EUROPA-
KOMMISSIONEN

Bruxelles, den 9.10.2024
COM(2024) 451 final

RAPPORT FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET OG RÅDET

om den første regelmæssige revision af, hvordan afgørelsen om tilstrækkeligheden af beskyttelsesniveauet i forbindelse med EU-USA-databeskyttelsesrammen fungerer

1. DEN FØRSTE REGELMÆSSIGE REVISION – BAGGRUND, FORBEREDELSE OG PROCES

I sin afgørelse af 10. juli 2023 ("afgørelsen om tilstrækkeligheden af beskyttelsesniveauet") fandt Kommissionen, at EU-USA-databeskyttelsesrammen giver et tilstrækkeligt beskyttelsesniveau for personoplysninger, der overføres fra Den Europæiske Union til organisationer i Amerikas Forenede Stater[1]. I henhold til afgørelsen om tilstrækkeligheden af beskyttelsesniveauet skal Kommissionen foretage regelmæssige revisioner, hvoraf den første bør finde sted et år efter datoen for meddelelsen af afgørelsen om tilstrækkeligheden af beskyttelsesniveauet til medlemsstaterne. Denne rapport afslutter den første revision.

Som krævet i betragtning 211 til afgørelsen om tilstrækkeligheden af beskyttelsesniveauet fokuserede denne første revision, der fandt sted efter det første års anvendelse af den nye ramme, på at kontrollere, om alle de elementer, der er fastsat i rammen, er blevet gennemført og fungerer effektivt. Revisionen omfattede alle aspekter af rammens funktion, herunder i lyset af den retlige udvikling, der har fundet sted, siden afgørelsen om tilstrækkeligheden af beskyttelsesniveauet blev vedtaget.

Som forberedelse til revisionen indsamlede Kommissionen oplysninger fra relevante interessenter, navnlig fra ikkestatslige organisationer (NGO'er) med ekspertise inden for digitale rettigheder og privatlivets fred[2], organisationer certificeret i henhold til databeskyttelsesrammen gennem deres brancheorganisationer[3] samt fra de amerikanske myndigheder, der er involveret i gennemførelsen af rammen. Desuden har Kommissionen også indsamlet feedback fra offentligheden ved hjælp af en specifik indkaldelse af feedback på portalen "Deltag i debatten"[4].

Der blev afholdt et revisionsmøde i Washington D.C. den 18.-19. juli 2024. Det blev indledt af EU-kommissær for retlige anliggender og forbrugere Didier Reynders og USA's handelsminister Gina Raimondo.[5]

---

[1] Kommissionens gennemførelsesafgørelse (EU) 2023/1795 af 10. juli 2023 i henhold til Europa-Parlamentets og Rådets forordning (EU) 2016/679 om et tilstrækkeligt beskyttelsesniveau for personoplysninger inden for EU-USA-databeskyttelsesrammen.

[2] Kommissionen sendte et spørgeskema til ni NGO'er (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 og Center for Democracy and Technology) med fokus på den relevante udvikling i USA's retlige rammer, tilsyns- og håndhævelsesmekanismer og klagemekanismernes funktion. Kommissionens tjenestegrene og repræsentanter for Databeskyttelsesrådet mødtes også online med disse NGO'er den 9. juli 2024.

[3] Kommissionen sendte et spørgeskema til ni brancheorganisationer (Software & Information Industry Association, U.S. Chamber of Commerce, Information Technology Industry Council, Software Alliance, Centre for Information Policy Leadership, Interactive Advertising Bureau, United States Council for International Business, Computer and Communications Industry Association og Engine) med fokus på de erfaringer, som organisationer certificeret i henhold til databeskyttelsesrammen har gjort sig, navnlig hvad angår certificeringsprocessen, de skridt, der er taget for at overholde principperne i databeskyttelsesrammen, mekanismer til behandling af anmodninger og klager fra enkeltpersoner osv.

[4] Den modtagne feedback findes på følgende link: 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_da.

[5] Revisionsmødet var tilrettelagt efter emne, og hvert særligt dagsordenspunkt blev introduceret med en kort præsentation ved den relevante amerikanske myndighed, EU-repræsentant eller organisation efterfulgt af en detaljeret spørgerunde. Den første dag blev rammens "kommercielle aspekter" (dvs. anvendelsen og

For EU's vedkommende blev revisionen foretaget af repræsentanter for Europa-Kommissionens Generaldirektorat for Retlige Anliggender og Forbrugere sammen med fem repræsentanter udpeget af Det Europæiske Databeskyttelsesråd og fra forskellige nationale databeskyttelsesmyndigheder og Den Europæiske Tilsynsførende for Databeskyttelse[6]. På amerikansk side deltog repræsentanter fra handelsministeriet, udenrigsministeriet, Federal Trade Commission (den amerikanske konkurrencemyndighed, FTC), transportministeriet, Office of the Director of National Intelligence (kontoret for direktøren for den nationale efterretningstjeneste, ODNI), justitsministeriet, Inspector General for the Intelligence Community (efterretningstjenesternes generalinspektør) samt medlemmer af Privacy and Civil Liberties Oversight Board (rådet for tilsyn med privatlivets fred og borgerlige rettigheder, PCLOB). Desuden gav repræsentanter fra organisationer, der tilbyder uafhængige tvistbilæggelsestjenester, og American Arbitration Association oplysninger under de relevante revisionsmøder. Endelig blev revisionen suppleret med præsentationer ved organisationer certificeret i henhold til databeskyttelsesrammen om, hvordan virksomheder overholder rammens krav.

Kommissionens konklusioner er blevet yderligere underbygget af offentligt tilgængeligt materiale såsom retsafgørelser, relevante amerikanske myndigheders gennemførelsesbestemmelser og -procedurer, rapporter og undersøgelser fra ikkestatslige organisationer, gennemsigtighedsrapporter udarbejdet af virksomheder certificeret i henhold til databeskyttelsesrammen, årlige rapporter fra uafhængige klageinstanser samt medieomtaler.

2. UNDERSØGELSESRESULTATER

2.1. Kommercielle aspekter

2.1.1. Certificeringsprocessen

For at kunne modtage personoplysninger, der overføres fra EU på grundlag af databeskyttelsesrammen, skal en amerikansk virksomhed certificere og derefter årligt recertificere deres overholdelse af specifikke databeskyttelseskrav ("principperne i databeskyttelsesrammen") over for handelsministeriet. Certificeringen kræver, at en virksomhed er underlagt FTC's eller transportministeriets undersøgelses- og håndhævelsesbeføjelser, offentligt erklærer sin forpligtelse til at overholde principperne i databeskyttelsesrammen og offentliggør sin politik til beskyttelse af privatlivets fred og gennemfører sådanne krav fuldt ud[7]. Før en certificering færdiggøres, kontrollerer handelsministeriet, om virksomheden har opfyldt alle certificeringskrav[8].

På revisionsmødet forklarede handelsministeriet, at der i dette første år af databeskyttelsesrammen har været fokus på at indføre certificeringsprocessen, herunder udvikling af særlige IT-værktøjer, ajourføring af procedurer, samarbejde med virksomheder og gennemførelse af andre opsøgende aktiviteter/oplysningsaktiviteter. På datoen for revisionsmødet var mere end 2 800 virksomheder blevet certificeret i henhold til

håndhævelsen af de krav, der gælder for virksomheder, der er certificeret i henhold til databeskyttelsesrammen) behandlet, mens spørgsmål vedrørende myndighedsadgang til personoplysninger blev drøftet den følgende dag.

[6] Repræsentanter for Kommissionen og Databeskyttelsesrådet mødtes den 12. juni og den 10. juli 2024 for at forberede revisionen, drøfte de modtagne input og fastlægge, hvilke aspekter der kræver yderligere indsamling og præcisering af oplysninger.

[7] Afsnit I.2 i bilag I til afgørelsen om tilstrækkeligheden af beskyttelsesniveauet.

[8] Bilag III til afgørelsen om tilstrækkeligheden af beskyttelsesniveauet.

databeskyttelsesrammen. Det betyder, at flere virksomheder er blevet certificeret i henhold til databeskyttelsesrammen i dens første driftsår end under den tidligere ramme, privatlivsskjoldet [9]. Ifølge oplysninger fra handelsministeriet er 70 % af deltagerne SMV'er, og et stort antal virksomheder (47 %) tilhører informations-, kommunikations- og teknologisektoren (IKT). Endvidere er 60 % af virksomhederne udelukkende certificeret til data, der ikke vedrører menneskelige ressourcer, 2,5 % af virksomhederne er udelukkende certificeret til data vedrørende menneskelige ressourcer, og 37,5 % er certificeret til data, der vedrører og ikke vedrører menneskelige ressourcer.

Handelsministeriet har vedtaget de nødvendige procedurer for behandling af ansøgninger fra virksomheder. Virksomhederne skal indgive deres ansøgninger om certificering via handelsministeriets websted for databeskyttelsesrammen (https://www.dataprivacyframework.gov/). Det indeholder oplysninger om, hvordan man tilslutter sig databeskyttelsesrammen[10], og om virksomhedens forpligtelser i henhold til rammen[11]. Et særligt team i handelsministeriet, der ledes af en særlig direktør for databeskyttelsesrammen, er ansvarligt for alle aspekter vedrørende forvaltningen og administrationen af databeskyttelsesrammen, herunder certificeringsprocessen og overvågningen af overholdelsen. Hver ansøgning er tildelt en bestemt medarbejder, der er ansvarlig for den relevante virksomhed gennem hele certificeringsprocessen.

For at blive certificeret i henhold til rammen indgiver virksomheder deres ansøgning, herunder et udkast til politik til beskyttelse af privatlivets fred. Handelsministeriet kontrollerer, om den er i overensstemmelse med de relevante krav i databeskyttelsesrammen. Når organisationer ønsker at certificere forskellige enheder inden for en koncern (f.eks. forskellige datterselskaber), anmoder handelsministeriet om og gennemgår enten en overordnet politik til beskyttelse af privatlivets fred, der klart angiver alle de enheder, der vil være omfattet, eller separate politikker for hver enhed. Handelsministeriet kontrollerer også med den uafhængige klagemekanisme [12], som er angivet i ansøgningen, om organisationen rent faktisk har registreret sig hos den. For virksomheder, der vælger databeskyttelsesmyndighedens panel (f.eks. fordi de behandler data vedrørende menneskelige ressourcer), kontrollerer handelsministeriet, om virksomheden har betalt de nødvendige gebyrer for at gøre brug af panelet. Om nødvendigt kontrollerer handelsministeriet også, om ansøgeren er omfattet af FTC's eller transportministeriets jurisdiktion (og derfor er berettiget til at tilslutte sig databeskyttelsesrammen).

Hvis alle betingelser er opfyldt, underretter handelsministeriet organisationen om, at den på sit websted kan offentliggøre sin politik til beskyttelse af privatlivets fred med henvisning til databeskyttelsesrammen. Når politikken til beskyttelse af privatlivets fred er offentliggjort, bekræfter handelsministeriet certificeringen og tilføjer virksomheden på listen over organisationer, der deltager i databeskyttelsesrammen, på sit websted. Databeskyttelsesrammen kan anvendes til at modtage personoplysninger fra EU fra den dato, hvor handelsministeriet opfører organisationen på denne liste[13].

---

[9] I den tilsvarende periode var 2 400 virksomheder certificeret i henhold til privatlivsskjoldet.

[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] Tvistbilæggelsesorganer i den private sektor, hvorved den enkeltes klager og tvister undersøges og løses hurtigt uden omkostninger for den enkelte.

[13] Afsnit I, punkt 3, i bilag I til afgørelsen om tilstrækkeligheden af beskyttelsesniveauet.

Som forklaret på revisionsmødet har de kontroller, som handelsministeriet hidtil har foretaget, resulteret i, at 33 ansøgninger er blevet afvist, fordi de ikke opfyldte databeskyttelsesrammens krav. Generelt samarbejder handelsministeriet med virksomheden om at afhjælpe eventuelle mangler. Hvis handelsministeriet identificerer mangler, underretter den virksomheden om, at den skal afhjælpe disse, og at manglende svar inden for en given frist eller anden undladelse af at gennemføre selvcertificeringen i overensstemmelse med handelsministeriets procedurer vil føre til, at dens ansøgning anses som opgivet. Hvis den indledende certificering ikke er afsluttet/ændret inden for 12 måneder, anser handelsministeriet den for opgivet.

Fristen for den årlige recertificering er angivet for hver virksomhed i listen over organisationer, der deltager i databeskyttelsesrammen. For at minde virksomhederne om behovet for at ansøge om recertificering har handelsministeriet oprettet et system med påmindelser om, at certificeringen er ved at udløbe. Organisationer modtager en påmindelse en måned før, derefter to uger før og til sidst en dag før fristen. De, der lader deres certificering udløbe, fjernes fra listen over organisationer, der deltager i beskyttelsesrammen. Som beskrevet i bilag III til afgørelsen om tilstrækkeligheden af beskyttelsesniveauet har handelsministeriet på sit websted et særligt afsnit med en liste over de amerikanske organisationer, der ikke længere er aktive deltagere, og med angivelse af de respektive årsager til, at de pågældende virksomheder (f.eks. udløb eller udtræden) er blevet fjernet fra listen ("den inaktive liste"). Når organisationer fjernes fra listen over deltagende organisationer for at have ladet deres certificering udløbe, kontakter handelsministeriet dem for at bekræfte, om de ønsker at udtræde eller i stedet agter at foretage recertificering, og, hvis dette er tilfældet, for at kontrollere, at de i den periode, hvor deres certificering var udløbet, har anvendt principperne i databeskyttelsesrammen på personoplysninger, der er modtaget under databeskyttelsesrammen, og for at præcisere, hvilke skridt de vil tage for at afhjælpe de uløste problemer, der har forsinket deres recertificering. Når virksomheder meddeler handelsministeriet, at de ønsker at udtræde af databeskyttelsesrammen, kræver handelsministeriet, at de bekræfter, om de vil tilbagesende eller slette de oplysninger, de har modtaget under databeskyttelsesrammen, beholde dem og fortsat anvende principperne i databeskyttelsesrammen på sådanne oplysninger (som skal bekræftes årligt) eller beholde dem og indføre anden beskyttelse (f.eks. standardkontraktbestemmelser vedtaget af Europa-Kommissionen).

Feedback fra brancheorganisationer og virksomheder viser, at virksomheder certificeret i henhold til databeskyttelsesrammen har taget en række skridt til at sikre overholdelse af principperne i databeskyttelsesrammen. For at overholde *princippet om klageadgang, håndhævelse og ansvar* har organisationer f.eks. foretaget intern kontrol enten ved hjælp af selvevaluering eller via ekstern kontrol af overholdelsen. De to private uafhængige klagemekanismer, der deltog i revisionsmødet, forklarede, at de også foretager ekstern kontrol af overholdelse ved at gennemgå politikkerne til beskyttelse af privatlivets fred, og en af de private uafhængige klagemekanismer forklarede, at den også foretager revisioner og stikprøvekontroller med fokus på f.eks. principperne om *indsigt*, *valgfrihed* og *videreoverførsel*. Derudover har certificerede virksomheder udviklet interne overholdelsesprogrammer og tilsynsmekanismer, uddannet medarbejdere, gennemført mekanismer, der giver enkeltpersoner mulighed for at udøve deres rettigheder, foretaget analyser af konsekvenserne for privatlivets fred og gennemgået eksisterende aftaler.

2.1.2. Overvågning af overholdelse, falske påstande om deltagelse og håndhævelse

I henhold til databeskyttelsesrammen er handelsministeriet ansvarligt for at overvåge overholdelsen af principperne i databeskyttelsesrammen ved hjælp af forskellige værktøjer,

herunder ex officio-kontrol (på eget initiativ), ad hoc-stikprøvekontrol og spørgeskemaer om overholdelse. Dette omfatter søgning efter og håndtering af falske påstande om deltagelse i rammen, f.eks. gennem internetsøgninger[14].

For at overvåge at virksomheder certificeret i henhold til databeskyttelsesrammen overholder principperne, har handelsministeriet hovedsagelig baseret sig på ad hoc-websøgninger og (sociale) mediekontroller i løbet af det seneste år. Handelsministeriet rapporterede, at det ikke har konstateret problemer med overholdelsen af principperne i databeskyttelsesrammen i det første år og ikke har henvist nogen virksomheder til FTC eller transportministeriet med henblik på eventuelle håndhævelsesforanstaltninger. Den har også oprettet et særligt kontaktpunkt for at lette samarbejdet med databeskyttelsesmyndigheder og modtage klager fra enkeltpersoner og henvisninger fra andre myndigheder (f.eks. databeskyttelsesmyndigheder eller FTC). Der er imidlertid ikke modtaget nogen henvisninger eller klager i løbet af det seneste år. Mens det første år af databeskyttelsesrammens anvendelse var fokuseret på at etablere rammen og certificeringsprocessen, forklarede handelsministeriet på revisionsmødet, at det planlægger at foretage automatiske kontroller af overholdelsen for at udføre dem på en mere systematisk måde, og at det i øjeblikket udvikler de nødvendige IT-værktøjer med henblik herpå.

Kommissionen erkender, at handelsministeriet i det første år var nødt til at koncentrere sin indsats om at etablere rammen og certificeringsprocessen. Fremover er det vigtigt, at handelsministeriet intensiverer sine bestræbelser på at overvåge og kontrollere overholdelsen af principperne, hvilket er vigtigt for at sikre en fortsat høj grad af overholdelse af rammen og afsløre sager, der kræver yderligere håndhævelsesforanstaltninger, herunder eventuelle falske påstande om virksomheders deltagelse. I denne forbindelse glæder Kommissionen sig over, at handelsministeriet bekræftede sin hensigt om at udvikle og anvende (automatiserede) værktøjer til mere effektivt og systematisk at identificere problemer med overholdelse og falske påstande, og er af den opfattelse, at dette bør være en del af en bredere indsats for at gøre større brug af de forskellige værktøjer, det har til rådighed (f.eks. stikprøvekontroller, spørgeskemaer om kontrol af overholdelse og anmodninger om oplysninger), herunder for at kontrollere overholdelsen af specifikke krav i henhold til databeskyttelsesrammen[15].

Organisationer inden for databeskyttelsesrammen er underlagt FTC's og transportministeriets jurisdiktion. Under revisionsmødet bekræftede transportministeriet, at det har alle processer på plads til at træffe passende håndhævelsesforanstaltninger. Det forklarede også, at meget få selskaber under dens jurisdiktion har tilsluttet sig databeskyttelsesrammen (dvs. nogle få billetagenter, men ingen luftfartsselskaber). FTC bekræftede, at den systematisk kontrollerer overtrædelser af databeskyttelsesrammen i hver af sine undersøgelser af privatlivets fred. Indtil videre har FTC ikke modtaget nogen henvisninger fra andre myndigheder. Den har modtaget nogle få klager, der nævner databeskyttelsesrammen, skønt to af dem vedrørte virksomheder på den "inaktive liste", to vedrørte virksomheder, der ikke deltog i rammen, og en ikke vedrørte personoplysninger, der blev overført fra EU. På tidspunktet for udarbejdelsen af denne rapport havde FTC ikke truffet afgørelser om at håndhæve overholdelsen af databeskyttelsesrammen,

[14] Se bilag III til afgørelsen om tilstrækkeligheden af beskyttelsesniveauet. Der kan f.eks. opstå falske påstande, når en virksomhed hævder at deltage i databeskyttelsesrammen, og den enten aldrig har påbegyndt certificeringsprocessen eller har påbegyndt den, men ikke har færdiggjort den eller har ladet sin certificering udløbe.

[15] F.eks. med hensyn til videreoverførsel ved at gøre brug af muligheden i henhold til princip 3, litra b), i databeskyttelsesrammen om at anmode om et sammendrag eller en repræsentativ kopi af de relevante bestemmelser om beskyttelse af privatlivets fred i aftaler om videreoverførsel.

men den bekræftede, at flere virksomheder, der er certificeret i henhold til databeskyttelsesrammen, i øjeblikket undersøges.

Kommissionen glæder sig over, at FTC systematisk kontrollerer overtrædelser af databeskyttelsesrammen i alle sine undersøgelser af privatlivets fred. Da databeskyttelsesrammens fortsatte effektivitet afhænger af dens solide håndhævelse, forventes det, at FTC yderligere vil udøve sine undersøgelsesbeføjelser i henhold til rammen, herunder ved proaktivt at gennemføre "rent hus"-aktioner med fokus på overholdelse af specifikke krav i databeskyttelsesrammen og/eller visse sektorer.

2.1.3. Behandling af klager

Databeskyttelsesrammen giver EU-borgere forskellige klagemuligheder i tilfælde af certificerede organisationers manglende overholdelse af principperne i databeskyttelsesrammen[16]. Dette omfatter at finde en løsning gennem direkte kontakter med en organisation inden for databeskyttelsesrammen, som skal fremsende et svar til den berørte person inden for 45 dage. Enkeltpersoner kan også indgive en klage til en uafhængig klagemekanisme, der er udpeget af en organisation til at undersøge og afgøre klager. Afhængigt af omstændighederne kan dette enten være et alternativt tvistbilæggelsesorgan eller en databeskyttelsesmyndighed[17]. Endelig kan enkeltpersoner, hvis ingen af de andre tilgængelige klagemuligheder har afgjort den registreredes klage på tilfredsstillende vis, kræve, at en sag afgøres ved bindende voldgift af panelet i EU-USA-databeskyttelsesrammen som en "sidste udvej".

2.1.3.1. Virksomheders klagebehandling

Det fremgår af brancheorganisationers og virksomheders svar på spørgeskemaer fra Kommissionen, at virksomheder certificeret i henhold til databeskyttelsesrammen har modtaget meget få – om nogen – klager fra enkeltpersoner vedrørende manglende overholdelse af principperne i databeskyttelsesrammen. Samtidig har virksomhederne indført forskellige mekanismer og værktøjer, der gør det muligt for enkeltpersoner at udøve deres rettigheder og indgive klager, herunder via webbaserede formularer, e-mail og telefon.

2.1.3.2. *Uafhængige klagemekanismer*

Den feedback, der blev modtaget på revisionsmødet, og oplysningerne fra brancheorganisationerne viser, at der er indgivet ganske få klager til uafhængige klagemekanismer. Blandt de uafhængige klagemekanismer, der er blevet udvalgt af virksomheder, er BBB National Programs, JAMS, TRUSTe og VeraSafe. I henhold til databeskyttelsesrammen skal de uafhængige klagemekanismer offentliggøre en årlig rapport med aggregeret statistik over brugen af deres tvistbilæggelsestjenester. På tidspunktet for vedtagelsen af denne rapport havde alle berørte uafhængige klagemekanismer offentliggjort deres årsrapporter[18].

---

[16] Se afsnit 2.4 i afgørelsen om tilstrækkeligheden af beskyttelsesniveauet.

[17] Organisationer inden for databeskyttelsesrammen er forpligtede til at samarbejde med databeskyttelsesmyndigheden i forbindelse med undersøgelsen og afgørelsen af en klage, enten når det drejer sig om behandling af oplysninger om menneskelige ressourcer, der er indsamlet i forbindelse med ansættelsesforhold, eller når den pågældende organisation frivilligt har underlagt sig databeskyttelsesmyndighedernes tilsyn.

[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-

Desuden fremlagde BBB og VeraSafe på revisionsmødet detaljerede redegørelser for deres aktiviteter i det forløbne år. De rapporterede om en stigning i antallet af erhvervsdeltagere, der vælger deres tjenester i forhold til de tidligere rammer, og nævnte, at de havde modtaget nogle klager, selv om langt de fleste var uberettigede. BBB modtog f.eks. 87 klager fra enkeltpersoner i EU, hvoraf kun to var berettigede til bilæggelse. Selv om BBB forklarede, at klager i gennemsnit behandles inden for fem arbejdsdage, blev disse to klager i sidste ende afsluttet på grund af manglende svar fra enkeltpersonerne. VeraSafe modtog 26 klager, hvoraf seks kunne bilægges. To af dem, som vedrørte anmodninger om indsigt og sletning, blev bilagt, mens to stadig er under behandling, og to blev enten trukket tilbage eller afsluttet på grund af manglende svar fra enkeltpersonen. Begge uafhængige klagemekanismer forklarede, at de sigter mod at besvare klager på enkeltpersonens sprog.

Virksomheder inden for databeskyttelsesrammen, der behandler data om menneskelige ressourcer overført fra EU, skal vælge de europæiske databeskyttelsesmyndigheder som deres uafhængige klagemekanisme for disse data, mens en virksomhed inden for databeskyttelsesrammen på frivillig basis kan vælge de europæiske databeskyttelsesmyndigheder som deres uafhængige klagemekanisme for andre typer personoplysninger, der overføres under databeskyttelsesrammen. Faktisk valgte mere end halvdelen af de virksomheder, der var certificeret i henhold til databeskyttelsesrammen på tidspunktet for revisionen, denne løsning[19], hvilket hilses velkommen. Siden afgørelsen om tilstrækkeligheden af beskyttelsesniveauet blev vedtaget, har Databeskyttelsesrådet vedtaget forretningsordenen for det "uformelle panel af europæiske databeskyttelsesmyndigheder". Panelet har kompetence til at afgive bindende anbefalinger til de amerikanske organisationer om endnu ikke afgjorte klager fra enkeltpersoner over behandlingen af personoplysninger, der er blevet overført fra EU under databeskyttelsesrammen. I henhold til sin forretningsorden består panelet af en databeskyttelsesmyndighed, der fungerer som ledende databeskyttelsesmyndighed, og andre udpegede medundersøgende databeskyttelsesmyndigheder[20]. Det afgiver bindende anbefalinger inden for 60 dage efter modtagelsen af en klage inden for databeskyttelsesrammen. Databeskyttelsesrådet har også offentliggjort en skabelon til klageformular til indgivelse af klager til databeskyttelsesmyndighederne,[21] samt et dokument med ofte stillede spørgsmål om

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

[19] Kort tid efter revisionsmødet fremgik det af databeskyttelsesrammens websted, at 1 511 af de 2 892 deltagere havde en europæisk databeskyttelsesmyndighed som klagemekanisme.

[20] Den 17.4.2024 vedtog Databeskyttelsesrådet forretningsordenen for det "uformelle panel af europæiske databeskyttelsesmyndigheder" i henhold til EU-USA-databeskyttelsesrammen. Den kan tilgås her: 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_da.

databeskyttelsesrammen til enkeltpersoner ("FAQ for European individuals")[22] og et til virksomheder ("FAQ for European businesses")[23]. Panelet havde ikke modtaget nogen klager på tidspunktet for revisionen.

2.1.3.3. Den bindende voldgiftsordning

Det Internationale Center for Tvistbilæggelse (ICDR), som er den internationale afdeling af American Arbitration Association, blev valgt af handelsministeriet til at administrere den bindende voldgiftsordning. Efter vedtagelsen af afgørelsen om tilstrækkeligheden af beskyttelsesniveauet udvalgte handelsministeriet sammen med Kommissionen 11 voldgiftsmænd med erfaring inden for privatlivets fred og med forskellig baggrund, herunder inden for voldgift, retsvæsenet, den akademiske verden og civilsamfundet[24]. Desuden er voldgiftsreglerne[25] for panelet i databeskyttelsesrammen og en adfærdskodeks for voldgiftsmænd[26] blevet vedtaget, og disse er tilgængelige på ICDR's websted. På tidspunktet for revisionen var voldgiftsordningen endnu ikke blevet udløst af nogen enkeltperson i EU.

2.1.4. Vejledning, samarbejde og oplysning

Siden databeskyttelsesrammen trådte i kraft, har handelsministeriet gennemført forskellige oplysningsaktiviteter ved at tilrettelægge roadshows, webinarer og konferencer, række ud til brancheorganisationer og interagere direkte med mere end 3 000 virksomheder for at informere om databeskyttelsesrammen. Det har også offentliggjort vejledninger, bl.a. i form af ofte stillede spørgsmål rettet til enkeltpersoner samt til virksomheder i EU og USA[27]. Databeskyttelsesrådet har til gengæld udarbejdet klageformularer og ofte stillede spørgsmål rettet til enkeltpersoner og virksomheder. Kommissionen offentliggjorde ligeledes et dokument med ofte stillede spørgsmål og et faktablad om databeskyttelsesrammen, da den vedtog sin afgørelse om tilstrækkeligheden af beskyttelsesniveauet[28].

Samtidig viste det sig på revisionsmødet, at der er behov for en større indsats for at oplyse enkeltpersoner og yde vejledning til virksomheder. Input fra virksomheder og uafhængige klagemekanismer og et meget lavt antal klager tyder på, at enkeltpersoner måske ikke altid er klar over deres rettigheder og/eller mekanismen til at udøve dem. På revisionsmødet udtrykte handelsministeriet interesse i at samarbejde med de europæiske databeskyttelsesmyndigheder om at øge kendskabet til rammen blandt enkeltpersoner i EU. Kommissionen støtter sådanne initiativer og tager også skridt til at informere enkeltpersoner bedre, herunder ved at give yderligere oplysninger om databeskyttelsesrammen på sit websted, f.eks. ved at indarbejde links og henvisninger til relevante vejledningsdokumenter vedtaget af Databeskyttelsesrådet, handelsministeriet og andre amerikanske myndigheder.

Med hensyn til vejledning om principperne i databeskyttelsesrammen blev Databeskyttelsesrådets repræsentanter på revisionsmødet enige om i de kommende måneder at

[22] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-faq-european-individuals_da.
[23] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-faq-european-businesses_da.
[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 f.eks. https://www.dataprivacyframework.gov/US-Businesses.
[28] https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_da.

samarbejde for at give yderligere præciseringer af begrebet data om menneskelige ressourcer i henhold til databeskyttelsesrammen og de specifikke forpligtelser, der gælder for behandlingen af sådanne data. Forskellige elementer, der skal indgå i en sådan vejledning, blev undersøgt. Denne vejledning kan f.eks. omhandle visse praktiske scenarier, hvor medarbejderoplysninger vil blive behandlet i henhold til databeskyttelsesrammen (f.eks. af en cloududbyder), og med hensyn til sådanne scenarier forklare, hvilke forpligtelser i henhold til databeskyttelsesrammen der vil være relevante. Desuden kan den foreslå virksomheder, der modtager medarbejderdata om EU-borgere (men ikke nødvendigvis anvender sådanne data i forbindelse med et ansættelsesforhold), at vælge panelet i databeskyttelsesrammen som deres uafhængige klagemekanisme. Dette vil sikre, at disse borgere kan henvende sig til en myndighed, der er "tæt på hjemmet", og som om nødvendigt er mere bekendt med gældende national lovgivning, der finder anvendelse på data om menneskelige ressourcer.

Desuden vedrører et specifikt aspekt, hvor det ser ud til, at mere vejledning ville være nyttig (også baseret på input fra brancheorganisationer), databeskyttelsesrammens krav til videreoverførsler. Handelsministeriet anførte desuden, at det vil være værd at undersøge, om nogle sektorer kan drage fordel af yderligere vejledning om anvendelsen af principperne i databeskyttelsesrammen på deres aktiviteter, f.eks. inden for sundhedsforskning og finansielle tjenesteydelser.

Kommissionen glæder sig over, at begge parter er rede til at udarbejde retningslinjer, og forventer, at arbejdet med ovennævnte emner snart vil blive indledt.

Mere generelt er der oprettet flere mekanismer for at sikre udveksling og samarbejde mellem de amerikanske myndigheder og databeskyttelsesmyndighederne, herunder gennem udpegelse af særlige kontaktpunkter inden for FTC og handelsministeriet til at behandle forespørgsler og henvisninger fra databeskyttelsesmyndighederne.

2.1.5. Relevante udviklinger i det amerikanske retssystem

Siden afgørelsen om tilstrækkeligheden af beskyttelsesniveauet blev vedtaget, er der sket en række udviklinger i den amerikanske retlige ramme på området privatlivets fred. Dette omfatter udviklinger inden for lovgivning, regulering og retspraksis. De signalerer generelt en øget konvergens mellem EU's og USA's tilgange til visse udfordringer med hensyn til privatlivets fred, herunder gennem anvendelse af lignende juridiske begreber. Visse af disse udviklingstendenser er i gang og vil skulle overvåges yderligere.

På føderalt plan udstedte præsidenten flere præsidentielle dekreter, der er relevante for anvendelsen af personoplysninger. Navnlig forbyder eller begrænser præsidentielt dekret 14117 af 28. februar 2024[29] transaktioner, der involverer visse kategorier af følsomme personoplysninger (f.eks. sundhedsdata, biometriske identifikatorer og humane genomdata), med enheder i visse "lande, der giver anledning til bekymring"[30]. Det vedtagne dekret pålægger justitsministeren at foreslå forordninger – som endnu ikke er udstedt på tidspunktet for vedtagelsen af denne rapport – for yderligere at præcisere dets gennemførelse. Desuden

[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] Disse omfatter, som foreslået af justitsministeren i en forhåndsmeddelelse om foreslået regelfastsættelse, der blev udstedt den 3. maj 2024, Kina, Cuba, Hongkong og Macao, Iran, Nordkorea og 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.

fokuserer præsidentielt dekret 14110 af 30. oktober 2023 om kunstig intelligens[31] på udvikling af sikker, tryg og pålidelig kunstig intelligens. Det kræver, at flere føderale agenturer udvikler AI-relaterede sikkerhedsstandarder og retningslinjer, herunder om specifikke AI-risici for privatlivets fred og om teknikker til beskyttelse af privatlivets fred.

Med hensyn til lovgivningsarbejde har 20 amerikanske stater, samtidig med at Kongressen i de seneste år har vedtaget føderale love om privatlivets fred, vedtaget omfattende love om privatlivets fred pr. juli 2024, hvoraf otte er trådt i kraft: Californien, Colorado, Oregon, Virginia, Connecticut, Utah, Texas og Florida. Desuden har 17 amerikanske stater vedtaget lovgivning om automatisk behandling (eller i det mindste visse former for automatisk behandling) og generelt givet mulighed for fravalg for visse typer beslutningstagning baseret på "profilering"[32].

Med hensyn til udviklingen i retspraksis har flere repræsentanter for civilsamfundet peget på højesterets nylige dom i Loper Bright Enterprises mod Raimondo (af 28.6.2024). Denne dom tilsidesætter tidligere retspraksis vedrørende Chevron-doktrinen, hvorved domstolene anvender princippet om respekt for et reguleringsagenturs rimelige fortolkning af loven i tilfælde af tvetydighed i en lov, der håndhæves af dette agentur. Nogle NGO'er har navnlig udtrykt bekymring over virkningen af denne højesteretsafgørelse på FTC's regeludstedende myndighed på området for privatlivets fred, samtidig med at de anerkender, at der muligvis ikke er nogen eller kun begrænset indvirkning på dens håndhævelsesbeføjelser. På revisionsmødet oplyste FTC, at det stadig er for tidligt at kende de nøjagtige konsekvenser af denne dom. Samtidig forklarede den, at FTC's regelfastsættelse sker i henhold et retsgrundlag i FTC-loven, som er forskelligt fra andre administrative agenturer, og for hvilket Chevron-doktrinen er mindre relevant. Den nylige dom kan derfor have begrænset virkning på dette område.

Desuden orienterede FTC om den seneste udvikling i sin tilgang til automatiseret behandling og kunstig intelligens. Dette omfatter vedtagelse af en fælles erklæring sammen med andre håndhævende myndigheder mod forskelsbehandling og forudindtagethed i automatiserede systemer[33] samt flere håndhævelsesforanstaltninger, hvor FTC bl.a. fokuserer på gennemsigtighed, retfærdighed i den automatiserede behandling og enkeltpersoners mulighed for at anfægte resultater. Det mest bemærkelsesværdige tilfælde i denne henseende er FTC's afgørelse vedrørende Rite Aid i marts 2024, som pålagde denne virksomhed et femårigt forbud

---

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

[32] Selv om der er forskelle i, hvad der menes med "profilering" mellem de forskellige stater, defineres profilering generelt som enhver form for automatisk behandling af personoplysninger med henblik på at evaluere, analysere eller forudsige personlige aspekter vedrørende en identificeret eller identificerbar fysisk persons økonomiske situation, helbred, personlige præferencer, interesser, pålidelighed, adfærd, placering eller bevægelser. Det er typisk forbrugerne, der kan fravælge profilering. Følgende stater har udarbejdet lovgivning 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 (Maryland Online Data Privacy Act of 2024, vedtaget den 9.5.2024), 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 Island Data Transparency and Privacy Protection Act, vedtaget den 29.6.2024), Tennessee (Tenn. Code Ann. § 47-18-3304), Texas (Tex. Bus. & Com. Code Ann. § 541.051) og 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.

mod at anvende ansigtsgenkendelsesteknologi til sikkerhedsformål[34]. FTC fastslog bl.a., at Rite Aid undlod at træffe rimelige foranstaltninger til at forhindre fejlagtige resultater og informere forbrugerne om den anvendte teknologi. Mere generelt behandlede FTC på revisionsmødet sine nuværende prioriteter og navnlig de områder, som den mener fortjener en mere proaktiv håndhævelsesstrategi fremadrettet. Dette omfatter beskyttelse af følsomme oplysninger (f.eks. sundhedsoplysninger, biometriske oplysninger og geolokalisering)[35], beskyttelse af børn[36] og mindreårige online og datasikkerhed.[37]

Kommissionen vil fortsat nøje følge denne og andre udviklinger i USA, navnlig eventuelle yderligere skridt i retning af en omfattende føderal lov om privatlivets fred og den mulige indvirkning af højesterets seneste retspraksis på FTC's rolle på området for privatlivets fred.

Kommissionen glæder sig over FTC's oplysninger om dens seneste håndhævelsesaktiviteter og nuværende prioriteter, som i vid udstrækning svarer til tendenser og prioriteter inden for håndhævelse af databeskyttelse i Europa. FTC deltager også aktivt i det netværk, der samler lande, som er omfattet af en EU-afgørelse om tilstrækkeligheden af beskyttelsesniveauet, og som Kommissionen lancerede i marts 2024[38]. Denne øgede konvergens bør tilskynde til og fremme et tættere samarbejde mellem håndhævere af privatlivets fred på begge sider af Atlanten, navnlig om spørgsmål, der er relevante for, hvordan databeskyttelsesrammen fungerer.

2.2. Aspekter vedrørende amerikanske offentlige myndigheders adgang til og brug af personoplysninger, der overføres under EU-USA-databeskyttelsesrammen

Afgørelsen om tilstrækkeligheden af beskyttelsesniveauet indeholder en detaljeret vurdering af de regler, der gælder for amerikanske offentlige myndigheders indsamling og anvendelse af personoplysninger, der overføres fra EU til virksomheder, der er certificeret i henhold til databeskyttelsesrammen, navnlig med henblik på strafferetlig håndhævelse og national sikkerhed. Siden vedtagelsen af afgørelsen om tilstrækkeligheden af beskyttelsesniveauet har der, som bekræftet af de amerikanske myndigheder på revisionsmødet, ikke været nogen relevant udvikling med hensyn til den retlige ramme, der gælder for adgang til data med henblik på retshåndhævelse eller regulering i databeskyttelsesrammens første år. Nedenstående resultater vedrører derfor kun udviklingen på området national sikkerhed.

Konklusionerne i afgørelsen om tilstrækkeligheden af beskyttelsesniveauet vedrørende efterretningstjenesters adgang til data bygger på en analyse af de betingelser og begrænsninger, der gælder for signalefterretningsoperationer i henhold til flere relevante retsgrundlag – navnlig

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

[35] Se f.eks. FTC's nylige afgørelse vedrørende X-Mode om salg og deling af følsomme lokaliseringsoplysninger (https://www.ftc.gov/system/files/ftc_gov/pdf/X-ModeSocialDecisionandOrder.pdf) og vedrørende Monument om videregivelse af følsomme sundhedsdata til tredjeparter til markedsføringsformål (https://www.ftc.gov/system/files/ftc_gov/pdf/MonumentOrderFiled.pdf).

[36] FTC har f.eks. for nylig bebudet en undersøgelse, der fører til en retssag mod TikTok og dets moderselskab, Bytedance, for angiveligt at krænke børns ret til privatlivets fred. Det hævdes, at begge virksomheder ikke opfyldte kravet om at underrette og indhente forældresamtykke, inden de indsamlede og anvendte personoplysninger fra børn 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 oversigten over de seneste håndhævelsesaktiviteter i FTC 2023 Privacy and Data Security Update: https://ec.europa.eu/commission/presscorner/detail/da/mex_24_1307.

[38] Se https://ec.europa.eu/commission/presscorner/detail/da/mex_24_1307. Som følge af mødet i marts 2024 blev det besluttet at afholde en række tematiske møder. Det første fandt sted i juli 2024 og fokuserede på at udvikle værktøjer, der kan hjælpe små og mellemstore virksomheder med at overholde lovgivningen om privatlivets fred.

Section 702 i Foreign Intelligence Surveillance Act (lov om overvågning af efterretningsvirksomhed i udlandet, FISA) og præsidentielt dekret 12333 [39] som suppleret og styrket ved præsidentielt dekret 14086 om fremme af garantier i de amerikanske signalefterretningsaktiviteter (Executive Order 14086 "Enhancing Safeguards for United States Signals Intelligence" (EO 14086)), der blev vedtaget af den amerikanske præsident den 7. oktober 2022. De garantier, der er fastsat i EO 14086, finder anvendelse på alle amerikanske signalefterretningsaktiviteter, uanset hvilket retsgrundlag sådanne aktiviteter er baseret på, og hvor de finder sted, og beskytter oplysninger om ikkeamerikanske personer (herunder europæere)[40]. EO 14086 indførte også en ny klagemekanisme, hvorigennem disse bindende garantier kan påberåbes og håndhæves af enkeltpersoner i EU.

I de næste afsnit beskrives de skridt, som de amerikanske myndigheder har taget siden vedtagelsen af afgørelsen om tilstrækkeligheden af beskyttelsesniveauet for at efterkomme EO 14086, samt den relevante udvikling i forbindelse med ovennævnte retlige ramme.

2.2.1. Relevante udviklinger med hensyn til den amerikanske retlige ramme

2.2.1.1. Efterretningstjenesternes gennemførelse af præsidentielt dekret 14086

De begrænsninger og garantier, der blev indført ved præsidentielt dekret 14086 (EO 14086), supplerer de begrænsninger og garantier, der er fastsat i Section 702 i FISA og EO 12333. De er bindende for alle efterretningstjenester og er blevet yderligere operationaliseret gennem politikker og procedurer, der er vedtaget af de enkelte agenturer.

Som led i den første revision bekræftede de amerikanske myndigheder, at der ikke er foretaget ændringer af EO 14086 siden vedtagelsen. Det blev desuden præciseret, at den amerikanske præsident ikke har gjort brug af den beføjelse, der er omhandlet i Section 2(b)(i)(B) og 2(b)(ii)(C) i EO 14086, til at ajourføre listen over legitime mål, for hvilke der kan foretages signalefterretninger, eller listen over formål, hvortil massedata kan anvendes[41]. For at fastlægge mere specifikke efterretningsprioriteter, for hvilke der rent faktisk kan indsamles signalefterretninger, indførte EO 14086 en specifik procedure. Navnlig skal den ansvarlige for beskyttelse af borgerlige rettigheder under ODNI (ODNI CLPO) høres for med hensyn til hver prioritet at vurdere, om den 1) fremmer et eller flere af de legitime mål i det præsidentielle dekret, 2) hverken er udformet til eller forventes at resultere i indsamling af signalefterretninger med henblik på et af de forbudte formål i det præsidentielle dekret, og 3) er fastlagt, efter at der er taget behørigt hensyn til privatlivets fred og de borgerlige frihedsrettigheder for alle personer[42]. ODNI CLPO bekræftede på revisionsmødet, at hun gennemgik de prioriteter, som direktøren for den nationale efterretningstjeneste havde foreslået i rammen for de nationale efterretningsprioriteter for 2023, konkluderede, at de opfyldte ovennævnte krav, og delte sin

[39] Andre foranstaltninger, der kan træffes i henhold til FISA med hensyn til oplysninger, der overføres fra EU, er individualiseret elektronisk overvågning (Section 105 i FISA), fysiske søgninger (Section 302 i FISA), brug af pen-registre- eller trap and trace-anordninger (Section 402 i FISA) og indsamling af forretningspapirer fra visse virksomheder (fælles transportvirksomheder, offentlige indkvarteringsfaciliteter, biludlejningsfaciliteter eller opbevaringsfaciliteter, Section 501 i FISA). Disse forskellige retsgrundlag analyseres nærmere i afgørelsen om tilstrækkeligheden af beskyttelsesniveauet (betragtning 142-152).

[40] Se afsnit 3.2.1.2 i afgørelsen om tilstrækkeligheden af beskyttelsesniveauet for yderligere oplysninger.

[41] Disse legitime mål/formål omfatter f.eks. beskyttelse mod spionage, sabotage, mord eller andre efterretningsaktiviteter, der udføres af, på vegne af eller med bistand fra en udenlandsk regering, organisation eller person, beskyttelse mod terrorisme, gidseltagning og tilbageholdelse af personer, der udføres af eller på vegne af en udenlandsk regering, organisation eller person.

[42] Section 2(b)(iii) i EO 14086.

konklusion med direktøren for den nationale efterretningstjeneste, som derefter forelagde prioriteterne for præsidenten til validering. ODNI CLPO sørgede også for uddannelse i kravene i EO 14086 for de dele af efterretningstjenesterne, der er involveret i udviklingen af efterretningsprioriteter.

Desuden har de amerikanske myndigheder i det forløbne år taget yderligere praktiske skridt til at gennemføre EO 14086 i deres daglige virke. Efterretningstjenesterne har navnlig indført yderligere interne politikker og retningslinjer for anvendelsen af dekretet, f.eks. interne processer (gennem interne godkendelseskrav, dokumenteret adgangskontrol, så kun de personer, der er behørigt uddannet og opfylder kravene i forbindelse med opgaven, har adgang til oplysningerne osv.) for at sikre, at kravene om nødvendighed og proportionalitet overholdes i forbindelse med både målrettet indsamling og masseindsamling[43]. Desuden er personale fra forskellige efterretningstjenester (f.eks. NSA, CIA og FBI) blevet uddannet i EO 14086, herunder årlige kurser og ad hoc-kurser tilrettelagt af ODNI CLPO og obligatoriske kurser for alt nyt personale, som ODNI ansætter.

Kommissionen glæder sig over de forskellige foranstaltninger, der er truffet for at gennemføre og sikre overholdelse af EO 14086. Efterhånden som der indhøstes flere erfaringer med den praktiske anvendelse af det præsidentielle dekrets garantier, vil Kommissionen sætte pris på muligheden for i forbindelse med fremtidige revisioner at drøfte konkrete eksempler på, hvordan dekretet anvendes i praksis (under hensyntagen til gældende fortrolighedshensyn).

2.2.1.2. Fornyet godkendelse af Section 702 i FISA

I henhold til Section 702 i FISA kan der foretages målrettet overvågning af ikkeamerikanske personer, der med rimelighed kan formodes at befinde sig uden for USA med henblik på at indhente efterretningsoplysninger. Indhentningen sker på grundlag af årlige certificeringer, der indsendes til og godkendes af Foreign Intelligence Surveillance Court (amerikansk domstol for overvågning af efterretningsvirksomhed i udlandet, FISC). Disse certificeringer identificerer specifikke kategorier af udenlandske efterretningsoplysninger, der skal indsamles. Den 21. juli 2023 meddelte ODNI, at der er tre godkendte certificeringer i henhold til Section 702 i FISA, der dækker følgende kategorier af udenlandske efterretninger: 1) udenlandske regeringer og tilknyttede enheder, 2) terrorbekæmpelse og 3) bekæmpelse af spredning[44]. Certificeringerne skal også omfatte målretnings- og minimeringsprocedurer, der er godkendt af FISC[45]. Målretning foretages navnlig ved at anmode amerikanske virksomheder, der opfylder FISA's definition af "udbyder af elektroniske kommunikationstjenester", om at offentliggøre elektroniske kommunikationsdata for kommunikation, der sendes til eller fra "selektorer", som identificerer en specifik kommunikationskonto, f.eks. et telefonnummer eller en e-mailadresse. Den amerikanske regering har offentliggjort en række materialer om Section 702 i FISA for at informere offentligheden om overvågningsprogrammers funktion, gældende krav og beskyttelsen af privatlivets fred samt FISC's rolle[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 3.7.2023.

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

[45] Sådanne procedurer begrænser indsamlingen af data med hensyn til et specifikt udenlandsk efterretningsformål, begrænser adgangen til databaser, hvor oplysninger, der er indhentet i henhold til Section 702 i FISA, lagres (herunder gennem adgangskontrol), og indfører begrænsninger for anvendelsen, opbevaringen og videregivelsen af sådanne oplysninger.

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

På grund af en udløbsklausul skulle Section 702 i FISA udløbe ved udgangen af 2023, medmindre den blev godkendt på ny af Kongressen. Efter en midlertidig fornyet godkendelse uden ændringer vedtog Kongressen den 19. april 2024 Reforming Intelligence and Securing America Act (lov om reform af efterretningsvirksomhed og sikring af Amerika, RISAA), hvorved Section 702 i FISA blev godkendt på ny for en periode på to år, og der blev indført flere ændringer. Disse kan i store træk opdeles i to kategorier: 1) ændringer i omfanget af overvågningsaktiviteter, der er tilladt i henhold til Section 702 i FISA, og 2) institutionelle og proceduremæssige ændringer.

Ændringer i omfanget af overvågningsaktiviteter, der er tilladt i henhold til Section 702 i FISA

RISAA har indført tre vigtige ændringer af omfanget af de overvågningsaktiviteter, der kan udføres i henhold til Section 702 i FISA.

For det første er indsamling af "abouts" definitivt blevet forbudt[47]. Dette henviser til indsamling af kommunikation, hvor Section 702-selektoren (f.eks. en e-mailadresse) ikke findes i "til" eller "fra" i kommunikationen, men der i stedet er en henvisning til en sådan selektor i kommunikationen (f.eks. e-mailkommunikation, der ikke sendes til eller fra den valgte e-mailadresse, men omfatter den valgte e-mailadresse i e-mailteksten eller brødteksten). Selv om en sådan indsamling allerede var udelukket efter en ændring af FISA i 2018, gav FISA stadig mulighed for at genoptage "abouts"-indsamlingen i fremtiden efter en særlig godkendelsesprocedure, der involverede FISC og Kongressen. Den seneste ændring, som RISAA har indført, har fjernet denne mulighed.

For det andet er definitionen af udenlandske efterretningsoplysninger blevet udvidet til at omfatte oplysninger vedrørende narkotikabekæmpelse[48]. På revisionsmødet forklarede de amerikanske myndigheder, at dette blev indført i lyset af den nuværende fentanylkrise og den stigende nationale sikkerhedstrussel fra internationale narkotikahandlere og -producenter. På denne baggrund blev det bekræftet, at dette begreb falder ind under flere af de legitime mål, der er anført i EO 14086, dvs. forståelse eller vurdering af de kapaciteter, hensigter eller aktiviteter, som udenlandske organisationer har eller udfører, og som udgør en aktuel eller potentiel trussel mod USA's eller dets allieredes nationale sikkerhed, forståelse eller vurdering af tværnationale trusler, der påvirker den globale sikkerhed, herunder risici for folkesundheden, og beskyttelse mod grænseoverskridende kriminelle trusler[49].

For det tredje udvidede RISAA definitionen af "udbyder af elektroniske kommunikationstjenester", hvorved anvendelsesområdet for virksomheder, der kan være tvunget til at fremlægge oplysninger i henhold til Section 702 i FISA, udvides[50]. Definitionen omfatter nu andre tjenesteydere, der har "adgang til udstyr, der anvendes eller kan anvendes til at overføre eller lagre trådbaseret eller elektronisk kommunikation", men udelukker udtrykkeligt offentlige indkvarteringsfaciliteter, boliger, fællesfaciliteter og restaurationsvirksomheder. I et brev til Kongressen henviste justitsministeriet til denne ændring som en teknisk ændring, der skulle dække et "ekstremt lille" antal teknologivirksomheder, som ifølge nylige afgørelser fra FISC og Foreign Intelligence Surveillance Court of Review (appeldomstolen for overvågning af efterretningsvirksomhed i udlandet, FISCR) ikke var

[47] Section 22 i RISAA.
[48] Section 23 i RISAA.
[49] Section 2(b)(ii)(A),(2), (3) og (10) i EO 14086.
[50] Section 25 i RISAA.

omfattet af den tidligere definition af udbyder af elektroniske kommunikationstjenester[51]. I samme brev forpligtede justitsministeriet sig til at indsnævre anvendelsesområdet ved udelukkende at anvende denne definition på den type tjenesteyder, der var omhandlet i den tvist, der førte til FISC-afgørelsen. Som følge heraf er de pågældende virksomheder nævnt i et klassificeret bilag til Kongressen. Flere NGO'er, herunder dem, der gav feedback som led i revisionen, udtrykte bekymring over denne udvidelse og hævdede, at den potentielt kunne dække mange amerikanske virksomheder (da mange af dem leverer en eller anden form for tjeneste og har adgang til kommunikationsudstyr). I lyset af disse betænkeligheder er der med støtte fra efterretningstjenesterne blevet foreslået en yderligere ændring i et udkast til en lov om tilladelse til efterretningsvirksomhed for regnskabsåret 2025, som i øjeblikket behandles i Kongressen. Denne ændring vil, hvis den vedtages af Kongressen, sikre, at de yderligere virksomheder, der er omfattet af definitionen af udbyder af elektroniske kommunikationstjenester, kun vil være begrænset til dem, der er nævnt i ovennævnte FISC-afgørelser. Lovforslaget indeholder også bestemmelser om, at alle direktiver, der er rettet til et sådant selskab, skal indberettes til FISC, så sidstnævnte kan undersøge, om selskabet rent faktisk er omfattet af anvendelsesområdet. I sit brev til Kongressen forpligtede justitsministeriet sig til at aflægge rapport til Kongressen hver sjette måned om enhver anvendelse af den ajourførte definition for at give Kongressen mulighed for at føre passende tilsyn med den snævre anvendelse af definitionen.

Det er vigtigt at bemærke, at det på revisionsmødet blev bekræftet af de amerikanske myndigheder og PCLOB, at alle garantier i EO 14086 fortsat finder fuld anvendelse på al dataindsamling og -anvendelse i henhold til Section 702 i FISA, herunder efter disse ændringer. Selv om RISAA i nogen grad udvider anvendelsesområdet for virksomheder, der kan få et pålæg, begrænser den således ikke udøvelsen af rettigheder. Ikke desto mindre vil det være vigtigt at overvåge den videre udvikling (lovgivning og rapportering) og modtage oplysninger om anvendelsen af disse nye regler i praksis. Dette omfatter f.eks. virkningen af udvidelsen af definitionerne af udenlandske efterretninger og udbyder af elektroniske kommunikationstjenester på antallet af mål under Section 702 i FISA (som meddelt årligt af ODNI, se nedenfor om gennemsigtighed). Den fremtidige opfølgningsrapport til PCLOB's nylige rapport om Section 702 i FISA (se nedenfor) bør være særlig informativ i denne henseende.

Institutionelle og proceduremæssige ændringer

Med hensyn til institutionelle og proceduremæssige ændringer kodificerede RISAA flere procedurer, der allerede blev fulgt i praksis, og indførte nye garantier. Mens nogle af disse kun vedrører amerikanske personer, øger flere ændringer beskyttelsen af både amerikanske og ikkeamerikanske personer, hvis oplysninger kan indsamles i henhold til Section 702 i FISA[52], og er derfor relevante for databeskyttelsesrammens funktion.

[51] https://www.justice.gov/opa/media/1348621/dl?inline. Se FISC's afgørelse fra 2022 (https://www.intel.gov/assets/documents/702%20Documents/declassified/2022-FISC-ECSP-OPINION.pdf) og afgørelsen fra appeldomstolen for overvågning af efterretningsvirksomhed i udlandet, som stadfæstede denne afgørelse (https://www.intel.gov/assets/documents/702%20Documents/declassified/2023_FISC-R_ECSP_Opinion.pdf).

[52] Desuden indførte RISAA visse ændringer med hensyn til traditionel individualiseret elektronisk overvågning i henhold til Section 105 i FISA (på grundlag af en FISC-kendelse, der udstedes, hvis der er begrundet mistanke ("probable cause")). En anmodning fra en efterretningstjeneste til justitsministeren om en kendelse om at foretage

For det første blev der indført en række yderligere krav til ansvarlighed, tilsyn og rapportering. Navnlig skal FBI-personale nu årligt uddannes i de regler, der gælder for søgninger i oplysninger, der er indhentet i henhold til Section 702 i FISA[53]. FBI skal også rapportere til Kongressen om sine søgningsaktiviteter (f.eks. antallet af søgninger ved hjælp af "batchjobteknologier", dvs. hvor der foretages søgninger af flere udtryk som led i en enkelt søgning) og om de ansvarlighedsforanstaltninger, der er indført for at sikre overholdelse af de retlige krav til søgninger (Section 11 og 12 i RISAA). Desuden pålægges justitsministeriets generalinspektør at udarbejde en rapport om FBI's overholdelse af søgningskravene (Section 9 i RISAA). Mere generelt skal ODNI og justitsministeren for at øge gennemsigtigheden i procedurerne indbragt for FISC nu afslutte afklassificeringsgennemgangen af FISC's afgørelser inden for 180 dage (Section 7 i RISAA). Desuden skal udskrifter af alle retsmøder ved FISC og FISCR (hvortil FISC's afgørelser kan appelleres) opbevares og fremsendes til Kongressen (Section 8 i RISAA).

For det andet indførte RISAA yderligere begrænsninger for FBI's anvendelse af data indsamlet i henhold til Section 702 i FISA. Section 2(d) i RISAA fastsætter, at en søgning ved hjælp af "batchteknologi" kun kan foretages efter godkendelse fra en advokat i FBI, medmindre der foreligger hastende omstændigheder. Desuden er det nu forbudt for FBI automatisk at kontrollere ikkeminimerede oplysninger, der er indhentet i henhold til Section 702 i FISA, og FBI skal i stedet sikre, at analytikere bevidst vælger at søge i sådanne oplysninger. RISAA har også forbudt FBI at foretage søgninger, der udelukkende har til formål at finde og udtrække beviser for kriminel aktivitet (medmindre der er rimelig grund til at antage, at de kan bidrage til at afbøde eller fjerne en trussel mod liv eller alvorlig legemsbeskadigelse, eller hvor det er nødvendigt for at overholde oplysningsforpligtelserne i retssager)[54]. Desuden er det forbudt for FBI at indlæse ikkeminimerede data i analytiske datalagre, medmindre den pågældende person er relevant for en eksisterende national sikkerhedsundersøgelse[55].

For det tredje er visse bestemmelser vedrørende status og rollen som amicus curiae ved FISC blevet ændret[56]. Amicus curiae udpeges som eksperter til at bistå domstolen (og FISCR) i spørgsmål vedrørende privatlivets fred og borgerlige rettigheder eller til at bidrage med at afklare teknologiske spørgsmål i forbindelse med behandlingen af en specifik regerings anmodning. Mens FISA tidligere krævede, at amicus curiae havde ekspertise inden for privatlivets fred og borgerlige frihedsrettigheder, indsamling af efterretninger, kommunikationsteknologi eller andre relevante områder, kræver den i princippet nu ekspertise inden for privatlivets fred/borgerlige frihedsrettigheder og indsamling af efterretninger. Domstolen havde allerede mulighed for at udpege en amicus curiae i alle tilfælde, hvor den fandt det hensigtsmæssigt, og var forpligtet til at gøre det i forbindelse med en ny eller væsentlig fortolkning af loven. Efter den fornyede godkendelse skal FISC nu også udpege en amicus curiae hver gang den anmodes om at godkende en Section 702 FISA-certificering og

individuel elektronisk overvågning kræver nu en erklæring på tro og love, der begrunder overbevisningen om, at betingelserne i Section 105 i FISA er opfyldt (Section 6(a) i RISAA). Den mulige varighed af elektronisk overvågning med hensyn til fremmede magter eller agenter for fremmede magter er blevet forlænget fra 120 dage til et år (Section 6(g), i RISAA).

[53] Section 2(d) i RISAA.

[54] Section 3(a) i RISAA.

[55] Section 3(b) i RISAA. Hvor det er nødvendigt på grund af presserende omstændigheder, kan FBI's direktør træffe afgørelse om en undtagelse fra denne bestemmelse, som skal meddeles Kongressen.

[56] Af klarhedshensyn berører disse ændringer ikke de særlige advokaters status og rolle ved DPRC, som bekræftet af USA på revisionsmødet.

ledsagende procedurer (f.eks. målretningsprocedurer), medmindre den finder, at dette ikke vil være hensigtsmæssigt eller sandsynligvis vil medføre unødig forsinkelse[57]. I stedet for kun at udnævne en enkelt, kan domstolen nu beslutte at udnævne en eller flere amicus curiae. Det præciseres også, at de oplysninger, der skal gives af amici curiae skal være "begrænset til at behandle de specifikke spørgsmål, som domstolen har identificeret", selv om de områder, hvor amici curiae kan afgive bemærkninger, fortsat er brede (dvs. juridiske argumenter og oplysninger vedrørende beskyttelse af amerikanske personers ret til privatlivets fred og borgerlige frihedsrettigheder, indsamling af efterretninger og kommunikationsteknologi eller ethvert andet relevant område).

Endelig oprettes der ved Section 18 i RISAA en "FISA-reformkommission" – bestående af bl.a. medlemmer af Kongressen, formanden for PCLOB, ledende vicedirektør for den nationale efterretningstjeneste og vicejustitsministeren samt yderligere medlemmer, der skal udnævnes af Kongressen[58] – til at anbefale yderligere FISA-reformer.

Kommissionen vil nøje overvåge den videre udvikling med hensyn til Section 702 i FISA, herunder i forbindelse med PCLOB's tilsynsaktiviteter (se nedenfor), reformkommissionens arbejde og den kommende revision af FISA efter to år.

2.2.1.3. Overvågningsaktiviteter i praksis: tal og tendenser

ODNI's årlige rapport om statistisk gennemsigtighed vedrørende efterretningstjenesternes brug af nationale sikkerhedsovervågningsmyndigheder for kalenderåret 2023 (offentliggjort i april 2024)[59] viser, at antallet af mål i henhold til Section 702 i FISA steg fra 245 073 i kalenderåret 2022 til 268 590 i kalenderåret 2023. I rapporten forklares det, at udsving i antallet af mål kan være knyttet til en række forskellige årsager, herunder ændringer i operationelle prioriteter, verdensbegivenheder, tekniske kapaciteter, måladfærd og ændringer i telekommunikationssektoren. Rapporten viser også, at ingen ikkeamerikanske personer (sammenlignet med 1 i 2021 og 0 i 2022) var mål i henhold til Section 402 i FISA (pen-register og trap and trace), mens der blev udstedt seks kendelser (sammenlignet med 11 kendelser i både 2021 og 2022) vedrørende seks mål (sammenlignet med 13 i 2021 og 11 i 2022) i henhold til Section 501 i FISA (adgang til forretningsoplysninger om fælles transportvirksomheder, køretøjsudlejningsfaciliteter eller fysiske opbevaringsfaciliteter), der omfattede 5 412 entydige identifikatorer (sammenlignet med 23 157 i 2021 og 55 431 i 2022), som blev anvendt til at meddele oplysninger indsamlet i henhold til sådanne kendelser.

Justitsministeriets årlige rapport til Kongressen om lov om overvågning af efterretningsvirksomhed i udlandet viser, at der i kalenderåret 2023 blev indgivet 327 anmodninger til FISC om at foretage elektronisk overvågning og/eller fysisk søgning til udenlandske efterretningsformål i henhold til henholdsvis Section 105 og 302 i FISA[60]. Det samlede antal omfattede personer var mellem 500 og 999. Med hensyn til nationale sikkerhedsbreve (National Security Letters, NSL'er) fremgår det af rapporten, at der blev fremsat 10 115 anmodninger (eksklusive anmodninger om abonnentoplysninger) om

[57] Section 5(b) i RISAA.
[58] Section 18 kræver specifikt repræsentation uden for kongressen.
[59] https://www.dni.gov/files/CLPT/documents/2024_ASTR_for_CY2023.pdf.
[60] https://www.justice.gov/nsd/media/1350236/dl?inline.

oplysninger om ikkeamerikanske personer, hvorved der søgtes oplysninger om 3 033 forskellige ikkeamerikanske personer[61].

Flere virksomheder certificeret i henhold til databeskyttelsesrammen (f.eks. Google og Meta) gør brug af muligheden i henhold til amerikansk lovgivning for at offentliggøre gennemsigtighedsrapporter, der informerer om antallet af FISA- og NSL-anmodninger, de har modtaget i en given rapporteringsperiode. På tidspunktet for udarbejdelsen af denne rapport forelå der endnu ikke statistikker over FISA-anmodninger efter juli 2023. Google rapporterede f.eks. at have modtaget 500-999 NSL-anmodninger, der påvirkede 2000-2499 konti, mellem juli og december 2023[62]. Meta rapporterede, at den modtog 0-499 NSL-anmodninger, der påvirkede 500-999 konti, i samme rapporteringsperiode[63]. Tallene har været ret stabile i de seneste år. For yderligere at øge gennemsigtigheden offentliggør nogle virksomheder (f.eks. Google) proaktivt NSL'er, som de har modtaget, når fortrolighedsbegrænsningerne ophæves[64].

2.2.1.4. Andre udviklinger

I forbindelse med forberedelsen af revisionen har flere NGO'er rejst spørgsmål om nye former for dataindsamling, som amerikanske efterretningstjenesters foretager gennem køb af data fra kommercielle enheder, navnlig datamæglere. De forklarede, at selv om data, der indsamles på dette grundlag, stadig skal behandles i overensstemmelse med andre krav, herunder f.eks. i henhold til EO 12333[65], finder en sådan erhvervelse sted uden for rammerne af FISA og EO 14086.

I den forbindelse bør det erindres, at enhver form for frivillig udveksling af data med tredjeparter er underlagt flere detaljerede betingelser i databeskyttelsesrammen. For det første kan en certificeret organisation ikke dele data med en tredjepart (der ikke fungerer som mandatar/databehandler) uden at underrette de berørte personer og give dem mulighed for at træffe et valg[66]. I overensstemmelse med *princippet om ansvar for videreoverførsel* må videreoverførsel for det andet kun foretages 1) til begrænsede og specifikke formål, 2) på grundlag af en aftale mellem organisationen under EU-USA-databeskyttelsesrammen og den pågældende tredjepart og 3) udelukkende, hvis denne aftale sikrer, at tredjeparten sikrer det samme beskyttelsesniveau som principperne[67].

Som det også blev drøftet på revisionsmødet, har FTC desuden truffet håndhævelsesforanstaltninger over for datamæglere, der sælger følsomme forbrugeroplysninger. I en sag mod X-Mode og dens efterfølger Outlogic vedtog FTC den 9. januar 2024 f.eks. et påbud, der forbyder virksomheden at sælge geolokaliseringsdata til tredjeparter og at slette data, som den havde anvendt og delt ulovligt. FTC's undersøgelse viste

[61] Disse tal har stort set været stabile i forhold til det foregående rapporteringsår (2022). Til sammenligning blev der i 2022 indgivet 317 endelige anmodninger til FISC om at foretage elektronisk overvågning og/eller fysiske søgninger til udenlandske efterretningsformål. Det samlede antal personer, der var genstand for kendelser om elektronisk overvågning, var mellem 0 og 499. FBI fremsatte 9 103 NSL-anmodninger om oplysninger om ikkeamerikanske personer i 2022 (eksklusive anmodninger om abonnentoplysninger). Kilde: https://irp.fas.org/agency/doj/fisa/2022rept.pdf.

[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 f.eks. Section 2.4 i EO 12333 om indsamlingsteknikker.

[66] Se betragtning 40 til afgørelsen om tilstrækkeligheden af beskyttelsesniveauet.

[67] Se betragtning 38 til afgørelsen om tilstrækkeligheden af beskyttelsesniveauet.

bl.a., at virksomheden ikke fuldt ud informerede enkeltpersoner om brugen og salget af deres geolokaliseringsdata, ikke indførte foranstaltninger, der gjorde det muligt for enkeltpersoner at fravælge sporing, tillod brugen af dataene til potentielt diskriminerende formål og undlod at sætte grænser for tredjeparters brug af sådanne oplysninger[68]. Kommissionen forventer, at FTC vil følge samme tilgang, hvis virksomheder certificeret i henhold til databeskyttelsesrammen deler data i strid med ovennævnte bestemmelser.

Endelig er det værd at nævne, at ODNI i maj 2024 udsendte efterretningstjenesternes politiske ramme for kommercielt tilgængelige oplysninger[69]. Denne ramme fastsætter en række principper og krav, som efterretningstjenesterne skal følge, herunder for at minimere risiciene for privatlivets fred og borgerlige frihedsrettigheder, når de indhenter og anvender oplysninger i forbindelse med en handelstransaktion.

2.2.2. Uafhængigt tilsyn

De amerikanske efterretningstjenesters aktiviteter er underlagt tilsyn af forskellige organer, herunder Privacy and Civil Liberties Officers (databeskyttelsesansvarlige), generalinspektører, kongressen og PCLOB. Navnlig kræver EO 14086, at de enkelte efterretningstjenester har ledende juridiske samt tilsyns- og kontrolansvarlige embedsmænd, som sikrer, at gældende amerikansk lovgivning overholdes. Denne tilsynsfunktion varetages af embedsmænd, der er udpeget til at varetage en kontrolfunktion, samt af databeskyttelsesansvarlige og generalinspektører[70]. De skal føre regelmæssigt tilsyn med signalefterretningsaktiviteter og sikre, at enhver manglende overholdelse afhjælpes. Efterretningstjenesterne skal give sådanne embedsmænd adgang til alle relevante oplysninger, så de kan udføre deres tilsynsfunktioner, og må ikke træffe foranstaltninger for at hindre eller påvirke deres tilsynsaktiviteter uretmæssigt.

Chefjuristen i efterretningstjenesternes generalinspektorat (ICIG) i ODNI – som har brede beføjelser til at føre tilsyn med hele den amerikanske efterretningstjeneste og til at undersøge klager eller oplysninger om påstande om ulovlig praksis eller magtmisbrug – deltog i revisionsmødet. Han bekræftede, at ICIG systematisk kontrollerer overholdelsen af EO 14086 som led i sine tilsynsaktiviteter. Han henviste også til de seneste tilsynsaktiviteter, som andre generalinspektører i efterretningstjenesterne har udført, og som er beskrevet i regelmæssige rapporter. F.eks. underrettede NSA's generalinspektør i sin halvårlige rapport til Kongressen for april-september 2023[71] om en evaluering af en intern NSA-kontrolramme for målretning af

[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. Efterretningstjenesterne har siden august 2024 været forpligtet til at overholde rammen.

[70] Hver efterretningstjeneste har en generalinspektør, som er lovmæssigt uafhængig og ansvarlig for at foretage revisioner og undersøgelser vedrørende de aktiviteter, der udføres af den pågældende tjeneste af hensyn til den nationale sikkerhed. De har adgang til alt relevant (herunder klassificeret) materiale, om nødvendigt på grundlag af et pålæg, og kan indhente vidneudsagn. Generalinspektørerne henviser sager om formodede strafferetlige overtrædelser til retsforfølgning og fremsætter anbefalinger om korrigerende foranstaltninger for tjenesternes ledere. Selv om deres anbefalinger ikke er bindende, offentliggøres deres rapporter, herunder om opfølgende foranstaltninger (eller manglen herpå), generelt, og de sendes til Kongressen. Jf. i denne forbindelse fodnote 136 i afgørelsen om tilstrækkeligheden af beskyttelsesniveauet vedrørende generalinspektørens rolle.

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

afgørelser og anmodninger. Det konkluderedes i rapporten, at denne ramme fungerede korrekt med hensyn til at sikre overholdelse af de love, direktiver og politikker, der beskytter borgerlige frihedsrettigheder og privatlivets fred. I samme rapport nævnes også en undersøgelse, der afslørede en NSA-medarbejders misbrug af et signalefterretningsværktøj til uautoriserede formål.

I henhold til EO 14086 er PCLOB[72] betroet specifikke tilsynsfunktioner[73]. Formanden for PCLOB og dets tre medlemmer deltog i revisionsmødet og oplyste, at PCLOB ydede rådgivning til efterretningstjenester om deres udkast til politikker og procedurer til gennemførelse af EO 14086 i april 2023 og blev hørt om udnævnelsen af dommere og særlige advokater ved Data Protection Review Court (databeskyttelsesappelretten, DPRC). Rådet iværksatte også et tilsynsprojekt med henblik på 1) at gennemgå gennemførelsen af de ajourførte politikker og procedurer, som efterretningstjenesterne har vedtaget for at sikre, at de er i overensstemmelse med dekretet, og 2) at foretage en årlig gennemgang af, hvordan den nye klagemekanisme fungerer (se nedenfor)[74]. PCLOB's medlemmer bekræftede, at bestyrelsen planlægger at foretage begge revisioner i den nærmeste fremtid. Med hensyn til klageadgangen forklarede de, at i mangel af klager vil PCLOB's revision fokusere på de politikker og procedurer, der er indført for at oprette mekanismen.

Med hensyn til andre tilsynsaktiviteter udsendte PCLOB den 28. september 2023 en rapport om Section 702 i FISA[75]. Denne rapport er en opfølgning på en tidligere rapport fra 2014 og indeholder ajourførte faktuelle og juridiske oplysninger om anvendelsen af overvågningsprogrammer i henhold til Section 702 i FISA. Rapporten indeholder også anbefalinger om efterretningstjenesters overholdelse af gældende krav og forslag til Kongressen om yderligere at styrke flere aspekter af Section 702 i FISA i forbindelse med dens fornyede godkendelse (herunder ved at kodificere de legitime mål for de overvågningsaktiviteter, der er anført i EO 14086).[76] På revisionsmødet oplyste PCLOB, at det forventer snart at modtage svar fra efterretningstjenesterne om gennemførelsen af dets anbefalinger, som vil indgå i en fremtidig opfølgningsrapport. Andre igangværende tilsynsprojekter omfatter et om bekæmpelse af indenlandsk terrorisme og dens indvirkning på privatlivets fred og borgerlige frihedsrettigheder og FBI's indsamling af open source-data eller kommercielt tilgængelige data[77].

Endelig gav NGO'er, der blev hørt i forbindelse med revisionen, udtryk for bekymring over, at mandatperioden for flere PCLOB-medlemmer forventes at udløbe i den nærmeste fremtid,

---

[72] PCLOB er et uafhængigt agentur med ansvar for terrorbekæmpelsespolitikker og gennemførelsen heraf med henblik på at beskytte privatlivets fred og borgerlige frihedsrettigheder. Det kan få adgang til alle relevante (herunder klassificerede) oplysninger, gennemføre interviews og indhente vidneudsagn. Det kan udstede anbefalinger til de retshåndhævende myndigheder og efterretningsmyndighederne og aflægger regelmæssigt rapport til Kongressen og præsidenten. Dets rapporter gøres i videst muligt omfang offentligt tilgængelige.

[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 bemærker, at nogle af disse anbefalinger er blevet indarbejdet som en del af RISAA, herunder anbefalingen om "abouts"-indsamlinger eller anbefalingen om styrkelse af FISC-eksperternes rolle (amici).

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

hvilket potentielt vil betyde, at PCLOB ikke er beslutningsdygtigt. Navnlig er formandens mandatperiode udløbet, og den periode, hvor hun kan sidde i venteposition, udløber i januar 2025, mens et andet mandat er ledigt, og et tredje mandat også vil blive ledigt i januar næste år. Under revisionsmødet forklarede medlemmerne, at de ikke forventer, at PCLOB ender uden et beslutningsdygtigt antal medlemmer, da der allerede er foretaget en indstilling til det mandat, der i øjeblikket er ledigt (hvilket afventer Senatets bekræftelse)[78]. De understregede også, at selv om rådet måtte miste sin beslutningsdygtighed, vil dette ikke påvirke dens kapacitet til fortsat at gennemføre tilsynsprojekter. Ikke desto mindre vil Kommissionen i betragtning af PCLOB's vigtige rolle med hensyn til at gennemgå gennemførelsen af EO 14086 nøje overvåge status for fremtidige ledige mandater og nomineringer/udnævnelser.

2.2.3. Klageadgang

EO 14086, suppleret af en forordning fra justitsministeren, indførte en ny klagemekanisme til at behandle og løse kvalificerede klager fra enkeltpersoner vedrørende amerikanske signalefterretningsaktiviteter[79]. Enhver person i EU har ret til at indgive en klage til klagemekanismen vedrørende en påstået overtrædelse af amerikansk lovgivning om signalefterretningsaktiviteter (f.eks. EO 14086, Section 702 i FISA og EO 12333) med hensyn til personoplysninger, der overføres til USA, og som krænker vedkommendes interesser med hensyn til privatlivets fred og borgerlige frihedsrettigheder. Enkeltpersoner kan indgive en klage til en databeskyttelsesmyndighed i en EU-medlemsstat, som via Databeskyttelsesrådets sekretariat kanaliserer klagen til klagemekanismen. Mekanismen består af to lag, hvor den indledende klagebehandling foretages af ODNI CLPO, og hvor enkeltpersoner har mulighed for at klage over CLPO's afgørelse til en uafhængig DPRC. Når ODNI CLPO's eller DPRC's behandling er afsluttet, underrettes enkeltpersoner gennem den nationale myndighed om, at "behandlingen enten ikke identificerede nogen overtrædelse, eller at ODNI CLPO/DPRC udstedte en beslutning om passende afhjælpning". ODNI CLPO's og DPRC's afgørelser er bindende for efterretningstjenesterne.

Siden vedtagelsen af afgørelsen om tilstrækkeligheden af beskyttelsesniveauet er der taget yderligere skridt til at gøre klagemekanismen fuldt operationel.

Med hensyn til oprettelsen af DPRC blev der den 14. november 2023 udnævnt otte dommere (dvs. to yderligere dommere end det minimumsantal, der kræves i henhold til EO 14086, som suppleret af justitsministerens bestemmelser ved 28 C.F.R. § 201.3(a)) til domstolen[80]. De blev udnævnt på grundlag af kriterierne i EO 14086 og i overensstemmelse med den deri fastsatte proces, herunder efter høring af bl.a. PCLOB[81]. De omfatter tidligere føderale distriktsdomstols- og appeldomstolsdommere, en tidligere amerikansk justitsminister og et tidligere medlem af PCLOB. Som krævet af EO har mindst halvdelen af dommerne forudgående juridisk erfaring. Desuden blev der i april 2024 udpeget to særlige advokater, der aktive inden for retsvæsenet med ekspertise inden for både privatlivets fred og national sikkerhed, til at repræsentere enkeltpersoners interesser ved DPRC. Det blev på revisionsmødet bekræftet, at alle dommere og særlige advokater har fået den højeste sikkerhedsgodkendelse og derfor kan få adgang til klassificeret materiale, når de udfører deres opgaver for DPRC.

[78] https://documents.pclob.gov/prod/Documents/EventsAndPress/deb9cd13-12af-4250-998e-a520a2419a6b/PCLOB%20nominee%20press%20release%206-13-24.pdf.
[79] Betragtning 176-194 i afgørelsen om tilstrækkeligheden af beskyttelsesniveauet.
[80] https://www.justice.gov/opa/pr/attorney-general-merrick-b-garland-announces-judges-data-protection-review-court.
[81] Section 3(d)(A) i EO 14086.

DPRC har også offentliggjort en række ofte stillede spørgsmål med flere oplysninger om dets rolle, uafhængighed og funktion[82].

Med hensyn til behandling af klager vedtog ODNI den 6. december 2022 efterretningstjenesternes direktiv 126, som (ved at fastsætte frister, oprette et sikkert elektronisk register og sikre kommunikationskanaler, kræve, at CLPO og efterretningstjenesternes enheder samarbejder med PCLOB i forbindelse med den årlige revision af klagemekanismen osv.) i detaljer regulerer forskellige aspekter af processen for undersøgelse og pådømmelse af klager[83]. Dette direktiv finder anvendelse på tværs af de amerikanske efterretningstjenester og er blevet suppleret med yderligere interne procedurer vedtaget af de enkelte efterretningstjenester om deres samarbejde med ODNI CLPO i forbindelse med behandlingen af en klage (f.eks. udvikling af et sikkert register til deling af klager og udbedte dokumenter og sikker kommunikation mellem de relevante organer). DPRC vil også i de kommende måneder udstede mere detaljerede regler for behandling af klager og andre proceduremæssige aspekter.

Der blev truffet en række yderligere foranstaltninger i Den Europæiske Union og USA for at informere offentligheden og lette indgivelsen og behandlingen af klager. Dette omfatter Databeskyttelsesrådets vedtagelse af en orienterende note om den nye klagemekanisme[84], en klageformular (der skal oversættes og offentliggøres af alle databeskyttelsesmyndigheder på deres nationale sprog)[85] og en forretningsorden, der regulerer samarbejdet mellem de nationale tilsynsmyndigheder og Databeskyttelsesrådets sekretariat[86]. På samme måde offentliggjorde ODNI et dokument med ofte stillede spørgsmål og et faktablad om den nye klagemekanisme og deltog i offentlige oplysningsaktiviteter[87].

Desuden har Databeskyttelsesrådet og de relevante amerikanske myndigheder i det seneste år arbejdet tæt sammen om flere operationelle aspekter. Som bekræftet på revisionsmødet indførte de navnlig en krypteret kommunikationskanal til overførsel af klager fra nationale myndigheder i EU til Databeskyttelsesrådets sekretariat, fra Databeskyttelsesrådets sekretariat til ODNI CLPO samt til Office of Privacy and Civil Liberties of the Department of Justice ((justitsministeriets kontor for privatlivets fred og borgerlige frihedsrettigheder, OPCL) og mellem ODNI CLPO og andre amerikanske myndigheder (f.eks. DPRC). Desuden forklarede ODNI CLPO, at der er indført yderligere interne procedurer for de enkelte efterretningstjenesters samarbejde med ODNI CLPO med hensyn til klagebehandlingen.

Endelig oplyste OPCL, som yder administrativ støtte til DPRC, også, at DPRC opererer under sin egen særlige budgetpost og har de nødvendige faciliteter til at udføre sine opgaver, herunder sikre computere og bærbare computere, telefoner osv. Som krævet i EO 14086 har handelsministeriet desuden truffet de nødvendige foranstaltninger, herunder ved at oprette en krypteret kommunikationskanal med ODNI CLPO, for at føre en fortegnelse over alle

[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_da.
[85] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/template-complaint-form-us-office-director-national_da.
[86] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/rules-procedure-data-protection-framework-redress_da.
[87] https://www.dni.gov/files/CLPT/documents/Fact_Sheets/The_Role_of_the_ODNI_CLPO_FAQs.pdf og https://www.dni.gov/files/CLPT/documents/Fact_Sheets/Data_Privacy_Framework.pdf.

modtagne kvalificerede klager. Handelsministeriet vil regelmæssigt kontakte ODNI CLPO om, hvorvidt oplysninger vedrørende en individuel klage er blevet afklassificeret. Hvis dette er tilfældet, underretter handelsministeriet den pågældende person herom for at give vedkommende mulighed for at få adgang til sådanne oplysninger.

På tidspunktet for revisionsmødet havde EU's tilsynsmyndigheder ikke modtaget nogen klager, og den nye klagemekanisme var derfor endnu ikke blevet aktiveret.

3. KONKLUSION

På grundlag af de oplysninger, der er indsamlet under denne første revision, konkluderer Kommissionen, at de amerikanske myndigheder har indført de nødvendige strukturer og procedurer for at sikre, at databeskyttelsesrammen fungerer effektivt. I denne forbindelse sætter Kommissionen stor pris på det meget gode samarbejde med de amerikanske myndigheder om at gennemføre revisionen.

Selv om denne første revision naturligt nok fokuserede på at kontrollere, om alle rammens grundlæggende elementer er på plads, er erfaringerne med den praktiske anvendelse af de garantier, der gælder for både certificerede virksomheders behandling af data og offentlige myndigheders adgang til data, nødvendigvis begrænsede efter blot et års drift. Kommissionen vil derfor nøje overvåge den relevante udvikling i de kommende måneder og år med særlig vægt på 1) PCLOB's kommende rapporter om gennemførelsen af EO 14086 og funktionen af signalefterretningernes klagemekanisme, navnlig DPRC, 2) eventuelle yderligere ændringer af Section 702 i FISA og 3) nominering og udnævnelse af medlemmer til PCLOB med henblik på besættelse af kommende ledige mandater.

For at sikre en fortsat og effektiv funktion finder Kommissionen det desuden vigtigt:

- at handelsministeriet som meddelt på revisionsmødet i højere grad gør brug af de forskellige værktøjer i databeskyttelsesrammen til overvågning af virksomhedernes overholdelse af principperne og afsløring af falske påstande om deltagelse
- at FTC videreudvikler sin proaktive tilgang til undersøgelse og håndhævelse af certificerede virksomheders overholdelse af principperne i databeskyttelsesrammen
- at handelsministeriet, FTC og de europæiske databeskyttelsesmyndigheder udvikler fælles vejledningsinstrumenter om centrale krav i henhold til principperne i databeskyttelsesrammen, f.eks. om data om menneskelige ressourcer og videreoverførsler.

I lyset af dette resultat af revisionen og som omhandlet i betragtning 211 i afgørelsen om tilstrækkeligheden af beskyttelsesniveauet finder Kommissionen det hensigtsmæssigt at foretage den næste regelmæssige revision efter tre år. Dette skulle gøre det muligt at høste flere erfaringer med den praktiske anvendelse af databeskyttelsesrammen og tage hensyn til ovennævnte kommende udvikling. Kommissionen vil derfor i overensstemmelse med artikel 3, stk. 4, i afgørelsen om tilstrækkeligheden af beskyttelsesniveauet høre Databeskyttelsesrådet og det udvalg, der er nedsat i henhold til artikel 93, stk. 1, i den generelle forordning om databeskyttelse, om hyppigheden af fremtidige revisioner.