EUROPEISKA
KOMMISSIONEN

Bryssel den 9.10.2024
COM(2024) 451 final

# RAPPORT FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET OCH RÅDET

## om den första regelbundna översynen av hur beslutet om adekvat skyddsnivå enligt ramen för dataskydd mellan EU och Förenta staterna fungerar

## 1. DEN FÖRSTA REGELBUNDNA ÖVERSYNEN – BAKGRUND, FÖRBEREDELSE OCH PROCESS

I sitt beslut av den 10 juli 2023 (*beslutet om adekvat skyddsnivå*) konstaterade kommissionen att ramen för dataskydd mellan EU och Förenta staterna ger en adekvat skyddsnivå för personuppgifter som överförs från EU till organisationer i Förenta staterna[1]. Enligt beslutet om adekvat skyddsnivå ska kommissionen genomföra regelbundna översyner, varav den första bör göras ett år efter det datum då beslutet om adekvat skyddsnivå meddelades medlemsstaterna. Denna rapport avslutar den första översynen.

I enlighet med skäl 211 i beslutet om adekvat skyddsnivå skulle denna första översyn ske efter den nya ramens första verksamhetsår och vara inriktad på att kontrollera om alla delar av ramen har genomförts och fungerar ändamålsenligt. Översynen omfattade alla aspekter av ramens funktion, även mot bakgrund av den rättsliga utveckling som ägt rum sedan beslutet om adekvat skyddsnivå antogs.

Som förberedelse inför översynen samlade kommissionen in information från relevanta berörda parter, särskilt från icke-statliga organisationer med sakkunskap om digitala rättigheter och integritetsskydd[2] och organisationer certifierade enligt dataskyddsramen, genom deras branschorganisationer[3], samt från de amerikanska myndigheter som deltar i genomförandet av ramen. Dessutom har kommissionen samlat in återkoppling från allmänheten genom en särskild inbjudan att lämna synpunkter på portalen ”Kom med synpunkter”[4].

Ett översynsmöte hölls i Washington D.C. den 18 och 19 juli 2024. Det öppnades av EU:s kommissionsledamot med ansvar för rättsliga frågor och konsumentfrågor, Didier Reynders, och Förenta staternas handelsminister, Gina Raimondo[5].

För EU:s räkning genomfördes översynen av företrädare för Europeiska kommissionens generaldirektorat för rättsliga frågor och konsumentfrågor, tillsammans med fem företrädare

[1] Kommissionens genomförandebeslut (EU) 2023/1795 av den 10 juli 2023 i enlighet med Europaparlamentets och rådets förordning (EU) 2016/679 om adekvat skydd av personuppgifter enligt ramen för dataskydd mellan EU och Förenta staterna.

[2] Kommissionen skickade ett frågeformulär till nio icke-statliga organisationer (Human Rights Watch, American Civil Liberties Union, Consumer Federation of America, Center for Digital Democracy, New America Open Technology Institute, Access Now, Electronic Frontier Foundation, Electronic Privacy Information Center och Center for Democracy and Technology), med fokus på relevant utveckling i Förenta staternas rättsliga ram, tillsyns- och verkställighetsmekanismer och hur prövningsmekanismerna fungerar. Kommissionens avdelningar och EDPB:s företrädare träffade även dessa icke-statliga organisationer online den 9 juli 2024.

[3] Kommissionen skickade ett frågeformulär till nio branschorganisationer (Software & Information Industry Association, U.S. Chamber of Commerce, Information Technology Industry Council, the Software Alliance, Centre for Information Policy Leadership, Interactive Advertising Bureau, United States Council for International Business, Computer and Communications Industry Association och Engine), med fokus på erfarenheterna från företag som är certifierade enligt dataskyddsramen, särskilt certifieringsprocessen, åtgärder som vidtagits för att följa dataskyddsramens principer, mekanismer för att hantera förfrågningar och klagomål från enskilda personer osv.

[4] Den mottagna återkopplingen finns på följande länk: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14379-EU-US-Data-Privacy-Framework-report-of-the-Commission-on-how-the-framework-is-functioning_sv.

[5] Översynsmötet organiserades per ämne och varje särskild punkt på dagordningen introducerades genom en kortfattad presentation av den berörda amerikanska myndigheten, EU-företrädaren eller EU-organisationen, följt av en detaljerad frågestund. Ramens ”kommersiella aspekter” (dvs. tillämpning och genomförande av krav som gäller för företag som certifierats enligt dataskyddsramen) togs upp den första dagen, medan frågor som rör regeringens tillgång till personuppgifter diskuterades den andra dagen.

som utsetts av Europeiska dataskyddsstyrelsen (EDPB) och som kommer från olika nationella dataskyddsmyndigheter och Europeiska datatillsynsmannen[6]. För Förenta staternas räkning deltog företrädare från handelsministeriet, utrikesministeriet, den federala konkurrensmyndigheten, transportministeriet, den nationella underrättelsetjänsten, justitieministeriet, generalinspektören för underrättelsegemenskapen samt ledamöter av styrelsen för tillsyn av personlig integritet och medborgerliga friheter (PCLOB). Därutöver lämnade företrädare för organisationer som erbjuder oberoende tvistlösningstjänster och den amerikanska skiljedomssammanslutningen (American Arbitration Association, AAA) information under de relevanta översynssessionerna. Dessutom informerades översynsdeltagarna genom presentationer från organisationer som certifierats enligt dataskyddsramen om hur företag uppfyller ramens krav.

Kommissionens iakttagelser bygger också på offentligt tillgängligt material, t.ex. domstolsbeslut, relevanta amerikanska myndigheters genomförandebestämmelser och genomförandeförfaranden, rapporter och studier från icke-statliga organisationer, insynsrapporter från företag som certifierats enligt dataskyddsramen, årsrapporter från oberoende tillsynsorgan samt medierapporter.

## 2. IAKTTAGELSER

### 2.1. Kommersiella aspekter

#### 2.1.1. Certifieringen

För att kunna ta emot personuppgifter som överförs från EU på grundval av dataskyddsramen måste ett amerikanskt företag certifiera, och sedan årligen återcertifiera, hos handelsministeriet att det följer särskilda dataskyddskrav (*dataskyddsramens principer*). Certifieringen kräver att ett företag omfattas av den federala konkurrensmyndighetens eller transportministeriets utrednings- och verkställighetsbefogenheter, offentliggör sitt åtagande att följa dataskyddsramens principer och offentliggör sin integritetsskyddspolicy och genomför dessa krav fullt ut[7]. Innan en certifiering slutförs kontrollerar handelsministeriet om företaget har uppfyllt alla certifieringskrav[8].

Vid översynsmötet förklarade handelsministeriet att fokus under dataskyddsramens första år har legat på att införa certifieringsprocessen, inbegripet att utveckla särskilda it-verktyg, uppdatera förfaranden, samarbeta med företag och genomföra annan uppsökande/medvetandehöjande verksamhet. Vid tidpunkten för översynsmötet hade mer än 2 800 företag blivit certifierade enligt dataskyddsramen. Detta innebär att fler företag har blivit certifierade enligt dataskyddsramen än enligt den tidigare ramen, skölden för skydd av privatlivet, under det första verksamhetsåret[9]. Enligt information från handelsministeriet är 70 % av deltagarna små och medelstora företag och ett stort antal av de företag som är certifierade enligt dataskyddsramen (47 %) är verksamma inom sektorn för information, kommunikation och teknik (IKT). Dessutom är 60 % av företagen certifierade enbart för andra

[6] Kommissionen och EDPB:s företrädare sammanträdde den 12 juni och den 10 juli 2024 för att förbereda översynen, diskutera de synpunkter som mottagits och identifiera vilka aspekter som kräver ytterligare informationsinsamling och förtydliganden.
[7] Avsnitt I.2 i bilaga I till beslutet om adekvat skyddsnivå.
[8] Bilaga III till beslutet om adekvat skyddsnivå.
[9] Under motsvarande period hade 2 400 blivit certifierade enligt skölden för skydd av privatlivet.

uppgifter än personaluppgifter, 2,5 % är certifierade enbart för personaluppgifter och 37,5 % är certifierade för båda uppgiftstyperna.

Handelsministeriet har antagit de förfaranden som krävs för att hantera ansökningar från företag. Företagen måste lämna in sina ansökningar om certifiering på handelsministeriets webbplats för dataskyddsramen (https://www.dataprivacyframework.gov/). Den innehåller information om hur man ansluter sig till dataskyddsramen[10] och om företagets skyldigheter enligt ramen[11]. Ett särskilt team på handelsministeriet, under ledning av en särskild direktör för dataskyddsramen, ansvarar för alla aspekter som rör förvaltningen och administrationen av dataskyddsramen, inbegripet certifieringsprocessen och övervakningen av efterlevnaden. Varje ansökan tilldelas en viss anställd som förblir ansvarig för det berörda företaget under hela certifieringsprocessen.

För att certifieras enligt ramen lämnar företagen in sin ansökan, inbegripet ett utkast till integritetsskyddspolicy. Handelsministeriet kontrollerar om den uppfyller de relevanta kraven i dataskyddsramen. När organisationer vill certifiera olika enheter inom en företagskoncern (t.ex. olika dotterbolag) begär och granskar handelsministeriet antingen en övergripande integritetsskyddspolicy som tydligt anger alla enheter som ska omfattas eller separata policyer för varje enhet. Handelsministeriet kontrollerar också med den oberoende instansen för handläggning av klagomål[12] som anges i ansökan huruvida organisationen faktiskt har registrerat sig hos den. För företag som väljer panelen för dataskyddsmyndigheter (t.ex. på grund av att de behandlar personaluppgifter) kontrollerar handelsministeriet om företaget har betalat de avgifter som krävs för att använda panelen. Vid behov kontrollerar handelsministeriet också huruvida sökanden omfattas av den federala konkurrensmyndighetens eller transportministeriets behörighetsområde (och därför är berättigad att ansluta sig till dataskyddsramen).

Om alla villkor är uppfyllda informerar handelsministeriet organisationen om att den kan publicera sin integritetsskyddspolicy med hänvisning till dataskyddsramen på sin webbplats. När integritetsskyddspolicyn är offentlig bekräftar handelsministeriet certifieringen och inkluderar företaget i förteckningen över organisationer som omfattas av dataskyddsramen på sin webbplats. Dataskyddsramen kan användas för att ta emot personuppgifter från EU från och med den dag då handelsministeriet för upp organisationen på förteckningen[13].

Såsom förklarades under översynsmötet har de kontroller som utförs av handelsministeriet hittills lett till att 33 ansökningar avslagits, eftersom de inte uppfyllde dataskyddsramens krav. I allmänhet samarbetar handelsministeriet med företaget för att åtgärda eventuella brister. Om handelsministeriet upptäcker brister informerar det företaget om att det måste åtgärda dessa och att underlåtenhet att svara inom en viss tidsram eller annan underlåtenhet att slutföra sin självcertifiering i enlighet med handelsministeriets förfaranden, kommer att leda till att ansökan anses ha avbrutits. Om den ursprungliga certifieringen inte slutförs/ändras inom tolv månader anser handelsministeriet att den har avbrutits.

[10] https://www.dataprivacyframework.gov/program-articles/How-to-Join-the-Data-Privacy-Framework-(DPF)-Program-(part%E2%80%931).

[11] https://www.dataprivacyframework.gov/key-requirements.

[12] Mekanismer för tvistlösning inom den privata sektorn genom vilka varje enskild persons klagomål och tvister utreds och snabbt får en lösning utan kostnad för den enskilde.

[13] Avsnitt I punkt 3 i bilaga I till beslutet om adekvat skyddsnivå.

Förfallodatumet för årlig återcertifiering anges i förteckningen över organisationer som omfattas av dataskyddsramen för varje företag. För att påminna företagen om att de måste ansöka om återcertifiering har handelsministeriet skapat ett system med påminnelser om att certifieringen håller på att löpa ut. Organisationerna får en påminnelse en månad före, sedan två veckor före och därefter en dag före förfallodagen. De som låter certifieringen upphöra tas bort från förteckningen över organisationer som omfattas av dataskyddsramen. Såsom beskrivs i bilaga III till beslutet om adekvat skyddsnivå har handelsministeriet ett särskilt avsnitt på sin webbplats med en förteckning över de amerikanska organisationer som inte längre är aktiva deltagare och som identifierar respektive skäl (t.ex. att certifieringen löpt ut eller utträde) till att de berörda företagen har strukits från förteckningen (*förteckningen över inaktiva organisationer*). När organisationer stryks från förteckningen över organisationer som omfattas av dataskyddsramen för att de har låtit sin certifiering löpa ut kontaktar handelsministeriet dem för att bekräfta om de vill utträda eller i stället vill återcertifiera sig, och i så fall kontrollera att de efter att certifieringen löpte ut har tillämpat dataskyddsramens principer på personuppgifter som mottagits inom dataskyddsramen och för att klargöra vilka åtgärder de kommer att vidta för att ta itu med de kvarstående problem som har fördröjt återcertifieringen. När företag meddelar handelsministeriet att de vill utträda ut dataskyddsramen kräver handelsministeriet att de bekräftar huruvida de kommer att återlämna eller radera de uppgifter som mottagits inom dataskyddsramen, spara dem och fortsätta att tillämpa dataskyddsramens principer på sådana uppgifter (vilka måste bekräftas årligen) eller spara dem och införa andra skyddsåtgärder (t.ex. standardavtalsklausuler som antagits av Europeiska kommissionen).

Återkoppling från branschorganisationer och företag tyder på att företag som är certifierade enligt dataskyddsramen har vidtagit ett antal åtgärder för att säkerställa efterlevnad av dataskyddsramens principer. För att följa *principen om rättsmedel, genomförande och ansvar* har organisationer till exempel utfört interna kontroller antingen genom självbedömning eller genom extern efterlevnadskontroll. De två privata oberoende instanserna för handläggning av klagomål som deltog i översynsmötet förklarade att de även tillhandahåller extern efterlevnadskontroll genom att granska integritetsskyddspolicyer, och en av dem förklarade att den även tillhandahåller revisioner och slumpvisa kontroller, med fokus till exempel på principerna om *tillgång*, *valmöjlighet* och *vidare överföring*. Dessutom har certifierade företag utvecklat interna efterlevnadsprogram och tillsynsmekanismer, utbildat anställda, infört mekanismer som gör det möjligt för enskilda att utöva sina rättigheter, genomfört konsekvensbedömningar avseende integritetsskydd och sett över befintliga avtal.

#### 2.1.2. Övervakning av efterlevnad, falska påståenden om deltagande och verkställighet

Inom dataskyddsramen ansvarar handelsministeriet för att övervaka efterlevnaden av dataskyddsramens principer genom användning av olika verktyg, inbegripet kontroller på eget initiativ, särskilda stickprovskontroller och frågeformulär om efterlevnaden. Detta inbegriper att söka efter och ta itu med falska påståenden om deltagande i ramen, till exempel genom internetsökningar[14].

För att övervaka de certifierade företagens efterlevnad av dataskyddsramens principer har handelsministeriet främst förlitat sig på särskilda webbsökningar och kontroller av (sociala)

[14] Se bilaga III till beslutet om adekvat skyddsnivå. Felaktiga påståenden kan till exempel uppstå när ett företag påstår sig delta i dataskyddsramen och det antingen aldrig har inlett certifieringsprocessen, eller har inlett den men inte avslutat den eller har låtit sin certifiering löpa ut.

medier under det senaste året. Handelsministeriet rapporterade att det inte har upptäckt några problem med efterlevnaden av dataskyddsramens principer under det första året och inte har hänvisat några företag till den federala konkurrensmyndigheten eller transportministeriet för eventuella verkställighetsåtgärder. Det har också inrättat en särskild kontaktpunkt för att underlätta samarbetet med dataskyddsmyndigheter och ta emot klagomål från enskilda personer och hänskjutanden från andra myndigheter (t.ex. dataskyddsmyndigheter eller den federala konkurrensmyndigheten). Inga hänskjutanden eller klagomål har dock inkommit under det senaste året. Dataskyddsramens första verksamhetsår var inriktat på att inrätta ramen och certifieringsprocessen, men vid översynsmötet förklarade handelsministeriet att det planerar att utföra automatiserade efterlevnadskontroller för att göra dessa mer systematiskt, och man håller för närvarande på att utveckla de nödvändiga it-verktygen för att göra detta.

Kommissionen medger att handelsministeriet under det första året behövde fokusera sina insatser på att inrätta ramen och certifieringsprocessen. Framöver är det viktigt att handelsministeriet intensifierar sina insatser för att övervaka och kontrollera efterlevnaden av principerna, vilket är nödvändigt för att säkerställa en fortsatt hög nivå av efterlevnad av ramen och upptäcka fall som kräver ytterligare verkställighetsåtgärder, inbegripet eventuella falska påståenden om deltagande från företag. I detta avseende välkomnar kommissionen att handelsministeriet bekräftade sin avsikt att utveckla och använda (automatiserade) verktyg för att mer ändamålsenligt och systematiskt identifiera efterlevnadsproblem och falska påståenden och anser att detta bör ingå i en bredare insats för att i större utsträckning använda de olika verktyg som står till förfogande (t.ex. stickprovskontroller, frågeformulär för efterlevnadskontroll, förfrågningar om information osv.), inbegripet för att kontrollera efterlevnaden av särskilda krav enligt dataskyddsramen[15].

Organisationer som är certifierade enligt dataskyddsramen omfattas av den federala konkurrensmyndighetens och transportministeriets behörighetsområde. Under översynsmötet bekräftade transportministeriet att det har alla förfaranden på plats för att vidta lämpliga verkställighetsåtgärder. Det förklarade också att mycket få företag inom dess behörighetsområde har anslutit sig till dataskyddsramen (t.ex. några biljettombud men inga flygbolag). Den federala konkurrensmyndigheten bekräftade att den systematiskt kontrollerar överträdelser av dataskyddsramen i var och en av sina integritetsskyddsutredningar. Den federala konkurrensmyndigheten har hittills inte mottagit några hänskjutanden från andra myndigheter. Den har mottagit ett antal klagomål som nämner dataskyddsramen, även om två av dem gällde företag på förteckningen över inaktiva företag, två gällde företag som inte deltog i ramen och ett inte gällde personuppgifter som överfördes från EU. Vid tidpunkten för denna rapport hade den federala konkurrensmyndigheten inte fattat några beslut om att verkställa efterlevnad av dataskyddsramen, även om den bekräftade att flera företag som är certifierade enligt dataskyddsramen för närvarande är föremål för utredning.

Kommissionen välkomnar det faktum att den federala konkurrensmyndigheten systematiskt kontrollerar överträdelser av dataskyddsramen i alla sina integritetsskyddsutredningar. Eftersom dataskyddsramens fortsatta ändamålsenlighet är beroende av dess robusta verkställighet förväntas den federala konkurrensmyndigheten ytterligare utöva sina utredningsbefogenheter inom ramen, bland annat genom att proaktivt genomföra

[15] När det gäller till exempel vidare överföringar, genom att utnyttja möjligheten enligt dataskyddsramens princip 3 b att begära en sammanfattning eller representativ kopia av de relevanta integritetsskyddsbestämmelserna i avtal om vidare överföring.

genomgripande åtgärder med fokus på efterlevnad av särskilda krav i dataskyddsramen och/eller vissa sektorer.

### 2.1.3. Handläggning av klagomål

Dataskyddsramen ger enskilda personer i EU olika prövningsmöjligheter i fall där certifierade organisationer inte efterlever dataskyddsramens principer[16]. Detta inbegriper tvistlösning genom direkta kontakter med en organisation som är certifierad enligt dataskyddsramen, som måste svara den berörda personen inom 45 dagar. Enskilda personer kan också lämna in ett klagomål till en oberoende instans för handläggning av klagomål som utsetts av en organisation för att utreda och lösa klagomål. Beroende på omständigheterna kan detta antingen vara ett organ för alternativ tvistlösning eller en dataskyddsmyndighet[17]. Om ingen av de andra tillgängliga prövningsmöjligheterna har löst den registrerades klagomål på ett tillfredsställande sätt, kan enskilda personer slutligen begära ett bindande skiljedomsförfarande inför arbetsgruppen för dataskyddsramen mellan EU och Förenta staterna som en sista utväg.

#### *2.1.3.1. Företagens handläggning av klagomål*

Svaren från branschorganisationer och företag på kommissionens frågeformulär tyder på att företag som är certifierade enligt dataskyddsramen har mottagit mycket få – om några – klagomål från enskilda personer om bristande efterlevnad av dataskyddsramens principer. Samtidigt har företagen infört olika mekanismer och verktyg för att göra det möjligt för enskilda att utöva sina rättigheter och lämna in klagomål, bland annat via webbaserade formulär, e-post och telefon.

#### 2.1.3.2. *Oberoende instanser för handläggning av klagomål*

Den återkoppling som mottogs under översynsmötet och den information som lämnats av branschorganisationer visar att antalet klagomål till oberoende instanser för handläggning av klagomål har varit mycket få. De oberoende instanser för handläggning av klagomål som har valts ut av företag omfattar BBB National Programs, JAMS, TRUSTe och VeraSafe. Enligt dataskyddsramen ska de oberoende instanserna för handläggning av klagomål offentliggöra en årlig rapport med sammanställd statistik om användningen av deras tvistlösningstjänster. Vid tidpunkten för antagandet av denna rapport hade alla berörda oberoende instanser för handläggning av klagomål offentliggjort sina årsrapporter[18].

---

[16] Se avsnitt 2.4 i beslutet om adekvat skyddsnivå.

[17] Organisationer som är certifierade enligt dataskyddsramen är skyldiga att samarbeta i en dataskyddsmyndighets utredning och lösning av ett klagomål antingen när det gäller behandling av personaluppgifter som samlats in inom ramen för ett anställningsförhållande eller när respektive organisation frivilligt har underställts dataskyddsmyndigheters tillsyn.

[18] ANA – https://www.ana.net/content/show/id/accountability-dpf-consumers,

BBB National Programs – https://assets.bbbprograms.org/docs/default-source/eu-privacy-shield/dpf_periodicalreport_072024.pdf, ICDR – AAA – https://go.adr.org/rs/294-SFS-516/images/Data%20Privacy%20Framework%20IRM%20Program%20Report%202023-2024%20FINAL.pdf?version=0,

Insights association – https://www.insightsassociation.org/Portals/INSIGHTS/Insights%20Association%20DPF%20Services%20Program%202024%20Annual%20Report_Final_1.pdf,
JAMS – https://www.jamsadr.com/files/Uploads/Documents/2024-Annual-Report-DPF-Cases.pdf,

Privacy Trust DPF Services –

Vid översynsmötet redogjorde BBB och VeraSafe dessutom ingående för sin verksamhet det senaste året. De rapporterade en ökning av antalet företagsdeltagare som valde deras tjänster jämfört med tidigare ramar och nämnde att de hade mottagit vissa klagomål, även om de allra flesta inte var berättigade. Exempelvis mottog BBB 87 klagomål från enskilda EU-medborgare, varav endast två var berättigade till lösning. Även om BBB förklarade att klagomål i genomsnitt behandlas på fem arbetsdagar, avslutades dessa två klagomål till slut på grund av brist på svar från de enskilda personerna. VeraSafe mottog 26 klagomål, varav sex var berättigade till lösning. Två av dem gällde begäran om tillgång och radering och de löstes, medan två fortfarande var under behandling, och två antingen drogs tillbaka eller avslutades på grund av brist på svar från den enskilda personen. Båda de oberoende instanserna för handläggning av klagomål förklarade att de avser att besvara klagomål på den enskilda personens språk.

Företag som är certifierade enligt dataskyddsramen och som behandlar personaluppgifter som överförs från EU måste välja dataskyddsmyndigheter i EU som oberoende instans för handläggning av klagomål för dessa uppgifter, medan ett företag som är certifierat enligt dataskyddsramen på frivillig basis kan välja dataskyddsmyndigheter i EU som oberoende instans för handläggning av klagomål för andra typer av personuppgifter som överförs i enlighet med dataskyddsramen. Mer än hälften av de företag som var certifierade enligt dataskyddsramen vid tidpunkten för översynen valde faktiskt denna lösning[19], vilket är välkommet. Sedan beslutet om adekvat skyddsnivå antogs har EDPB antagit arbetsordningen för den informella arbetsgruppen för EU:s dataskyddsmyndigheter. Arbetsgruppen är behörig att ge bindande råd till de amerikanska organisationerna om olösta klagomål avseende dataskyddsramen från enskilda personer rörande hanteringen av personuppgifter som har överförts från EU inom dataskyddsramen. Enligt arbetsordningen utgörs arbetsgruppen av en dataskyddsmyndighet som fungerar som ansvarig dataskyddsmyndighet och andra utsedda dataskyddsmyndigheter som bistår vid granskningen[20]. Den ger bindande råd inom 60 dagar efter mottagandet av ett klagomål avseende dataskyddsramen. EDPB har också offentliggjort en mall för klagomålsformulär för inlämning av klagomål till dataskyddsmyndigheter[21] samt vanliga frågor för europeiska enskilda personer[22] och företag[23] om dataskyddsramen. Arbetsgruppen hade inte mottagit några klagomål vid tidpunkten för översynen.

---

https://privacytrust.com/fserve/PrivacyTrust_Dispute_Resolution_Report_2023_2024.pdf,

TRUSTe Dispute Resolution – https://trustarc.com/wp-content/uploads/2024/07/2024-Independent-Recourse-Mechanism-Annual-Report.pdf,

Verasafe – https://verasafe.com/wp-content/uploads/2020/06/VeraSafe-DPF-Dispute-Resolution-Program-Annual-Report-2024.pdf.

[19] Kort efter datumet för översynsmötet angav dataskyddsmyndighetens webbplats att 1 511 av de 2 892 deltagarna hade en dataskyddsmyndighet i EU som sin instans för handläggning av klagomål.

[20] Den 17 april 2024 antog EDPB arbetsordningen för den informella arbetsgruppen för EU:s dataskyddsmyndigheter i enlighet med ramen för dataskydd mellan EU och Förenta staterna. Den finns här: https://www.edpb.europa.eu/system/files/2024-04/dpf_rules-of-procedure_informal-panel-dpas_en.pdf.

[21] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-template-complaint-form_en.

[22] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-faq-european-individuals_en.

[23] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-faq-european-businesses_en.

#### *2.1.3.3. Det bindande skiljedomsförfarandet*

Internationella centrumet för tvistlösning, International Centre for Dispute Resolution (ICDR), vilket är den internationella avdelningen inom den amerikanska skiljedomssammanslutningen, American Arbitration Association (AAA), valdes ut av handelsministeriet för att administrera det bindande skiljedomsförfarandet. Efter antagandet av beslutet om adekvat skyddsnivå valde handelsministeriet tillsammans med kommissionen ut elva skiljemän med erfarenhet av integritetsskydd och med olika bakgrunder, bland annat skiljedomsförfaranden, domstolsväsendet, den akademiska världen och det civila samhället[24]. Dessutom har skiljedomsreglerna[25] för arbetsgruppen för dataskyddsramen och en uppförandekod för skiljemän[26] antagits och finns alla tillgängliga på ICDR:s webbplats. Vid tidpunkten för översynen hade skiljedomsmekanismen ännu inte utlösts av någon enskild person i EU.

### 2.1.4. Vägledning, samarbete och medvetandehöjande åtgärder

Sedan dataskyddsramen trädde i kraft har handelsministeriet genomfört olika åtgärder för att öka medvetenheten genom att organisera evenemang, webbinarier och konferenser, nå ut till branschorganisationer och samverka direkt med över 3 000 företag för att informera om dataskyddsramen. Det har också offentliggjort vägledning, bland annat i form av vanliga frågor som riktar sig till enskilda personer samt till företag i EU och Förenta staterna[27]. EDPB har i sin tur utvecklat klagomålsformulär och vanliga frågor som riktar sig till enskilda personer och företag. På samma sätt offentliggjorde kommissionen frågor och svar och ett faktablad om dataskyddsramen när den antog sitt beslut om adekvat skyddsnivå[28].

Samtidigt framgick det av översynsmötet att det behövs mer arbete för att öka medvetenheten bland enskilda personer och ge vägledning till företag. Bidragen från företag och oberoende instanser för handläggning av klagomål, och mycket få klagomål, tyder på att enskilda personer inte alltid är medvetna om sina rättigheter och/eller mekanismen för att utöva dem. Under översynsmötet uttryckte handelsministeriet ett intresse för att samarbeta med EU:s dataskyddsmyndigheter för att öka medvetenheten om ramen bland enskilda personer i EU. Kommissionen uppmuntrar sådana initiativ och vidtar även åtgärder för att informera enskilda personer bättre, bland annat genom att tillhandahålla ytterligare information om dataskyddsramen på sin webbplats, till exempel genom att inkludera länkar och hänvisningar till relevanta vägledande dokument som antagits av EDPB, handelsministeriet och andra amerikanska myndigheter.

När det gäller vägledning om dataskyddsramens principer kom EDPB:s företrädare under översynsmötet överens om att samarbeta under de kommande månaderna för att lämna ytterligare förtydliganden om begreppet personaluppgifter inom dataskyddsramen och de särskilda skyldigheter som gäller behandling av sådana uppgifter. Olika faktorer som skulle ingå i en sådan vägledning undersöktes. Denna vägledning skulle till exempel kunna behandla vissa praktiska scenarier där personaluppgifter skulle behandlas inom dataskyddsramen (t.ex. av en molnleverantör) och för sådana scenarier förklara vilka skyldigheter enligt dataskyddsramen som skulle vara relevanta. Dessutom skulle det i vägledningen kunna föreslås

[24] https://go.adr.org/DPF_Arbitrator_Bios.html.
[25] https://go.adr.org/rs/294-SFS-516/images/IC.DR-AAA_EU-US_DPF_AnnexI_Arbitration_Rules.pdf.
[26] https://go.adr.org/rs/294-SFS-516/images/Code_of_Conduct_for_Arbitrators_Appointed_to_EU-US_DPF_AnnexI_Arbitrations.pdf.
[27] Se t.ex. https://www.dataprivacyframework.gov/US-Businesses.
[28] https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_sv.

att företag som tar emot personaluppgifter om enskilda personer i EU (men som inte nödvändigtvis använder sådana uppgifter inom ramen för ett anställningsförhållande) väljer dataskyddsmyndigheternas arbetsgrupp som sin oberoende instans för handläggning av klagomål. Detta skulle säkerställa att dessa personer kan vända sig till en myndighet som är ”nära hemmet” och vid behov är mer bekant med tillämplig nationell lagstiftning som gäller för personaluppgifter.

Dessutom finns det en särskild aspekt där det verkar som om mer vägledning skulle behövas (även baserat på synpunkter från branschorganisationer), nämligen dataskyddsramens krav på vidare överföringar. Därutöver angav handelsministeriet att det skulle vara värt att undersöka om vissa sektorer kan dra nytta av ytterligare vägledning om tillämpningen av dataskyddsramens principer på deras verksamhet, t.ex. inom hälsoforskning och finansiella tjänster.

Kommissionen välkomnar båda sidors beredvillighet att ta fram vägledning och förväntar sig att arbetet med ovannämnda frågor kommer att inledas snart.

I allmänhet har flera mekanismer inrättats för att säkerställa utbyte och samarbete mellan amerikanska myndigheter och dataskyddsmyndigheterna, bland annat genom att utse särskilda kontaktpunkter inom den federala konkurrensmyndigheten och handelsministeriet för att hantera utredningar och hänskjutanden från dataskyddsmyndigheter.

#### 2.1.5. Relevant utveckling i Förenta staternas rättssystem

Sedan beslutet om adekvat skyddsnivå antogs har det skett en rad förändringar inom Förenta staternas rättsliga ram på integritetsskyddsområdet. Detta inbegriper utveckling i fråga om lagstiftning, reglering och rättspraxis. Detta signalerar i allmänhet en ökad konvergens mellan EU:s och Förenta staternas strategier för vissa integritetsskyddsutmaningar, bland annat genom användning av liknande rättsliga begrepp. En del av denna utveckling pågår och kommer att behöva övervakas ytterligare.

På federal nivå utfärdade presidenten flera dekret som är relevanta för användningen av personuppgifter. I synnerhet i dekret 14117 av den 28 februari 2024[29] förbjuds eller begränsas transaktioner som omfattar vissa kategorier av känsliga personuppgifter (t.ex. hälsodata, biometriska kännetecken, genomiska data om människor) med enheter i vissa ”länder som ger upphov till oro”[30]. I det antagna dekretet instrueras justitieministern att föreslå bestämmelser – som fortfarande inte har utfärdats när denna rapport antas – för att ytterligare specificera genomförandet. Dessutom är dekret 14110 av den 30 oktober 2023 om artificiell intelligens[31] inriktat på utveckling av trygg, säker och tillförlitlig artificiell intelligens. Enligt dekretet ska flera federala myndigheter utarbeta AI-relaterade säkerhetsstandarder och riktlinjer, bland annat om specifika AI-risker för integritet och tekniker för integritetsskydd.

---

[29] https://www.federalregister.gov/documents/2024/03/01/2024-04573/preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related.

[30] Enligt justitieministerns förslag i ett förhandsmeddelande om föreslagna regler som utfärdades den 3 maj 2024 omfattar dessa Kina, Kuba, Hongkong och Macau, Iran, Nordkorea och Venezuela. Se https://www.federalregister.gov/documents/2024/03/05/2024-04594/national-security-division-provisions-regarding-access-to-americans-bulk-sensitive-personal-data-and.

[31] https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence.

När det gäller lagstiftningsarbete har federala lagförslag om integritet lagts fram i kongressen under de senaste åren, men 20 amerikanska delstater hade i juli 2024 antagit omfattande dataskyddslagar, varav åtta har trätt i kraft: Kalifornien, Colorado, Oregon, Virginia, Connecticut, Utah, Texas och Florida. Dessutom har 17 amerikanska delstater antagit lagstiftning om automatiserad behandling (eller åtminstone vissa former av automatiserad behandling) och i allmänhet om undantag för vissa typer av beslutsfattande baserat på ”profilering”[32].

När det gäller utvecklingen av rättspraxis har flera företrädare för det civila samhället hänvisat till Högsta domstolens dom nyligen i målet *Loper Bright Enterprises mot Raimondo* (den 28 juni 2024). Denna dom ogillar tidigare rättspraxis om *Chevron*-doktrinen, där domstolar tillämpar principen om uppskov på en tillsynsmyndighets rimliga tolkning av lagen i händelse av tvetydigheter i en lag som verkställs av denna myndighet. I synnerhet har vissa icke-statliga organisationer uttryckt oro över effekterna av denna dom från Högsta domstolen på den federala konkurrensmyndighetens regleringsbefogenhet på integritetsskyddsområdet, samtidigt som de erkänner att det kanske inte finns någon eller begränsad inverkan på dess verkställighetsbefogenheter. Vid översynsmötet informerade den federala konkurrensmyndigheten om att det fortfarande är för tidigt att veta exakt vilka följder denna dom får. Samtidigt förklarade myndigheten att dess reglering sker enligt en befogenhet i lagen om den federala konkurrensmyndigheten som skiljer sig från dem som gäller för andra administrativa myndigheter och för vilken *Chevron*-doktrinen var mindre relevant. Den nyligen fällda domen kan därför ha begränsad inverkan på detta område.

Dessutom informerade den federala konkurrensmyndigheten om den senaste utvecklingen när det gäller dess strategi för automatiserad behandling och artificiell intelligens. Detta inbegriper antagandet av ett gemensamt uttalande tillsammans med andra tillsynsmyndigheter mot diskriminering och partiskhet i automatiserade system[33], samt flera verkställighetsåtgärder – där den federala konkurrensmyndigheten bland annat fokuserar på insyn, rättvisa i den automatiserade behandlingen och enskilda personers förmåga att ifrågasätta resultaten. Det mest framträdande fallet i detta avseende är den federala konkurrensmyndighetens beslut mot *Rite Aid* i mars 2024, genom vilket ett femårigt förbud mot att använda ansiktsigenkänningsteknik för säkerhetsändamål infördes för företaget[34]. I synnerhet fann den federala konkurrensmyndigheten att *Rite Aid* inte vidtog rimliga åtgärder för att förhindra felaktiga resultat och informera konsumenter om den teknik som används. Den federala

[32] Även om det finns skillnader i vad som menas med ”profilering” mellan de olika delstaterna definieras profilering i allmänhet som varje typ av automatiserad behandling av personuppgifter för att utvärdera, analysera eller förutsäga personliga aspekter som rör en identifierad eller identifierbar fysisk persons ekonomiska situation, hälsa, personliga preferenser, intressen, tillförlitlighet, beteende, plats eller rörelser. Det är vanligtvis konsumenter som kan välja bort profilering. Följande stater har utarbetat lagstiftning om profilering: Colorado (Colo. Rev. Stat. Ann. § 6-1-1306), Connecticut (Conn. Gen. Stat. Ann. § 42-518), Delaware (Del. Code Ann. tit. 6, § 12D-104), Florida (Fla. Stat. Ann. § 501.705), Indiana (Ind. Code Ann. § 24-15-3-1), Kentucky (Ky. Rev. Stat. Ann. § 367.3615), Maryland (Marylands lag om dataskydd online från 2024, antagen den 9 maj 2024), Minnesota (Minn. Stat. Ann. § 325O.07), Montana (Mont. Code Ann. § 30-14-2808), Nebraska (Neb. Rev. Stat. Ann. § 87-1107), New Hampshire (N.H. Rev. Stat. Ann. § 507-H:4), New Jersey (N.J. Stat. Ann. § 56:8-166.8), Oregon (Or. Rev. Stat. Ann. § 646A.574), Rhode Island (Rhode Islands lag om datatransparens och dataskydd, antagen den 29 juni 2024), Tennessee (Tenn. Code Ann. § 47-18-3304), Texas (Tex. Bus. & Com. Code Ann. § 541.051) och Virginia (Va. Code Ann. § 59.1-577).

[33] https://files.consumerfinance.gov/f/documents/cfpb_joint-statement-enforcement-against-discrimination-bias-automated-systems_2023-04.pdf.

[34] https://www.ftc.gov/legal-library/browse/cases-proceedings/2023190-rite-aid-corporation-ftc-v.

konkurrensmyndighetens nuvarande prioriteringar behandlades mer allmänt vid översynsmötet, särskilt de områden som den anser förtjänar en mer proaktiv verkställighetsstrategi framöver. Detta inbegriper skydd av känsliga uppgifter (t.ex. hälsodata, biometriska uppgifter, geografisk plats)[35], skydd av barn[36] och minderåriga online samt datasäkerhet[37].

Kommissionen kommer att fortsätta att noga följa denna och annan utveckling i Förenta staterna, särskilt eventuella ytterligare steg mot en omfattande federal dataskyddslagstiftning och den eventuella effekten av Högsta domstolens senaste rättspraxis på den federala konkurrensmyndighetens roll på integritetsområdet.

Kommissionen välkomnar den information som lämnats av den federala konkurrensmyndigheten om dess nyligen genomförda tillsynsverksamhet och aktuella prioriteringar som till stor del motsvarar tendenser och prioriteringar när det gäller genomförandet av dataskyddet i Europa. Den federala konkurrensmyndigheten deltar också aktivt i nätverket som sammanför länder som omfattas av ett EU-beslut om adekvat skyddsnivå, som kommissionen startade i mars 2024[38]. Denna ökade konvergens bör uppmuntra och underlätta ett närmare samarbete mellan integritetsskyddstillämpare på båda sidor av Atlanten, särskilt i frågor som är relevanta för dataskyddsramens funktion.

### 2.2. Aspekter som rör tillgång till och användning av personuppgifter som överförts inom ramen för dataskydd mellan EU och Förenta staterna av amerikanska myndigheter

Beslutet om adekvat skyddsnivå innehåller en detaljerad bedömning av de regler som styr insamling och användning av personuppgifter som överförs från EU till företag som är certifierade enligt dataskyddsramen av amerikanska myndigheter, särskilt för brottsbekämpning och ändamål som rör den nationella säkerheten. Sedan beslutet om adekvat skyddsnivå antogs har det, enligt uppgift från de amerikanska myndigheterna under översynsmötet, inte skett någon relevant utveckling när det gäller den rättsliga ram som gäller för tillgång till uppgifter för brottsbekämpande ändamål eller regleringsändamål under dataskyddsramens första år. Av detta skäl gäller nedanstående iakttagelser endast utvecklingen på området nationell säkerhet.

Slutsatserna i beslutet om adekvat skyddsnivå om tillgång till uppgifter för underrättelsemyndigheter bygger på analysen av de villkor och begränsningar som gäller för

[35] Se t.ex. den federala konkurrensmyndighetens nyligen fattade beslut mot X-Mode för försäljning och delning av känslig platsinformation (https://www.ftc.gov/system/files/ftc_gov/pdf/X-ModeSocialDecisionandOrder.pdf) och mot Monument om röjande av känsliga hälsodata till tredje part i marknadsföringssyfte (https://www.ftc.gov/system/files/ftc_gov/pdf/MonumentOrderFiled.pdf).

[36] Den federala konkurrensmyndigheten har till exempel nyligen aviserat en utredning som leder till en stämning mot TikTok och dess moderbolag, Bytedance, för att de påstås bryta mot lagen om barns integritetsskydd. Det påstås att inget av företagen har uppfyllt kravet på att meddela föräldrarna och erhålla deras samtycke innan de samlar in och använder personuppgifter för barn under 13 år (https://www.ftc.gov/news-events/news/press-releases/2024/08/ftc-investigation-leads-lawsuit-against-tiktok-bytedance-flagrantly-violating-childrens-privacy-law).

[37] Se översikten över nyligen genomförda verkställighetsåtgärder i den federala konkurrensmyndighetens integritets- och datasäkerhetsuppdatering 2023: https://ec.europa.eu/commission/presscorner/detail/en/mex_24_1307.

[38] Se https://ec.europa.eu/commission/presscorner/detail/en/mex_24_1307. Till följd av mötet i mars 2024 beslutades det att en rad tematiska möten skulle hållas. Det första ägde rum i juli 2024 och var inriktat på att utveckla verktyg som kan hjälpa små och medelstora företag att följa dataskyddslagstiftningen.

underrättelseverksamhet inom flera relevanta rättsliga myndigheter – särskilt avsnitt 702 i lagen om underrättelseverksamhet och övervakning utomlands (Fisa) och dekret 12333[39] – som kompletterades och stärktes genom dekret 14086 om förbättrade skyddsåtgärder för Förenta staternas signalskydd (dekret 14086), som antogs av Förenta staternas president den 7 oktober 2022. De skyddsåtgärder som fastställs i dekret 14086 gäller för all amerikansk signalunderrättelseverksamhet, oavsett den rättsliga befogenhet som denna verksamhet baseras på och var den äger rum, och skyddar uppgifter om utländska medborgare (inbegripet européer)[40]. Dekret 14086 inrättar en ny prövningsmekanism genom vilken dessa bindande skyddsåtgärder kan åberopas och verkställas av enskilda personer i EU.

I de följande avsnitten beskrivs de åtgärder som vidtagits av de amerikanska myndigheterna sedan beslutet om adekvat skyddsnivå antogs för att uppfylla dekret 14086 samt relevant utveckling i förhållande till ovannämnda rättsliga ram.

### 2.2.1. Relevant utveckling när det gäller Förenta staternas rättsliga ram

#### *2.2.1.1. Genomförande av dekret 14086 av underrättelsemyndigheter*

De begränsningar och skyddsåtgärder som infördes genom dekret 14086 kompletterar dem som föreskrivs i avsnitt 702 i Fisa och dekret 12333. De är bindande för alla underrättelsemyndigheter och har blivit mer operativa genom policyer och förfaranden som antagits av varje myndighet.

Som en del av den första översynen bekräftade de amerikanska myndigheterna att det inte har skett några ändringar av dekret 14086 sedan det antogs. Dessutom klargjordes att Förenta staternas president inte har utnyttjat den befogenhet som anges i avsnitten 2 b i B och 2 b ii C i dekret 14086 att uppdatera förteckningen över legitima mål mot vilka signalunderrättelser kan utövas eller förteckningen över ändamål för vilka uppgifter som samlats in i bulk får användas[41]. För att fastställa mer specifika underrättelseprioriteringar för vilka signalunderrättelser faktiskt kan samlas in införde dekret 14086 ett särskilt förfarande. I synnerhet måste tjänstemannen med ansvar för skyddet av medborgerliga friheter vid den nationella underrättelsetjänsten (ODNI CLPO) rådfrågas för att för varje prioritering bedöma om den (1) främjar ett eller flera av de legitima mål som anges i dekretet, (2) varken utformades för eller förväntades leda till insamling av signalunderrättelser för ett förbjudet mål som förtecknas i dekretet och (3) upprättades efter vederbörlig hänsyn till alla personers integritet och medborgerliga friheter[42]. ODNI CLPO bekräftade under översynsmötet att hon hade granskat de prioriteringar som föreslagits av direktören för den nationella underrättelsetjänsten i 2023 års nationella ram för underrättelseprioriteringar, dragit slutsatsen att de uppfyllde ovanstående krav och delat sin slutsats med direktören för den nationella underrättelsetjänsten,

[39] Andra åtgärder som kan vidtas inom ramen för Fisa med avseende på uppgifter som överförs från EU är individuell elektronisk övervakning (avsnitt 105 i Fisa), fysiska sökningar (avsnitt 302 i Fisa), användning av samtals- och spårningsanordningar såsom pen register och trap and trace-anordningar (avsnitt 402 i Fisa) och insamling av affärsregister från vissa företag (gemensamma transportföretag, offentliga logianläggningar, uthyrningsanläggningar för fordon eller lagringsanläggningar, avsnitt 501 i Fisa). Dessa olika rättsliga grunder analyseras i detalj i beslutet om adekvat skyddsnivå (skälen 142–152).

[40] Se avsnitt 3.2.1.2 i beslutet om adekvat skyddsnivå för mer information.

[41] Dessa legitima mål/ändamål omfattar till exempel skydd mot spionage, sabotage, mord eller annan underrättelseverksamhet som bedrivs av, eller på uppdrag av, eller med bistånd av en utländsk regering, organisation eller person, skydd mot terrorism, tagande av gisslan och hållande av personer i fångenskap av en utländsk regering, organisation eller person eller på dessas vägnar.

[42] Avsnitt 2 b iii i dekret 14086.

som i sin tur lämnade in prioriteringarna till presidenten för validering. ODNI CLPO tillhandahöll också utbildning om kraven i dekret 14086 till delar av underrättelsegemenskapen som deltar i utvecklingen av underrättelseprioriteringar.

Dessutom har de amerikanska myndigheterna under det senaste året vidtagit ytterligare praktiska åtgärder för att genomföra dekret 14086 i sin dagliga verksamhet. I synnerhet har underrättelsemyndigheter inrättat ytterligare interna policyer och riktlinjer för tillämpningen av dekretet, till exempel interna processer (genom interna godkännandekrav, dokumenterade tillträdeskontroller så att endast de personer som har fått lämplig utbildning och uppfyller de nödvändiga uppdragskraven har tillgång till informationen osv.) för att säkerställa att kraven på nödvändighet och proportionalitet uppfylls i samband med både riktad insamling och bulkinsamling[43]. Dessutom har utbildning om dekret 14086 tillhandahållits personal vid olika underrättelsemyndigheter (t.ex. NSA, CIA, FBI), inbegripet årliga och särskilda utbildningstillfällen som anordnas av ODNI CLPO och obligatorisk utbildning för all ny personal som ansluter sig till den nationella underrättelsetjänsten.

Kommissionen välkomnar de olika åtgärder som vidtagits för att genomföra och säkerställa efterlevnaden av dekret 14086. I takt med att man får mer erfarenhet av den praktiska tillämpningen av dekretets skyddsåtgärder skulle kommissionen uppskatta möjligheten att diskutera konkreta exempel på hur dekretet tillämpas i praktiken (med beaktande av tillämpliga sekretessöverväganden) i framtida översyner.

#### *2.2.1.2. Förnyat godkännande av avsnitt 702 i Fisa*

Enligt avsnitt 702 i Fisa är målsökning av personer som inte är amerikanska medborgare som skäligen kan antas befinna sig utanför Förenta staterna tillåten för att inhämta utländska underrättelseuppgifter. Inhämtningen sker på grundval av årliga certifieringar som lämnas till och godkänns av domstolen för övervakning av utländsk underrättelseinformation (Foreign Intelligence Surveillance Court, FISC). I dessa certifieringar anges specifika kategorier av utländska underrättelseuppgifter som ska samlas in. Den 21 juli 2023 meddelade den nationella underrättelsetjänsten att det finns tre godkända certifieringar enligt avsnitt 702 i Fisa, som omfattar följande kategorier av utländska underrättelser: (1) utländska regeringar och anknutna enheter, (2) terrorismbekämpning och (3) bekämpande av spridning[44]. Certifieringarna ska också omfatta förfaranden för målinriktning och minimering som godkänts av FISC[45]. I synnerhet sker målinriktningen genom att amerikanska företag som uppfyller Fisas definition av ”leverantör av elektroniska kommunikationstjänster” ska lämna ut uppgifter om elektronisk kommunikation för kommunikation som skickas till eller från ”väljare”, som identifierar ett specifikt kommunikationskonto, t.ex. ett telefonnummer eller en e-postadress. Den amerikanska regeringen har offentliggjort ett antal material om avsnitt 702 i Fisa för att informera allmänheten om hur övervakningsprogram, tillämpliga krav och integritetsskydd fungerar samt om FISC:s roll[46].

---

[43] Se https://www.intel.gov/ic-on-the-record-database/results/oversight/1278-odni-releases-ic-procedures-implementing-new-safeguardsin-executive-order-14086, offentliggjort den 3 juli 2023.

[44] https://www.intelligence.gov/ic-on-the-record-database/results/1307-release-of-documents-related-to-the-2023-fisa-section-702-certifications.

[45] Sådana förfaranden begränsar insamlingen av uppgifter med avseende på ett specifikt utländskt underrättelseändamål, begränsar tillgången till databaser där information som erhållits enligt avsnitt 702 i Fisa lagras (inbegripet genom åtkomstkontroller) och begränsar användningen, lagringen och spridningen av sådan information.

[46] https://www.intel.gov/foreign-intelligence-surveillance-act.

På grund av en tidsfristklausul skulle avsnitt 702 i Fisa upphöra att gälla i slutet av 2023, såvida inte kongressen godkände det på nytt. Efter ett tillfälligt förnyat godkännande utan ändringar antog kongressen lagen om reform av underrättelsetjänsten och säkrande av Amerika (RISAA) den 19 april 2024, vilket godkände avsnitt 702 i Fisa på nytt för en period på två år och införde flera ändringar. Dessa kan i stort sett delas in i två kategorier: (1) ändringar av omfattningen av den övervakningsverksamhet som är tillåten enligt avsnitt 702 i Fisa och (2) institutionella och förfarandemässiga ändringar.

*Ändringar av omfattningen av den övervakningsverksamhet som är tillåten enligt avsnitt 702 i Fisa*

Genom RISAA infördes tre huvudsakliga ändringar av omfattningen av den övervakningsverksamhet som kan utföras enligt avsnitt 702 i Fisa.

För det första har ”abouts”-insamling förbjudits definitivt[47]. Detta avser den insamling av kommunikation där sektion 702-väljaren (t.ex. en e-postadress) inte finns i meddelandets till- eller från-rad, utan där det snarare finns en hänvisning till en sådan väljare i meddelandet (t.ex. e-postmeddelanden som inte skickas till eller från den valda e-postadressen, men som innehåller den valda e-postadressen i e-postmeddelandets ämnesrad eller brödtext). Även om en sådan insamling redan uteslöts till följd av en ändring av Fisa 2018, föreskrev Fisa fortfarande möjligheten att återuppta ”abouts”-insamlingen i framtiden, efter ett särskilt godkännandeförfarande som involverade FISC och kongressen. Den senaste ändringen som infördes genom RISAA har avlägsnat denna möjlighet.

För det andra har definitionen av utländsk underrättelseinformation utvidgats till att omfatta information om narkotikabekämpning[48]. Under översynsmötet förklarade de amerikanska myndigheterna att detta infördes mot bakgrund av den pågående fentanylkrisen och det ökande hotet mot den nationella säkerheten från internationella narkotikahandlare och narkotikatillverkare. Mot denna bakgrund bekräftades att detta begrepp omfattas av flera av de legitima mål som anges i dekret 14086, dvs. att förstå eller bedöma kapaciteten, avsikterna eller verksamheten hos utländska organisationer som utgör ett aktuellt eller potentiellt hot mot den nationella säkerheten i Förenta staterna eller dess allierade, förstå eller bedöma gränsöverskridande hot som påverkar den globala säkerheten, inbegripet risker för folkhälsan, och skydda sig mot gränsöverskridande brottshot[49].

För det tredje utvidgade RISAA definitionen av ”leverantör av elektroniska kommunikationstjänster” så att den kom att omfatta fler företag som kan tvingas lämna information i enlighet med avsnitt 702 i Fisa[50]. Definitionen omfattar nu även andra tjänsteleverantörer som har tillgång till utrustning som används eller kan användas för att sända eller lagra trådbunden eller elektronisk kommunikation, samtidigt som offentliga logianläggningar, bostäder, gemensamma lokaler och anläggningar för livsmedelstjänster uttryckligen undantas. I en skrivelse till kongressen hänvisade justitieministeriet till denna ändring som en teknisk ändring avsedd att omfatta ett ”extremt litet” antal teknikföretag som, enligt de senaste besluten från FISC och appellationsdomstolen för övervakning av utländsk underrättelseinformation (Foreign Intelligence Surveillance Court of Review, FISCR), inte omfattades av den tidigare definitionen av leverantör av elektroniska

[47] Avsnitt 22 i RISAA.
[48] Avsnitt 23 i RISAA.
[49] Avsnitt 2 b ii A 2, 3 och 10 i dekret 14086.
[50] Avsnitt 25 i RISAA.

kommunikationstjänster[51]. I samma skrivelse åtog sig justitieministeriet att begränsa omfattningen genom att tillämpa denna definition uteslutande för att täcka den typ av tjänsteleverantör som avses i den tvist som ledde fram till beslutet från FISC. Till följd av detta nämns de berörda företagen i en sekretessbelagd bilaga för kongressen. Flera icke-statliga organisationer, däribland de som lämnade återkoppling som en del av översynen, uttryckte oro över denna utvidgning och hävdade att den potentiellt skulle kunna omfatta många amerikanska företag (eftersom många av dem tillhandahåller någon typ av tjänst och har tillgång till kommunikationsutrustning). Mot bakgrund av dessa farhågor har ytterligare en ändring föreslagits med stöd av underrättelsegemenskapen i ett utkast till lag om underrättelsegodkännande för räkenskapsåret 2025, som för närvarande ligger hos kongressen. Om denna ändring godkänns av kongressen skulle den säkerställa att de ytterligare företag som omfattas av definitionen av leverantör av elektroniska kommunikationstjänster skulle begränsas till endast dem som nämns i ovannämnda avgöranden från FISC. I lagförslaget föreskrivs också att varje direktiv som riktar sig till ett sådant företag måste rapporteras till FISC, så att FISC kan granska om företaget verkligen omfattas av tillämpningsområdet. I sin skrivelse till kongressen åtog sig justitieministeriet att var sjätte månad rapportera till kongressen om varje tillämpning av den uppdaterade definitionen för att göra det möjligt för kongressen att utöva lämplig tillsyn över den snäva tillämpningen av definitionen.

Det är viktigt att påpeka att de amerikanska myndigheterna och PCLOB vid översynsmötet bekräftade att alla skyddsåtgärder i dekret 14086 fortsätter att gälla fullt ut för all uppgiftsinsamling och användning enligt avsnitt 702 i Fisa, även efter dessa ändringar. Även om RISAA i viss mån breddar tillämpningsområdet så att fler företag kan få ett beslut, begränsas inte utövandet av rättigheter. Det kommer dock att vara viktigt att övervaka utvecklingen (lagstiftning och rapportering) och få information om tillämpningen av dessa nya regler i praktiken. Detta inbegriper till exempel inverkan av breddningen av definitionerna av utländsk underrättelseverksamhet och leverantör av elektroniska kommunikationstjänster på antalet mål enligt avsnitt 702 i Fisa (som meddelas årligen av den nationella underrättelsetjänsten, se nedan om insyn). Den framtida uppföljningsrapporten till den senaste rapporten från PCLOB om avsnitt 702 i Fisa (se nedan) bör vara särskilt informativ i detta avseende.

*Institutionella och förfarandemässiga ändringar*

När det gäller institutionella och förfarandemässiga ändringar kodifierade RISAA flera förfaranden som redan hade följts i praktiken och införde nya skyddsåtgärder. Vissa av dessa rör endast amerikaner, men flera ändringar ökar skyddet för både amerikanska medborgare och utländska medborgare vars uppgifter kan samlas in enligt avsnitt 702 i Fisa[52] och är därför relevanta för dataskyddsramens funktion.

[51] https://www.justice.gov/opa/media/1348621/dl?inline. Se FISC:s beslut från 2022 (https://www.intel.gov/assets/documents/702%20Documents/declassified/2022-FISC-ECSP-OPINION.pdf) och domen från FISCR som bekräftar beslutet (https://www.intel.gov/assets/documents/702%20Documents/declassified/2023_FISC-R_ECSP_Opinion.pdf).

[52] Dessutom införde RISAA vissa ändringar med avseende på traditionell individuell elektronisk övervakning i enlighet med avsnitt 105 i Fisa (på grundval av FISC-ordern som utfärdas om en standard för sannolik orsak uppfylls). En ansökan från en underrättelsemyndighet till justitieministern om ett beslut om individuell elektronisk övervakning kräver nu en försäkran som styrker att villkoren i avsnitt 105 i Fisa är uppfyllda (avsnitt 6 a i RISAA).

För det första infördes ett antal ytterligare krav på ansvarsskyldighet, tillsyn och rapportering. I synnerhet måste FBI:s personal nu årligen utbildas om de regler som gäller för förfrågningar om information som erhållits enligt avsnitt 702 i Fisa[53]. FBI måste också rapportera till kongressen om sina förfrågningar (t.ex. antalet förfrågningar som tillämpar teknik för batchjobb, dvs. att köra flera söktermer som en del av en enda förfrågning) och om åtgärder för ansvarsskyldighet som vidtagits för att säkerställa efterlevnad av lagstadgade krav på förfrågningar (avsnitten 11–12 i RISAA). Dessutom instrueras justitieministeriets generalinspektör att utarbeta en rapport om FBI:s efterlevnad av kraven på förfrågningar (avsnitt 9 i RISAA). För att öka insynen i förfarandena inför FISC krävs nu mer allmänt att den nationella underrättelsetjänsten och justitieministern genomför en granskning om hävande av sekretess för FISC:s beslut inom 180 dagar (avsnitt 7 i RISAA). Dessutom måste utskrifter av alla förhandlingar vid FISC och FISCR (där FISC:s beslut kan överklagas) bevaras och översändas till kongressen (avsnitt 8 i RISAA).

För det andra införde RISAA ytterligare begränsningar av FBI:s användning av uppgifter som samlats in enligt avsnitt 702 i Fisa. Enligt avsnitt 2 d i RISAA kan en förfrågan med hjälp av ”batchteknik” endast göras efter godkännande från en advokat inom FBI, såvida det inte föreligger särskilda omständigheter. Dessutom är det nu förbjudet för FBI att automatiskt kontrollera ej minimerad information som erhållits enligt avsnitt 702 i Fisa, utan FBI måste i stället se till att analytikerna aktivt väljer att söka mot sådan information. Genom RISAA har det också blivit förbjudet för FBI att genomföra förfrågningar som enbart är avsedda att hitta och hämta bevis på brottslig verksamhet (om det inte finns en rimlig anledning att tro att de skulle kunna bidra till att mildra eller undanröja ett hot mot liv eller om allvarlig kroppsskada, eller vid behov för att uppfylla skyldigheterna att lämna ut uppgifter i rättstvister)[54]. Dessutom är det förbjudet för FBI att föra in ej minimerade uppgifter i analysdatabaser, såvida inte personen som är föremål för förfrågan är relevant för en befintlig nationell säkerhetsutredning[55].

För det tredje har vissa bestämmelser om status och roll för *amici curiae* inför FISC ändrats[56]. *Amici curiae* utses till experter för att bistå domstolen (och FISCR) i frågor som rör integritetsskydd och medborgerliga friheter eller för att bidra till att klargöra tekniska frågor när en viss regerings ansökan behandlas. Enligt Fisa krävdes tidigare att *amici curiae* skulle ha sakkunskap om integritetsskydd och medborgerliga friheter, insamling av underrättelser, kommunikationsteknik eller andra relevanta områden, men nu krävs i princip expertis om integritet/medborgerliga friheter och insamling av underrättelser. Domstolen hade redan möjlighet att utse en *amicus* i alla fall där det ansågs lämpligt och var skyldig att göra detta när den hanterade en ny eller betydande tolkning av lagen. Efter det förnyade godkännandet måste FISC nu också utse en *amicus* varje gång den ombes att godkänna certifieringar och tillhörande förfaranden (t.ex. målinriktningsförfaranden) enligt avsnitt 702 i Fisa, om inte FISC anser att detta inte skulle vara lämpligt eller sannolikt skulle leda till onödigt dröjsmål[57]. Dessutom kan

Den möjliga varaktigheten för elektronisk övervakning med avseende på utländska makter eller ombud för utländska makter har förlängts från 120 dagar till 1 år (avsnitt 6 g i RISAA).

[53] Avsnitt 2 d i RISAA.

[54] Avsnitt 3 a i RISAA.

[55] Avsnitt 3 b i RISAA. Vid behov kan FBI:s direktör på grund av tvingande omständigheter besluta om ett undantag från denna bestämmelse, som måste meddelas kongressen.

[56] För tydlighetens skull påpekas att dessa ändringar inte påverkar de särskilda försvararnas status och roll inför dataskyddsdomstolen, vilket bekräftades av Förenta staterna vid översynsmötet.

[57] Avsnitt 5 b i RISAA.

domstolen nu besluta att utse en eller flera *amici*, i stället för att bara utse en. Det klargörs också att den information som *amici* ska tillhandahålla måste begränsas till hantering av de specifika frågor som domstolen har identifierat, även om de områden där *amici* kan kommentera har förblivit omfattande (dvs. rättsliga argument och information om skydd av enskilda amerikaners integritet och medborgerliga friheter, insamling av underrättelser och kommunikationsteknik eller något annat relevant område).

Slutligen inrättas i avsnitt 18 i RISAA en reformkommission för Fisa – som bland annat består av kongressledamöter, ordföranden för PCLOB, den vice direktören för den nationella underrättelsetjänsten och den vice justitieministern samt ytterligare medlemmar som ska utses av kongressen[58] – för att rekommendera ytterligare Fisa-reformer.

Kommissionen kommer att noga övervaka den fortsatta utvecklingen med avseende på avsnitt 702 i Fisa, bland annat i samband med den tillsynsverksamhet som bedrivs av PCLOB (se nedan), reformkommissionens arbete och den kommande översynen av Fisa efter två år.

#### *2.2.1.3. Övervakning i praktiken: siffror och trender*

Den nationella underrättelsetjänstens årliga rapport om insyn i statistiken om underrättelsegemenskapens användning av nationella säkerhetsmyndigheter för kalenderåret 2023 (offentliggjord i april 2024)[59] visar att antalet mål enligt avsnitt 702 i Fisa ökade från 245 073 under kalenderåret 2022 till 268 590 under kalenderåret 2023. I rapporten förklaras att variationer i antalet mål kan vara kopplade till en rad olika orsaker, däribland förändringar i operativa prioriteringar, världshändelser, teknisk kapacitet, målets beteende och förändringar inom telekommunikationssektorn. I rapporten anges också att inga utländska medborgare (jämfört med 1 under 2021 och 0 under 2022) målsöktes enligt avsnitt 402 i Fisa (pen register och trap and trace-anordningar), medan sex beslut (jämfört med 11 under både 2021 och 2022) för sex mål (jämfört med 13 under 2021 och 11 under 2022) utfärdades enligt avsnitt 501 i Fisa (tillgång till affärsregister för gemensamma transportföretag, uthyrningsanläggningar för fordon eller fysiska lagringsanläggningar), vilket omfattar 5 412 unika identifierare (jämfört med 23 157 under 2021 och 55 431 under 2022) som användes för att lämna information som samlats in i enlighet med sådana beslut.

Enligt justitieministeriets årliga rapport om lagen om underrättelseverksamhet och övervakning utomlands till kongressen lämnades under kalenderåret 2023 327 ansökningar in till FISC om genomförande av elektronisk övervakning och/eller fysiska sökningar för utländska underrättelseändamål enligt avsnitt 105 respektive 302 i Fisa[60]. Totalt var mellan 500 och 999 personer föremål för övervakning. När det gäller nationella säkerhetsskrivelser anges i rapporten att 10 115 förfrågningar (med undantag för begäran endast om abonnentinformation) utfärdades för information om utländska medborgare, för att inhämta information om 3 033 olika utländska medborgare[61].

---

[58] I avsnitt 18 krävs särskilt företrädare som står utanför kongressen.

[59] https://www.dni.gov/files/CLPT/documents/2024_ASTR_for_CY2023.pdf.

[60] https://www.justice.gov/nsd/media/1350236/dl?inline.

[61] Dessa siffror har i stort sett varit stabila jämfört med föregående rapporteringsår (2022). Som jämförelse fanns det under 2022 317 slutliga ansökningar hos FISC om elektronisk övervakning och/eller fysiska sökningar för utländska underrättelseändamål. Det totala antalet personer som var föremål för beslut om elektronisk övervakning var mellan 0 och 499. FBI utfärdade 9103 nationella säkerhetsskrivelseförfrågningar om information om utländska medborgare under 2022 (med undantag för begäran endast om abonnentinformation). Källa: https://irp.fas.org/agency/doj/fisa/2022rept.pdf.

Flera företag som är certifierade enligt dataskyddsramen (t.ex. Google, Meta) utnyttjar möjligheten enligt amerikansk lagstiftning att offentliggöra insynsrapporter som informerar om antalet Fisa-förfrågningar och nationella säkerhetsskrivelseförfrågningar som de har mottagit under en viss rapporteringsperiod. Vid tidpunkten för utarbetandet av denna rapport var statistiken över Fisa-förfrågningar efter juli 2023 ännu inte tillgänglig. Google uppgav till exempel att företaget hade tagit emot 500–999 nationella säkerhetsskrivelseförfrågningar, som berörde mellan 2 000 och 2 499 konton mellan juli och december 2023[62]. Meta rapporterade att företaget hade tagit emot 0–499 nationella säkerhetsskrivelseförfrågningar, som berörde 500–999 konton, under samma rapporteringsperiod[63]. Antalet har varit relativt stabilt under de senaste åren. För att ytterligare öka insynen publicerar vissa företag (t.ex. Google) proaktivt nationella säkerhetsskrivelser som de har mottagit när begränsningarna av utlämningen av uppgifter har upphävts[64].

#### *2.2.1.4. Annan utveckling*

I samband med förberedelserna inför översynen har flera icke-statliga organisationer ställt frågor om amerikanska underrättelsemyndigheters nya sätt att samla in uppgifter genom inköp av uppgifter från kommersiella enheter, särskilt datamäklare. De förklarade att även om uppgifter som samlats in på grundval av detta fortfarande måste behandlas i enlighet med andra krav, till exempel enligt dekret 12333[65], sker ett sådant förvärv utanför ramen för Fisa och dekret 14086.

I detta avseende bör det erinras om att alla typer av frivilligt utbyte av uppgifter med tredje parter omfattas av flera detaljerade villkor enligt dataskyddsramen. För det första kan en certifierad organisation inte dela uppgifter med en tredje part (inte agera som ombud/personuppgiftsbiträde) utan att meddela de berörda personerna och ge dem en valmöjlighet[66]. För det andra får vidare överföringar, i enlighet med *principen om ansvar för vidare överföring*, endast utföras (1) för begränsade och specificerade ändamål, (2) på grundval av ett avtal mellan organisationen som är certifierad enligt dataskyddsramen mellan EU och Förenta staterna och den tredje parten och (3) endast om det avtalet kräver att den tredje parten tillhandahåller samma skyddsnivå som den som garanteras genom principerna[67].

Dessutom har den federala konkurrensmyndigheten vidtagit verkställighetsåtgärder mot datamäklare som säljer känsliga konsumentuppgifter, vilket också diskuterades under översynsmötet. I ett fall mot *X-Mode* och dess efterföljare *Outlogic* antog den federala konkurrensmyndigheten den 9 januari 2024 till exempel ett beslut om att förbjuda företaget att sälja geolokaliseringsuppgifter till tredje part och radera uppgifter som det använt och delat olagligt. Den federala konkurrensmyndighetens utredning visade bland annat att företaget inte fullt ut informerade enskilda personer om användningen och försäljningen av deras geolokaliseringsuppgifter, underlät att införa åtgärder för att göra det möjligt för enskilda att välja bort spårning, möjliggjorde användning av uppgifterna för potentiellt diskriminerande

[62] https://transparencyreport.google.com/user-data/us-national-security.
[63] https://transparency.meta.com/reports/government-data-requests/country/US/.
[64] https://transparencyreport.google.com/user-data/us-national-security..
[65] Se t.ex. avsnitt 2.4 i dekret 12333 om insamlingstekniker.
[66] Se skäl 40 i beslutet om adekvat skyddsnivå.
[67] Se skäl 38 i beslutet om adekvat skyddsnivå.

ändamål och underlät att begränsa tredje parters användning av sådana uppgifter[68]. Kommissionen förväntar sig att den federala konkurrensmyndigheten kommer att tillämpa samma strategi om företag som är certifierade enligt dataskyddsramen skulle utbyta uppgifter i strid med ovannämnda bestämmelser.

Slutligen är det värt att nämna att den nationella underrättelsetjänsten i maj 2024 utfärdade underrättelsegemenskapens politiska ram för kommersiellt tillgänglig information[69]. I denna ram fastställs ett antal principer och krav som underrättelsemyndigheter bör följa, bland annat för att minimera riskerna för den personliga integriteten och de medborgerliga friheterna, när de förvärvar och använder information i samband med en kommersiell transaktion.

### 2.2.2. Oberoende tillsyn

Förenta staternas underrättelsemyndigheter övervakas av olika organ, däribland tjänstemän inom integritetsskydd och medborgerliga friheter, generalinspektörer, kongressen och PCLOB. I synnerhet kräver dekret 14086 att det vid varje underrättelsemyndighet ska finnas högre tjänstemän inom juridik, tillsyn och efterlevnad för att säkerställa efterlevnad av tillämplig amerikansk lagstiftning. Denna tillsynsfunktion utförs av tjänstemän med en utsedd efterlevnadsroll samt tjänstemän inom integritetsskydd och medborgerliga friheter och generalinspektörer[70]. De måste utföra regelbunden tillsyn av signalunderrättelseverksamhet och se till att fall av bristande efterlevnad åtgärdas. Underrättelsemyndigheterna måste ge sådana tjänstemän tillgång till all relevant information de behöver för att kunna utföra sina tillsynsuppgifter och får inte vidta några åtgärder för att hindra eller otillbörligt påverka deras tillsynsverksamhet.

Chefsjuristen vid generalinspektörskontoret för underrättelsegemenskapen inom den nationella underrättelsetjänsten – som har omfattande behörighet för hela underrättelsegemenskapen och befogenhet att utreda klagomål eller information om påstått olagligt handlande eller maktmissbruk – deltog vid översynsmötet. Han bekräftade att generalinspektörskontoret för underrättelsegemenskapen systematiskt kontrollerar efterlevnaden av dekret 14086 som en del av sin tillsynsverksamhet. Han hänvisade också till den nyligen genomförda tillsynen av andra generalinspektörer inom underrättelsegemenskapen, som beskrivs i regelbundna rapporter. I sin halvårsrapport till kongressen för april–september 2023[71] informerade generalinspektören för NSA om en utvärdering av en intern NSA-kontrollram för beslut och förfrågningar om målinriktning. Slutsatsen drogs att denna ram fungerade korrekt för att säkerställa efterlevnad

[68] https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data.

[69] https://www.dni.gov/files/ODNI/documents/CAI/Commercially-Available-Information-Framework-May2024.pdf. Underrättelsemyndigheterna måste efterleva ramen sedan augusti 2024.

[70] Varje underrättelsemyndighet har en generalinspektör som enligt lag är oberoende och ansvarig för att genomföra revisioner och utredningar om den verksamhet som bedrivs av respektive myndighet för ändamål som rör den nationella säkerheten. De har tillgång till allt relevant (inbegripet sekretessbelagt) material, vid behov genom föreläggande, och får ta upp vittnesmål. Generalinspektörer hänskjuter fall av misstänkta brott till åtal och utfärdar rekommendationer om korrigerande åtgärder till myndighetschefer. Även om deras rekommendationer inte är bindande offentliggörs i allmänhet deras rapporter, inbegripet om uppföljningsåtgärder (eller avsaknad av sådana), och skickas till kongressen. Se i detta avseende fotnot 136 i beslutet om adekvat skyddsnivå om generalinspektörens roll.

[71] https://oig.nsa.gov/reports/Article/3609957/semiannual-report-to-congress-1-april-2023-to-30-september-2023/.

av lagar, direktiv och policyer som skyddar medborgerliga friheter och personlig integritet. I samma rapport nämns också en utredning som avslöjade att en anställd vid NSA missbrukade ett signalunderrättelseverktyg för otillåtna ändamål.

Enligt dekret 14086 har PCLOB[72] anförtrotts särskilda tillsynsfunktioner[73]. Ordföranden för PCLOB och dess tre ledamöter deltog i översynsmötet och informerade om att PCLOB gav råd till underrättelsemyndigheter om deras utkast till riktlinjer och förfaranden för genomförande av dekret 14086 i april 2023, och rådfrågades om nomineringen av domare och särskilda försvarare vid dataskyddsdomstolen. Styrelsen inledde också ett tillsynsprojekt för att (1) se över genomförandet av de uppdaterade riktlinjer och förfaranden som antagits av underrättelsemyndigheterna för att säkerställa att de är förenliga med dekretet och (2) genomföra en årlig översyn av hur den nya prövningsmekanismen fungerar (se nedan)[74]. PCLOB:s ledamöter bekräftade att man planerar att genomföra båda översynerna inom en snar framtid. När det gäller prövningen förklarade de att PCLOB:s översyn, i avsaknad av klagomål, kommer att inriktas på de riktlinjer och förfaranden som införts för att inrätta mekanismen.

När det gäller annan tillsynsverksamhet utfärdade PCLOB en rapport om avsnitt 702 i Fisa den 28 september 2023[75]. Denna rapport är en uppföljning av en tidigare rapport från 2014 och innehåller uppdaterad faktisk och rättslig information om tillämpningen av övervakningsprogrammen enligt avsnitt 702 i Fisa. Rapporten innehåller även rekommendationer om underrättelsemyndigheternas efterlevnad av tillämpliga krav och förslag till kongressen om att ytterligare stärka flera aspekter av avsnitt 702 i Fisa i samband med dess förnyade godkännande (bland annat genom att kodifiera de legitima mål för övervakningsverksamhet som anges i dekret 14086)[76]. Under översynsmötet informerade PCLOB om att man inom kort förväntar sig att få svar från underrättelsemyndigheter om genomförandet av dess rekommendationer, vilket kommer att bidra till en framtida uppföljningsrapport. Andra pågående tillsynsprojekt omfattar ett om bekämpning av inhemsk terrorism och dess inverkan på den personliga integriteten och de medborgerliga friheterna och FBI:s insamling av uppgifter från öppna källor eller kommersiellt tillgängliga uppgifter[77].

Slutligen uttryckte icke-statliga organisationer som rådfrågats i samband med översynen oro över att flera PCLOB-ledamöters mandat kommer att löpa ut inom en snar framtid, vilket kan leda till att PCLOB inte längre är beslutsför. Framför allt har ordförandens mandatperiod löpt ut och den övergångsperiod under vilken hon kan tjänstgöra löper ut i januari 2025, samtidigt som en annan plats är vakant, och en tredje plats kommer också att bli vakant i januari nästa

[72] PCLOB är en oberoende byrå som har anförtrotts ansvar för politiken för bekämpning av terrorism och för dess genomförande, i syfte att skydda den personliga integriteten och de medborgerliga friheterna. Den kan få tillgång till all relevant (inbegripet sekretessbelagd) information, genomföra intervjuer och ta upp vittnesmål. Den kan utfärda rekommendationer till brottsbekämpande myndigheter och underrättelsemyndigheter och rapporterar regelbundet till kongressen och till presidenten Rapporterna offentliggörs i största möjliga utsträckning.

[73] https://documents.pclob.gov/prod/Documents/EventsAndPress/834a1977-f420-4b2a-ae93-8a522b2c7c74/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL)%20-%20Completed%20508%20-%2010202022.pdf.

[74] https://www.pclob.gov/OversightProjects/Details/1115.

[75] https://documents.pclob.gov/prod/Documents/OversightReport/8ca320e5-01d3-4d6a-8106-3384aad6ff31/2023%20PCLOB%20702%20Report%20-%20Nov%2017%202023%20-%201446.pdf.

[76] Kommissionen noterar att vissa av dessa rekommendationer har införlivats som en del av RISAA, däribland rekommendationen om ”abouts”-insamling eller rekommendationen om att stärka FISC-experternas roll (amici).

[77] https://www.pclob.gov/OversightProjects.

år. Under översynsmötet förklarade ledamöterna att de inte förväntar sig att PCLOB ska sakna beslutsförhet, eftersom en nominering redan har utfärdats för den plats som för närvarande är vakant (och väntar på senatens bekräftelse)[78]. De betonade också att även om styrelsen inte är beslutsför skulle detta inte påverka dess förmåga att fortsätta att genomföra tillsynsprojekt. Med tanke på PCLOB:s viktiga roll för att se över genomförandet av dekret 14086 kommer kommissionen dock att noga övervaka statusen för framtida vakanta platser och nomineringar/utnämningar.

### 2.2.3. Prövningsmöjligheter

Genom dekret 14086, kompletterad med en förordning från justitieministern, inrättades en ny prövningsmekanism för att hantera och lösa kvalificerande klagomål från enskilda personer om Förenta staternas signalunderrättelseverksamhet[79]. Alla enskilda personer i EU har rätt att lämna in klagomål till prövningsmekanismen avseende påstådda överträdelser av amerikansk lagstiftning som reglerar signalunderrättelseverksamhet (t.ex. dekret 14086, avsnitt 702 i Fisa, dekret 12333) med avseende på personuppgifter som överförs till Förenta staterna som inverkar negativt på deras intressen rörande integritetsskydd och medborgerliga friheter Enskilda personer kan lämna in ett klagomål till en dataskyddsmyndighet i en EU-medlemsstat, som via EDPB:s sekretariat skickar vidare klagomålet till prövningsmekanismen. Mekanismen består av två skikt, där den inledande utredningen av klagomål utförs av ODNI CLPO och enskilda har möjlighet att överklaga dess beslut inför en oberoende dataskyddsdomstol. När översynen av ODNI CLPO eller dataskyddsdomstolen har slutförts informeras den enskilda personen, via den nationella myndigheten, om att översynen antingen inte identifierade några överträdelser som omfattas eller att ODNI CLPO/dataskyddsdomstolen utfärdat ett beslut som kräver lämpligt avhjälpande. Beslut från ODNI CLPO och dataskyddsdomstolen är bindande för underrättelsemyndigheter.

Sedan beslutet om adekvat skyddsnivå antogs har ytterligare åtgärder vidtagits för att göra prövningsmekanismen fullt operativ.

När det gäller inrättandet av dataskyddsdomstolen utnämndes den 14 november 2023 åtta domare (dvs. två domare mer än det minsta antal som krävs enligt dekret 14086, kompletterat med justitieministerns förordningar 28 C.F.R. § 201.3 a) till domstolen[80]. De utnämndes på grundval av kriterierna i dekret 14086 och i enlighet med det förfarande som fastställs däri, bland annat efter samråd med PCLOB[81]. De omfattar f.d. domare från den federala distriktsdomstolen och appellationsdomstolen, en f.d. amerikansk justitieminister och en f.d. ledamot av PCLOB. I enlighet med dekretet har minst hälften av domarna tidigare rättslig erfarenhet. I april 2024 utnämndes dessutom två särskilda försvarare – rättstillämpare med sakkunskap om både integritetsskydd och nationell säkerhet – till att företräda enskilda personers intressen inför dataskyddsdomstolen. Vid översynsmötet bekräftades att alla domare och särskilda försvarare har fått det högsta säkerhetsgodkännandet och därför kan få tillgång till sekretessbelagt material när de utför sina uppgifter för dataskyddsdomstolen.

[78] https://documents.pclob.gov/prod/Documents/EventsAndPress/deb9cd13-12af-4250-998e-a520a2419a6b/PCLOB%20nominee%20press%20release%206-13-24.pdf.
[79] Se skäl 176–194 i beslutet om adekvat skyddsnivå.
[80] https://www.justice.gov/opa/pr/attorney-general-merrick-b-garland-announces-judges-data-protection-review-court.
[81] Avsnitt 3 d A i dekret 14086.

Dataskyddsdomstolen hade också offentliggjort en rad vanliga frågor med mer information om dess roll, oberoende och funktion[82].

När det gäller handläggning av klagomål antog den nationella underrättelsetjänsten den 6 december 2022 direktiv 126 om underrättelsegemenskapen, som i detalj reglerar (genom att fastställa tidsfrister, inrätta en säker elektronisk databas och säkra kommunikationskanaler, kräva att tjänstemannen med ansvar för skyddet av medborgerliga friheter och underrättelsegemenskapen samarbetar med PCLOB i samband med den årliga översynen av prövningsmekanismen osv.) olika aspekter av förfarandet för utredning och beslut om klagomål[83]. Detta direktiv är tillämpligt i hela den amerikanska underrättelsegemenskapen och har kompletterats med ytterligare interna förfaranden som antagits av enskilda underrättelsemyndigheter om deras samarbete med ODNI CLPO i samband med handläggningen av ett klagomål (t.ex. utveckling av en säker databas för utbyte av klagomål och tillhörande handlingar samt säker kommunikation mellan berörda myndigheter). Under de kommande månaderna kommer dataskyddsdomstolen också att utfärda mer detaljerade regler om handläggningen av klagomål och andra förfarandeaspekter.

Ett antal ytterligare åtgärder vidtogs i Europeiska unionen och Förenta staterna för att informera allmänheten samt för att underlätta inlämning och handläggning av klagomål. Detta inbegriper EDPB:s antagande av ett informationsmeddelande om den nya prövningsmekanismen[84], en mall för klagomålsformulär (som ska översättas och offentliggöras av alla dataskyddsmyndigheter på deras nationella språk)[85] och en arbetsordning som reglerar samarbetet mellan nationella tillsynsmyndigheter och EDPB:s sekretariat[86]. På samma sätt offentliggjorde den nationella underrättelsetjänsten vanliga frågor och ett faktablad om den nya prövningsmekanismen och engagerade sig i åtgärder för att öka allmänhetens medvetenhet[87].

Dessutom har EDPB och de berörda amerikanska myndigheterna under det senaste året haft ett nära samarbete om flera operativa aspekter. I synnerhet, vilket bekräftades under översynsmötet, inrättade de en krypterad kommunikationskanal för att överföra klagomål från nationella myndigheter i EU till EDPB:s sekretariat, från EDPB:s sekretariat till ODNI CLPO samt till justitieministeriets kansli för integritet och medborgerliga friheter och mellan ODNI CLPO och andra myndigheter på den amerikanska sidan (t.ex. dataskyddsdomstolen). Dessutom förklarade ODNI CLPO att ytterligare interna förfaranden har införts för samarbete mellan enskilda underrättelsemyndigheter och ODNI CLPO när det gäller handläggningen av klagomål.

Slutligen informerade kansliet för integritet och medborgerliga friheter, som tillhandahåller administrativt stöd till dataskyddsdomstolen, också om att dataskyddsdomstolen verkar inom ramen för sin egen särskilda budgetpost och får de resurser som krävs för att utföra sina uppgifter, inbegripet säkra stationära och bärbara datorer, telefoner osv. I enlighet med dekret

[82] https://www.justice.gov/opcl/dprc-resources.
[83] https://www.dni.gov/files/documents/ICD/ICD_126-Implementation-Procedures-for-SIGINT-Redress-Mechanism.pdf.
[84] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/information-note-data-protection-framework-redress_en.
[85] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/template-complaint-form-us-office-director-national_en.
[86] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/rules-procedure-data-protection-framework-redress_en.
[87] https://www.dni.gov/files/CLPT/documents/Fact_Sheets/The_Role_of_the_ODNI_CLPO_FAQs.pdf och https://www.dni.gov/files/CLPT/documents/Fact_Sheets/Data_Privacy_Framework.pdf.

14086 har handelsministeriet dessutom vidtagit nödvändiga åtgärder, bland annat genom att inrätta en krypterad kommunikationskanal med ODNI CLPO, för att föra register över alla kvalificerande klagomål som mottagits. Handelsministeriet ska regelbundet kontakta ODNI CLPO om huruvida sekretessen har hävts för information om ett enskilt klagomål. I så fall ska handelsministeriet underrätta den berörda personen om detta för att ge honom eller henne möjlighet att få tillgång till sådan information.

Vid tidpunkten för översynsmötet hade inga klagomål inkommit till EU:s tillsynsmyndigheter och den nya prövningsmekanismen hade därför ännu inte utlösts.

## 3. SLUTSATS

På grundval av den information som samlats in under den första översynen drar kommissionen slutsatsen att de amerikanska myndigheterna har infört de strukturer och förfaranden som krävs för att säkerställa att dataskyddsramen fungerar ändamålsenligt. I detta sammanhang värdesätter kommissionen i hög grad det mycket goda samarbetet med de amerikanska myndigheterna för att genomföra översynen.

Även om denna första översyn naturligtvis inriktades på att kontrollera om alla de inslag som ingår i ramen är på plats, är erfarenheten av den praktiska tillämpningen av de skyddsåtgärder som gäller både för certifierade företags behandling av uppgifter och för offentliga myndigheters tillgång till uppgifter givetvis begränsad efter bara ett års verksamhet. Kommissionen kommer därför att noga övervaka den relevanta utvecklingen under de kommande månaderna och åren, med särskild uppmärksamhet på (1) PCLOB:s kommande rapporter om genomförandet av dekret 14086 och om hur prövningsmekanismen för signalunderrättelser fungerar, särskilt dataskyddsdomstolen, (2) eventuella ytterligare ändringar av avsnitt 702 i Fisa och (3) nominering och utnämning av ledamöter i PCLOB för tillsättning av kommande vakanta platser.

För att säkerställa en fortsatt och ändamålsenlig funktion anser kommissionen dessutom att det är viktigt att

- handelsministeriet, såsom tillkännagavs vid översynsmötet, fullt ut utnyttjar de olika verktyg som tillhandahålls i dataskyddsramen för att övervaka företagens efterlevnad av principerna och upptäcka falska påståenden om deltagande,
- den federala konkurrensmyndigheten vidareutvecklar sin proaktiva strategi för att utreda och se till att certifierade företag efterlever dataskyddsramens principer, och
- handelsministeriet, den federala konkurrensmyndigheten och EU:s dataskyddsmyndigheter utarbetar gemensamma vägledningsinstrument om viktiga krav enligt dataskyddsramens principer, t.ex. om personaluppgifter och vidare överföringar.

Mot bakgrund av detta resultat av översynen och såsom anges i skäl 211 i beslutet om adekvat skyddsnivå anser kommissionen att det är lämpligt att genomföra nästa regelbundna översyn efter tre år. Detta bör göra det möjligt att få mer erfarenhet av den praktiska tillämpningen av dataskyddsramen och ta hänsyn till den ovannämnda kommande utvecklingen. Kommissionen kommer därför, i enlighet med artikel 3.4 i beslutet om adekvat skyddsnivå, att samråda med

EDPB och den kommitté som inrättats enligt artikel 93.1 i den allmänna dataskyddsförordningen om frekvensen för framtida översyner.