zakharov om att kravet på förutsägbarhet i sammanhang av hemliga övervakningsåtgärder inte kan ”betyda att en enskild person ska kunna förutse när myndigheterna ska komma att avlyssna dennes kommunikation och anpassa denna därefter”. Klara och detaljerade regler för hemliga övervakningsåtgärder är dock avgörande för att minimera riskerna för godtycke när en befogenhet som den verkställande makten tilldelats utövas i hemlighet. Den inhemska lagen måste vara tillräckligt

[112] Se utkastet till beslut, skäl 120.

[113] Detta presidentdekret upphäver PPD-28 med undantag för avsnitten 3 och 6 samt den sekretessbelagda bilagan till PPD-28, vilka fortfarande gäller. Se presidentens nationella säkerhetsmemorandum av den 7 oktober 2022.

[114] Rekommendationer 02/2020 om europeiska nödvändiga garantier för övervakningsåtgärder (antagna den 10 november 2020). Se punkterna 175 och 180 i Schrems II-domen samt yttrande 1/15 (PNR-avtal mellan EU och Kanada) av den 26 juli 2017, punkt 139 och där angiven rättspraxis.

[115] Se Schrems II, punkterna 174–175 och där angiven rättspraxis. Se även, när det gäller tillgång för myndigheter i medlemsstaterna, mål C-623/17, Privacy International, ECLI:EU:C:2020:790 (nedan kallad *Privacy International-domen*), punkt 65 och Quadrature du Net-domen, punkt 175.

[116] Privacy International-domen, punkt 68.

[117] Europadomstolens dom av den 26 april 1979, Sunday Times/Förenade kungariket (nr 1), CE:ECHR:1979:0426JUD000653874 (nedan kallad *Europadomstolens dom i målet Sunday Times/Förenade kungariket (nr 1)*, punkt 49.

[118] Europadomstolens dom i målet Sunday Times/Förenade kungariket (nr 1), punkt 49.

tydlig, så att medborgarna får en tillfredsställande indikation på de omständigheter enligt vilka och villkoren för när offentliga

myndigheter har rätt att tillgripa sådana åtgärder[119].

110. EU-domstolen har dessutom klargjort att bedömningen av den tillämpliga lagstiftningen i tredjelandet bör inriktas på huruvida den kan åberopas och anföras av enskilda vid en domstol. I synnerhet ska de registrerades rättigheter vara verkställbara, och enskilda måste ges rättigheter som kan göras gällande mot myndigheter[120], vilket inte var fallet inom ramen för den tidigare PPD-28. Numera föreskrivs genom dekret 14086, som enligt dataskyddsstyrelsens förståelse har samma rättsverkan inom den amerikanska rättsordningen som PPD-28 (dvs. bindande för den verkställande makten), rättigheter som kan göras gällande mot myndigheter. En detaljerad bedömning av de registrerades nya verkställbara rättigheter ges i avsnittet om prövning.

111. Skälen 114–152 i utkastet till beslut samt bilaga VII innehåller en sammanfattning av vissa aspekter av den gällande rättsliga ramen, begränsningar avseende insamling, lagring och spridning av uppgifter, efterlevnad och tillsyn, öppenhet och prövning. Den amerikanska rättsordningen avseende underrättelseverksamhet består av ett antal olika dokument, däribland enskilda organs rapporter, riktlinjer och förfaranden. I detta avseende är dataskyddsstyrelsens bedömning inriktad på ett begränsat antal frågor som den anser vara avgörande.

112. Enligt skälen 115–119 i utkastet till beslut får åtkomst av överförda personuppgifter från USA:s nationella säkerhetsmyndigheter ske endast inom ramen för Fisa, i enlighet med andra lagbestämmelser (12 U.S.C. § 3414, 15 U.S.C. § 1681u-1681v och 18 U.S.C. § 2709) eller, när det gäller personuppgifter som håller på att överföras, på grundval av dekret 12333. Det är uppgifterna i skälen 116 och 118 i utkastet till beslut som är anledningen till att kommissionen inriktar sin bedömning när det gäller USA:s nationella säkerhetsmyndigheters tillgång till personuppgifter på sections 105, 302, 402, 501 och 702 i Fisa (utländsk underrättelseverksamhet riktad mot utländska medborgare som befinner sig utanför USA) samt på dekret 12333 (utländsk underrättelseverksamhet avseende personuppgifter under överföring), då kommissionen betraktar dessa bestämmelser som de mest relevanta. Dataskyddsstyrelsens yttrande är därför begränsat till kommissionens bedömning av dessa bestämmelser, med beaktande av de begränsningar och skyddsåtgärder som anges i dekret 14086[121].

113. I detta sammanhang bör det noteras att alla rättsliga instrument som nämns i utkastet till beslut är tillgängliga för allmänheten (inom och utanför USA) och går att konsultera på nätet. Dessutom är presidentdekretets krav bindande för hela underrättelsesamfundet[122] och gäller övergripande för all utländsk underrättelseverksamhet.

114. Begreppet ”signals intelligence” (signalspaning) definieras inte i dekret 14086. I den senare hänvisas det till de definitioner som fastställs i dekret 12333 för att ange omfattningen av utländska underrättelser och kontraspionage, vilka definieras brett. I detta sammanhang vill dataskyddsstyrelsen, även om det har hävdats att dekret 12333 sedan införandet av Fisa endast kan

---

[119] Europadomstolen, Zakharov/Ryssland, 4 december 2015 (nedan kallad *Europadomstolens dom i målet Zakharov*), punkt 229.

[120] Schrems II-domen, punkt 181.

121 Detta presidentdekret upphäver PPD-28 med undantag för sections 3 och 6 samt den sekretessbelagda bilagan till PPD-28, vilka fortfarande gäller. Se presidentens nationella säkerhetsmemorandum av den 7 oktober 2022.

122 Se utkastet till beslut, skäl 120.

användas för insamling av uppgifter utanför USA:s territorium, påminna om att dekret 12333, som fortsätter gälla till fullo, i sig inte innehåller tillräckligt detaljerade uppgifter om dekretets geografiska tillämpningsområde, i vilken utsträckning uppgifter kan samlas in, lagras eller spridas vidare, vilken typ av brott som kan ge upphov till övervakning eller vilken sorts information som kan komma att samlas in eller användas. I princip kan all sådan insamling av utländska underrättelseuppgifter som omfattas av dekret 12333 ske enligt den amerikanska presidentens gottfinnande[123]. Enligt dataskyddsstyrelsens uppfattning är dock huvudsyftet med dekret 14086 att fastställa gränserna för insamling och behandling av personuppgifter när det gäller utländska underrättelser, oavsett vilket övervakningsprogram som används och varifrån uppgifterna erhålls. Dataskyddsstyrelsen är därför av uppfattningen att de ytterligare skyddsåtgärder som föreskrivs i dekret 14086 omfattar även övervakningsprogram som kan tillämpas på personuppgifter under överföring i enlighet med dekret 12333[124].

115. I detta avseende anges i dekret 14086 tolv legitima mål som bör eftersträvas vid insamling av signalspaningsuppgifter och fem mål för vilka insamling av signalspaningsuppgifter inte får utföras[125], samt sex legitima mål för användning av uppgifter som samlas in i bulk[126]. Vissa av dessa mål är relativt specifika (t.ex. ”räddning av gisslan”), medan andra är mer allmänt hållna (t.ex. ”global säkerhet”). Dekret 14086 innehåller också en förteckning över förbjudna mål, som bland annat omfattar att undertrycka eller begränsa ”legitima integritetsintressen”[127]. Dekret 14086 ger också USA:s president möjlighet att lägga till fler mål i förteckningen över mål för vilka insamling är tillåten samt att besluta att dessa nya mål inte ska offentliggöras, om presidenten anser att ett offentliggörande skulle utgöra en nationell säkerhetsrisk för USA[128]. Sådana uppdateringar får godkännas endast ”mot bakgrund av nya tvingande krav avseende den nationella säkerheten”.

116. Målen i sig kan inte åberopas av underrättelsemyndigheterna för att motivera insamling av signalspaningsuppgifter, utan måste, för operativa syften, underbyggas ytterligare och omvandlas till konkreta prioriteringar som motiverar att insamling av signalspaningsuppgifter tillåts. I dekret 14086 beskrivs också förfarandet för godkännande av de prioriteringar som motiverar att insamling av signalspaningsuppgifter tillåts[129]. Dataskyddsstyrelsen är medveten om att processen för fastställande av de godkända underrättelseprioriteringarna i princip är beroende av chefen för den amerikanska underrättelsesamfundet (*Director of the Intelligence Community*) och att denna process i regel ska inbegripa en bedömning av den nationella underrättelsetjänstens tjänsteman med ansvar för skyddet av medborgerliga friheter (*Civil Liberties Protection Officer of the Office of the Director of National Intelligence*, CLPO), vilken chefen för underrättelsesamfundet kan vara oense med. I så fall ska chefen för underrättelsesamfundet, när denne presenterar prioriteringsramen för nationell underrättelseverksamhet (*National Intelligence Priorities Framework*) för presidenten, redovisa såväl tjänstemannens bedömning som sina egna synpunkter[130].

---

[123] Enligt artikel II i den amerikanska konstitutionen är det presidenten, i egenskap av överbefälhavare för de väpnade styrkorna, som har ansvaret för att garantera den nationella säkerheten, inbegripet i synnerhet insamlingav utländska underrättelser.

[124] Se utkastet till beslut, skäl 134.

[125] Se presidentdekret 14086 (*dekret 14086*), section 2, (b), (ii), A, 1–5.

[126] Se utkastet till beslut, skäl 134 och dekret 14086, section 2(c)(ii).

[127] Se dekret 14086, section 2(b)(ii)(A)(2).

[128] Se dekret 14086, section 2(b)(i)(B).

[129] Se utkastet till beslut, skäl 129.

[130] Se dekret 14086, section 2(b)(iii)(B).

117. Dataskyddsstyrelsen konstaterar dock också att ”godkänd underrättelseprioritering” är definierat så att det avseende *merparten av USA:s åtgärder för insamling av signalspaningsuppgifter*[131] betyder en prioritering som är godkänd enligt section 2(b)(iii) i presidentdekretet (se föregående punkt). Det finns fall där processen för godkännande under ”snäva omständigheter” kan skilja sig från den som beskrivs ovan. I dessa fall kan presidenten eller chefen för ett organ som ingår underrättelsesamfundet fastställa en prioritering, ”i den mån det är möjligt” i enlighet med de kriterier som anges i section 2(b)(iii)(A)(1)-(3)), vilka innefattar ett krav på lämpligt beaktande av samtligas personliga integritet och medborgerliga friheter, men utan medverkan från CLPO.

118. Det understryks dessutom i dekret 14086 att ”åtgärder för insamling av signalunderrättelser i den mån det är möjligt ska skräddarsys” för att främja en godkänd underrättelseprioritering samt att ”underrättelsesamfundet ska överväga tillgängligheten, genomförbarheten och lämpligheten hos andra, mindre inkräktande källor”. Dekret 14086 innehåller också allmänna krav på nödvändighet och proportionalitet[132].

119. Vidare inrättas genom section 5(h) i dekret 14086 en rätt att lämna in giltiga klagomål till CPLO och att få CPLO:s beslut omprövade av domstolen för dataskyddsgranskning i enlighet med den prövningsmekanism som fastställs i section 3 i det aktuella dekretet.

120. Fisa framstår som tydligare och mer exakt än dekret 12333 när det gäller vilka typer av underrättelseverksamhet som kan godkännas. Fisa och dekret 12333 måste nu tillämpas mot bakgrund av dekret 14086 och i synnerhet med beaktande av bland annat nödvändighets- och proportionalitetsprinciperna.

121. De krav som fastställs i dekret 14086 måste genomföras vidare genom ändringar i myndigheternas regler och förfaranden för att på så sätt omvandlas till konkreta riktlinjer för den dagliga verksamheten. I detta avseende ger dekret 14086 amerikanska underrättelsemyndigheter ett år på sig (dvs. till den 7 oktober 2023) att uppdatera sina befintliga regler och förfaranden så att de överensstämmer med presidentdekretets krav. De uppdaterade reglerna och förfarandena måste utarbetas i samråd med justitieministern, CLPO och styrelsen för tillsyn av personlig integritet och medborgerliga friheter (*Privacy and Civil Liberties Oversight Board*, PCLOB) och göras tillgängliga för allmänheten i största möjliga utsträckning[133].

122. Dataskyddsstyrelsen skulle gärna se att inte endast ikraftträdandet utan även antagandet av beslutet gjordes avhängigt att alla amerikanska underrättelsetjänster antar uppdaterade regler och förfaranden för att genomföra dekret 14086. Dataskyddsstyrelsen rekommenderar kommissionen att utvärdera dessa uppdaterade regler och förfaranden och låta dataskyddsstyrelsen ta del av utvärderingen.

123. Slutligen konstaterar dataskyddsstyrelsen, när det gäller lagring av överförda uppgifter som en gång samlats in för ändamål rörande den nationella säkerheten, att dekret 14086 säkerställer att de regler som gäller för amerikanska medborgares personuppgifter även gäller för utländska medborgares personuppgifter[134]. Av utkastet till beslut framgår att dessa regler fastställs i section 309 i *Intelligence Authorization Act for Fiscal Year 2015*[135], där en principiell längsta lagringstid på fem år för all icke-offentlig telefonkommunikation eller elektronisk kommunikation som inhämtats utan samtycke anges.

[131] Se dekret 14086, section 4, (n).
[132] Se dekret 14086, section 2(c)(i)(A) och (B).
[133] Se dekret 14086, section 2(c)(iv)(B) och (C).
[134] Utkastet till beslut, skäl 150.
[135] Utkastet till beslut, fotnot 272.

I detta avseende rekommenderar dataskyddsstyrelsen kommissionen att förtydliga sin bedömning av reglerna för lagring av amerikanska medborgares personuppgifter i beslutet.

3.2.2 Garanti B – Nödvändighet och proportionalitet ska säkerställas för legitima mål

3.2.2.1 Övergripande skyddsåtgärder i det nya presidentdekretet EO 14086 – nödvändighet och proportionalitet

124. Det nya presidentdekretet, dekret 14086, som i stort ersätter PPD-28, syftar till att fastställa regler som stärker skyddsåtgärderna för amerikansk signalspaningsverksamhet. Reglerna ska genomföras vidare av de organ som ingår i underrättelsesamfundet och på så sätt införlivas i deras interna regler och förfaranden.

125. Genom dekret 14086 införs två nya krav i amerikansk lag, vilka återspeglar de krav som EU-domstolen erinrar om i Schrems II-domen, nämligen att signalspaning ska bedrivas endast i den utsträckning det är nödvändigt för en insamling som främjar en godkänd underrättelseprioritering och då endast i en omfattning och på ett sätt som står i proportion till den godkända underrättelseprioriteringen[136].

126. Enligt dataskyddsstyrelsens uppfattning har dessa delar medtagits för att återspegla de principer om nödvändighet och proportionalitet som föreskrivs i EU-lagstiftningen och i EU-domstolens och Europadomstolens rättspraxis och som syftar till att säkerställa att insamling och behandling av uppgifter begränsas till vad som är nödvändigt och proportionerligt.

127. I detta avseende vill dataskyddsstyrelsen påminna om den fastställda processen för godkännande av underrättelseprioriteringar samt möjligheten till undantag från denna (se punkterna 116 och 117).

128. Vidare konstaterar dataskyddsstyrelsen att de principer om nödvändighet och proportionalitet som anges i presidentdekretet inom ett år måste operationaliseras och införlivas i de regler och förfaranden som tillämpas av vart och ett av de organ som ingår i underrättelsesamfundet[137].

3.2.2.2 Särskilda skyddsåtgärder för insamling av signalunderrättelser

129. Dataskyddsstyrelsen noterar också att dekret 14086 innehåller begränsningar när det gäller de ändamål för vilka personuppgifter får respektive inte får samlas in i samband med insamling av signalunderrättelser[138].

130. Dataskyddsstyrelsen välkomnar det faktum att riktad insamling enligt dekretet ska prioriteras framför insamling i bulk[139]. Avseende insamling av signalunderrättelser innehåller dekretet en förteckning över tolv mål för vilka uppgifter får samlas in, vilka måste underbyggas ytterligare och omvandlas till konkreta underrättelseprioriteringar (se punkt 117), samt en förteckning över fem mål för vilka insamling av signalunderrättelser inte får utföras[140]. Dessa bestämmelser utgör i princip en garanti för uppgiftsinsamlingens nödvändighet.

[136] Se dekret 14086, section 2, (a), (ii), A och B.
[137] Se dekret 14086, section 2, (c), (iv), B.
[138] Se dekret 14086, section 2, (b), (i), A, 1–12.
[139] Se dekret 14086, section 2, (c), (ii), A.
[140] Se dekret 14086, section 2, (b), (ii), A, 1–5.

131. Dataskyddsstyrelsen erinrar dock om att dekret 14086 också ger USA:s president möjlighet att lägga till andra mål i förteckningen (se punkterna 114 och 115)[141].

3.2.2.3 Särskilda skyddsåtgärder för bulkinsamling

132. EU-domstolen underströk i Schrems I-domen att ”[…] skyddet av den grundläggande rätten till respekt för privatlivet på unionsnivå [kräver] att undantag från och begränsningar av skyddet för personuppgifter ska inskränkas till vad som är strängt nödvändigt”[142] och fastställde att ”en lagstiftning som tillåter myndigheterna generell åtkomst till innehållet i elektroniska kommunikationer anses kränka det väsentliga innehållet i den grundläggande rätten till respekt för privatlivet, som garanteras i artikel 7 i stadgan”.

133. I Schrems II-domen[143] betonade EU-domstolen, så som erinras om ovan, i sin analys avseende bulkinsamling mot bakgrund av en jämförande läsning av dekret 12 333 och PPD-28, i synnerhet i punkterna 183–185, att möjligheten till bulkinsamling, ”som inom ramen för övervakningsprogram som grundar sig på E.O. 12333 gör det möjligt att få åtkomst till uppgifter som befinner sig i transit till Förenta staterna utan att denna åtkomst är underkastad någon som helst domstolskontroll […] [under alla omständigheter inte fastställs] […] på ett sätt som tillräckligt tydligt och precist reglerar omfattningen av en sådan bulkinsamling av personuppgifter ”.

134. Dataskyddsstyrelsen konstaterar således att EU-domstolen inte principiellt utesluter bulkinsamling, utan i stället, i sitt beslut i Schrems II-målet, fastslår att sådan bulkinsamling för att vara laglig måste ske inom ramen för tillräckligt tydliga och precisa regler som begränsar insamlingens omfattning.

135. Dataskyddsstyrelsen är också medveten om att dekret 14086, som ersätter PPD-28, innebär att nya skyddsåtgärder och begränsningar avseende insamling och användning av uppgifter som samlas in utanför USA införs, i och med att de begränsningar som anges i Fisa och andra mer specifika delar av den amerikanska lagen inte är tillämpliga.

136. När det gäller bulkinsamling konstaterar dataskyddsstyrelsen att detta enligt dekret 14086 även fortsättningsvis tillåts. Faktum är att dataskyddsstyrelsen vill framhålla att definitionen av bulkinsamling förblir densamma som i den tidigare gällande PPD-28: *insamling av signalunderrättelser som samlas in i ”bulk” avser tillåten insamling av stora mängder signalunderrättelseuppgifter som, på grund av tekniska eller operativa hänsyn, samlas in utan urvalsfaktorer (t.ex. utan specifika identifierare eller urvalstermer)*[144].

137. Sedan Schrems II-domen har EU-domstolen inte preciserat exakt vilka skyddsåtgärder som krävs i samband med bulkinsamling. Dataskyddsstyrelsen påminner dock om att Europadomstolen har utfärdat viktiga beslut om bulkinsamling och relevanta skyddsåtgärder i detta sammanhang.

138. Dataskyddsstyrelsen påminner om att bulkinsamling, eftersom det innebär insamling av stora mängder data utan urvalsfaktorer, innebär större risker för individerna[145] än riktad insamling och därför kräver ytterligare skyddsåtgärder.

---

[141] Se dekret 14086, section 2, (b), (i), B.
[142] Schrems I-domen, punkt 92.
[143] Se Schrems II-domen.
[144] Se dekret 14086, section 4, (b).
[145] Se exempelvis Europadomstolen (stora avdelningen), Big Brother Watch m.fl./Förenade kungariket, dom av den 25 maj 2021 (nedan kallad *Europadomstolens dom i målet Big Brother Watch*), skäl 363, där Europadomstolen anger att den *inte är övertygad om att det är mindre inkräktande när relaterade kommunikationsuppgifter inhämtas genom bulkavlyssning än när innehåll förvärvas.*

139. Dataskyddsstyrelsen noterar också att EU-domstolen fastslagit ytterligare rättspraxis gällande lagring av trafik- och lokaliseringsuppgifter och senare tillgång till dessa uppgifter som lagras av telekommunikationsoperatörer, även för ändamål som rör den nationella säkerheten, som, även om den inte kan anses vara direkt tillämplig i detta sammanhang, i viss mån kan vara relevant för den aktuella bedömningen av bulkinsamling inom ramen för dekret 12333.

1) Ändamålsbegränsning

140. Dekret 12333 föreskriver att bulkinsamling ska användas endast sedan det fastställs att *de uppgifter som krävs för att främja en godkänd underrättelseprioritering inte rimligen kan erhållas genom riktad insamling*[146], samt att den berörda delen av underrättelsesamfundet ska *tillämpa rimliga metoder och tekniska åtgärder för att begränsa uppgiftsinsamlingen till vad som är nödvändigt för att främja en godkänd underrättelseprioritering, samtidigt som insamlingen av irrelevanta uppgifter minimeras*[147]. Utöver dessa skyddsåtgärder erkänner dataskyddsstyrelsen också att användningen av de uppgifter som samlats in i bulk är begränsad till användning som syftar till att uppnå ett eller flera av de mål som anges i förteckningen[148]. Dataskyddsstyrelsen betonar vidare att även om dessa mål är mer detaljerade än de som angavs i det tidigare gällande PPD-28, som nu i stort sett har ersatts av dekret 14086, är omfattningen av den insamling som får göras fortfarande potentiellt bred, dvs. den kan omfatta stora datavolymer.

141. Även här vill dataskyddsstyrelsen erinra om att dekret 14086 också ger USA:s president möjlighet att lägga till andra mål i förteckningen (se punkt 115)[149].

2) Oberoende förhandstillstånd

142. Dataskyddsstyrelsen betonar att Europadomstolen fäster stor vikt vid oberoende förhandstillstånd i samband med bulkinsamling av uppgifter för ändamål som rör den nationella säkerheten. Domstolen fastslår i synnerhet att *för att minimera risken för missbruk av befogenheten att bulkavlyssna anser domstolen att processen måste vara föremål för "heltäckande skyddsåtgärder", vilket innebär att det på nationell nivå ska göras en bedömning av åtgärdernas nödvändighet och proportionalitet i varje steg i processen, att bulkavlyssning ska kräva oberoende tillstånd från det att insatsen inleds, det vill säga när dess syfte och omfattning fastställs och att insatsen ska vara föremål för tillsyn och oberoende efterhandsgranskning. Enligt domstolens uppfattning är dessa skyddsåtgärder grundläggande och utgör hörnstenarna i varje regelverk för bulkavlyssning som överensstämmer med artikel 8*[150].

143. Dataskyddsmyndigheten noterar också följande stycke i denna dom i stora avdelningen, där Europadomstolen ytterligare framhåller att den *instämmer i avdelningens uppfattning att även om rättsligt tillstånd är ett "viktigt skydd mot godtycke" är det inte ett "nödvändigt krav"* (se punkterna 318–320 i avdelningens dom). *Icke desto mindre bör bulkavlyssning kräva tillstånd från ett oberoende organ, det vill säga ett organ som är fristående från den verkställande makten*[151].

[146] Dekret 14086, section 2(c)(ii)(A).
[147] Dekret 14086, section 2(c)(ii)(A).
[148] Dekret 14086, section 2(c)(ii)(B).
[149] Se dekret 14086, section 2(c)(ii)(C).
[150] Se Europadomstolens dom i målet Big Brother Watch, punkt 350.
[151] Se Europadomstolens dom i målet Big Brother Watch, punkt 351.

144. I detta sammanhang konstaterar dataskyddsstyrelsen att presidentdekretet inte innehåller några bestämmelser om ett sådant oberoende förhandstillstånd för bulkinsamling och att detsamma gäller dekret 12333 (se avsnittet nedan om dekret 12333).

3) Lagringsregler

145. Dataskyddsstyrelsen påminner om att reglerna om varaktigheten av insamling och lagring av uppgifter utgör en annan viktig uppsättning skyddsåtgärder. I detta avseende betonar Europadomstolen *att nationell lagstiftning bör fastställa gränser för avlyssningens varaktighet, det förfarande som ska iakttas för att undersöka, använda och lagra de erhållna uppgifterna, de försiktighetsåtgärder som ska vidtas när uppgifterna kommuniceras till andra parter samt de omständigheter under vilka uppgifter som erhållits genom avlyssning får eller måste raderas eller förstöras*[152] eftersom dessa skyddsåtgärder *är lika relevanta för bulkavlyssning*[153].

146. I detta avseende är det dataskyddsstyrelsens uppfattning att presidentdekretet omfattar lagringsregler för personuppgifter som samlats in genom signalspaning, inbegripet i bulk[154]. Dataskyddsstyrelsen noterar att enligt dekret 14086, section 2(c)(iii)(A) ska varje del av underrättelsesamfundet som hanterar personuppgifter som samlats in genom signalspaning fastställa och tillämpa regler och förfaranden för att minimera spridning och lagring av personuppgifter insamlade genom signalspaning. I dessa bestämmelser anges dock ingen specifik lagringstid. I stället i hänvisar man i allmänhet till motsvarande regler för lagring av uppgifter om amerikanska medborgare och till situationer där det saknas slutgiltigt fastställd lagringstid. Dataskyddsstyrelsen vill därför uttrycka sin oro över att det, precis som när det gäller riktad insamling (se punkt 122), i dessa sammanhang saknas tydligt fastställda lagringstider i det aktuella presidentdekretet. Kommissionen uppmanas att offentliggöra sin bedömning av nödvändigheten och proportionaliteten hos de lagringstider som gäller för på amerikanska medborgare samt av den information som finns att tillgå om faktiska lagringstider på de områden där slutgiltigt fastställda lagringstider saknas i amerikansk lag. Utkastet till beslut innehåller nämligen, i sin nuvarande form, endast en enda kort punkt med en påminnelse om denna allmänna regel[155] samt en fotnot[156], vilket inte är tillräckligt för att fastställa om de aktuella lagringstiderna är nödvändiga och proportionerliga. Eftersom det här, som Europadomstolen understrukit, handlar om en skyddsåtgärd som är avgörande för de registrerades möjlighet att utöva sina rättigheter i ett sammanhang där det redan i utgångsläget vidtas en synnerligen inkräktande åtgärd för att samla in deras uppgifter, uppmanar dataskyddsstyrelsen kommissionen att göra ytterligare förtydliganden om de olika lagringstiderna i praktiken.

4) Skyddsåtgärder avseende spridning

147. Dataskyddsstyrelsen påminner om att Europadomstolen erkänner vikten av lagstadgade bestämmelser rörande vidare spridning av uppgifter som samlats in, inbegripet när det gäller bulkinsamling, för att säkerställa att principerna om nödvändighet, proportionalitet och ändamålsbegränsning får genomslag[157].

[152] Se Europadomstolens dom i målet Big Brother Watch, punkt 348.
[153] Se Europadomstolens dom i målet Big Brother Watch, punkt 348.
[154] Se dekret 14086, section 2, (c), (iii), A, (2)(a)–(c).
[155] Se utkastet till beslut, skäl 150.
[156] Se utkastet till beslut, fotnot 271.
[157] Se Europadomstolens dom i målet Big Brother Watch, punkt 348.

148. I section 2(c)(iii)(A)(1)(c) i dekret 14086 anges det att uppgifter om utländska medborgare som samlats in genom signalspaningsverksamhet endast får spridas om en behörig person med lämplig utbildning rimligen tror att personuppgifterna kommer att skyddas på lämpligt sätt och att mottagaren har ett behov av att känna till uppgifterna.

149. Mot bakgrund av detta är dataskyddsstyrelsens uppfattning att bestämmelserna om spridning i dekret 14086 inte omfattar något uttryckligt förbud mot spridning för andra ändamål än sådana som rör den nationella säkerheten när det gäller spridning till behöriga amerikanska myndigheter[158]. Dataskyddsstyrelsen uppmanar kommissionen att ytterligare klargöra de tillämpliga reglerna och skyddsåtgärderna i detta fall.

150. Dataskyddsstyrelsen befarar därför att uppgifter som erhållits av behöriga myndigheter inom underrättelsesamfundet i ett senare skede skulle kunna spridas till andra behöriga myndigheter i USA för ändamål som rör brottsbekämpning, inbegripet bekämpning av allvarliga brott, i samband med brottsutredningar. På så sätt skulle brottsbekämpande myndigheter, utan några specifika ytterligare begränsningar, kunna erhålla uppgifter som det hade varit förbjudet för dem att själva samla in. Dataskyddsstyrelsen uppmanar därför kommissionen att fördjupa sin bedömning av denna punkt.

151. När det gäller vidare överföring (spridning till mottagare utanför den amerikanska förvaltningen, inbegripet till en annan stat eller en internationell organisation[159]) påminner dataskyddsstyrelsen om att den är av uppfattningen att uppgiftsskyddet ska upprätthållas även i samband med vidare överföringar, inbegripet på området för nationell säkerhet[160].

152. I detta avseende innehåller presidentdekretet vissa skyddsåtgärder i form av ett krav på att innan uppgifterna sprids, vederbörligen beakta ändamålet för spridningen – även om det inte uttryckligen krävs att ändamålet också måste röra den nationella säkerheten – arten och omfattningen av de personuppgifter som sprids samt potentiella skadeverkningar för den eller de berörda personerna.

153. Dataskyddsstyrelsen erkänner att vissa av dessa skyddsåtgärder, i synnerhet kravet att beakta potentiella skadeverkningar[161] för berörda registrerade, återspeglar vissa av Europadomstolens krav, men vill också betona att Europadomstolen utöver detta kräver att det ska finnas en rättsligt bindande skyldighet *att analysera och fastställa huruvida den utländska mottagaren erbjuder en godtagbar miniminivå av skyddsåtgärder*[162], vilket dataskyddsstyrelsen inte uttryckligen hittar i presidentdekretets bestämmelser om spridning till utländska mottagare. Dataskyddsstyrelsen uppmanar därför kommissionen att ytterligare bedöma denna aspekt.

154. Dataskyddsstyrelsen noterar också att kommissionen inte, som en del av sin bedömning av adekvat skyddsnivå, beaktat befintliga internationella avtal som ingåtts med tredjeländer eller internationella organisationer och som kan innehålla särskilda bestämmelser om underrättelsetjänsters internationella överföring av personuppgifter till tredjeländer. Dataskyddsstyrelsen anser att ingåendet av bilaterala eller multilaterala avtal syftande till underrättelsesamarbete med tredjeländer sannolikt påverkar den rättsliga ram för dataskydd som är föremål för bedömning.

---

[158] Se dekret 14086, section 2.(c)(iii)(A)(1).

[159] Se dekret 14086, särskilt section 2.(c)(iii)(A)(1), (d).

[160] Se exempelvis dataskyddsstyrelsens yttrande 14/2021 om Europeiska kommissionens utkast till genomförandebeslut enligt förordning(EU) 2016/679 om adekvat skydd av personuppgifter i Förenade kungariket, antaget den 13 april 2021, avsnitten 4.3.2.1 och 4.3.2.2.

[161] Se dekret 14086, section 2.(c)(iii)(A)(1), (d).

[162] Se Europadomstolen (stora avdelningen), dom i målet Centrum för rättvisa/Sverige av den 25 maj 2021, punkt 326.

155. Dataskyddsstyrelsen uppmanar därför kommissionen att klargöra huruvida det finns sådana avtal och på vilka villkor sådana avtal får ingås samt att bedöma huruvida bestämmelserna i internationella avtal kan påverka den skyddsnivå för personuppgifter som överförs från EES som säkerställs genom den rättsliga ramen och de metoder som används för vidare överföringar för ändamål som rör den nationella säkerheten.

5) Tillfällig bulkinsamling i syfte att stödja den inledande tekniska fasen av en riktad insamling

156. Dataskyddsstyrelsen påminner om att diskussionerna i samband med den senaste gemensamma översynen av skölden för skydd av privatlivet i huvudsak kretsade kring tolkningen och tillämpningen av den ytterligare grund (situation/scenario) för bulkinsamling som anges i första meningen i fotnot 5 i section 2 i PPD-28, där följande fastslås: *Begränsningarna i denna section är inte tillämpliga på signalspaningsuppgifter som inhämtas tillfälligt i syfte att underlätta riktad insamling*. De amerikanska myndigheterna förklarade vid den tidpunkten innebörden av ”signalspaningsuppgifter som inhämtas tillfälligt i syfte att underlätta riktad insamling”. Av dessa diskussioner drog dataskyddsstyrelsen slutsatsen att den aktuella fotnoten innebär att uppgifter får samlas in i bulk – oaktat de sex ändamål för detta som anges – om det görs tillfälligt, med avsikten att fastställa en identifierare för ett fastställt mål. Detta skulle då utgöra ytterligare en grund för bulkinsamling av uppgifter, och i detta fall skulle endast de allmänna principerna i section 1 i PPD-28 gälla. Såsom påpekas ovan anger EU-domstolen avseende bulkinsamling i Schrems II-domen att den anser att dekret 12333 och PPD-28 tillsammans inte ”tillräckligt tydligt och precist reglerar omfattningen av en sådan bulkinsamling av personuppgifter”[163].

157. Dataskyddsstyrelsen noterar att dekret 14086 fortfarande innehåller ett undantag som medger sådan bulkinsamling[164], men välkomnar det faktum att undantaget har begränsats jämfört med PPD-28 och att ytterligare skyddsåtgärder införts genom dekret 14086.

158. Dataskyddsstyrelsen är medveten om att det nya dekret 14086 innehåller skyddsåtgärder som förblir tillämpliga i samband med denna typ av tillfällig, teknisk bulkinsamling, i synnerhet de allmänna principerna om nödvändighet och proportionalitet i förhållande till den godkända underrättelseprioriteringen när uppgifter inhämtas utan urvalsfaktorer innan en riktad insamling äger rum (dekret 14086, section 2(a)-(b), section 2(c)(i)). Dataskyddsstyrelsen är också av uppfattningen att sådan bulkinsamling till stöd för en senare riktad insamling av signalunderrättelser också omfattas av de ytterligare skyddsåtgärder som anges i subsection (2)(c)(iii) och framåt[165].

159. Dataskyddsstyrelsen påminner dock (se punkt 117 ovan) om att definitionen av ”godkänd underrättelseprioritering” innefattar bestämmelser om ett undantagsförfarande där den nationella underrättelsetjänstens tjänsteman med ansvar för skyddet av medborgerliga friheter (CLPO) inte deltar.

160. Dataskyddsstyrelsen konstaterar också att skyddsåtgärderna i den subsection om bulkinsamling inte är tillämpliga på tillfällig bulkinsamling som används för att stödja den inledande tekniska fasen av en riktad insamling av signalunderrättelser, så som beskrivs i dekret 14086, section 2(c)(ii)(D), vilket bland annat innebär att uppgifter som samlas in i bulk i detta sammanhang kan komma att användas för andra ändamål än de som förtecknas i subsection 2 (c)(ii). Dataskyddsstyrelsen skulle gärna se att det i utkastet till beslut förtydligades för vilka ändamål uppgifter som samlats in i bulk i detta sammanhang

[163] Schrems II-domen, punkt 183.
[164] Se dekret 14086, section 2 (c), (ii), D och utkastet till beslut, fotnot 226.
[165] Se föregående avsnitt för ytterligare kommentarer till dessa bestämmelser.

kan användas samt vad som gäller avseende tillämpningen av de begränsningar för insamlingen av signalunderrättelser i allmänhet som anges i subsection 2(c)(i) (dvs. att insamling får ske endast för de legitima mål som förtecknas där) på tillfällig bulkinsamling.

161. Sammanfattningsvis vill dataskyddsstyrelsen framhålla att det fortfarande finns oklarheter kring det undantag som medger tillfällig bulkinsamling syftande till riktad insamling och de skyddsåtgärder som ska tillämpas i samband med det, i synnerhet avseende vilka av de skyddsåtgärder som fastställs i dekret 14086 som är tillämpliga på vilken fas (bulkinsamling, vidare riktad insamling), och uppmanar kommissionen att ytterligare bedöma dessa aspekter, samt att i framtida gemensamma översyner bedöma hur de fungerar i praktiken.

162. Dataskyddsstyrelsen beklagar också att begreppet ”tillfällig” enligt dataskyddsstyrelsens uppfattning fortfarande, även om det beskrivs något mer utförligt i presidentdekretet än det gjorde i PPD-28, verkar innebära att bulkinsamling får fortsätta så länge något mål inte har fastställts. I detta avseende påminner dataskyddsstyrelsen om att det är nödvändigt att ha tydliga och exakta regler och betonar det avgörande skydd som dessa regler utgör för de registrerade.

163. Sammanfattningsvis är dataskyddsstyrelsen, när det gäller de skyddsåtgärder som är tillämpliga på bulkinsamling, fortfarande oroad över att möjligheten att samla in uppgifter i bulk, dvs. utan identifierare, trots de ytterligare skyddsåtgärder som införts genom dekret 14086, kvarstår och inte omfattas av viktiga skyddsåtgärder såsom förhandsgodkännande av uppgiftsinsamlingen, inbegripet i det undantagsfall där tillfällig, teknisk bulkinsamling tillåts. Aspekter som också bör beaktas är behovet av ytterligare förtydliganden och den oro som uttryckts gällande ändamålsbegränsningen avseende åtkomst till uppgifterna i ett senare skede, tydliga och stränga regler för lagring av uppgifterna och strängare skyddsåtgärder för spridning av uppgifter som samlats in i bulk, inbegripet vid vidare överföringar.

164. Rent allmänt vill dataskyddsstyrelsen framhålla att det beslut från Europadomstolen som nämns ovan återigen understryker hur viktigt det är med en omfattande tillsyn från oberoende tillsynsmyndigheter. Dataskyddsstyrelsen betonar att oberoende tillsyn över alla faser i den process där myndigheterna får tillgång till uppgifter för ändamål som rör den nationella säkerheten utgör ett viktigt skydd mot godtyckliga övervakningsåtgärder och att sådan tillsyn därmed också är betydelsefull för bedömningen av en adekvat dataskyddsnivå. Syftet med att garantera tillsynsmyndigheternas oberoende i den mening som avses i artikel 8.3 i stadgan är att säkerställa en ändamålsenlig och tillförlitlig övervakning av efterlevnaden av bestämmelserna om skydd för enskilda med avseende på behandling av personuppgifter. Detta gäller särskilt under omständigheter där den enskilde på grund av övervakningens hemliga karaktär inte kan begära granskning eller delta direkt i ett eventuellt granskningsförfarande före eller under utförandet av övervakningsåtgärden.

165. Dataskyddsstyrelsen påminner om att den anser att bedömningen av huruvida en adekvat skyddsnivå säkerställs beror på alla omständigheter i fallet, i synnerhet effektiviteten hos den efterhandstillsyn och den rättsliga prövning som fastställs i den rättsliga ramen.

3.2.2.4 Rättslig ram för särskild insamling för ändamål rörande den nationella säkerheten av organ inom underrättelsesamfundet på och utanför USA:s territorium

166. I Schrems II-domen framhåller EU-domstolen att det inte går att utläsa av section 702 i Fisa att ”det föreligger några begränsningar av behörigheten enligt denna artikel att genomföra övervakningsprogram för att inhämta utländska underrättelseuppgifter, och inte heller att det finns

några garantier för icke-amerikaner som eventuellt omfattas av dessa program”[166]. EU-domstolen är därför av följande uppfattning: ”Mot denna bakgrund kan denna bestämmelse […] inte säkerställa en skyddsnivå som är väsentligen likvärdig med den som garanteras i stadgan, såsom den tolkats i den rättspraxis som anges i punkterna 175 och 176 ovan. Enligt denna rättspraxis måste en rättslig grund som gör ingreppet i de grundläggande rättigheterna möjligt – för att uppfylla kraven enligt proportionalitetsprincipen – i sig definiera räckvidden av begränsningen i utövandet av den aktuella rättigheten och innehålla tydliga och precisa bestämmelser som reglerar räckvidden och tillämpningen av den aktuella åtgärden samt fastställer minimikrav”[167].

167. Vad avser dekret 12333 (av EU-domstolen kallat *E.O. 123333*) konstaterar EU-domstolen att ”det dekretet inte heller ger några rättigheter som kan göras gällande mot amerikanska myndigheter vid domstol”[168]. Efter en analys av de villkor på vilka bulkinsamling får ske enligt det aktuella dekretet jämfört med PPD-28 drar EU-domstolen slutsatsen att möjligheten till bulkinsamling ”som inom ramen för övervakningsprogram som grundar sig på E.O. 12333 gör det möjligt att få åtkomst till uppgifter som befinner sig i transit till Förenta staterna utan att denna åtkomst är underkastad någon som helst domstolskontroll – [under alla omständigheter inte] fastställs […] på ett sätt som tillräckligt tydligt och precist reglerar omfattningen av en sådan bulkinsamling av personuppgifter”[169].

168. När det gäller dessa särskilda former för uppgiftsinsamling föreskrivs genom dekret 14086 nu nya regler.

3.2.2.4.1 Insamling av uppgifter för ändamål rörande den nationella säkerheten i enlighet med section 702 i Fisa

169. Gällande Fisa 702[170] påminner dataskyddsstyrelsen om att PCLOB i sin senaste rapport välkomnar slutsatsen att även personer som inte är amerikanska medborgare *i praktiken omfattas […] av de begränsningar för tillgång och lagring som krävs enligt de olika myndigheternas minimerings- och eller målinriktningsförfaranden, på grund av kostnaderna för och svårigheterna att identifiera och avlägsna uppgifter som rör amerikanska medborgare i en stor mängd uppgifter, vilket innebär att hela datamängden brukar behandlas i enlighet med de strängare amerikanska normerna*.

170. Enligt rapporten *bedrivs inte insamling av kommunikation i bulk inom ramen för programmet*. Såväl 2014 som 2021 års utgåva av *Statistical Transparency Report* från ODNI bekräftar denna slutsats. Enligt PCLOB:s rapport används dessutom ”särskilda urvalsfaktorer”, t.ex. en e-postadress eller ett telefonnummer för att rikta övervakningen.

171. Dataskyddsstyrelsen påminner dock också om att det å andra sidan, rörande section 702, klargjordes i samband med den senaste översynen av skölden för skydd av privatlivet att en ”person” som ska identifieras som mål kan avse flera individer med samma identifierare, förutsatt att samtliga dessa individer är utländska medborgare och uppfyller de tillämpliga kriterierna för att utgöra ett mål. Dataskyddsstyrelsen påminner också om att man i samband med den tredje årliga gemensamma översynen av skölden för skydd av privatlivet 2019 begärde ytterligare förtydliganden om programmet

[166] Se Schrems II-domen, punkt 180.
[167] Se Schrems II-domen, punkt 180.
[168] Se Schrems II-domen, punkt 182.
[169] Se Schrems II-domen, punkt 183.
[170] Se Privacy and Civil Liberties Oversight Board: *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, s. 100.

Upstream för att utesluta omfattande och urskillningslös tillgång till utländska medborgares personuppgifter[171].

172. Dataskyddsstyrelsen påminner också om att det faktum att insamling av uppgifter enligt section 702 i Fisa ska uppfylla villkoret att ”ett viktigt syfte med insamlingen är att erhålla utländska underrättelseuppgifter” inte undanröjer all osäkerhet avseende insamlingens ändamålsbegränsning och nödvändighet. Dataskyddsstyrelsen noterar dock att signalspaning enligt dekret 14086, section 2(a)(A) och (B) ska bedrivas endast sedan det fastställts att åtgärderna är nödvändiga för att främja en godkänd underrättelseprioritering och då endast i en omfattning och på ett sätt som står i proportion till den prioriteringen samt att åtgärderna i den mån det är möjligt ska skräddarsys för att främja den godkända prioriteringen, med beaktande av relevanta faktorer som hur inkräktande insamlingen är, hur känsliga uppgifterna är samt att den negativa inverkan på den personliga integriteten och de medborgerliga friheterna inte får vara oproportionerligt stor. Dataskyddsstyrelsen väntar sig fortfarande ytterligare förtydliganden av hur detta konkret ska genomföras och operationaliseras, inbegripet när det gäller tillämpningen av section 702 i Fisa.

173. Efter uppdateringen av Fisa efterlyste dataskyddsstyrelsen, eftersom den själv inte har direkt tillgång till denna information, en oberoende bedömning av nödvändighet och proportionalitet när det gäller definitionen av ”mål” och begreppet ”utländska underrättelseuppgifter” i section 702 i Fisa (inbegripet i samband med Upstream-programmet). Dataskyddsstyrelsens tidigare efterlysning av en fördjupad oberoende bedömning av processen för tillämpning av urvalstermer i särskilda fall (”tasking of selectors”) samt av ytterligare förtydliganden avseende programmet Upstream är fortfarande relevant. Mot bakgrund av det nya presidentdekretet dekret 14086 vill dataskyddsstyrelsen därför efterlysa mer information i syfte att kunna bedöma och övervaka även hur och i vilken utsträckning de nyligen införda principerna om nödvändighet och proportionalitet tillämpas i praktiken i detta sammanhang. Dataskyddsstyrelsen förväntar sig också att denna aspekt bedöms i kommande gemensamma översyner.

174. Dataskyddsstyrelsen välkomnar det faktum att den fullt verksamma styrelsen för tillsyn av personlig integritet och medborgerliga friheter (PCLOB) i egenskap av oberoende tillsynsmyndighet har beslutat att genomföra ”ett tillsynsprojekt för att undersöka det övervakningsprogram som den verkställande makten bedriver i enlighet med section 702 i lagen om underrättelseverksamhet och övervakning utomlands (Fisa), som en förberedelse inför slutdatumet för section 702 i december 2023 och allmänhetens och kongressens följande övervägande av dess förnyade godkännande”[172]. Dataskyddsstyrelsen välkomnar också det faktum att översynen omfattar utvalda fokusområden för utredning, inklusive men inte nödvändigtvis begränsat till, begäranden om information om amerikanska medborgare som samlats in i enlighet med section 702 och insamling inom ramen för Upstream som bedrivits i enlighet med section 702[173] samt att den också inbegriper en översyn av programmets historiska och prognostiserade värde och effektivitet, liksom av huruvida de befintliga skyddsmekanismerna för personlig integritet och medborgerliga friheter är tillräckliga[174]. Dataskyddsstyrelsen betonar följaktligen att tillgång till de resultat PCLOB kommer fram till i sin rapport om section 702 behövs för att kunna göra en adekvat och heltäckande bedömning av de åtgärder för integritetsskydd som föreskrivs och tillämpas i samband med detta övervakningsprogram.

[171] Se tredje gemensamma översynen, sidan 17, punkt 83.

[172] Se *NOTICE OF THE PCLOB OVERSIGHT PROJECT EXAMINING SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA)*.

[173] Se ovan.

[174] Se ovan.

175. Mot bakgrund av det nya presidentdekretet dekret 14086 efterlyser dataskyddsstyrelsen mer information i syfte att kunna bedöma och övervaka även hur och i vilken utsträckning de nyligen införda principerna om nödvändighet och proportionalitet, samt de övriga skyddsåtgärder som anges i texten, tillämpas i praktiken i detta sammanhang.

3.2.2.4.2 Insamling av uppgifter för ändamål rörande den nationella säkerheten i enlighet med dekret 12333

176. Som EU-domstolen påpekar i Schrems II-domen bör analysen av lagstiftningen i det tredjeland för vilket adekvat skyddsnivå bedöms inte begränsas till de lagar och den praxis som medger övervakning inom det aktuella landets gränser utan även omfatta en analys av de bestämmelser i tredjelandets lagstiftning som kan utgöra rättslig grund för övervakningsoperationer utanför landets territorium när det gäller EU-uppgifter. Nödvändiga begränsningar av myndigheternas tillgång till uppgifter bör omfatta även personuppgifter under överföring till det land vars skyddsnivå erkänns som adekvat.

177. Dataskyddsstyrelsen välkomnar PCLOB:s allmänna offentliga rapport om presidentdekret 12333, som offentliggjordes i april 2021, men noterar att det endast är allmän information som kan utläsas av rapporten, då den till största delen är sekretessbelagd.

178. I detta sammanhang vill dataskyddsstyrelsen återigen, givet den osäkerhet och brist på klarhet som råder kring hur dekret 12333 hittills har tillämpats samt vikten av att klargöra hur det kommer att tillämpas i ljuset av nya dekret 14086, lyfta fram hur viktiga PCLOB:s kommande rapporter om denna text är[175]. Dataskyddsstyrelsen inser dock att innehållet i dessa rapporter till största delen kommer att förbli sekretessbelagt och att ingen ytterligare information om hur dekret 12333 används i praktiken eller om dess nödvändighet och proportionalitet därför kommer att bli tillgänglig för allmänheten eller för dataskyddsstyrelsen.

179. Dataskyddsstyrelsen skulle därför särskilt uppskatta om PCLOB:s rapport om tillämpningen av dekret 14086 inte sekretessbelades utan blev tillgänglig i sin helhet när den slutförs, inbegripet bedömningen av hur skyddsåtgärderna i dekret 14086 ska tillämpas på insamling av uppgifter i enlighet med dekret 12333. Dataskyddsstyrelsen uppmanar också kommissionen att vara särskilt uppmärksam på detta i samband med de framtida gemensamma översynerna.

180. Allmänt sett skulle dataskyddsstyrelsen när det gäller de olika instrument i den amerikanska rättsliga ramen som ger amerikanska underrättelsemyndigheter möjlighet att samla in och vidare ta del av och behandla uppgifter gärna se förtydliganden av hur de samspelar med nya dekret 14086. Dataskyddsstyrelsen väntar sig också försäkranden om att de farhågor den uttryckt i sina tidigare yttranden skulle lösas genom antagandet av dessa nya skyddsåtgärder.

181. Dataskyddsstyrelsen uppmanar också kommissionen att ägna dessa aspekter särskild uppmärksamhet i samband med de framtida gemensamma översynerna.

3.2.2.4.3 PCLOB:s rapport

182. Dataskyddsstyrelsen välkomnar det faktum att dekret 14086 föreskriver att PCLOB ska utarbeta en rapport om dekretets genomförande. Dataskyddsstyrelsen betonar att denna rapport bör innefatta en

[175] Den allmänna rapporten om dekret 12333 har till största delen förblivit sekretessbelagd – endast en kortare version har offentliggjorts – liksom rapporten och rekommendationerna om CIA:s verksamhet mot terrorism i enlighet med dekret 12333, där sekretessen också hävts endast delvis.

bedömning av den särskilda möjlighet som presidentdekretet medger att samla in data för de förtecknade ändamålen genom riktad insamling och även genom bulkinsamling, inbegripet av tekniska skäl, för att klargöra de viktigaste villkoren i dekret 14086 och hur de tolkas och tillämpas praktiskt inom ramen för de olika övervakningsprogrammen. En sådan rapport skulle också krävas för att kunna bedöma hur organen i underrättelsesamfundet kommer att införliva presidentdekretet i sina interna regler och förfaranden.

3.2.3 Garanti C – Tillsyn

3.2.3.1 Inledning

183. Den amerikanska underrättelseverksamheten är föremål för en tillsynsprocess i flera nivåer. Strukturen kan delas upp i intern och extern tillsyn. Alla organ inom underrättelsesamfundet har tjänstemän med ansvar för tillsyn och efterlevnad som regelbundet utövar tillsyn över signalspaningsverksamheten, däribland tjänstemän med ansvar för skydd av personlig integritet och medborgerliga friheter och generalinspektörer. Därutöver finns det externa tillsynsorgan, t.ex. styrelsen för tillsyn av personlig integritet och medborgerliga friheter (PCLOB) och styrelsen för tillsyn av underrättelseverksamheten.

184. Dataskyddsstyrelsen påminner om att det sker ett ingrepp när uppgifterna samlas in, men också vid det tillfälle då en myndighet får tillgång till dem för vidare behandling. Europadomstolen har dessutom flera gånger fastställt att varje ingrepp i rätten till integritet och dataskydd bör omfattas av ett effektivt, oberoende och opartiskt system för tillsyn som ska säkerställas antingen av en domare eller av ett annat oberoende organ[176] (t.ex. en administrativ myndighet eller ett parlamentariskt organ).

185. Även om Europadomstolen uttryckt att den föredrar att det är en domare som ansvarar för att tillsyn utövas utesluter den inte att ett annat organ ges detta ansvar *förutsatt att myndigheten är tillräckligt oberoende av den verkställande makten*[177] och *av de myndigheter som utövar övervakningen samt har tillräckliga befogenheter och behörighet att utöva en effektiv, kontinuerlig kontroll*[178].

186. Europadomstolen tillade att *tillsättningssättet och den rättsliga ställningen för ledamöterna av tillsynsorganet*[179] måste beaktas vid bedömningen av organets oberoende.

187. Europadomstolen uppgav också att den ska undersöka huruvida tillsynsorganets verksamhet är öppen för offentlig granskning. Sådan öppenhet kan uppnås till exempel genom att organet regelbundet rapporterar till regeringen respektive lägger fram offentliga rapporter för parlamentet som sedan diskuterar dessa[180].

188. Den oberoende tillsynen av användningen av övervakningsåtgärder beaktas också av EU-domstolen i Schrems II-domen där det konstateras att ”[…] den kontroll som utförs av FISC [syftar] således till att kontrollera om dessa övervakningsprogram överensstämmer med syftet att erhålla utländska

[176] Europadomstolen, dom i målet Klass m.fl./Tyskland av den 6 september 1978 (nedan kallad *Europadomstolens dom i målet Klass*), punkterna 17 och 51.
[177] Europadomstolens dom i målet Zakharov, punkt 258, Europadomstolen, dom i målet Iordachi m.fl./Moldavien av 10 februari 2009, punkterna 40 och 51 samt Europadomstolen, dom i målet Dumitru Popescu/Rumänien av den 26 april 2007, punkterna 70–73.
[178] Europadomstolens dom i målet Klass, punkt 56.
[179] Europadomstolens dom i målet Zakharov, punkt 278.
[180] Europadomstolens dom i målet Zakharov, punkt 283, Europadomstolen, dom i målet L./Norge av den 9 juni 1990, Europadomstolen, dom i målet Kennedy/Förenade kungariket av den 18 maj 2010, punkt 166.

underrättelseuppgifter, men den avser inte 'huruvida målinriktningen för de utvalda personerna är lämplig för att inhämta utländska underrättelseuppgifter'"[181].

3.2.3.2 Intern tillsyn

3.2.3.2.1 Generalinspektörer

189. Dataskyddsstyrelsen konstaterar att generalinspektörerna har getts en rad olika befogenheter som är nödvändiga för att övervaka underrättelseverksamheten. Generalinspektörerna har framför allt tillgång till all den information som behövs för att på ett övergripande plan bedöma hur väl myndigheterna i sitt arbete efterlever lagstiftningen, inbegripet, men inte begränsat till, lagarna om integritet och dataskydd. De kan också utfärda förelägganden och låta personer vittna under ed inom ramen för en utredning som de bedriver.

190. På grundval av ovanstående anser dataskyddsstyrelsen att generalinspektörerna generellt sett har omfattande utredningsbefogenheter. De har dock inte befogenhet att besluta om bindande korrigerande åtgärder och utfärdar endast icke-bindande rekommendationer[182].

191. Dataskyddsstyrelsen erkänner att generalinspektörerna i princip inte får hindras eller förbjudas att inleda, utföra eller slutföra revisioner eller utredningar eller utfärda förelägganden i samband med revisioner eller utredningar[183]. I detta sammanhang konstaterar dataskyddsstyrelsen dock också att generalinspektörerna är underställda chefen för den aktuella myndigheten och verkar under dennes ledning och kontroll. Myndighetscheferna kan förbjuda generalinspektörerna att ta del av information, genomföra en utredning eller utfärda förelägganden i ärenden där ett sådant förbud enligt chefens bedömning är nödvändigt för att skydda den nationella säkerheten. De ansvariga utskotten i den amerikanska kongressen måste dock informeras om utövandet av denna befogenhet[184].

192. Dataskyddsstyrelsen noterar att generalinspektörer kan avsättas endast av presidenten, som måste motivera avsättandet inför kongressen.

193. Dataskyddsstyrelsen noterar att det inte har gjorts några betydande ändringar av den interna tillsynsmekanismen sedan yttrandena från artikel 29-gruppen och därefter från dataskyddsstyrelsen. Dataskyddsstyrelsen anser därför, i linje med artikel 29-gruppens yttrande 01/2016[185], att det generellt sett finns tillräckliga interna tillsynsmekanismer.

3.2.3.3 Extern tillsyn

194. Dataskyddsstyrelsen noterar att det utöver de organ som nämns nedan finns flera andra organ inom den amerikanska förvaltningen som övervakar de amerikanska underrättelsemyndigheternas verksamhet, såsom styrelsen för tillsyn av underrättelseverksamhet (IOB) eller kongressens utskott. De senare kan utföra egna undersökningar och publicera egna rapporter.

---

[181] Schrems II-domen, punkt 179.

[182] Utkast till beslut, skäl 105.

[183] Se lagen om generalinspektörer från 1978, § 3 (a).

[184] Se exempelvis lagen om generalinspektörer från 1978, § 8 (avseende försvarsdepartementet), § 8E (avseende justitiedepartementet), § 8G (d)(2)(A),(B) (avseende NSA), 50. U.S.C. § 403q (b) (avseende CIA), Intelligence Authorization Act For Fiscal Year 2010, section 405(f) (avseende underrättelsesamfundet).

[185] Artikel 29-gruppens yttrande 01/2016.

3.2.3.3.1 Styrelsen för tillsyn av personlig integritet och medborgerliga friheter (PCLOB)

195. Dataskyddsstyrelsen erkänner PCLOB:s omfattande roll i tillsynen av den nya prövningsmekanismen och genomförandet av dekret 14086.

196. För det första omfattar dess nya funktioner samråd med justitieministern om utnämningen av domare till domstolen för dataskyddsgranskning och av de särskilda advokaterna. För det andra kommer PCLOB årligen att se över prövningsprocessen, dvs. behandlingen av giltiga klagomål inom ramen för prövningsmekanismen. I översynen ingår en bedömning av huruvida tjänstemannen med ansvar för skyddet av medborgerliga friheter (CLPO) och domstolen för dataskyddsgranskning har behandlat giltiga klagomål inom rimlig tid, får fullständig tillgång till nödvändig information och verkar i enlighet med dekret 14086 samt en bedömning av underrättelsesamfundets efterlevnad av de beslut som CLPO och domstolen för dataskyddsgranskning fattar.

197. Dessutom måste underrättelsemyndigheterna samråda med PCLOB när de uppdaterar sina interna regler och förfaranden för att genomföra dekret 14086. Därutöver ska PCLOB granska de uppdaterade reglerna och förfarandena och bedöma deras överensstämmelse med dekret 14086[186]. PCLOB:s slutsatser är visserligen inte i strikt mening bindande, men chefen för varje del av underrättelsesamfundet är skyldig att noggrant överväga och genomföra eller på annat sätt beakta alla de rekommendationer som ges vid en sådan granskning, i enlighet med tillämplig lagstiftning[187]. Dataskyddsstyrelsen uppmanar kommissionen att, om utkastet till beslut antas, i framtida översyner ägna särskild uppmärksamhet åt huruvida PCLOB:s rekommendationer har genomförts på myndighetsnivå, och i så fall hur.

198. Dataskyddsstyrelsen påminner om att PCLOB, eftersom den är oberoende, inte har någon skyldighet, utan endast ”uppmuntras” att granska huruvida skyddsåtgärderna i dekret 14086 iakttas korrekt och huruvida underrättelsesamfundet till fullo uppfyller de krav som prövningsförfarandet ställer. Det är dock dataskyddsstyrelsens uppfattning att PCLOB, både i sin kompletterande förklaring till dataskyddsstyrelsen och offentligt[188], har förklarat att man kommer att ta på sig den roll som beskrivs i dekret 14086.

199. Dataskyddsstyrelsen välkomnar också det faktum att man planerar att offentliggöra resultaten av PCLOB:s rapporter. Med tanke på att de organ som är involverade i prövningsmekanismen och de organ som ingår i underrättelsesamfundet i princip måste genomföra, eller annars på annat sätt beakta, rekommendationerna i PCLOB:s rapporter anser dataskyddsstyrelsen att dessa rekommendationer utgör viktiga integritetsskyddsåtgärder.

200. Dataskyddsstyrelsen noterar att PCLOB:s tillgång till information begränsas i fall där USA:s president tillåter departement, organ eller enheter i den amerikanska förvaltningen att vidta ”hemliga åtgärder”[189][190].

---

[186] Dekret 14086, section 2(c)(iv) och section 2(c)(v).
[187] Dekret 14086, section 2(c)(v)(B).
[188] https://documents.pclob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e-2687b14ed9b9/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL).pdf.
[189] Enligt 50 U.S.C. § 3093(e)(1) avser termen *covert action* (hemlig åtgärd) en åtgärd eller åtgärder som vidtas av den amerikanska regeringen i syfte att påverka politiska, ekonomiska eller militära förhållanden utomlands, där den amerikanska regeringens roll inte kommer att vara uppenbar eller erkännas offentligt, men som inte omfattar 1) åtgärder som främst syftar till att inhämta underrättelser, konventionella åtgärder för kontraspionage […].
[190] 42 U.S.C. § 2000ee (g) (5), 50 U.S.C. § 3093(a).

201. I linje med sina tidigare yttranden anser dataskyddsstyrelsen att PCLOB, i egenskap av oberoende organ vars rekommendationer på ett betydelsefullt sätt bidragit till reformer i USA och vars rapporter har varit en särskilt användbar källa för att förstå hur de olika övervakningsprogrammen fungerar, utgör en viktig del i tillsynsstrukturen.

202. Dataskyddsstyrelsen beklagade dock i den tredje årliga gemensamma översynen av den tidigare skölden för skydd av privatlivet i EU och USA att PCLOB endast gav dataskyddsstyrelsen tillgång till samma information som allmänheten. Det är också beklagligt att PCLOB inte efter sin första rapport gav ut några uppföljande rapporter om PPD-28 för att ge ytterligare information om hur skyddsåtgärderna i PPD-28 tillämpas och inte heller någon generell uppdaterad rapport om section 702 i Fisa.

203. Dataskyddsstyrelsen välkomnar därför PCLOB:s besked att en uppföljningsrapport om section 702 i Fisa förväntas bli publicerad inom en snar framtid. Dataskyddsstyrelsen är också tillfreds med PCLOB:s åtagande att tillåta offentliggörande av sina rapporter om dekret 14086. Dataskyddsstyrelsen erinrar dock om att utlämnandet av icke sekretessbelagda rapporter är reglerat i amerikansk lag och måste samordnas med underrättelsesamfundets organ; PCLOB kan alltså inte besluta om detta på egen hand.

204. Dataskyddsstyrelsen påminner därför om att dess säkerhetsprövade experter, om utkastet till beslut antas, i samband med framtida översyner av EU:s och USA:s dataskyddsram bör få granska ytterligare dokument och diskutera ytterligare sekretessbelagda uppgifter i den utsträckning det behövs för att säkerställa att informationen i rapporterna kan bedömas på ett adekvat sätt, med beaktande av relevanta nationella säkerhetsintressen och tillämpliga åtgärder för integritetsskydd.

205. Dataskyddsstyrelsen välkomnar PCLOB:s oberoende och den tillsyn som organet utövar över den nationella underrättelsesamfundet som måste följa, eller annars på annat sätt beakta, dess rekommendationer, vilket är föremål för rapportering av PCLOB till den amerikanska kongressen.

206. Med beaktande av att Europadomstolen, när det gäller offentlig granskning[191], kräver att rapporter från ett tillsynsorgan ska läggas fram för och diskuteras av parlamentet anser dataskyddsstyrelsen att det är tillräckligt att PCLOB minst en gång per halvår inkommer med en rapport till USA:s president och i synnerhet till kongressens (senatens och representanthusets) utskott[192], dvs. till de amerikanska parlamentariska organen.

3.2.3.3.2 Domstolen för övervakning av utländsk underrättelseinformation (FISC)

207. Domstolen för övervakning av utländsk underrättelseinformation (Foreign Intelligence Surveillance Court, FISC) ansvarar för tillsynen av insamlingen av personuppgifter i enlighet med section 702 i Fisa[193]. Domstolens beslut kan överklagas till appellationsdomstolen för övervakning av utländsk underrättelseinformation (Foreign Intelligence Surveillance Court of Review, FISCR).

208. FISC övervakar certifieringsförfarandet för insamling av utländsk underrättelseinformation enligt seCtion 702 i Fisa och sköter tillståndsgivningen för elektronisk övervakning, fysisk genomsökning och andra utredningsåtgärder för ändamål rörande utländska underrättelser[194]. FISC godkänner också förfarandena för målinriktning, minimering och sökning i certifieringarna som är rättsligt bindande för

[191] Europadomstolens dom i målet Zakharov, punkt 283, Europadomstolen, dom i målet L./Norge av den 9 juni 1990, Europadomstolen, dom i målet Kennedy/Förenade kungariket av den 18 maj 2010, punkt 166.
[192] 42 U.S.C. § 2000ee, (e).
[193] 50 U.S.C. 1881 (a).
[194] www.fisc.uscourts.gov/about-foreign-intelligence-surveillance-court.

de amerikanska underrättelsemyndigheterna[195]. Om FISC anser att kraven inte har uppfyllts får domstolen helt eller delvis avslå certifiering och kräva att förfarandena ändras.

209. Om överträdelser av förfarandena för målinriktning konstateras kan FISC kräva att det berörda underrättelseorganet vidtar korrigerande åtgärder[196]. Dessa korrigerande åtgärder kan vara på individnivå eller strukturell nivå, dvs. allt från upphörande med insamlingen av uppgifter och radering av olagligt insamlade uppgifter till förändringar av insamlingsrutinerna, inbegripet vägledning och utbildning av personal.

210. Dataskyddsstyrelsen är medveten om att dekret 14086 föreskriver att CLPO och domstolen för dataskyddsgranskning ska rapportera överträdelser till biträdande ministern för nationell säkerhet som ska rapportera dessa överträdelser till FISC[197].

211. Som EU-domstolen konstaterade i sin dom i Schrems II-målet är det inte enskilda övervakningsåtgärder, utan hela övervakningsprogram, som är föremål för godkännande från FISC[198]. Dataskyddsstyrelsens farhågor att FISC inte säkerställer effektiv rättslig tillsyn över målsökningen av personer som inte är amerikanska medborgare kvarstår därför. Problemet verkar inte lösas genom det nya dekret 14086.

212. När det gäller oberoende förhandstillstånd[199] för övervakning enligt section 702 i Fisa beklagar dataskyddsstyrelsen att FISC, så vitt dataskyddsstyrelsen kan förstå av utkastet till beslut[200] och de förklaringar som den amerikanska regeringen har gett, inte är bunden av de ytterligare skyddsåtgärder som införs genom dekret 14086 vid sin certifiering av program som medger målinriktning mot personer som inte är amerikanska medborgare. Dataskyddsstyrelsen anser att de ytterligare skyddsåtgärder som detta dekret innehåller icke desto mindre bör beaktas i detta sammanhang. Dataskyddsstyrelsen erinrar om att rapporter från PCLOB skulle vara ett särskilt användbart verktyg för att bedöma hur skyddsåtgärderna i dekret 14086 kommer att genomföras och hur de tillämpas när uppgifter samlas in i enlighet med section 702 i Fisa.

3.2.4 Garanti D – Enskilda personer ska ha tillgång till effektiva rättsmedel

213. Dataskyddsstyrelsen påminner om att effektiva och verkställbara rättigheter för individen är av grundläggande betydelse för att skyddsnivån i ett tredjeland ska kunna betraktas som adekvat. Registrerade måste ha tillgång ett effektivt rättsmedel för att tillvarata sina rättigheter när de anser att dessa rättigheter inte respekteras eller inte har respekterats. EU-domstolen förklarar i domarna i Schrems I- och Schrems II-målen att ”[e]n lagstiftning i vilken det inte föreskrivs någon möjlighet för enskilda att använda rättsmedel för att erhålla tillgång till, rätta eller radera uppgifter som rör dem, respekterar inte det väsentliga innehållet i den grundläggande rätten till effektivt domstolsskydd, vilken är stadfäst i artikel 47 i stadgan”[201].

---

[195] 50 U.S.C.1881a (i).
[196] 50 U.S.C. § 1803 (h).
[197] Dekret 14086, section 3 (c) (i) (D), dekret 14086 section 3 (d) (i) (F).
[198] Schrems II-domen, punkt 179.
[199] När det gäller insamling av uppgifter i bulk i enlighet med dekret 12333 där FISC inte är behörig, är dataskyddsstyrelsen oroad över det faktum att det inte finns någon process för förhandstillstånd för insamling av uppgifter i bulk (se även garanti B).
[200] Utkastet till beslut, skäl 165.
[201] Schrems I-domen, punkt 95, Schrems II-domen, punkt 187.

214. När det gäller rättsmedlen finns det i det amerikanska systemet en betydelsefull begränsning som gör det mycket svårt att väcka talan mot amerikanska statens övervakningsåtgärder vid allmänna domstolar. Enligt den amerikanska konstitutionen måste den enskilda kunna visa att han eller hon har talerätt, dvs. kunna visa på ”konkret, specifik och faktisk skada eller överhängande risk för sådan skada”[202]. I ärenden som rör övervakning verkar detta krav sakna giltighet, eftersom enskilda personer inte meddelas om övervakningen ens när åtgärderna har avslutats.

215. I detta sammanhang välkomnar dataskyddsstyrelsen inrättandet, genom dekret 14086, av en särskild prövningsmekanism för att hantera och lösa klagomål från utländska medborgare avseende amerikanska signalspaningsåtgärder. Inom ramen för denna nya prövningsmöjlighet är talerättskravet inte tillämpligt: enligt section 4(k)(ii) i dekret 14086 behöver klaganden inte visa att hans eller hennes uppgifter verkligen har varit föremål för amerikansk signalspaning. De registrerade kan alltså åberopa de skyddsåtgärder som föreskrivs i dekret 14086, inbegripet de som föreskrivs i de andra relevanta lagar och bestämmelser som avses i section 4(d)(iii) i dekret 14086[203]. I detta avseende tillför den nya mekanismen en möjlighet till prövning som annars inte skulle finnas.

216. Den nya mekanismen består av två nivåer. På första nivån kan enskilda personer lämna in klagomål till nationella underrättelsetjänstens tjänsteman med ansvar för skyddet av medborgerliga friheter (CLPO). På andra nivån har enskilda personer möjlighet att överklaga CLPO:s beslut till ett nybildat organ, den så kallade domstolen för dataskyddsgranskning (DPRC). I avsnitten nedan ligger fokus främst på prövningsmekanismens andra nivå. Dataskyddsmyndigheten anser att CLPO, i egenskap av regeringstjänsteman, inte är tillräckligt oberoende från den verkställande makten och därför inte i sig kan uppfylla kraven i artikel 47 i stadgan på ett tillfredsställande sätt. Denna bedömning har bekräftats av kommissionen vid flera tillfällen.

3.2.4.1 Kan inrättandet av domstolen för dataskyddsgranskning på grundval av ett presidentdekret i sig vara tillräckligt?

217. Domstolen för dataskyddsgranskning är inte en allmän domstol som inrättats av kongressen i enlighet med artikel III i konstitutionen, utan har inrättats på grundval av ett dekret utfärdat av presidenten. Även om dataskyddsstyrelsen är medveten om och generellt sett välkomnar det underliggande syftet, nämligen att undvika kravet att visa talerätt (se även punkt 215), väcker detta en grundläggande fråga, nämligen huruvida en sådan prövningsmekanism kan uppfylla kraven i artikel 47 i stadgan (överhuvudtaget)? Enligt denna artikel har var och en vars unionsrättsligt garanterade fri- och rättigheter har kränkts rätt till ett effektivt rättsmedel inför en domstol som har inrättats enligt lag.

218. I den engelska versionen av artikel 47 i stadgan nämns en ”tribunal”, medan man i andra språkversioner har valt ett ord motsvarande ”domstol”[204]. I Schrems II-domen upprepar EU-domstolen att ”enskilda ska ha möjlighet att utöva sin rätt till rättslig prövning inför en oavhängig och opartisk domstol för att erhålla tillgång till, rätta eller radera personuppgifter som rör dem”[205]. I samma sammanhang, dvs. bedömning av adekvat skyddsnivå, uttrycker dock EU-domstolen uppfattningen att ett effektivt rättsligt skydd mot sådana inkräktningar kan säkerställas inte endast av en domstol utan även av en annan typ av organ som kan ge garantier som är väsentligen likvärdiga med de som krävs

[202] Clapper/Amnesty International USA, 568 U.S. 398 (2013) II. s. 10.
[203] Section 5(h) i dekret 14086 ger uttryckligen registrerade rätt att inkomma med klagomål inom ramen för prövningsmekanismen.
[204] Exempelvis ”Gericht” i den tyska versionen.
[205] Schrems II-domen, punkt 194.

enligt artikel 47 i stadgan[206]. På samma sätt föreskrivs det i den europeiska konventionen om de mänskliga rättigheterna att ”[v]ar och en, vars i denna konvention angivna fri- och rättigheter kränkts, skall ha tillgång till ett effektivt rättsmedel inför en nationell myndighet”[207], som inte, i enlighet med den uppfattning som Europadomstolen konsekvent uttrycker, nödvändigtvis behöver vara en rättslig myndighet[208]. Det är snarare myndighetens befogenheter och möjligheter att garantera rättssäkerheten, i synnerhet dess oberoende från den verkställande makten och förmåga att säkerställa att förfarandena är rättvisa, som är relevanta för bedömningen av hur effektivt ett förfarande inför myndigheten är som rättsmedel[209]. Det verkar som om båda domstolarna grundar sin bedömning på mer än rent formalistiska kriterier, och anser att de materiella skyddsåtgärderna är avgörande.

219. I Schrems II-målet ägnade EU-domstolen särskild uppmärksamhet åt förekomsten av effektiv prövning i samband i med åtkomst till personuppgifter för nationella säkerhetsändamål. Dataskyddsstyrelsen konstaterar dock att EU-domstolen inte i detta sammanhang diskuterade formuleringen ”som har inrättats enligt lag” i artikel 47 i stadgan, trots att ombudsmannen för skölden för skydd av privatlivet inte heller hade sin grund i den amerikanska lagstiftningen. I stället för att behandla denna fråga bedömde EU-domstolen andra aspekter för att pröva om skyddsnivån var adekvat, såsom bristen på korrigerande befogenheter. Schrems II-domen ger alltså ingen ledning för hur ”som har inrättats enligt lag” i stadgans artikel 47 ska bedömas. Det finns dock andra avgöranden där EU-domstolen har kommenterat denna fråga. Med hänvisning till fast rättspraxis från Europadomstolen på området erinrar EU-domstolen i sina domar i målen C-487/19 och C-132/20 om att införandet av uttrycket ”inrättats enligt lag” syftar till att undvika att organisationen av domstolsväsendet i ett demokratiskt samhälle överlåts till den verkställande maktens fria skön, och ska säkerställa att detta område regleras av en lag som antas av den lagstiftande makten på ett sätt som är förenligt med de bestämmelser som reglerar utövandet av dess behörighet[210]. Som framgår av detta uttalande har rätten till en domstol som inrättats enligt lag ett mycket nära samband med garantin om oberoende.

220. Mot bakgrund av detta drar dataskyddsstyrelsen slutsatsen att den särskilda prövningsmekanism som inrättats genom dekret 14086 inte per definition är otillräcklig bara för att den inte utgör en domstol som inrättats i enlighet med artikel III i konstitutionen. Avgörande för analysen av skyddsnivån i detta avseende är huruvida de skyddsåtgärder som föreskrivs i dekret 14086 och som kompletteras av dekretet från justitieministern i tillräcklig utsträckning säkerställer domstolen för dataskyddsgransknings beroende i förhållande till andra aktörer.

221. Kommissionen bör kontinuerligt övervaka om reglerna i dekret 14086 och de bestämmelser som kompletterar dekretet till fullo genomförs och fungerar effektivt i praktiken. Detta gäller i synnerhet de regler som syftar till att stärka oberoendet för domstolen för dataskyddsgranskning. Dessutom bör alla eventuella ändringar av ramen noggrant granskas med avseende på konsekvenserna för kommissionens bedömning enligt utkastet till beslut. I detta sammanhang konstaterar dataskyddsstyrelsen att ändringar i dekret 14086 eller i justitieministerns dekret skulle kunna utlösa antagandet av omedelbart tillämpliga genomförandeakter om att upphäva, dra tillbaka eller ändra beslutet om adekvat skyddsnivå[211].

---

[206] Se Schrems II-domen, punkt 197.

[207] Artikel 13 i den europeiska konventionen om de mänskliga rättigheterna.

[208] Europadomstolens dom i målet Klass, punkt 67, Europadomstolens dom i målet Big Brother Watch, punkt 359.

[209] Europadomstolens dom i målet Klass, punkt 67, Europadomstolens dom i målet Big Brother Watch, punkt 359.

[210] Se EU-domstolens dom av den 6 oktober 2021, C-487/19, W.Ż, ECLI:EU:C:2021:798 och EU-domstolens dom av den 29 mars 2022, C-132/20, Getin Noble Bank S.A., ECLI:EU:C:2022:235, punkterna 129 och 121.

[211] Utkastet till beslut, skäl 212.

3.2.4.2 Tillräckligt oberoende från den verkställande makten

222. I Schrems II-domen understryker EU-domstolen att domstolens eller organets oberoende måste säkerställas, i synnerhet i förhållande till den verkställande makten, genom alla nödvändiga garantier, även när det gäller villkoren för återkallande av ett förordnande eller ogiltigförklaring av en tillsättning. Mer specifikt har EU-domstolen kritiserat att ombudsmannen utsågs av utrikesministern och rapporterade direkt till denne. Ombudsmannen ansågs utgöra en integrerad del av det amerikanska utrikesdepartementet. EU-domstolen fann också att ett återkallat förordnande eller en ogiltigförklaring av ombudsmannens tillsättning inte omfattades av några särskilda garantier, vilket kunde äventyra ombudsmannens oberoende av den verkställande makten.

223. Dataskyddsstyrelsen medger att bestämmelserna i dekret 14086 och det kompletterande dekretet från justitieministern inte ålägger domstolen för dataskyddsgranskning att rapportera till justitieministern, så som skulle vara fallet om det rörde sig om en relation mellan en överordnad och en underordnad part. Domstolen för dataskyddsgranskning är inte heller föremål för löpande tillsyn från justitieministerns sida[212]. Dessa skyddsåtgärder utgör en betydande förbättring jämfört med skölden för skydd av privatlivet. Domstolen för dataskyddsgranskning har dock inrättats inom den verkställande makten, närmare bestämt justitiedepartementet. Framför allt av detta skäl kommer det att vara genomförandet av skyddsåtgärderna samt deras effektivitet i praktiken som till stor del avgör om domstolen för dataskyddsgranskning, som å ena sidan inrättats inom ramen för den verkställande makten men å andra sidan inte utgör någon integrerad del av justitiedepartementet, kan betraktas som tillräckligt oberoende i praktiken. Dataskyddsstyrelsen uppmanar kommissionen att noggrant övervaka huruvida skyddsåtgärderna till fullo omsätts i praktik. Dataskyddsstyrelsen föreslår också att uttrycket ”löpande tillsyn” ändras, så att det i stället framgår av texten att ”domarna” vid domstolen för dataskyddsgranskning inte är föremål för tillsyn överhuvudtaget. Kommissionen har bekräftat att formuleringen om ”löpande tillsyn” är avsedd att tolkas på det sättet.

224. Utöver ovanstående skyddsåtgärder omfattar dataskyddsramen också vissa garantier avseende tillsättning och avsättande av ”domarna” i domstolen för dataskyddsgranskning. De utses visserligen av justitieministern, men tillsättningen baseras på de kriterier som används för att utvärdera sökande till federala domarämbeten samt inbegriper ett samråd med PCLOB. Att avsätta en ”domare” innan hans eller hennes ämbetsperiod löpt ut eller under ett pågående förfarande är möjligt endast under snävt definierade omständigheter som, efter vad dataskyddsstyrelsen förstår, bygger på de bestämmelser som gäller för federala domare[213]. Tillämpningen av dessa regler utgör ytterligare ett steg för att stärka oberoendet för domstolen för dataskyddsgranskning. Även när det gäller dessa regler kommer det praktiska genomförandet att vara avgörande. Det framgår dock inte tydligt av utkastet till beslut i sig om och i så fall hur efterlevnaden av dessa krav kommer att övervakas i USA. Utifrån de ytterligare förklaringar som kommissionen och den amerikanska regeringen har gett är dataskyddsstyrelsens bild att PCLOB kan ta upp de ovan nämnda bestämmelserna i sin årliga översyn av prövningsprocessen och att det ansvar att övervaka och säkerställa efterlevnaden av alla rättsliga krav som tillfaller justitiedepartementets generalinspektör även omfattar kraven i dekret 14086 och i de dekret genom vilka domstolen för dataskyddsgranskning inrättas. Dataskyddsstyrelsen uppmanar kommissionen att klargöra denna aspekt i utkastet till beslut. Med det sagt bör kommissionen ta hänsyn till dessa skyddsåtgärder när den övervakar användningen av de metoder för personuppgiftsbehandling som bedöms i utkastet till beslut.

[212] Justitieministerns dekret, § 201.7 (d).
[213] Dekret 14086, section 3(d)(iv), justitieministerns dekret, § 201.7.

225. I utkastet till beslut behandlas inte frågan om huruvida den amerikanska presidenten har rätt att avsätta ”domare” från domstolen för dataskyddsgranskning, och i så fall under vilka omständigheter. Det är dataskyddsstyrelsens uppfattning att presidenten inte har någon sådan befogenhet, så som förklarats av kommissionen och bekräftats av företrädare för den amerikanska regeringen. Dataskyddsstyrelsen föreslår att denna aspekt förtydligas i beslutet om adekvat skyddsnivå.

226. ”Domare” till domstolen för dataskyddsgranskning utses för en förnybar period om fyra och får inte ha varit anställda inom den verkställande makten under de två föregående åren[214]. Under sin ämbetstid vid domstolen för dataskyddsgranskning får de inte ha några andra officiella förpliktelser eller någon annan anställning inom den amerikanska förvaltningen[215]. De får dock, till skillnad från federala domare, delta i utomrättslig verksamhet, inbegripet affärsverksamhet, finansiell verksamhet, ideell insamlingsverksamhet, förvaltningsverksamhet och tjänstgöring som jurist så länge verksamheten inte inkräktar på deras opartiska fullgörande av sina förpliktelser eller på effektiviteten och oberoendet hos domstolen för dataskyddsgranskning[216]. Rättsligt oberoende bygger inte bara på frånvaron av instruktioner, utan också på personligt oberoende. I detta sammanhang är faktorer som ämbetsperiodens längd, möjligheten att tillsättas för ännu en period och risken för intressekonflikter relevanta. Den period på fyra år som fastställs i dekret 14086 respektive justitieministerns dekret är visserligen kortare än exempelvis ämbetsperioden för domare vid EU-domstolen (som är sex år med möjlighet till förlängning) och för domare vid Europadomstolen (nio år utan möjlighet till förlängning), men ger inte i sig upphov till oro. Enligt vad dataskyddsstyrelsen känner till finns det ingen rättspraxis som föreskriver någon viss minimilängd för ämbetsperioderna[217]. Dataskyddsstyrelsen erkänner också att domarna får bedriva utomrättslig verksamhet endast under förutsättning att denna, enkelt uttryckt, inte ger upphov till intressekonflikter som riskerar att påverka deras arbete vid domstolen för dataskyddsgranskning. Den amerikanska regeringens ytterligare förklaringar ger vid handen att dessa krav dessutom är föremål för granskning och övervakning av PCLOB och justitiedepartementets generalinspektör (se punkt 226 ovan). Hur detta krav tillämpas och demonstreras i praktiken bör granskas vid de gemensamma översynerna.

227. Enligt section 3(d)(i)(B) i dekret 14086 måste samtliga ”domare” vid domstolen för dataskyddsgranskning ha genomgått säkerhetsprövning för att få hantera sekretessbelagda uppgifter, dvs. för att kunna utföra just den handläggning av ärenden som rör den nationella säkerheten som är deras uppgift[218]. Vissa EU-lagar och -förordningar om säkerhetsprövning undantar i stället domare från kravet på säkerhetsprövning avseende deras utförande av sina rättsliga åligganden, eftersom en så detaljerad granskning anses kunna stå i konflikt med rättsväsendets oberoende[219]. Enligt förklaringar från den amerikanska regeringen genomgår kandidater till utnämningar inom rättsväsendet visserligen en grundlig granskning, men den som utsetts att tjänstgöra som domare i en federal domstol i USA behöver sedan inte genomgå någon säkerhetsprövning för att få tillgång till sekretessbelagda handlingar som är relevanta för ett ärende.

228. Enligt dataskyddsstyrelsens uppfattning visar de omständigheter som beskrivs ovan delvis på skillnader mellan den ställning och status som en federal domare åtnjuter jämfört med en ”domare” vid

[214] Justitieministerns dekret, § 201.3 (a).
[215] Justitieministerns dekret, § 201.3 (c).
[216] Justitieministerns dekret, § 201.7 (c).
[217] Se även, i tillämpliga delar, Europadomstolen (stora avdelningen), dom i målet Centrum för rättvisa/Sverige av den 25 maj 2021, punkt 346.
[218] Se justitieministerns dekret, § 201.11 (b) och utkastet till beslut, skäl 177.
[219] T.ex. § 2.3 i den tyska lagen om säkerhetsprövning.

domstolen för dataskyddsgranskning. De skyddsåtgärder som finns på plats ger dock inte anledning att tvivla på om domstolen för dataskyddsgransknings är oberoende. Dataskyddsstyrelsen uppmanar kommissionen att, om utkastet till beslut antas, prioritera de ovan nämnda skyddsåtgärderna i samband med den första gemensamma översynen av dataskyddsramen. Vidare förväntar sig dataskyddsstyrelsen att kommissionen lever upp till sitt åtagande att dra tillbaka, ändra eller upphäva beslutet om den verkställande makten i USA väljer att begränsa de skyddsåtgärder som fastställs i presidentdekretet[220].

3.2.4.3 Domstolen för dataskyddsgransknings befogenheter

3.2.4.3.1 Tillgång till information

229. Ett effektivt rättsligt skydd förutsätter att en domstol har tillräckliga utredningsbefogenheter för att pröva den omtvistade åtgärden. I sin dom i Kadi II-målet fastställde EU-domstolen med avseende på artikel 47 i stadgan att unionsdomstolarna ska förvissa sig om att det föreligger faktiska omständigheter som utgör ett tillräckligt underlag för ett visst beslut[221]. EU-domstolen anger att det ”ankommer […] på unionsdomstolen att vid sin prövning vid behov anmoda den behöriga unionsmyndigheten att inkomma med uppgifter eller bevisning, oavsett om det rör sig om hemliga handlingar, som är av relevans för domstolens prövning”[222] och att det i samband med detta ”inte kan göras gällande att uppgifterna eller bevisen är sekretessbelagda eller hemliga”[223].

230. Enligt skäl 181 i utkastet till beslut ska domstolen för dataskyddsgranskning pröva de beslut som fattats av CLPO på grundval av, åtminstone, CLPO:s utredning samt alla eventuella uppgifter och inlagor som inkommit från klaganden, den särskilda advokaten eller en underrättelsemyndighet. I utkastet till beslut anges vidare att domstolen för dataskyddsgranskning ska ha tillgång till alla nödvändiga uppgifter och kan erhålla dessa från CLPO. Detta grundar sig på den bestämmelse i § 201.9(b) i justitieministerns dekret som ger domstolen för dataskyddsgranskning befogenhet att begära att CLPO vid ODNI kompletterar utredningen med specifika förklarande eller klargörande uppgifter samt tar fram ytterligare faktauppgifter om så krävs för att domstolen för dataskyddsgranskning ska kunna genomföra sin prövning. Dataskyddsstyrelsens uppfattning är att domstolen dataskyddsgransknings bedömning alltså inte på något sätt är begränsad till CLPO:s slutsatser på den första nivån i den nya prövningsmekanismen. Tvärtom kan domstolen för dataskyddsgranskning efterfråga både ytterligare rättslig information och, framför allt, ytterligare faktauppgifter att lägga till grund för sin analys av huruvida en överträdelse som omfattas av regelverket har begåtts. Samtidigt noterar dataskyddsstyrelsen också att dessa generellt sett omfattande utredningsbefogenheter inte omfattar direkt tillgång till de uppgifter om den enskilde som finns lagrade. Kommissionen har förklarat att CLPO alltid kommer att fungera som mellanhand när domstolen för dataskyddsgranskning begär ytterligare information. Domstolen för dataskyddsgransknings tillgång till den information som krävs för att den på ett oberoende sätt ska kunna handlägga en begäran om prövning är alltså i viss mån avhängig CLPO:s tillhandahållande av den nödvändiga informationen. Dataskyddsstyrelsen erkänner att CLPO har en skyldighet att ge domstolen för dataskyddsgranskning ”allt nödvändigt stöd” och att underrättelsemyndigheterna är skyldiga att ge CLPO tillgång till de uppgifter som domstolen för

---

220 Utkastet till beslut, skäl 212.

221 EU-domstolens dom i de förenade målen C-584/10 P, C-593/10 P och C-595/10 P, Europeiska kommissionen m.fl./Yassin Abdullah Kadi av den 18 juli 2013 (nedan kallad *Kadi II-domen*), punkt 119.

222 Kadi II-domen, punkt 120.

223 Kadi II-domen, punkt 125.

dataskyddsgranskning behöver för sina prövningar[224]. Dataskyddsstyrelsen noterar dock också att CLPO i sig inte är oberoende och att CLPO genomför den inledande utredningen av ett klagomål i det första skedet av prövningsförfarandet. Dataskyddsstyrelsen välkomnar därför att PCLOB vid sina årliga översyner av prövningsmekanismen kommer att kontrollera huruvida domstolen för dataskyddsgranskning har fått fullständig tillgång till all nödvändig information[225]. Dataskyddsstyrelsen uppmanar dessutom kommissionen att, om utkastet till beslut antas, inkludera denna aspekt i de gemensamma översynerna för att undersöka vad systemet innebär i praktiken.

3.2.4.3.2 Korrigerande befogenheter

231. En av de centrala bristerna i skölden för skydd av privatlivet, och det som ledde till att EU-domstolen ogiltigförklarade skölden i Schrems II-domen, var det faktum att ombudsmannen saknade tvingande korrigerande befogenheter. EU-domstolen fann att det inte fanns ”någon uppgift om att ombudsmannen skulle vara behörig att fatta bindande beslut i förhållande till dessa myndigheter” (dvs. underrättelsetjänsterna)[226]. Ett (politiskt) åtagande från den amerikanska regeringen om att underrättelsesamfundet skulle korrigera alla eventuella överträdelser av tillämpliga regler som upptäcktes av ombudsmannen var inte tillräckligt för att säkerställa en skyddsnivå som är väsentligen likvärdig med den som stadfästs i artikel 47 i stadgan.

232. Inom ramen för den nya prövningsmekanismen har däremot de beslut som fattas av CLPO och domstolen för dataskyddsgranskning bindande verkan[227]. Dataskyddsstyrelsen erkänner, å ena sidan, att denna befogenhet inte är begränsad till specifika åtgärder, utan omfattar ” lämpliga korrigerande åtgärder” för att ”till fullo gottgöra” en konstaterad överträdelse som omfattas av regelverket. I synnerhet nämns uttryckligen radering av olagligt insamlade uppgifter i section 4(a) i dekret 14086. Å andra sidan noterar dataskyddsstyrelsen också att ordvalet i section 4(a) i dekret 14086 skapar viss osäkerhet avseende processen för att fastställa vad som utgör ” lämpliga korrigerande åtgärder”. Medan en åtgärd ska utformas så att den till fullo gottgör den aktuella överträdelsen ska hänsyn också tas till det sätt på vilket överträdelser av den typ som konstaterats tidigare normalt sett har hanterats[228]. Innebörden och effekten av ett detta krav är oklara. Därför uppmanar dataskyddsstyrelsen kommissionen att noga övervaka de korrigerande åtgärder som faktiskt vidtas.

3.2.4.4 Ingivande av klagomål enligt den nya prövningsmekanismen

233. Den prövningsmekanism som inrättas genom dekret 14086 är endast tillämplig på giltiga klagomål som överförs av den relevanta behöriga myndigheten i en villkorsuppfyllande stat och som rör amerikansk signalspaningsverksamhet i samband med en överträdelse som omfattas[229]. Det finns alltså flera villkor som måste uppfyllas av den som vill utnyttja detta rättsliga skydd.

3.2.4.4.1 Status som villkorsuppfyllande stat

234. För det första måste den stat eller regionala organisation för ekonomisk integration från vilken uppgifterna överfördes till USA ha fastställts vara en villkorsuppfyllande stat innan den uppgiftsöverföring som ligger till grund för klagomålet ägde rum[230]. Det är självklart mycket viktigt att

[224] Dekret 14086, section 3(c)(i)(H) och section 3(d)(iii).
[225] Dekret 14086, section 3(e)(i).
[226] Schrems II-domen, punkt 196.
[227] Dekret 14086, section 3(c)(ii), respektive section 3(d)(ii).
[228] Dekret 14086, section 4(a).
[229] Dekret 14086, section 3(a).
[230] Dekret 14086, section 4(d)(i), 4(k)(i).

den prövningsmekanism som inrättats är tillgänglig när beslutet om adekvat skyddsnivå börjar tillämpas. I skäl 196 i utkastet till beslut föreskrivs därför att beslutets ikraftträdande förutsätter, bland annat, att EU har fått status som villkorsuppfyllande enhet med avseende på prövningsmekanismen. Faktum är att kommissionen verkar utgå från att EU ska ges denna status innan beslutet antas, eftersom utkastet har utrymme för justitieministerns godkännande av EU som villkorsuppfyllande stat[231] (i stället för att detta godkännande tas upp som ett suspensivt villkor i den operativa delen av utkastet till beslut).

3.2.4.4.2 Negativ påverkan på klagandens intressen i fråga om personlig integritet och medborgerliga friheter samt "talerätt"

235. Ett "giltigt klagomål" måste grunda sig på en påstådd "överträdelse som omfattas av regelverket", vilket i sin tur innebär att det måste röra sig om en överträdelse som har en negativ påverkan på klagandens personliga intressen i fråga om personlig integritet och medborgerliga friheter[232]. På grundval av kommissionens ytterligare förklaringar anser dataskyddsstyrelsen inte att villkoret om "negativ påverkan" innebär någon form av begränsning av ett klagomåls behörighet. Som kommissionen uppgett är det snarare så att sådan negativ påverkan skulle föreligga vid alla klagomål avseende behandling av personuppgifter i samband med signalspaningsverksamhet som bryter mot de bestämmelser som avses i section 4(d)(iii), dvs. säkerhetsåtgärderna i dekret 14086. Dataskyddsstyrelsen beklagar att detta inte specificeras i utkastet till beslut och uppmanar kommissionen att ytterligare klargöra begreppet "negativ påverkan" för att säkerställa att alla överträdelser av registrerades rättigheter bedöms och åtgärdas samt att det inte finns någon "grad av allvar" som måste bevisas för att få tillgång till prövning och lämpliga korrigerande åtgärder.

236. Som redan nämnts kräver ett klagomål enligt dekret 14086 inte att klaganden ska visa talerätt (se punkt 215[233]). Dataskyddsstyrelsen välkomnar förtydligandet i section 4(k) i dekret 14086 om att ett "belief test" ska tillämpas, och att det inte krävs att klaganden kan visa att hans eller hennes uppgifter faktiskt har inhämtats via signalspaningsverksamhet. Inrättandet av prövningsmekanismen är ett viktigt steg, eftersom kravet att visa talerätt gör det mycket svårt att bestrida övervakningsåtgärder vid allmänna domstolar i USA.

237. På grund av ovanstående anser dataskyddsstyrelsen inte att möjligheten att väcka talan vid allmän domstol, som också nämns i utkastet till beslut[234], räcker för att säkerställa en adekvat skyddsnivå[235]. I detta avseende påminner dataskyddsstyrelsen om de farhågor som den upprepade gånger har uttryckt avseende kravet att visa talerätt för att kunna vända sig till allmän domstol[236]. Det är dessutom dataskyddsstyrelsens uppfattning, baserat på kompletterande uttalanden från den amerikanska regeringen, att det, trots att talan vid allmän domstol inte utesluts i dekret 14086, är oklart hur en sådan domstol skulle tillämpa det dekretet. Denna fråga skulle kunna undersökas vidare vid framtida översyner om utkastet till beslut antas.

---

[231] Utkastet till beslut, fotnot 320.
[232] Dekret 14086, section 4(k)(i) och 4(d)(ii).
[233] Clapper/Amnesty International USA, 568 U.S. 398 (2013) II. s. 10.
[234] Utkastet till beslut, skäl 187 ff.
[235] Se även Schrems II-domen, punkterna 191 och 192.
[236] Se Artikel 29-gruppens yttrande 01/2016, s. 43.

3.2.4.4.3 Klagomålsförfarande

238. Dataskyddsstyrelsen ställer sig i princip bakom det förfarande enligt vilket klagomål vidarebefordras av medlemsstaternas tillsynsmyndigheter och anser fortfarande att klaganden bör identifieras på EU:s territorium. I utkastet till beslut föreskrivs dock att den som vill lämna in ett sådant klagomål, på samma sätt som inom ramen för skölden för skydd av privatlivets ombudsmannamekanism, måste lämna in klagomålet till en tillsynsmyndighet i en EU-medlemsstat med behörighet att utöva tillsyn över nationella säkerhetstjänsters verksamhet och/eller myndigheters personuppgiftsbehandling[237]. I detta sammanhang påminner dataskyddsstyrelsen om de farhågor som redan uttryckts i artikel 29-gruppens yttrande om skölden för skydd av privatlivet, exempelvis att det kan vara svårt för enskilda att veta vilken myndighet som är behörig, med tanke på den mångfald av olika tillsynsmekanismer för nationella säkerhetstjänster som finns i de olika medlemsstaterna[238]. Med tanke på de nationella dataskyddsmyndigheternas medverkan i tillämpningen och tillsynen av dataskyddsramen vore det lämpligare att kanalisera klagomålen via dem.

3.2.4.5 Domstolen för dataskyddsgranskningens beslut

239. När domstolen för dataskyddsgranskning har granskat klagandens ansökan ska den inte röja huruvida klaganden faktiskt har varit föremål för amerikansk signalspaning. I stället meddelas klaganden att antingen några överträdelser som omfattas av regelverket inte har upptäckts vid granskningen eller så har domstolen för dataskyddsgranskning utfärdat ett beslut med krav på lämpliga korrigerande åtgärder[239]. Detta standardsvar tjänar det generellt sett legitima syftet att skydda känsliga uppgifter om amerikansk underrättelseverksamhet. Dataskyddsstyrelsen vill dock uttrycka sin oro över att dekret 14086 saknar bestämmelser om undantag från standardsvaret.

240. I Kadi II-målet behandlade EU-domstolen intressekonflikten mellan å ena sidan bevarandet av statshemligheter och å den andra ett rättvist och i möjligaste mån kontradiktoriskt förfarande. EU-domstolen fastställde att det i fall där det finns tvingande hänsyn rörande den nationella säkerheten som utgör hinder för att lämna ut uppgifter eller bevisning till den berörda personen ändå ankommer på domstolarna att inom ramen för sin domstolsprövning använda sig av metoder som gör det möjligt att förena berättigade säkerhetshänsyn när det gäller arten av och källorna till uppgifterna med nödvändigheten av att i tillräcklig utsträckning säkerställa den enskildes processuella rättigheter, såsom rätten att yttra sig och principen om ett kontradiktoriskt förfarande[240]. EU-domstolen preciserar vidare att det är domstolarnas sak att, med beaktande av samtliga rättsliga och faktiska omständigheter som åberopats av den behöriga unionsmyndigheten, avgöra om det finns stöd för de skäl för att motsätta sig utlämning av uppgifterna som myndigheten har anfört[241]. Om det visar sig att de skäl som har anförts av den behöriga unionsmyndigheten faktiskt utgör hinder för att den berörda personen informeras om uppgifterna eller bevisningen, måste det ändå göras en lämplig avvägning mellan å ena sidan rätten till ett effektivt domstolsskydd och å andra sidan den nationella säkerheten[242]. Vid en sådan intresseavvägning är det tillåtet att välja sådana alternativ som att lämna ut en sammanfattning av de uppgifter och den bevisning som är i fråga[243]. Även om domstolens slutsatser inte innehåller några krav på de beslut som utfärdas av domstolar, utan handlar om den

---

[237] Utkastet till beslut, skäl 169.

[238] Artikel 29-gruppens yttrande 01/2016, punkterna 48 och 49.

[239] Dekret 14086, section 3(d)(i)(H). I dekret 14086 fastställs att detta svar gäller även för CLPO.

[240] Kadi II-domen, punkt 125.

[241] Kadi II-domen, punkt 126.

[242] Kadi II-domen, punkt 128.

[243] Kadi II-domen, punkt 129.

behöriga myndighetens beslut och domstolsförfarandet, ger de en fingervisning om avvägningen mellan de olika aktuella intressena i samband med rätten till ett effektivt rättsskydd. Ytterligare vägledning återfinns i domen i Big Brother Watch-målet, där Europadomstolen, med hänvisning till kravet på ett rättvist förfarande och i synnerhet principen om ett kontradiktoriskt förfarande, ansåg att ett rättsligt eller annat oberoende organ bör motivera sina beslut[244].

241. Dataskyddsstyrelsen erkänner att domstolen för dataskyddsgranskningsbeslut är motiverade. Domstolen är uttryckligen skyldig att utfärda skriftliga beslut där den redogör för sina avgöranden och preciserar eventuella lämpliga korrigerande åtgärder[245]. Dataskyddsstyrelsen noterar dessutom att den enskilda ska meddelas om sekretessen hävs för uppgifter som har att göra med en granskning som domstolen genomfört[246]. Dataskyddsstyrelsen erkänner också de särskilda advokaternas roll i den nya prövningsmekanismen, som inbegriper att företräda klagandens intressen i ärendet[247]. Mot bakgrund av vad den rättspraxis från EU-domstolen och Europadomstolen som nämns ovan innebär och med tanke på att de beslut som domstolen för dataskyddsgranskning fattar inte kan överklagas utan är slutgiltiga[248] är dataskyddsstyrelsen bekymrad över den generella tillämpningen av standardsvaret från domstolen för dataskyddsgranskning. Dataskyddsstyrelsen påminner om att PCLOB ska göra oberoende översyner av den nya prövningsmekanismen och uppmanar kommissionen att ägna ämnet, däribland eventuella bedömningar från PCLOB:s sida, särskild uppmärksamhet vid framtida översyner av beslutet, om det antas.

4 GENOMFÖRANDE OCH ÖVERVAKNING AV UTKASTET TILL BESLUT

242. När det gäller övervakning och översyner av utkastet till beslut noterar dataskyddsstyrelsen att rättspraxis från EU-domstolen indikerar att det ”[m]ot bakgrund av omständigheten att den skyddsnivå som säkerställs i ett tredjeland kan komma att förändras, ankommer […] på kommissionen, efter det att den antagit ett beslut med stöd av [artikel 45 i dataskyddsförordningen], att regelbundet kontrollera att konstaterandet att det aktuella tredjelandet säkerställer en adekvat skyddsnivå fortfarande är sakligt och rättsligt motiverat. En sådan kontroll krävs under alla förhållanden när det finns uppgifter som ger upphov till tvivel i detta hänseende”[249].

243. Därutöver noterar dataskyddsstyrelsen att det i skrivelsen från handelsdepartementet anges att handelsdepartementet, och andra amerikanska organ efter vad som är lämpligt, ska hålla regelbundna möten med kommissionen, berörda dataskyddsmyndigheter i EU och företrädare för dataskyddsstyrelsen[250].

244. Dataskyddsstyrelsen anser att följande aspekter bör ägnas särskild uppmärksamhet i samband med de kommande periodiska översynerna: det rättsliga skyddet på delstatsnivå i samband med brottsbekämpande myndigheters tillgång till uppgifter, det undantag som medger att amerikanska nationella säkerhetsmyndigheter tillfälligt samlar in uppgifter i bulk i syfte att förbereda för riktad insamling, den praktiska tillämpningen av de nyligen införda principerna om nödvändighet och proportionalitet – inbegripet i samband med programmet Upstream – samspelet mellan dekret 14086 och de olika amerikanska rättsinstrument som tillåter att amerikanska underrättelsemyndigheter

[244] Europadomstolens dom i målet Big Brother Watch, punkt 359.
[245] Justitieministerns dekret, § 201.9 (g).
[246] Dekret 14086, section 3(d)(v).
[247] Justitieministerns dekret, § 201.8 (g).
[248] Justitieministerns dekret, § 201.9 (g).
[249] Schrems I-domen, punkt 76. Se även utkastet till beslut, artikel 3.4.
[250] Utkastet till beslut, bilaga III.

samlar in och vidare behandlar personuppgifter, genomförandet av interna regler och förfaranden, hur dessa säkerhetsåtgärder beaktas även i samband med den tillsyn som utövas under ledning av FISC, prövningsmekanismens effektivitet samt frågorna om vidare överföring, automatiserat beslutsfattande, en omfattande och effektiv tillsyn och kontroll av efterlevnaden av ramens principer och tillgången till effektiv prövning.

245. Dataskyddsstyrelsen noterar att en översyn av konstaterandet att skyddsnivån är adekvat ska göras ett år efter det datum då beslutet om adekvat skyddsnivå meddelas medlemsstaterna och därefter minst vart fjärde år[251]. För att ytterligare stärka den kontinuerliga övervakningen av beslutet om adekvat skyddsnivå uppmanar dataskyddsstyrelsen kommissionen att genomföra de senare översynerna minst vart tredje år.

246. När det gäller dataskyddsstyrelsens och dess företrädares praktiska medverkan i förberedelserna och genomförandet av framtida periodiska översyner upprepar dataskyddsstyrelsen att all relevant dokumentation, inbegripet korrespondens, bör delges dataskyddsstyrelsen skriftligen, i tillräckligt god tid före översynerna. Dataskyddsstyrelsen rekommenderar att tillvägagångssätten för översynen fastställs och avtalas mellan kommissionen, den amerikanska regeringen och dataskyddsstyrelsen senaste tre månader innan översynen ska äga rum, så som var fallet med översynerna avseende skölden för skydd av privatlivet.

247. Dataskyddsstyrelsen konstaterar också med tillfredsställelse att det i skäl 212 i utkastet till beslut ges exempel på ändringar som undergräver skyddsnivån och som kan motivera att ett särskilt skyndsamt upphävandeförfarande inleds. Exemplen gäller främst ändringar av presidentdekret 14086 och det relaterade dekretet från justitieministern.

För Europeiska dataskyddsstyrelsen

Ordförande

(Andrea Jelinek)

[251] Utkastet till beslut, artikel 3.4.