EUROPA-
KOMMISSIONEN

Bruxelles, den 24.6.2020
SWD(2020) 115 final

ARBEJDSDOKUMENT FRA KOMMISSIONENS TJENESTEGRENE

[…]

Ledsagedokument til

MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET OG RÅDET

Databeskyttelse som en hjørnesten i borgernes indflydelse og EU's tilgang til den digitale omstilling - to års anvendelse af den generelle forordning om databeskyttelse

{COM(2020) 264 final}

Indholdsfortegnelse

1 KONTEKST

Den generelle forordning om databeskyttelse[1] (i det følgende "persondataforordningen") er resultatet af otte års forberedelse, udarbejdelse og forhandlinger mellem institutionerne, og den trådte i kraft den 25. maj 2018 efter en overgangsperiode på to år (maj 2016–maj 2018). I henhold til artikel 97 i persondataforordningen aflægger Kommissionen rapport om evalueringen og revisionen af forordningen, første gang efter to års anvendelse og derefter hvert fjerde år.

Evalueringen er ligeledes en del af en mangesidet tilgang, som Kommissionen allerede har fulgt, før persondataforordningen trådte i kraft, og som den er fortsat med at følge aktivt siden da. Som led i denne tilgang indledte Kommissionen løbende bilaterale dialoger med medlemsstaterne om national lovgivnings overholdelse af persondataforordningen, og bidrog aktivt til arbejdet i Det Europæiske Databeskyttelsesråd (i det følgende benævnt "Databeskyttelsesrådet") ved at stille sin erfaring og ekspertise til rådighed, støttede databeskyttelsesmyndighederne og opretholdt tætte forbindelser med en lang række interessenter om den praktiske anvendelse af forordningen.

Evalueringen bygger på den statusopgørelse, som Kommissionen har foretaget i det første år af persondataforordningens anvendelse, og som blev sammenfattet i den meddelelse, der blev udsendt i juli 2019[2]. Den følger også op på meddelelsen om anvendelsen af GDPR, der blev offentliggjort i januar 2018[3]. Kommissionen vedtog også vejledningen om anvendelse af personoplysninger i en valgsammenhæng, som blev offentliggjort i september 2018, og vejledningen om apps, der støtter bekæmpelsen af covid-19-pandemien, der blev offentliggjort i april 2020.

Selv om dens fokus er på de to spørgsmål, der er fremhævet i artikel 97, stk. 2, i persondataforordningen, nemlig internationale overførsler og samarbejds- og sammenhængsmekanismer, anlægger denne evaluering en bredere tilgang for at behandle spørgsmål, der er blevet rejst af forskellige aktører i løbet af de seneste to år.

For at forberede evalueringen har Kommissionen inddraget bidragene fra:

- Rådet[4]
- Europa-Parlamentet (Udvalget om Borgernes Rettigheder og Retlige og Indre Anliggender)[5]
- Databeskyttelsesrådet[6] og de individuelle databeskyttelsesmyndigheder[7], baseret på et spørgeskema fra Kommissionen
- Feedback fra medlemmerne af flerpartsekspertgruppen til støtte for anvendelsen af persondataforordningen[8], ligeledes baseret på et spørgeskema fra Kommissionen

---

1 Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (EUT L 119 af 4.5.2016, s. 1).

2 Meddelelse fra Kommissionen til Europa-Parlamentet og Rådet, Databeskyttelsesregler som en tillidsskabende katalysator i og uden for EU – status (COM(2019) 374 final af 24.7.2019).

3 Meddelelse fra Kommissionen til Europa-Parlamentet og Rådet: Stærkere beskyttelse, nye muligheder – Kommissionens vejledning om den direkte anvendelse af den generelle forordning om databeskyttelse fra den 25. maj 2018 (COM/2018/043 final).

4 Rådets holdning og resultater vedrørende anvendelse af den generelle forordning om databeskyttelse (GDPR) (14994/2/19 Rev2 af 15.1.2020): https://data.consilium.europa.eu/doc/document/ST-14994-2019-REV-2/en/pdf

5 Skrivelse fra Europa-Parlamentets LIBE-Udvalg af 21.2.2020 til kommissær Reynders, ref.: IPOL-COM-LIBE D (2020) 6525.

6 Databeskyttelsesrådets bidrag til evalueringen af persondataforordningen i henhold til artikel 97, vedtaget den 18.2.2020: https://edpb.europa.eu/our-work-tools/our-documents/other/contribution-edpb-evaluation-gdpr-under-article-97_en

7 https://edpb.europa.eu/individual-replies-data-protection-supervisory-authorities_en

8 Flerpartsekspertgruppen vedrørende persondataforordningen, der er oprettet af Kommissionen, inddrager civilsamfundet og repræsentanter for erhvervslivet, akademikere og fagfolk: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3537 Flerpartsgruppens rapport findes på:

- og ad hoc-bidrag fra interessenter.

2 HÅNDHÆVELSE AF PERSONDATAFORORDNINGEN OG SAMARBEJDS- OG SAMMENHÆNGSMEKANISMERNES FUNKTION

Persondataforordningen indførte et innovativt forvaltningssystem og skabte grundlaget for en egentlig europæisk databeskyttelseskultur, der har til formål at sikre ikke blot en harmoniseret fortolkning, men også en harmoniseret anvendelse og håndhævelse af databeskyttelsesreglerne. Dens søjler er de uafhængige nationale databeskyttelsesmyndigheder og det nyligt oprettede Databeskyttelsesråd.

Da databeskyttelsesmyndighederne er af afgørende betydning for, at hele EU's databeskyttelsessystem fungerer, overvåger Kommissionen nøje deres reelle uafhængighed, herunder for så vidt angår tilstrækkelige finansielle, menneskelige og tekniske ressourcer.

Det er endnu for tidligt at foretage en fuldstændig vurdering af samarbejds- og sammenhængsmekanismernes funktion på grund af den korte periode til at indsamle erfaringer[9]. Desuden har databeskyttelsesmyndighederne endnu ikke udnyttet den fulde palet af værktøjer, som persondataforordningen har stillet til rådighed til at styrke deres samarbejde yderligere.

2.1 Brug af databeskyttelsesmyndighedernes styrkede beføjelser

Ved databeskyttelsesforordningen oprettes uafhængige databeskyttelsesmyndigheder, som tildeles harmoniserede og styrkede håndhævelsesbeføjelser. Eftersom persondataforordningen finder anvendelse, har disse myndigheder taget en bred vifte af korrigerende beføjelser i brug i henhold til persondataforordningen, f.eks. administrative bøder (22 EU-/EØS-myndigheder)[10], advarsler og kritik (23), påbud om at imødekomme den registreredes anmodninger (26), påbud om at bringe behandlingsaktiviteter i overensstemmelse med persondataforordningen (27), og påbud om berigtigelse, sletning eller begrænsning af behandling (17). Omkring halvdelen af databeskyttelsesmyndighederne (13) har indført midlertidige eller definitive begrænsninger i behandlingen, herunder forbud. Dette er bevis på en bevidst brug af alle de korrigerende foranstaltninger, der er fastsat i persondataforordningen. Databeskyttelsesmyndighederne holdt sig ikke tilbage fra at pålægge administrative bøder ud over eller i stedet for andre korrigerende foranstaltninger afhængigt af omstændighederne i de enkelte sager.

Administrative bøder:

Mellem 25. maj 2018 og 30. november 2019 udstedte 22 databeskyttelsesmyndigheder i EU/EØS omkring 785 bøder. Kun få myndigheder har endnu ikke pålagt administrative bøder, selv om de igangværende procedurer kan føre til sådanne bøder. De fleste bøder vedrørte overtrædelser af: princippet om lovlighed gyldigt samtykke beskyttelse af følsomme oplysninger forpligtelsen til gennemsigtighed, de registreredes rettigheder og brud på persondatasikkerheden.

Eksempler på bøder pålagt af databeskyttelsesmyndigheder omfatter[11]:

- 200 000 EUR for manglende overholdelse af retten til at modsætte sig direkte markedsføring i Grækenland

https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=21356

[9] Dette forhold fremhæves navnlig af Rådet i dets holdning og konklusioner vedrørende anvendelsen persondataforordningen og af Databeskyttelsesrådet i dets bidrag til evalueringen.

[10] Tallene i parentes angiver antallet af EU/EØS-databeskyttelsesmyndigheder, der har gjort brug af den anførte beføjelse mellem maj 2018 og slutningen af november 2019. Se Databeskyttelsesrådets bidrag, s. 32-33.

[11] En række afgørelser om bøder er stadig ved at blive prøvet ved domstolene.

- 220 000 EUR til et dataformidlingsselskab i Polen, som ikke havde oplyst kunderne om, at deres oplysninger blev behandlet
- 250 000 EUR til den spanske fodboldliga La Liga på grund af manglende gennemsigtighed i udformningen af dens smartphone-applikation
- 14,5 mio. EUR til en tysk ejendomsvirksomheds overtrædelse af databeskyttelsesprincipperne, navnlig ulovlig lagring
- 18 mio. EUR til de østrigske posttjenester for ulovlig behandling af særlige kategorier af oplysninger i stor skala
- 50 mio. EUR til Google i Frankrig på grund af betingelserne for at opnå samtykke fra brugere.

Persondataforordningens succes bør ikke måles på antallet af udstedte bøder, idet persondataforordningen opstiller en bredere palet af korrigerende beføjelser. Afhængigt af omstændighederne kan den afskrækkende virkning af et forbud mod behandling eller suspension af overførsel af oplysninger være meget stærkere.

Specifikke forhold gældende for den offentlige sektor

Persondataforordningen giver medlemsstaterne mulighed for at afgøre, om og i hvilket omfang offentlige myndigheder og organer kan pålægges administrative bøder. Hvis medlemsstaterne gør brug af denne mulighed, fratager dette ikke databeskyttelsesmyndighederne muligheden for at anvende alle de øvrige korrigerende beføjelser over for offentlige myndigheder og organer[12].

Et andet specifikt forhold er tilsynet med domstolene: selv om persondataforordningen også finder anvendelse på domstolenes aktiviteter, er disse fritaget for databeskyttelsesmyndigheders tilsyn, når de handler i deres egenskab af domstol. Chartret og TEUF forpligter imidlertid medlemsstaterne til at overlade det til et uafhængigt organ at føre tilsyn med sådanne databehandlingsaktiviteter[13].

Samarbejde med andre reguleringsorganer

Som anført i meddelelsen af juli 2019 støtter Kommissionen interaktionen med andre reguleringsorganer, idet den fuldt ud respekterer deres respektive kompetencer. Lovende samarbejdsområder omfatter forbrugerbeskyttelse og konkurrence. Databeskyttelsesrådet gav udtryk for sin villighed til at samarbejde med andre tilsynsmyndigheder, navnlig i forbindelse med koncentration på de digitale markeder[14]. Kommissionen anerkendte betydningen af privatlivets fred og databeskyttelse som et kvalitetsparameter for konkurrencen[15]. Databeskyttelsesrådets medlemmer deltog i fælles workshopper med netværket for forbrugerbeskyttelsessamarbejde om samarbejde om bedre håndhævelse af EU's forbruger- og databeskyttelseslovgivning. Denne tilgang vil blive anvendt til at fremme en fælles forståelse og udvikle praktiske måder til løsning af konkrete problemer, som forbrugere oplever, navnlig i den digitale økonomi.

For at sikre en konsekvent tilgang til beskyttelse af privatlivets fred og beskyttelse af personoplysninger, og indtil e-databeskyttelsesforordningen er vedtaget, er et tæt samarbejde med de myndigheder, der har kompetence til at håndhæve e-databeskyttelsesdirektivet[16], som er lex specialis i forhold til elektronisk kommunikation, helt uomgængeligt. Et tættere samarbejde med de kompetente myndigheder i henhold til

---

[12] Persondataforordningens artikel 83, stk. 7.

[13] Chartrets artikel 8, stk. 3, artikel 16, stk. 2, i TEUF, betragtning 20 i persondataforordningen.

[14] Jf. Databeskyttelsesrådets erklæring om virkningerne af økonomisk koncentration, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_economic_concentration_en.pdf.

[15] Se sag COMP M. 8124, Microsoft/LinkedIn.

[16] Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (direktivet om databeskyttelse inden for elektronisk kommunikation) (EFT L 201 af 31.7.2002, s. 37).

NIS-direktivet[17], og NIS-samarbejdsgruppen vil være til gensidig fordel for disse myndigheder og databeskyttelsesmyndighederne.

2.2 Samarbejds- og sammenhængsmekanismerne

Ved persondataforordningen blev samarbejdsmekanismen (one-stop-shop-system for operatører, fælles aktiviteter og gensidig bistand mellem databeskyttelsesmyndigheder) og sammenhængsmekanismen oprettet med det formål at fremme en ensartet anvendelse af databeskyttelsesreglerne gennem en konsekvent fortolkning og løsning af eventuel uenighed mellem myndighederne.

Databeskyttelsesrådet, der samler alle databeskyttelsesmyndigheder, er oprettet som et EU-organ med status som juridisk person og er fuldt operationelt med støtte fra et sekretariat[18]. Det er afgørende for de to ovennævnte mekanismers funktion. Ved udgangen af 2019 havde Databeskyttelsesrådet vedtaget 67 dokumenter, herunder 10 nye retningslinjer[19] og 43 udtalelser[2021].

Den vigtige rolle, som Databeskyttelsesrådet spiller, opstod, hvor der var behov for hurtigt at sikre en ensartet fortolkning af persondataforordningen og finde løsninger, der kunne finde øjeblikkelig anvendelse på EU-plan. I forbindelse med covid-19-udbruddet vedtog Databeskyttelsesrådet f.eks. i marts 2020 en erklæring om behandling af personoplysninger, der bl.a. omhandler lovligheden af behandling og anvendelse af mobile lokaliseringsdata i denne forbindelse[22], og i april 2020 vedtog det retningslinjer for behandling af helbredsoplysninger til videnskabelig forskning i forbindelse med covid-19-udbruddet [23] samt retningslinjer for anvendelse af lokaliseringsdata og kontaktopsporingsredskaber i forbindelse med covid-19-udbruddet[24]. Udvalget ydede også et betydeligt bidrag til udformningen af EU's strategi til Kommissionens og medlemsstaternes sporings-apps.

Det daglige samarbejde mellem databeskyttelsesmyndighederne, hvad enten de handler på egne vegne eller som medlemmer af Databeskyttelsesrådet, er baseret på udveksling af oplysninger og meddelelser om sager, der er indledt af myndighederne. For at lette kommunikationen mellem myndighederne ydede Kommissionen betydelig støtte ved at give dem et informationsudvekslingssystem[25]. De fleste myndigheder mener, at den er tilpasset samarbejds- og sammenhængsmekanismerne, selv om den kan finjusteres yderligere, f.eks. ved at gøre den mere brugervenlig.

Selv om det stadig er tidligt, kan der allerede nu afdækkes en række resultater og udfordringer, som præsenteres nedenfor. De viser, at databeskyttelsesmyndighederne hidtil har gjort effektiv brug af samarbejdsværktøjerne med præference for mere fleksible løsninger.

One-stop-shop

---

[17] Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (EUT L 194 af 19.7.2016, s. 1).

[18] Se nærmere oplysninger om sekretariatets aktiviteter i Databeskyttelsesrådets bidrag, s. 24-26.

[19] Ud over de 10 retningslinjer, som Artikel 29-Gruppen har vedtaget op til persondataforordningens ikrafttræden, og som Databeskyttelsesrådet har godkendt. Desuden har Databeskyttelsesrådet vedtaget yderligere 4 retningslinjer mellem januar og maj 2020 og ajourført en eksisterende vejledning.

[20] 42 af disse udtalelser blev vedtaget i henhold til persondataforordningens artikel 64, og én blev vedtaget i henhold til persondataforordningens artikel 70, stk. 1, litra s), og vedrørte afgørelsen om tilstrækkeligheden af beskyttelsesniveauet vedrørende Japan.

[21] Se Databeskyttelsesrådets bidrag, s. 18-23, for et fuldstændigt overblik over Databeskyttelsesrådets aktiviteter.

[22] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf.

[23] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032020-processing-data-concerning-health-purpose_en.

[24] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_da.pdf.

[25] Informationssystemet for det indre marked (IMI).

I grænseoverskridende sager kan en medlemsstats databeskyttelsesmyndighed generelt være involveret enten i) som ledende myndighed, når operatørens hovedvirksomhed er beliggende i denne medlemsstat, eller ii) som berørt myndighed, når operatøren har en virksomhed på denne medlemsstats område, når personer i denne medlemsstat berøres væsentligt, eller når der er indgivet en klage til dem.

Et sådant tæt samarbejde er blevet daglig praksis: Siden datoen for persondataforordningens anvendelse er databeskyttelsesmyndigheder i alle medlemsstater på et tidspunkt blevet konstateret enten som ledende myndigheder eller som berørte myndigheder i grænseoverskridende sager, om end i forskelligt omfang.

Fra maj 2018 til slutningen af 2019 fungerede databeskyttelsesmyndigheden i Irland som ledende myndighed i det højeste antal grænseoverskridende sager (127), efterfulgt af Tyskland (92), Luxembourg (87), Frankrig (64) og Nederlandene (45). Denne rækkefølge afspejler især den særlige situation i Irland og Luxembourg, som er værtslande for flere store multinationale teknologivirksomheder.

Anderledes ser rækkefølgen ud, for så vidt angår berørte myndigheder, hvor myndighederne i Tyskland er involveret i det højeste antal sager (435), efterfulgt af Spanien (337), Danmark (327), Frankrig (332) og Italien (306)[26].

Mellem 25. maj 2018 og 31. december 2019 blev der indgivet 141 udkast til afgørelser via one-stop-shop-proceduren, hvoraf 79 førte til endelige afgørelser. Pr. datoen for offentliggørelsen af denne rapport afventes der i flere vigtige sager med en grænseoverskridende dimension, og som er omfattet af one-stop-shop-mekanismen, en afgørelse. Nogle af disse afgørelser involverer store multinationale teknologivirksomheder[27]. De forventes at skabe klarhed og bidrage til en mere samordnet fortolkning af persondataforordningen.

Gensidig bistand

Databeskyttelsesmyndigheder har i vid udstrækning gjort brug af redskabet til gensidig bistand.

Ved udgangen af 2019 havde der været 115 procedurer for gensidig bistand[28], navnlig til gennemførelse af undersøgelser, hvoraf de fleste var foretaget af databeskyttelsesmyndighederne i Spanien (26), Tyskland (20), Danmark (13), Polen (12) og Tjekkiet (10). På den anden side havde Irland (19), Frankrig (11), Østrig (10), Tyskland (10) og Luxembourg (9) modtaget de fleste anmodninger [29].

Langt de fleste myndigheder anser gensidig bistand for at være et meget nyttigt samarbejdsværktøj og er ikke stødt på væsentlige hindringer for anvendelsen af proceduren for gensidig bistand. Den frivillige udveksling af gensidig bistand, for hvilken der ikke er nogen juridisk frist, eller hvor der ikke er streng pligt til at svare, er blevet anvendt hyppigere, nemlig i 2 427 procedurer. Irlands databeskyttelsesmyndighed sendte og modtog det højeste antal anmodninger om gensidig bistand (527 sendt og 359 modtaget), efterfulgt af de tyske myndigheder (260 sent/356 modtaget).

Omvendt er der ikke endnu blevet gennemført fælles aktiviteter[30], der ville gøre det muligt for flere medlemsstaters databeskyttelsesmyndigheder at blive involveret allerede i undersøgelserne af grænseoverskridende sager. Der er løbende overvejelser i gang i Databeskyttelsesrådet om den praktiske gennemførelse af dette redskab, og hvordan dets brug kan fremmes.

---

[26] Se Databeskyttelsesrådets bidrag, s. 8.

[27] F.eks. har den irske databeskyttelsesmyndighed den 22.5.2020 fremsendt et udkast til afgørelse til andre berørte myndigheder i overensstemmelse med forordningens artikel 60 vedrørende en undersøgelse af Twitter International Company i forbindelse med en underretning om brud på datasikkerheden. Samme dag meddelte den irske databeskyttelsesmyndighed tillige, at et udkast til afgørelse om WhatsApp Ireland Limited i medfør af artikel 60 var under forberedelse i forbindelse med gennemsigtighed, herunder gennemsigtighed med hensyn til, hvilke oplysninger der deles med Facebook.

[28] Persondataforordningens artikel 61.

[29] Se Databeskyttelsesrådets bidrag, s. 12-14.

[30] Persondataforordningens artikel 62.

Sammenhængsmekanisme

Indtil videre er kun sammenhængsmekanismens første del blevet udnyttet, nemlig vedtagelsen af Databeskyttelsesrådets udtalelser[31]. Omvendt er der endnu ikke forekommet tilfælde af tvistbilæggelse i Databeskyttelsesrådet[32] eller taget en hasteprocedure i brug[33].

I perioden fra 25. maj 2018 til 31. december 2019 afgav Databeskyttelsesrådet 36 udtalelser i forbindelse med et af dets medlemmers vedtagelse af foranstaltningers[34]. De fleste af disse (31) vedrørte vedtagelsen af nationale lister over aktiviteter, der kræver en konsekvensanalyse vedrørende databeskyttelse. To udtalelser vedrørte bindende virksomhedsregler, to andre vedrørte udkast til akkrediteringskrav til et kontrolorgan for adfærdskodeks, og én vedrørte standardkontraktbestemmelsers[35].

Bestyrelsen vedtog endvidere efter anmodning seks udtalelsers[36]. Tre af disse udtalelser vedrørte nationale lister til bestemmelse af behandlinger, der ikke kræver en konsekvensanalyse vedrørende databeskyttelse. De andre vedrørte henholdsvis en administrativ ordning for overførsel af personoplysninger mellem finanstilsynsmyndigheder inden for EØS og finanstilsynsmyndigheder uden for EØS, samspillet mellem e-databeskyttelsesdirektivet og persondataforordningen og en tilsynsmyndigheds kompetence i tilfælde af en ændring i omstændighederne vedrørende hovedvirksomhed eller eneste etablering[37].

Udfordringer

Selv om databeskyttelsesmyndighederne har samarbejdet meget aktivt i Databeskyttelsesrådet og i forvejen intensivt anvender samarbejdsværktøjet for gensidig bistand, er opbygningen af en egentlig fælles kultur stadig en pågående proces.

Navnlig kræver håndteringen af grænseoverskridende sager en mere effektiv og harmoniseret tilgang og en effektiv anvendelse af alle samarbejdsværktøjer i persondataforordningen. Der er bred enighed om dette punkt, da det blev rejst på forskellige måder af Europa-Parlamentet, Rådet, Den Europæiske Tilsynsførende for Databeskyttelse, interessenter (inden for og uden for flerpartsgruppen) og databeskyttelsesmyndighederne.

De vigtigste forhold, der skal tages op i denne forbindelse, er forskelle i:

- nationale administrative procedurer, navnlig vedrørende: klagebehandlingsprocedurer, antagelighedskriterier for klager, varigheden af procedurer på grund af forskellige tidsrammer eller manglende frister, det tidspunkt i proceduren, hvor retten til at blive hørt bevilges, oplysninger om og inddragelse af klagerne i proceduren
- fortolkninger af begreber vedrørende samarbejdsmekanismen, f.eks. relevante oplysninger, begrebet "straks", "klage", det dokument, der defineres som "udkastet til afgørelse" af den ledende databeskyttelsesmyndighed, mindelig løsning (navnlig den procedure, der fører til en mindelig løsning, løsningens retlige form), og
- på hvilken måde samarbejdsproceduren skal indledes, inddrage de berørte databeskyttelsesmyndigheder og formidle oplysninger til dem. Klagerne savner også klarhed om, hvordan deres sager håndteres i grænseoverskridende situationer, hvilket flere medlemmer af flerpartsgruppen har understreget. Desuden nævner virksomhederne, at de nationale databeskyttelsesmyndigheder i visse tilfælde ikke henviste sager til den ledende databeskyttelsesmyndighed, men håndterede dem som lokale sager.

---

31 Baseret på persondataforordningens artikel 64.
32 Persondataforordningens artikel 65.
33 Persondataforordningens artikel 66.
34 I henhold til persondataforordningens artikel 64, stk. 1.
35 Persondataforordningens artikel 28, stk. 8.
36 I henhold til persondataforordningens artikel 64, stk. 2.
37 Se Databeskyttelsesrådets bidrag, s. 15.

Kommissionen er tilfreds med, at Databeskyttelsesrådet har meddelt, at det er begyndt at gøre sig overvejelser om, hvordan man kan løse disse problemer. Databeskyttelsesrådet anførte navnlig, at det vil præcisere de proceduremæssige skridt, der er taget i samarbejdet mellem den ledende databeskyttelsesmyndighed og de berørte databeskyttelsesmyndigheder, analysere de nationale administrative procedureregler, arbejde hen imod en fælles fortolkning af nøglebegreber og styrke kommunikation og samarbejde (herunder fælles aktiviteter). Databeskyttelsesrådets overvejelser og analyser bør føre til mere effektive arbejdsordninger i grænseoverskridende sager[38], herunder ved at bygge på medlemmernes ekspertise og ved at styrke inddragelsen af dets sekretariat. Det skal desuden bemærkes, at Databeskyttelsesrådets ansvar med hensyn til at sikre en konsekvent fortolkning af persondataforordningen ikke kan opfyldes ved blot at finde den laveste fællesnævner.

Endelig skal Databeskyttelsesrådet som EU-organ også anvende EU's forvaltningsret og sikre gennemsigtighed i beslutningsprocessen.

2.3 Rådgivning og vejledning

Databeskyttelsesmyndighedernes oplysningsaktiviteter og rådgivning

Flere databeskyttelsesmyndigheder har skabt nye værktøjer, herunder hjælp til enkeltpersoner og virksomheder, og værktøjssæt til virksomheder[39]. Mange operatører glæder sig over den pragmatisme, som disse myndigheder har udvist med hensyn til at bistå med anvendelsen af persondataforordningen. Især har flere af dem aktivt kommunikeret og haft et tæt samarbejde med databeskyttelsesrådgivere, bl.a. gennem sammenslutninger af databeskyttelsesansvarlige. Mange myndigheder har også udstedt retningslinjer for de databeskyttelsesansvarliges rolle og forpligtelser med det formål at støtte de databeskyttelsesansvarlige i deres daglige aktiviteter og afholdt seminarer, der var specifikt henvendt til dem. Dette gælder imidlertid ikke for alle databeskyttelsesmyndigheder.

Ligeledes peger feedback fra interessenter på en række problemfelter omkring vejledning og rådgivning:

- manglen på en konsekvent strategi og vejledning mellem de nationale databeskyttelsesmyndigheder om visse forhold (f.eks. om cookies[40], anvendelsen af legitime interesser, anmeldelser af brud på persondatasikkerheden eller konsekvensanalyser vedrørende databeskyttelse) eller endda mellem databeskyttelsesmyndigheder i de samme medlemsstater (f.eks. i Tyskland om begreberne dataansvarlig og databehandler)
- uoverensstemmelsen mellem de retningslinjer, der vedtages på nationalt plan, og dem, der vedtages af Databeskyttelsesrådet
- manglende offentlige høringer om visse retningslinjer, der er vedtaget på nationalt plan
- forskellige niveauer af inddragelse af interessenter blandt databeskyttelsesmyndighederne
- forsinkelser i modtagelsen af svar på anmodninger om oplysninger
- vanskeligheder med at få praktisk og værdifuld rådgivning fra databeskyttelsesmyndighederne
- behovet for at øge den sektorspecifikke ekspertise hos nogle databeskyttelsesmyndigheder (f.eks. inden for sundhedssektoren og lægemiddelindustrien).

---

[38] Som påpeget i Rådets holdning og konklusioner.

[39] Se nedenfor under punkt 7.

[40] Indtil e-databeskyttelsesforordningen bliver vedtaget, er det vigtigt med et tæt samarbejde med de kompetente myndigheder, der er ansvarlige for håndhævelsen af e-databeskyttelsesdirektivet i medlemsstaterne. I overensstemmelse med dette direktiv er de myndigheder, der er kompetente til at håndhæve artikel 5, stk. 3, i e-databeskyttelsesdirektivet (som fastsætter betingelserne for brug af og adgang til "cookies" på en brugers terminaludstyr), i nogle medlemsstater ikke de samme som tilsynsmyndighederne i henhold til persondataforordningen.

Flere af disse forhold hænger også sammen med manglen på ressourcer hos flere databeskyttelsesmyndigheder (se nedenfor).

Afvigende praksis med hensyn til anmeldelse af brud på datasikkerheden[41]

Selv om Rådet fremhæver den byrde, der er forbundet med sådanne anmeldelser, er der betydelige forskelle i antallet af anmeldelser mellem medlemsstaterne: hvor der i perioden fra maj 2018 til udgangen af november 2019 i de fleste medlemsstater samlet set var under 2 000 anmeldelser, og i 7 medlemsstater mellem 2 000 og 10 000, indberettede de nederlandske og tyske databeskyttelsesmyndigheder i perioden hhv. 37 400 og 45 600 anmeldelser[42].

Dette kan tyde på, at der savnes en konsekvent fortolkning og gennemførelse, til trods for at der på EU-niveau findes retningslinjer for anmeldelser af brud på datasikkerheden.

Retningslinjer fra Det Europæiske Databeskyttelsesråd

Hidtil har Databeskyttelsesrådet vedtaget mere end 20 retningslinjer, der dækker centrale aspekter af persondataforordningen[43]. Retningslinjerne er et vigtigt redskab til at sikre en ensartet anvendelse af persondataforordningen og er derfor i stort omfang blevet modtaget positivt af interessenterne. Interessenterne har været glade for den systematiske offentlige høring (6-8 uger). De efterspørger imidlertid mere dialog med Databeskyttelsesrådet. I den forbindelse bør praksis med at arrangere workshopper om målrettede emner inden udarbejdelsen af retningslinjer fortsættes og styrkes for at sikre gennemsigtighed, inddragelse og relevans i Databeskyttelsesrådets arbejde. Interessenterne anmoder også om, at fortolkningen af de mest omstridte problemer behandles i retningslinjerne, da disse er genstand for offentlig høring, og ikke i udtalelser i henhold til persondataforordningens artikel 64, stk. 2. Nogle interessenter efterlyser også mere praktiske retningslinjer, der beskriver anvendelsen af begreber og bestemmelser i persondataforordningen[44]. Medlemmer af flerpartsgruppen understreger, at der er behov for mere konkrete eksempler, der så vidt muligt skal mindske risikoen for divergerende fortolkninger mellem databeskyttelsesmyndigheder. Samtidig bør anmodningerne om at præcisere, hvordan persondataforordningen skal anvendes, og om at skabe retssikkerhed, ikke føre til yderligere krav eller reducere fordelene ved den risikobaserede tilgang og ansvarlighedsprincippet.

De emner, som interessenterne gerne vil have yderligere retningslinjer for i Databeskyttelsesrådet, omfatter: rækkevidden af de registreredes rettigheder (herunder i ansættelsesforhold) ajourføring af udtalelsen om behandling på grundlag af legitime interesser begreberne den dataansvarlige, den fælles dataansvarlige og registerføreren samt de nødvendige aftaler mellem parterne[45] anvendelsen af persondataforordningen på nye teknologier (såsom blockchain og kunstig intelligens) behandling i forbindelse med videnskabelig forskning (herunder i forbindelse med internationalt samarbejde) behandling af børns personoplysninger pseudonymisering og anonymisering samt behandling af sundhedsdata.

Databeskyttelsesrådet har allerede tilkendegivet, at det vil udstede retningslinjer for mange af disse emner, og det arbejde, der allerede er påbegyndt for fleres vedkommende (f.eks. om anvendelsen af legitim interesse som retsgrundlag for behandling).

Interessenterne anmoder Databeskyttelsesrådet om at ajourføre og i givet fald revidere eksisterende retningslinjer under hensyntagen til de erfaringer, der er gjort siden deres offentliggørelse, og under hensyntagen til muligheden for at gå mere i detaljer, når det er nødvendigt.

---

41 Persondataforordningens artikel 33.

42 Se Databeskyttelsesrådets bidrag, s. 35.

43 Arbejdet med retningslinjer blev allerede indledt inden persondataforordningens ikrafttræden den 25. maj 2018 inden for rammerne af Artikel 29-Gruppen. Se den fulde liste over retningslinjer på https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en.

44 Dette har også Europa-Parlamentet og Rådet peget på.

45 Databeskyttelsesrådet er i gang med at udforme retningslinjer om dataansvarlige og databehandlere.

2.4 Databeskyttelsesmyndighedernes ressourcer

Det er en forudsætning for en effektiv udførelse af deres opgaver og udøvelsen af deres beføjelser, at de enkelte databeskyttelsesmyndigheder råder over de nødvendige menneskelige, tekniske og finansielle ressourcer, lokaler og infrastrukturer, og er derfor en væsentlig betingelse for deres uafhængighed[46].

De fleste databeskyttelsesmyndigheder har nydt godt af stigende personale og ressourcer, siden persondataforordningen trådte i kraft i 2016[47]. Mange af dem beretter dog stadig, at de ikke råder over tilstrækkelige ressourcer[48].

Antal medarbejdere, der arbejder for nationale databeskyttelsesmyndigheder

Det samlede antal medarbejdere hos databeskyttelsesmyndigheder i EØS steg over en kam med 42 % mellem 2016 og 2019 (med 62 %, hvis prognosen for 2020 tages med).

Antallet af medarbejdere hos de fleste myndigheder er steget i denne periode med den største stigning (i procent) registreret for myndigheder i Irland (+ 169 %), Nederlandene (+ 145 %), Island (+ 143 %), Luxembourg (+ 126 %) og Finland (+ 114 %). Omvendt faldt antallet af ansatte hos flere databeskyttelsesmyndigheder, med de mest markante fald i Grækenland (-15 %), Bulgarien (-14 %), Estland (-11 %), Letland (-10 %) og Litauen (-8 %). Hos nogle myndigheder skyldes faldet i antallet af medarbejdere også databeskyttelseseksperters fratrædelse til fordel for ansættelse i den private sektor, som kan tilbyde mere attraktive vilkår.

Generelt anslår prognosen for 2020, at der har været en stigning i antallet af medarbejdere i forhold til 2019, med undtagelse hos myndighederne i Østrig, Bulgarien, Italien, Sverige og Island (hvor antallet af medarbejdere forventes at forblive stabilt), Cypern og Danmark (hvor antallet af medarbejdere forventes at falde).

De tyske databeskyttelsesmyndigheder[49] har tilsammen det største antal medarbejdere (888 i 2019/anslået 1002 i 2020), efterfulgt af databeskyttelsesmyndighederne i Polen (238/260), Frankrig (215/225), Spanien (170/220), Nederlandene (179/188), Italien (170/170) og Irland (140/176).

De databeskyttelsesmyndigheder, der har det laveste antal medarbejdere, er i Cypern (24/22), Letland (19/31), Island (17/17), Estland (16/18) og Malta (13/15).

De nationale databeskyttelsesmyndigheders budget

Det samlede budget for databeskyttelsesmyndigheder i EØS er over en kam steget med 49 % mellem 2016 og 2019 (med 64 %, hvis prognosen for 2020 medregnes).

De fleste myndigheders budget steg i denne periode, med den største stigning (i procent) registreret for myndigheder i Irland (+ 223 %), Island (+ 167 %), Luxembourg (+ 165 %), Nederlandene (+ 130 %) og Cypern (+ 114 %). Omvendt oplevede nogle myndigheder kun en lille stigning i budgettet, med de mindste stigninger registreret for databeskyttelsesmyndigheder i Estland (7 %), Letland (4 %), Rumænien (3 %) og Belgien (1 %), mens myndigheden i Frankrig oplevede et fald (-2 %).

Generelt skønnes det ifølge prognosen for 2020, at der vil være en stigning i budgettet i forhold til 2019, undtagen for myndighederne i Østrig, Bulgarien, Estland og Nederlandene (hvis budgetter forventes at forblive stabile).

---

[46] Se persondataforordningens artikel 52, stk. 4.

[47] Forordningen trådte i kraft i maj 2016 og blev taget i anvendelse i maj 2018 efter en overgangsperiode på 2 år.

[48] Se Databeskyttelsesrådets bidrag, s. 26-30

[49] Der er 18 myndigheder i Tyskland, hvoraf den ene er en føderal myndighed, og 17 er regionale myndigheder (herunder to i Bayern).

De databeskyttelsesmyndigheder, der har det største budget, er Tyskland (76,6 mio. EUR i 2019/anslået 85,8 mio. EUR i 2020-prognosen), Italien (29,1/30,1), Nederlandene (18,6/18,6), Frankrig (18,5/20,1) og Irland (15,2/16,9).

De myndigheder, der har det laveste budget, er Kroatien (1,2 mio. EUR i 2019/anslået EUR 1,4 mio. EUR i 2020-prognosen), Rumænien (1,1/1,3), Letland (0,6/1,2), Cypern (0,5/0,5) og Malta (0,5/0,6).

Tabellen i bilag II giver et overblik over de nationale databeskyttelsesmyndigheders menneskelige og budgetmæssige ressourcer.

Ud over at påvirke deres evne til at håndhæve reglerne på nationalt plan begrænser manglen på ressourcer også databeskyttelsesmyndighedernes kapacitet til at deltage i og bidrage til samarbejds- og sammenhængsmekanismen og til det arbejde, der udføres i Databeskyttelsesrådet. Som fremhævet af Databeskyttelsesrådet afhænger den succes, som one-stop-shop-mekanismen har, af den tid og indsats, som databeskyttelsesmyndighederne kan bruge til håndtering af og samarbejde om individuelle grænseoverskridende sager. Ressourceproblemet forstærkes yderligere af myndighedernes øgede rolle i tilsynet med store IT-systemer, der i øjeblikket er under udvikling. Databeskyttelsesmyndighederne i Irland og Luxembourg har desuden specifikke ressourcebehov set i lyset af deres rolle som ledende myndigheder med hensyn til håndhævelsen af persondataforordningen over for store teknologivirksomheder, som befinder sig primært i disse medlemsstater.

Mens Rådet peger på virkningen af samarbejdsmekanismen og dens frister på databeskyttelsesmyndighedernes arbejde[50], er medlemsstaterne i henhold til persondataforordningen forpligtet til at tilføre deres nationale databeskyttelsesmyndigheder tilstrækkelige menneskelige, finansielle og tekniske ressourcer[51].

Databeskyttelsesrådets sekretariat, som forestås af Den Europæiske Tilsynsførende for Databeskyttelser[52], består i øjeblikket af 20 personer, herunder juridiske eksperter, IT-eksperter og kommunikationseksperter. Det skal vurderes, om dette tal skal udvides fremadrettet, således at det på effektiv vis kan opfylde sin funktion som analytisk, administrativ og logistisk støtte til Databeskyttelsesrådet og dets undergrupper, bl.a. ved forvaltningen af informationsudvekslingssystemet.

3 HARMONISEREDE REGLER, MEN FORTSAT EN VIS GRAD AF FRAGMENTERING OG DIVERGERENDE STRATEGIER

Persondataforordningen indeholder bestemmelser om en konsekvent tilgang til databeskyttelsesreglerne i hele EU, som erstatter de forskellige nationale ordninger, der eksisterede inden for rammerne af databeskyttelsesdirektivet af 1995.

3.1 Medlemsstaternes gennemførelse af persondataforordningen

Persondataforordningen har været direkte gældende i alle medlemsstater siden 25. maj 2018. Den forpligtede medlemsstaterne til at lovgive, navnlig for at oprette nationale databeskyttelsesmyndigheder og indføre generelle betingelser for deres medlemmer, for at sikre, at hver enkelt myndighed handler i fuld uafhængighed, når den udfører sine opgaver og udøver sine beføjelser i overensstemmelse med persondataforordningen. Retlige forpligtelser og offentlige opgaver kan kun udgøre retsgrundlaget for behandling af personoplysninger, hvis de er nedfældet i (EU-lovgivningen eller) national lovgivning.

[50] Persondataforordningens artikel 60.
[51] Persondataforordningens artikel 52, stk. 4.
[52] Persondataforordningens artikel 75.

Desuden skal medlemsstaterne fastsætte regler om sanktioner, navnlig for overtrædelser, der ikke er underlagt administrative bøder, og de skal skabe sammenhæng mellem retten til beskyttelse af personoplysninger og retten til ytrings- og informationsfrihed. National ret kan også fastsætte et retsgrundlag for undtagelsen fra det generelle forbud mod behandling af særlige kategorier af personoplysninger, f.eks. af hensyn til den væsentlige offentlige interesse på folkesundhedsområdet, herunder beskyttelse mod alvorlige grænseoverskridende sundhedstrusler. Desuden skal medlemsstaterne sikre akkreditering af certificeringsorganer.

Kommissionen overvåger gennemførelsen af persondataforordningen i national lovgivning. Alle medlemsstater, med undtagelse af Slovenien, har på tidspunktet for udarbejdelsen af denne rapport vedtaget ny databeskyttelseslovgivning eller tilpasset deres lovgivning på dette område. Kommissionen anmodede derfor Slovenien om at redegøre nærmere for de hidtidige fremskridt og opfordrede det indtrængende til at afslutte denne proces[53].

Desuden vurderes den nationale lovgivnings overensstemmelse med reglerne om databeskyttelse med hensyn til Schengenreglerne også i forbindelse med den Schengenevalueringsmekanismen, der koordineres af Kommissionen. Kommissionen og medlemsstaterne evaluerer i fællesskab, hvordan landene gennemfører og anvender Schengenreglerne på en række områder. For så vidt angår databeskyttelse vedrører dette store IT-systemer, som f.eks. Schengeninformationssystemet og visuminformationssystemet, og omfatter databeskyttelsesmyndighedernes rolle i forbindelse med overvågning af behandlingen af personoplysninger inden for disse systemer.

Arbejdet med at tilpasse sektorlovgivningen er stadig i gang på nationalt plan. Efter persondataforordningens indarbejdelse i aftalen om Det Europæiske Økonomiske Samarbejdsområde blev dens anvendelse udvidet til også at omfatte Norge, Island og Liechtenstein. Disse lande har ligeledes vedtaget nationale databeskyttelseslove.

Kommissionen vil gøre brug af alle de redskaber, den har til rådighed, herunder traktatbrudssager, for at sikre, at medlemsstaterne overholder persondataforordningen.

De vigtigste problemstillinger i forbindelse med national gennemførelse

De vigtigste problemstillinger, der hidtil er blevet afdækket som led i den igangværende vurdering af national lovgivning og de bilaterale udvekslinger med medlemsstaterne, omfatter:

- Begrænsninger i anvendelsen af persondataforordningen: nogle medlemsstater udelukker f.eks. fuldstændig det nationale parlaments aktiviteter.
- Forskelle i anvendelsen af nationale specificerende love. Nogle medlemsstater forbinder anvendelsen af deres nationale lovgivning med det sted, hvor varerne eller ydelserne udbydes, andre til den dataansvarliges eller databehandlerens hjemsted. Dette er i strid med den harmoniseringsmålsætning, der forfølges med persondataforordningen.
- Nationale love, der rejser tvivl om proportionaliteten af indgrebet i retten til databeskyttelse. Kommissionen indledte f.eks. en traktatbrudssag mod en medlemsstat, som havde vedtaget lovgivning, der pålagde dommere at offentliggøre specifikke oplysninger om deres ikke-erhvervsmæssige aktiviteter, hvilket er uforeneligt med retten til respekt for privatlivets fred og retten til beskyttelse af personoplysninger[54]

[53] Det skal bemærkes, at den nationale databeskyttelsesmyndighed i Slovenien er oprettet på grundlag af den nuværende nationale databeskyttelseslovgivning og fører tilsyn med anvendelsen af persondataforordningen i denne medlemsstat.

[54] Denne traktatbrudssag vedrører den polske lov om retsvæsenet af 20. december 2019, som griber ind i dommernes uafhængighed, og som bl.a. vedrører videregivelse af oplysninger om dommeres ansættelse i ikke-erhvervsmæssige aktiviteter: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_772.

- Mangel på et uafhængigt organ til at føre tilsyn med domstolenes behandling af oplysninger ved domstole, der handler i deres egenskab af domstole[55].
- Lovgivning på områder, der er fuldt reguleret af persondataforordningen, der går videre end manøvremargenen for specifikationer eller begrænsninger. Dette er navnlig tilfældet, når nationale bestemmelser fastsætter betingelser for behandling på grundlag af legitime interesser, ved at give anvisninger for, hvordan der foretages en afvejning mellem den dataansvarliges og de berørte personers respektive interesser, mens persondataforordningen forpligter hver enkelt dataansvarlige til at foretage en sådan afvejning individuelt og påberåbe sig dette retsgrundlag.
- Specifikationer og yderligere krav ud over behandling med henblik på overholdelse af en lovbestemt forpligtelse eller udførelse af en offentlig opgave (f.eks. videoovervågning i den private sektor eller direkte markedsføring) og for begreber, der anvendes i persondataforordningen (f.eks. "stor skala" eller "sletning").

Nogle af disse spørgsmål kan blive afklaret af Domstolen i fortsat verserende sager[56].

Afstemning af retten til beskyttelse af personoplysninger med ytrings- og informationsfrihed

Et specifikt forhold vedrører gennemførelsen af medlemsstaternes forpligtelse til ved lov at forene retten til beskyttelse af personoplysninger med ytrings- og informationsfriheden[57]. Dette forhold er meget komplekst, idet der ved en vurdering af balancen mellem disse grundlæggende rettigheder også skal tages hensyn til bestemmelser og sikkerhedsforanstaltninger i presse- og medielovgivning.

Vurderingen af medlemsstaternes lovgivning viser forskellige tilgange til tilpasningen mellem retten til beskyttelse af personoplysninger og ytrings- og informationsfrihed:

- Nogle medlemsstater fastsætter princippet om ytringsfrihedens forrang eller fritager i forbindelse med behandling af personoplysninger, der udelukkende finder sted i journalistisk øjemed eller med henblik på akademisk, kunstnerisk eller litterær virksomhed, hele kapitler, der er nævnt i persondataforordningens artikel 85, stk. 2. I en vis udstrækning indeholder medielove bestemmelser om visse garantier, for så vidt angår den registreredes rettigheder.
- Nogle medlemsstater har fastsat bestemmelser om, at beskyttelsen af personoplysninger har forrang, og giver kun mulighed for ikke at anvende databeskyttelsesreglerne i specifikke situationer, f.eks. hvor en person med offentlig status er berørt.
- Andre medlemsstater giver mulighed for, at lovgiveren i et vist omfang kan foretage en afvejning, og/eller at der kan foretages en vurdering i det enkelte tilfælde, for så vidt angår undtagelser fra visse bestemmelser i persondataforordningen.

Kommissionen vil fortsætte sin vurdering af national lovgivning med afsæt i kravene i chartret. Afstemningen skal være fastlagt i lovgivningen og skal respektere disse grundlæggende rettigheders væsentligste indhold og være proportionel og nødvendig (artikel 52, stk. 1, i chartret). Databeskyttelsesreglerne bør ikke påvirke udøvelsen af ytrings- og informationsfriheden, navnlig ved at skabe en begrænsende virkning eller ved at blive fortolket som et middel til at lægge pres på journalister for at afsløre deres kilder.

[55] Se chartrets artikel 8, stk. 3, artikel 16 i TEUF, betragtning 20 i persondataforordningen.
[56] F.eks. er fritagelsen af et parlamentarisk udvalg for anvendelsen af persondataforordningen genstand for en verserende retssag (C-272/19).
[57] Persondataforordningens artikel 85.

3.2 Bestemmelser om fakultativ specifikation og deres begrænsninger

Persondataforordningen giver medlemsstaterne mulighed for yderligere at specificere dens anvendelse på et begrænset antal områder. Denne manøvremargen for national lovgivning adskiller sig fra forpligtelsen til at gennemføre visse andre bestemmelser i persondataforordningen som nævnt ovenfor. Bestemmelserne om fakultative specifikationer er anført i bilag I.

Manøvremargenerne for medlemsstaternes lovgivning er underlagt de betingelser og begrænsninger, der er fastsat i persondataforordningen, og giver ikke mulighed for en samtidig national databeskyttelsesordning[58]. Medlemsstaterne er forpligtet til at ændre eller ophæve den nationale databeskyttelseslovgivning, herunder sektorspecifik lovgivning med databeskyttelsesaspekter.

Dertil kommer, at en medlemsstats relaterede lovgivning ikke må indeholde bestemmelser, der kunne skabe forvirring om den direkte anvendelse af persondataforordningen. Når persondataforordningen fastsætter, at der kan indføres specifikationer eller begrænsninger af dens regler ved medlemsstaternes nationale ret, kan medlemsstaterne, i det omfang det er nødvendigt af hensyn til sammenhængen og for at gøre de nationale bestemmelser forståelige for de personer, som de finder anvendelse på, indarbejde elementer af persondataforordningen i deres nationale ret[59].

Der er interessenter, der mener, at medlemsstaterne bør begrænse eller undlade at anvende bestemmelser om fakultative specifikationer, da de ikke bidrager til harmonisering. De nationale forskelle i både gennemførelsen af lovene og databeskyttelsesmyndighedernes fortolkning heraf øger omkostningerne ved overholdelse af lovgivningen i hele EU markant.

Fragmentering i forbindelse med anvendelse af klausuler om fakultative specifikationer

- Aldersgrænse for børns samtykke til informationssamfundstjenester

En række medlemsstater har gjort brug af muligheden for at fastsætte en lavere aldersgrænse end 16 år for samtykke i forbindelse med informationssamfundstjenester (persondataforordningens artikel 8, stk. 1). Ni medlemsstater anvender aldersgrænsen på 16 år, mens otte medlemsstater har valgt en grænse på 13 år, seks på 14 år og tre på 15 år[60].

Som følge heraf skal en virksomhed, der leverer informationssamfundstjenester til mindreårige i hele EU, sondre mellem de potentielle brugeres alder, afhængigt af hvilken medlemsstat de er bosiddende i. Dette er i strid med det generelle mål i persondataforordningen om at sikre ensartet beskyttelse af personer og forretningsmuligheder i alle medlemsstater.

Sådanne forskelle fører til situationer, hvor den medlemsstat, hvor den dataansvarlige er etableret, fastsætter en anden aldersgrænse end den medlemsstat, hvor de registrerede er bosiddende.

- Sundhed og forskning

Ved gennemførelsen af undtagelser fra det generelle forbud mod behandling af særlige kategorier af personoplysninger[61] følger medlemsstaternes lovgivning forskellige metoder, for så vidt angår specifikationernes og garantiernes niveau, herunder til sundheds- og forskningsformål. De fleste medlemsstater har indført eller opretholdt yderligere betingelser for behandling af genetiske data,

---

[58] Det meget anvendte begreb "åbningsbestemmelser" som udtryk for bestemmelser om specifikation er vildledende, da det kunne give indtryk af, at medlemsstaterne har manøvremargener ud over forordningens bestemmelser.

[59] Betragtning 8 i persondataforordningen.

[60] 13 år for Belgien, Danmark, Estland, Finland, Letland, Malta, Portugal og Sverige 14 år for Østrig, Bulgarien, Cypern, Spanien, Italien og Litauen 15 år for Tjekkiet, Grækenland og Frankrig 16 år for Tyskland, Ungarn, Kroatien, Irland, Luxembourg, Nederlandene, Polen, Rumænien og Slovakiet.

[61] Persondataforordningens artikel 9.

biometriske data eller sundhedsdata. Det gælder også for undtagelser i forbindelse med de registreredes rettigheder til forskningsmæssige formål[62], både med hensyn til omfanget af undtagelserne og de dertil knyttede garantier.

Databeskyttelsesrådets kommende retningslinjer for anvendelse af personoplysninger inden for videnskabelig forskning vil bidrage til en harmoniseret fremgangsmåde på dette område. Kommissionen vil komme med input til Databeskyttelsesrådet, navnlig for så vidt angår sundhedsforskning, herunder i form af konkrete spørgsmål og analyse af konkrete scenarier, som den har modtaget fra forskersamfundet. Det ville være nyttigt, om disse retningslinjer kunne vedtages inden lanceringen af Horisont Europa-rammeprogrammet med henblik på at harmonisere databeskyttelsespraksis og lette udvekslingen af data vedrørende forskningsresultater. Retningslinjer fra Databeskyttelsesrådet om behandling af personoplysninger på sundhedsområdet kunne også være nyttige.

Persondataforordningen udgør en solid ramme for national lovgivning på folkesundhedsområdet og omfatter udtrykkeligt grænseoverskridende sundhedstrusler og overvågning af epidemier og deres spredning[63], hvilket var relevant i forbindelse med bekæmpelsen af covid-19-pandemien.

På EU-plan vedtog Kommissionen den 8. april 2020 en henstilling om en fælles værktøjskasse med henblik på at udnytte teknik og data i denne forbindelse, herunder mobilapplikationer og anvendelse af anonymiserede mobilitetsdata[64], og den 16. april 2020 en vejledning om apps til støtte for bekæmpelse af pandemien i forbindelse med databeskyttelse[65]. I denne forbindelse offentliggjorde Databeskyttelsesrådet den 19. marts 2020 en erklæring om databehandling[66], efterfulgt den 21. april 2020 af retningslinjer om databehandling til forskningsformål og brug af lokaliseringsdata og kontaktopsporingsredskaber i forbindelse hermed[67]. Disse henstillinger og retningslinjer præciserer, hvordan principperne og reglerne for beskyttelse af personoplysninger finder anvendelse i forbindelse med bekæmpelsen af pandemien.

- Omfattende begrænsninger i registreredes rettigheder

De fleste nationale databeskyttelseslove, der begrænser den registreredes rettigheder, specificerer ikke de mål af almen offentlig interesse, der er sikret ved disse begrænsninger, og/eller opfylder ikke i tilstrækkelig grad de betingelser og garantier, der kræves i persondataforordningens artikel 23, stk. 2[68]. Flere medlemsstater giver ikke mulighed for en proportionalitetstest eller udvider restriktionerne selv ud over anvendelsesområdet for persondataforordningens artikel 23, stk. 1. For eksempel giver visse nationale love under henvisning til, at det vil kræve en uforholdsmæssig stor indsats fra den dataansvarliges side, ikke ret til adgang til personoplysninger, der lagres på grundlag af en opbevaringspligt eller i forbindelse med udførelsen af offentlige opgaver, uden at der sker en afgræsning af en sådan begrænsning til formål af generel samfundsinteresse.

- Yderligere krav til selskaber

Selv om kravet om en obligatorisk databeskyttelsesansvarlig er baseret på en risikobaseret tilgang[69], har én medlemsstat[70] udvidet den til et kvantitativt kriterium, der forpligter virksomheder, hvor mindst 20 medarbejdere er fast beskæftiget med automatiseret behandling af personoplysninger, til at udpege en

[62] Persondataforordningens artikel 89, stk. 2.
[63] Se persondataforordningens artikel 9, stk. 2, litra i), og betragtning 46.
[64] https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf.
[65] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020XC0417 (08) & from = EN.
[66] https://edpb.europa.eu/news/news/2020/statement-processing-personal-data-context-covid-19-outbreak_en.
[67] https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en.
[68] F.eks. fordi de blot gentager ordlyden af persondataforordningens artikel 23, stk. 1.
[69] Persondataforordningens artikel 37, stk. 1.
[70] Tyskland.

databeskyttelsesansvarlig. uafhængigt af de risici, der er forbundet med behandlingsaktiviteterne[71]. Dette har medført yderligere byrder.

4 SÆTTE ENKELTPERSONER I STAND TIL AT KONTROLLERE DERES DATA

Persondataforordningen bringer de grundlæggende rettigheder i anvendelse, navnlig retten til beskyttelse af personoplysninger, men også de andre grundlæggende rettigheder, der er anerkendt i chartret, herunder respekten for privatliv og familieliv, ytrings- og informationsfriheden, ikke-forskelsbehandling, retten til at tænke frit, samvittigheds- og religionsfriheden, friheden til at oprette og drive egen virksomhed og adgangen til effektive retsmidler. Disse rettigheder skal vejes op mod hinanden i overensstemmelse med proportionalitetsprincippet[72].

Persondataforordningen giver borgerne rettigheder, der kan håndhæves, såsom retten til indsigt, berigtigelse, sletning, indsigelse, portabilitet og øget gennemsigtighed. Det giver også enkeltpersoner ret til at indgive klage til en databeskyttelsesmyndighed, herunder gennem sager til varetagelse af forbrugerinteresser, og til domstolsprøvelse.

Borgerne er i stigende grad opmærksomme på deres rettigheder, som det fremgår af resultaterne af Eurobarometerundersøgelsen fra juli 2019[73] og undersøgelsen fra Agenturet for Grundlæggende Rettigheder[74].

Ifølge undersøgelsen om grundlæggende rettigheder foretaget af Agenturet for Grundlæggende Rettigheder:

- 69 % af befolkningen på 16 år og derover i EU har hørt om persondataforordningen
- 71 % af respondenterne i EU har hørt om deres nationale databeskyttelsesmyndighed; dette tal varierer fra 90 % i Tjekkiet til 44 % i Belgien
- 60 % af respondenterne i EU har kendskab til en lov, der gør det muligt for dem at få adgang til personoplysninger, som den offentlige forvaltning har om dem; denne procentsats falder dog til 51 % for private virksomheder
- mere end én ud af fem respondenter (23 %) i EU ønsker ikke at dele personoplysninger (f.eks. en persons adresse, statsborgerskab eller fødselsdato) med en offentlig administration, og 41 % ønsker ikke at dele disse data med private virksomheder.

Borgerne benytter sig i stigende grad af deres ret til at indgive klager til databeskyttelsesmyndigheder, enten individuelt eller gennem sager til varetagelse af forbrugerinteresser[75]. Kun nogle få medlemsstater har gjort det muligt for ikke-statslige organisationer at iværksætte foranstaltninger uden mandat i overensstemmelse med den mulighed, der er fastsat i persondataforordningen. Forslaget til direktiv om adgang til indbringelse af sager til varetagelse af forbrugernes kollektive interesser[76] vil, når det er vedtaget, styrke rammerne for sager til varetagelse af forbrugerinteresser, også på databeskyttelsesområdet.

Klager

Det samlede antal klager mellem maj 2018 og udgangen af november 2019 som indberettet af Databeskyttelsesrådet er ca. 275 000[77]. Dette tal bør dog tages med et gran salt, idet en klage ikke defineres

[71] Gøre brug af specifikationsbestemmelsen i persondataforordningens artikel 37, stk. 4.
[72] Jf. betragtning 4 i persondataforordningen.
[73] https://ec.europa.eu/commission/presscorner/detail/da/IP_19_2956
[74] Den Europæiske Unions Agentur for Grundlæggende Rettigheder (2020): Undersøgelse af grundlæggende rettigheder 2019. Databeskyttelse og teknologi: https://fra.europa.eu/en/publication/2020/fundamental-rights-survey-data-protection
[75] Persondataforordningens artikel 80.
[76] COM/2018/0184 final - 2018/089 (COD)
[77] Både i henhold til persondataforordningens artikel 77 og 80.

på samme måde af forskellige myndigheder. Det absolutte antal klager, som databeskyttelsesmyndigheder[78] modtager, er meget forskelligt fra medlemsstat til medlemsstat. Det største antal klager blev registreret i Tyskland (67 000), Nederlandene (37 000), Spanien og Frankrig (18 000 hver), Italien (14 000), Polen og Irland (med hver 12 000). To tredjedele af myndighederne rapporterede om mellem 8 000 og 600 klager. Det laveste antal klager blev registreret i Estland og Belgien (med hver ca. 500), Malta og Island (med hver under 200).

Antallet af klager modsvarer ikke nødvendigvis befolkningens størrelse eller BNP. F.eks. er der i Tyskland tæt på dobbelt så mange klager end i Nederlandene, og fire gange så mange klager som i Spanien og Frankrig.

Feedback fra flerpartsgruppen viser, at organisationer har iværksat en række foranstaltninger for at lette udøvelsen af de registreredes rettigheder, herunder gennemførelsesprocesser, der sikrer individuel behandling af anmodninger og svar fra den dataansvarlige, brug af flere kanaler (post, dedikeret e-mailadresse, websted osv.), ajourførte interne procedurer og politikker for rettidig intern behandling af anmodninger samt uddannelse af medarbejdere. Nogle virksomheder har indført digitale portaler, som kan tilgås via virksomhedens websted (eller selskabets intranet for medarbejdere) for at gøre det lettere for de registrerede at udøve deres rettigheder.

Der er dog behov for yderligere fremskridt på følgende punkter:

- Ikke alle dataansvarlige overholder deres forpligtelse til at lette udøvelsen af de registreredes rettigheder[79]. De skal sikre, at de registrerede har et effektivt kontaktpunkt, hvor de kan forklare om deres problemer. Dette kan være den databeskyttelsesansvarlige, hvis kontaktoplysninger skal gives proaktivt til den registrerede[80]. Kontaktmåderne må ikke være begrænset til e-mail, men skal også give den registrerede mulighed for at henvende sig til den dataansvarlige med andre midler.
- Enkeltpersoner støder fortsat på problemer, når de anmoder om adgang til deres data, f.eks. fra platforme, dataformidlere og AdTech-virksomheder.
- Retten til dataportabilitet udnyttes ikke fuldt ud. I den europæiske strategi for data (i det følgende benævnt "datastrategien")[81], som Kommissionen vedtog den 19. februar 2020, blev det understreget, at der er behov for at lette alle mulige anvendelser af denne ret (f.eks. ved at give mandat til tekniske grænseflader og maskinlæsbare formater, der tillader dataportabilitet i (nær) realtid). Erhvervsdrivende bemærker, at der undertiden er problemer med at levere dataene i et struktureret, almindeligt anvendt maskinlæsbart format (grundet manglende standarder). Det er kun organisationer i bestemte sektorer, f.eks. inden for bankvirksomhed, telekommunikation, vand- og varmemålere, der beretter, at de har oprettet de nødvendige grænseflader[82]. Der er udviklet nye teknologiske værktøjer, der skal gøre det lettere for personer at udøve deres rettigheder i henhold til persondataforordningen, der ikke er begrænset til dataportabilitet (f.eks. personlige dataområder og tjenester til forvaltning af personlige oplysninger).
- Børns rettigheder: Flere medlemmer af flerpartsgruppen understreger behovet for at give oplysninger til børn og det forhold, at mange organisationer ignorerer, at børn kan blive bekymret over behandlingen af deres personoplysninger. Rådet understregede, at man kunne være særlig opmærksom på beskyttelsen af

[78] Se Databeskyttelsesrådets bidrag, s. 31-32
[79] Persondataforordningens artikel 12, stk. 2.
[80] Persondataforordningens artikel 13, stk. 1, litra b), og artikel 14, stk. 1, litra b).
[81] https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf.
[82] Se flerpartsgruppens rapport.

børn ved udarbejdelsen af adfærdskodekser. Beskyttelse af børn er også et fokusområde for databeskyttelsesmyndigheder[83].

- Ret til information: nogle virksomheder har en meget legalistisk tilgang, idet de anser databeskyttelsesmeddelelser for at være en juridisk øvelse med oplysninger, der er ret komplekse, vanskelige at forstå eller ufuldstændige, hvorimod enhver information ifølge persondataforordningen skal være kortfattet, lettilgængelig og letforståelig[84]. Nogle virksomheder følger tilsyneladende ikke Databeskyttelsesrådets anbefalinger, f.eks. med hensyn til navnene på de enheder, som de deler data med.
- Flere medlemsstater har begrænset de registreredes rettigheder væsentligt gennem national ret, og nogle endda uden for den manøvremargen, der er fastsat i persondataforordningens artikel 23.
- Udøvelsen af enkeltpersoners rettigheder hindres af og til af nogle få store digitale aktørers praksis, som gør det vanskeligt for enkeltpersoner at vælge de indstillinger, der bedst beskytter deres privatliv (i strid med kravet om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger[85])[86].

Interessenterne venter utålmodigt på Databeskyttelsesrådets retningslinjer for registreredes rettigheder.

5 MULIGHEDER OG UDFORDRINGER FOR ORGANISATIONER, NAVNLIG SMÅ OG MELLEMSTORE VIRKSOMHEDER

Muligheder for organisationer

Persondataforordningen fremmer konkurrence og innovation. Sammen med forordningen om fri udveksling af andre data end personoplysninger[87] sikrer den fri udveksling af data inden for EU og skaber lige konkurrencevilkår for virksomheder, der ikke er etableret i EU. Ved at skabe en harmoniseret ramme for beskyttelse af personoplysninger sikrer persondataforordningen, at alle aktører på det indre marked er bundet af de samme regler og nyder samme muligheder, uanset om de er etableret, og hvor databehandlingen finder sted. Persondataforordningens teknologiske neutralitet skaber databeskyttelsesrammen for ny teknologisk udvikling. Principperne om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger tilskynder til innovative løsninger, som fra starten omfatter databeskyttelseshensyn og kan reducere omkostningerne ved overholdelse af databeskyttelsesreglerne.

Desuden bliver privatlivets fred en vigtig konkurrenceparameter, som personer i stigende grad tager med i deres overvejelser, når de skal vælge deres tjenester. Personer, der er mere informerede og opmærksomme på overvejelser om databeskyttelse, søger efter produkter og tjenesteydelser, der sikrer en effektiv beskyttelse af personoplysninger. Gennemførelsen af retten til dataportabilitet kan sikre virksomheder, der tilbyder innovative, databeskyttelsesvenlige tjenester, lettere adgang. Virkningerne af en potentielt bredere

---

[83] Se resultaterne af en offentlig høring om børns databeskyttelsesrettigheder, der blev gennemført af den irske databeskyttelsesmyndighed: https://www.dataprotection.ie/sites/default/files/uploads/2019-09/Whose%20Rights%20Are%20They%20Anyway_Trends%20and%20Hightlights%20from%20Stream%201.pdf. Ligeledes iværksatte den franske databeskyttelsesmyndighed en offentlig høring i april 2020: https://www.cnil.fr/fr/la-cnil-lance-une-consultation-publique-sur-les-droits-des-mineurs-dans-lenvironnement-numerique.

[84] Persondataforordningens artikel 12, stk. 1.

[85] Persondataforordningens artikel 25.

[86] Se rapport fra det norske forbrugerråd, Deceived by Design, som satte fokus på de "mørke mønstre", standardindstillinger og andre funktioner og teknikker, som virksomheder gør brug af for at puffe brugere i retning af indgribende løsninger: https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design/
Se også den forskning, der blev offentliggjort i december 2019 af Transatlantic Consumer Dialogue og Heinrich-Böll-Stiftung Brussels European Union, der analyserer praksis på tre store globale platforme: https://eu.boell.org/en/2019/12/11/privacy-eu-and-us-consumer-experiences-across-three-global-platforms.

[87] Europa-Parlamentets og Rådets forordning (EU) 2018/1807 af 14. november 2018 om en ramme for fri udveksling af andre data end personoplysninger i Den Europæiske Union (EUT L 303 af 28.11.2018, s. 59).

anvendelse af denne ret på markedet i forskellige sektorer bør overvåges. Overholdelse af databeskyttelsesreglerne og gennemskuelig anvendelse heraf vil skabe tillid til brugen af folks personoplysninger og dermed nye muligheder for virksomhederne.

I lighed med enhver anden regulering medfører databeskyttelsesreglerne overholdelsesomkostninger for virksomhederne. Disse omkostninger opvejes imidlertid af de muligheder og fordele, der ligger i at styrke tilliden til digital innovation og de samfundsmæssige fordele ved at respektere en grundlæggende rettighed. Ved at sikre lige vilkår og udstyre databeskyttelsesmyndighederne med det, de har brug for til at håndhæve reglerne effektivt, forhindrer persondataforordningen, at virksomheder, der ikke overholder reglerne, kan snylte på den tillid, der opbygges af dem, der følger reglerne.

Særlige udfordringer for små og mellemstore virksomheder (SMV'er)

Det er en almindelig opfattelse blandt interessenter, som også deles af Europa-Parlamentet, Rådet og databeskyttelsesmyndigheder, at anvendelsen af persondataforordningen skaber særlige udfordringer for mikrovirksomheder og små og mellemstore virksomheder, og for små frivillige og velgørende organisationer.

Ifølge den risikobaserede tilgang ville det ikke være hensigtsmæssigt at give mulighed for undtagelser baseret på operatørernes størrelse, da deres størrelse ikke i sig selv er en indikator for, hvilke risici deres databehandling kan medføre for personer. Den risikobaserede tilgang parrer fleksibilitet med effektiv beskyttelse. Den tager hensyn til behovene hos SMV'er, hvis hovedaktivitet ikke er behandling af personoplysninger, og justerer deres forpligtelser især med afsæt i sandsynligheden for og alvoren af de risici, der er forbundet med den specifikke databehandling, de udfører[88].

Databehandling, der indebærer en lille eller lav risiko, bør ikke behandles på samme måde som databehandling, der indebærer en høj risiko eller sker hyppigt – uafhængigt af størrelsen af den virksomhed, der udfører den. Derfor konkluderede udvalget, at "den risikobaserede tilgang, som lovgiveren har fremmet i teksten, under alle omstændigheder bør bibeholdes, da risiciene for de registrerede ikke afhænger af de dataansvarliges størrelse"[89]. Databeskyttelsesmyndighederne bør fuldt ud tage dette princip til sig, når de håndhæver persondataforordningen, helst med en fælles europæisk tilgang for ikke at skabe hindringer for det indre marked

Databeskyttelsesmyndighederne har udviklet flere værktøjer og har understreget, at de har til hensigt at forbedre dem yderligere. Nogle myndigheder har iværksat oplysningskampagner og vil endda afholde gratis "persondataforordningen-klasser" for SMV'er.

Eksempler på vejledning og værktøjer, som databeskyttelsesmyndigheder stiller til rådighed specifikt til SMV'er

- offentliggørelse af oplysninger til SMV'er
- seminarer for databeskyttelsesansvarlige og arrangementer for SMV'er, der ikke behøver at udpege en databeskyttelsesansvarlig
- interaktive vejledninger til støtte for SMV'er
- hotlines til konsultationer
- modeller for behandlingskontrakter og fortegnelser over behandlingsaktiviteter.

Databeskyttelsesrådets bidrag indeholder en beskrivelse af de aktiviteter, der udføres af databeskyttelsesmyndigheder[90].

[88] Persondataforordningens artikel 24, stk. 1.
[89] Se Databeskyttelsesrådets bidrag, s. 35.
[90] Se Databeskyttelsesrådets bidrag, s. 35-45.

Flere af de aktioner, der specifikt støtter SMV'er, har modtaget EU-støtte. Kommissionen ydede finansiel støtte i form af tilskud ad tre omgange på i alt 5 mio. EUR, hvor de seneste to specifikt havde til formål at hjælpe de nationale tilsynsmyndigheder i deres bestræbelser på at nå ud til personer og SMV'er. Som følge heraf blev der i 2018 tildelt 2 mio. EUR til ni databeskyttelsesmyndigheder til aktiviteter i 2018-2019 (Belgien, Bulgarien, Danmark, Ungarn, Litauen, Letland, Nederlandene, Slovenien og Island)[91], og i 2019 blev der tildelt 1 mio. EUR til fire databeskyttelsesmyndigheder til aktiviteter i 2020 (Belgien, Malta, Slovenien og Kroatien i partnerskab med Irland)92. Der vil i 2020 blive tildelt yderligere 1 mio. EUR.

Trods disse initiativer rapporterer SMV'er og nystartede virksomheder ofte om, at de kæmper med gennemførelsen af princippet om ansvarlighed, der er fastsat i persondataforordningen[93]. De gør især opmærksom på, at de ikke altid får tilstrækkelig vejledning og praktisk rådgivning fra de nationale databeskyttelsesmyndigheder, eller at den tid, det tager at få vejledning og råd, er for lang. Der har også været tilfælde, hvor myndighederne har været tilbageholdende med at gå ind i juridiske problemstillinger. Når SMV'er står over for sådanne situationer, henvender de sig ofte til eksterne rådgivere og advokater for at få dem til at tage sig af gennemførelsen af ansvarlighedsprincippet og den risikobaserede tilgang (herunder krav om gennemsigtighed, fortegnelser over databehandling og anmeldelser af brud på datasikkerheden). Dette kan også medføre yderligere omkostninger for dem.

Et specifikt problem er registreringen af behandlingsaktiviteter, som SMV'er og små sammenslutninger betragter som en tung administrativ byrde. Undtagelsen fra denne forpligtelse i persondataforordningens artikel 30, stk. 5, er ganske vist meget snæver. De bestræbelser, der er gjort for at overholde denne forpligtelse, bør dog ikke overvurderes. Hvis SMV'ers hovedaktivitet ikke involverer behandling af personoplysninger, kan sådanne fortegnelser være enkle og ikke byrdefulde. Det samme gælder for frivillige og andre foreninger. Det ville blive lettere at udarbejde sådanne forenklede fortegnelser ved hjælp af modeller for registreringer, således som det allerede er praksis hos nogle databeskyttelsesmyndigheder. Et grundlæggende krav i forbindelse med ansvarlighedsprincippet er, at alle, der behandler personoplysninger, under alle omstændigheder bør have et overblik over deres databehandling.

Udviklingen af praktiske redskaber på EU-niveau, såsom harmoniserede formularer til brug ved brud på datasikkerheden og forenklede fortegnelser over behandlingsaktiviteter, kan hjælpe SMV'er og små foreninger[94], hvis hovedaktivitet ikke fokuserer på behandling af personoplysninger, til at opfylde deres forpligtelser.

Forskellige erhvervssammenslutninger har gjort en indsats for at øge bevidstheden og informere deres medlemmer, f.eks. gennem konferencer og seminarer, der giver virksomheder oplysninger om de tilgængelige retningslinjer, eller ved at udvikle en tjeneste for medlemmerne for hjælp til beskyttelse af privatlivets fred. De melder også om et stigende antal seminarer, møder og arrangementer tilrettelagt af tænketanke og sammenslutninger af SMV'er om forhold, der vedrører persondataforordningen.

For at forbedre den frie bevægelighed for alle data i EU og sikre en konsekvent anvendelse af persondataforordningen og forordningen om fri udveksling af andre data end personoplysninger udsendte Kommissionen også en praktisk vejledning om regler for behandling af blandede datasæt, der består af både personoplysninger og andre data end personoplysninger; Den er især rettet mod SMV'er[95].

Værktøjskasse for virksomheder

---

91 https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/rec-rdat-trai- ag-2017.

92 https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules/eu-funding-supporting-implementation-gdpr_en.

93 Se rapporten fra flerpartsgruppen.

94 Se Rådets bidrag.

95 Meddelelse fra Kommissionen til Europa-Parlamentet og Rådet – Vejledning vedrørende forordningen om en ramme for fri udveksling af andre data end personoplysninger i Den Europæiske Union (COM/2019/250 final).

Persondataforordningen stiller værktøjer til rådighed, som kan hjælpe til med at påvise, at reglerne overholdes, f.eks. adfærdskodekser, certificeringsmekanismer og standardkontraktbestemmelser.

- Adfærdskodekser

Databeskyttelsesrådet har udstedt retningslinjer[96], der skal give støtte til og gøre det nemmere for "kodeksindehavere" at udarbejde, ændre eller udvide kodekser, og yde praktisk vejledning og hjælp til fortolkning. Disse retningslinjer præciserer også procedurerne for indgivelse, godkendelse og offentliggørelse af regler på både nationalt plan og EU-plan ved at fastsætte de minimumskrav, der skal opfyldes.

Interessenterne mener, at adfærdskodekser er meget nyttige værktøjer. Selv om mange kodekser gennemføres på nationalt plan, er en række EU-adfærdskodekser i øjeblikket under udarbejdelse (f.eks. vedrørende mobile sundhedsapps, sundhedsforskning i genomik, cloud computing, direkte markedsføring, forsikring, behandling gennem forebyggelse og rådgivningstjenester for børn)[97]. Erhvervsdrivende mener, at EU-dækkende adfærdskodekser bør indtage en mere fremtrædende plads, da de fremmer en ensartet anvendelse af persondataforordningen i alle medlemsstaterne.

Men adfærdskodekser kræver også tid og investeringer fra operatørerne, både i forbindelse med udviklingen af disse og med oprettelsen af de nødvendige uafhængige kontrolorganer. Repræsentanter for SMV'er understreger betydningen og nytten af adfærdskodekser, som er skræddersyet til deres situation, og som ikke medfører uforholdsmæssigt store omkostninger.

I konsekvens heraf har erhvervssammenslutninger i en række sektorer gennemført andre former for selvreguleringsværktøjer, såsom kodekser for god praksis eller vejledning. Selv om sådanne værktøjer kan give nyttige oplysninger, er de ikke godkendt af databeskyttelsesmyndigheder og kan ikke tjene som et redskab til at påvise overensstemmelse med persondataforordningen.

Rådet understreger, at adfærdskodekser skal lægge særlig vægt på behandlingen af børns data og sundhedsdata. Kommissionen støtter adfærdskodekser, der vil harmonisere strategien inden for sundhed og forskning og lette den grænseoverskridende behandling af personoplysninger[98]. Databeskyttelsesrådet er i færd med at godkende et udkast til akkrediteringskrav til organer for tilsyn med adfærdskodekser, således som en række databeskyttelsesmyndigheder har talt for[99]. Når tværnationale adfærdskodekser eller EU-adfærdskodekser er klar til at blive forelagt for databeskyttelsesmyndigheder til godkendelse, skal de sendes til høring i Databeskyttelsesrådet. En hurtig indførelse af tværnationale adfærdskodekser er særlig vigtig for områder, der omfatter behandling af betydelige datamængder (f.eks. cloud computing) eller følsomme data (f.eks. sundhed/forskning).

- Certificering

Certificering kan være et nyttigt instrument til at påvise overholdelse af specifikke krav i persondataforordningen. Det kan øge retssikkerheden for virksomheder og fremme persondataforordningen globalt.

Som påpeget i undersøgelsen om certificering, der blev offentliggjort i april 2019[100], bør målet være at fremme indførelsen af relevante ordninger. Udviklingen af certificeringsordninger i EU vil blive understøttet

---

[96] https://edpb.europa.eu/our-work-tools/our-documents/wytyczne/guidelines-12019-codes-conduct-and-monitoring-bodies-under_en.

[97] Se flerpartsgruppens rapport.

[98] Se de foranstaltninger, der er bebudet i den europæiske strategi for data, s. 30.

[99] I henhold til persondataforordningens artikel 41, stk. 3. Se Det Europæiske Databeskyttelsesråds udtalelser på: https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en.

[100] https://ec.europa.eu/info/study-data-protection-certification-mechanisms_en.

af de retningslinjer, som Databeskyttelsesrådet har udstedt om certificeringskriterier[101] og om akkreditering af certificeringsorganer[102].

Sikkerhed og databeskyttelse gennem design er vigtige elementer, som skal tages i betragtning i henhold til persondataforordningen, og til hvilke der med fordel kunne anlægges en fælles og ambitiøs tilgang i hele EU. Kommissionen vil fortsat støtte de nuværende kontakter mellem Den Europæiske Unions Agentur for Cybersikkerhed (ENISA), databeskyttelsesmyndighederne og Databeskyttelsesrådet.

Med hensyn til cybersikkerhed anmodede Kommissionen efter vedtagelsen af forordningen om cybersikkerhed om, at ENISA udarbejder to certificeringsordninger, herunder en ordning for cloudtjenester[103]. Yderligere ordninger, der vedrører cybersikkerhed af tjenester og produkter for forbrugerne, er under overvejelse. Selv om disse certificeringsordninger, der er oprettet i henhold til forordningen om cybersikkerhed, ikke udtrykkeligt omhandler databeskyttelse og privatlivets fred, bidrager de til at øge forbrugernes tillid til digitale tjenester og produkter. Sådanne ordninger kan dokumentere, at principperne om sikkerhed gennem design er overholdt, og at der er gennemført passende tekniske og organisatoriske foranstaltninger vedrørende sikkerheden i forbindelse med behandling af personoplysninger.

- Standardkontraktbestemmelser

Kommissionen arbejder i øjeblikket på standardkontraktbestemmelser mellem dataansvarlige og databehandlere,[104], også i lyset af moderniseringen af standardkontraktbestemmelserne for internationale overførsler (se afsnit 7.2). En EU-retsakt vedtaget af Kommissionen vil have bindende virkning for hele EU, hvilket vil sikre fuld harmonisering og retssikkerhed.

6 ANVENDELSEN AF PERSONDATAFORORDNINGEN PÅ NYE TEKNOLOGIER

En teknologineutral ramme åben for nye teknologier

Persondataforordningen er teknologineutral, tillidsfremmende og baseret på principper[105]. Disse principper, herunder lovlig og gennemskuelig databehandling, formålsbegrænsning og dataminimering, udgør et solidt grundlag for beskyttelse af personoplysninger, uanset hvilken behandlingsaktivitet og hvilke teknikker der anvendes.

Medlemmer af flerpartsgruppen rapporterer, at persondataforordningen generelt har en positiv indvirkning på udviklingen af nye teknologier og udgør et godt grundlag for innovation. Persondataforordningen betragtes som et væsentligt og fleksibelt redskab til at sikre udviklingen af nye teknologier i overensstemmelse med de grundlæggende rettigheder. Gennemførelsen af dens hovedprincipper er særlig vigtig i forbindelse med dataintensiv behandling. Persondataforordningens risikobaserede og teknologineutrale tilgang sikrer et databeskyttelsesniveau, der er tilstrækkeligt til at håndtere risikoen ved databehandling, herunder gennem nye teknologier.

Interessenter nævner navnlig, at persondataforordningens principper om formålsbegrænsning og yderligere forenelig databehandling, dataminimering, opbevaringsbegrænsning, gennemsigtighed, ansvarlighed og

[101] https://edpb.europa.eu/our-work-tools/our-documents/smjernice/guidelines-12018-certification-and-identifying-certification_en.

[102] https://edpb.europa.eu/our-work-tools/our-documents/retningslinjer/guidelines-42018-accreditation-certification-bodies_da. Flere tilsynsmyndigheder har allerede indsendt deres akkrediteringskrav til Databeskyttelsesrådet, både for så vidt angår tilsynsorganer for adfærdskodekser og for certificeringsorganer. Se oversigten på: https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en.

[103] https://ec.europa.eu/digital-single-market/en/news/towards-more-secure-and-trusted-cloud-europe

[104] Persondataforordningens artikel 28, stk. 7.

[105] Som anført af Rådet, Europa-Parlamentet og Databeskyttelsesrådet i deres bidrag til evalueringen.

betingelserne for, at automatiske beslutningsprocesser[106] kan anvendes lovligt, i stort omfang imødekommer de bekymringer, der er forbundet med brugen af kunstig intelligens.

Den fremtidssikrede og risikobaserede tilgang i persondataforordningen vil også blive anvendt i de mulige fremtidige rammer for kunstig intelligens og i forbindelse med gennemførelsen af datastrategien. Datastrategien har til formål at fremme tilgængeligheden af data og oprette fælles europæiske dataområder, der understøttes af centrale cloudinfrastrukturtjenester. Med hensyn til personoplysninger udgør persondataforordningen det vigtigste retsgrundlag, inden for hvilket der kan udvikles effektive løsninger fra sag til sag afhængigt af arten og indholdet af hvert enkelt dataområde.

Persondataforordningen har øget bevidstheden om beskyttelsen af personoplysninger både i og uden for EU og har fået virksomhederne til at tilpasse deres praksis for at tage hensyn til databeskyttelsesprincipperne i forbindelse med innovation. Civilsamfundsorganisationer bemærker imidlertid, at selv om persondataforordningen synes at indvirke positivt på udviklingen af nye teknologier, har de store digitale aktørers praksis endnu ikke ændret sig grundlæggende i retning af en databehandling, der bedre sikrer privatlivets fred. En stringent og effektiv håndhævelse af persondataforordningen over for store digitale platforme og integrerede virksomheder, herunder på områder som onlinereklame og mikromålretning, er et væsentligt element i beskyttelsen af enkeltpersoner.

Kommissionen er i færd med at analysere de bredere problemstillinger i relation til de store digitale aktørers adfærd på markedet inden for rammerne af pakken om digitale tjenester[107]. Med hensyn til forskning inden for sociale medier minder Kommissionen om, at persondataforordningen ikke kan bruges som undskyldning for sociale medieplatforme til at begrænse forskeres og faktatjekkeres adgang til andre data end personoplysninger, f.eks. statistikker, som er brugt som grundlag for målrettede annoncer til visse kategorier af personer, kriterierne for at udforme denne målretning, oplysninger om falske konti osv.

Persondataforordningens teknologineutrale og fremtidssikrede tilgang blev sat på prøve under covid-19-pandemien og har vist sig at være en succes. Dens principbaserede regler støttede udviklingen af værktøjer til bekæmpelse og overvågning af spredningen af virusset.

Udfordringer

Udviklingen og anvendelsen af nye teknologier sætter ikke spørgsmålstegn ved disse principper. Udfordringerne ligger i at præcisere, hvordan man anvender de etablerede principper på brugen af specifikke teknologier såsom kunstig intelligens, blockchain, tingenes internet, ansigtsgenkendelse eller kvantedatabehandling.

I denne forbindelse understregede Europa-Parlamentet og Rådet behovet for en løbende overvågning for at præcisere, hvordan persondataforordningen finder anvendelse på nye teknologier og store teknologivirksomheder. Desuden advarer interessenter om, at vurderingen af, hvorvidt persondataforordningen fortsat er egnet til formålet, også kræver konstant overvågning.

Interessenter fra industrien understreger, at innovation kræver, at persondataforordningen anvendes på en principbaseret måde i overensstemmelse med dens udformning snarere end på en usmidig og formel måde. De er af den opfattelse, at Databeskyttelsesrådets retningslinjer for anvendelsen af principperne i persondataforordningen, begreber og regler for nye teknologier såsom kunstig intelligens, blockchain eller tingenes internet, hvor der tages hensyn til den risikobaserede tilgang, vil bidrage til at skabe klarhed og skabe større retssikkerhed. Sådanne værktøjer med "blød" lovgivning er velegnede til at følge, hvordan persondataforordningen anvendes på de nye teknologier, da de giver større retssikkerhed og kan revideres i takt med den teknologiske udvikling. Nogle interessenter foreslår også, at sektorspecifik vejledning om, hvordan persondataforordningen skal anvendes på nye teknologier, kan være nyttig.

---

[106] Nogle interessenter bemærker imidlertid, at ikke alle automatiske beslutningsprocesser i forbindelse med kunstig intelligens falder ind under persondataforordningens artikel 22.

[107] https://ec.europa.eu/commission/presscorner/detail/da/ip_20_962.

Databeskyttelsesrådet har anført, at det fortsat vil tage hensyn til de nye teknologiers indvirkning på beskyttelsen af personoplysninger.

Nogle interessenter understreger også, at det er vigtigt for reguleringsmyndighederne at få en grundig forståelse af, hvordan teknologien anvendes, og til at indgå i en dialog med erhvervslivet om udviklingen af nye teknologier. De mener, at en tilgang, hvor forordningen bruges som en "reguleringsmæssig sandkasse" – dvs. som en måde at få en rettesnor for anvendelsen af reglerne – kunne være en interessant mulighed for at afprøve nye teknologier og hjælpe virksomhederne med at anvende princippet om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger i nye teknologier.

Med hensyn til yderligere politiske tiltag anbefaler interessenter, at alle fremtidige forslag til en politik om kunstig intelligens bør baseres på de eksisterende retsgrundlag og bringes i overensstemmelse med persondataforordningen. Potentielle specifikke forhold bør vurderes nøje på grundlag af relevant dokumentation, før der stilles nye forslag om konkrete forskrifter.

Kommissionens hvidbog om kunstig intelligens foreslår en række politiske løsningsmodeller, som interessenter blev bedt om at forholde sig til frem til den 14. juni 2020. For så vidt angår ansigtsgenkendelse, som er en teknologi, der kan påvirke den enkelte persons rettigheder væsentligt, mindede hvidbogen om det eksisterende retsgrundlag og iværksatte en offentlig debat om, hvorvidt der eventuelt er særlige omstændigheder, der kan berettige anvendelsen af kunstig intelligens med henblik på biometrisk fjernidentifikation på offentlige steder, og om fælles garantier.

7 INTERNATIONALE OVERFØRSLER OG GLOBALT SAMARBEJDE

7.1 Privatlivets fred: et globalt problem

Kravet om beskyttelse af personoplysninger kender ingen grænser, da fysiske personer i hele verden i stigende grad værdsætter og værner om privatlivets fred og sikkerhed for deres data.

Samtidig er betydningen af overførsel af oplysninger for enkeltpersoner, regeringer, virksomheder og mere generelt samfundet som helhed en uundgåelig kendsgerning i vores indbyrdes forbundne verden. De er en fast bestanddel af samhandelen, samarbejdet mellem offentlige myndigheder og de sociale interaktioner. I den forbindelse sætter den aktuelle covid-19-pandemi også fokus på, hvor kritisk overførsel og udveksling af personoplysninger er for mange vigtige aktiviteter, herunder sikring af kontinuitet i de offentlige og erhvervslivets aktiviteter – ved at muliggøre fjernarbejde og andre løsninger, der er stærkt afhængige af informations- og kommunikationsteknologier, udvikling af samarbejde om videnskabelig forskning i diagnosticering, behandlinger og vacciner og bekæmpelse af nye former for cyberkriminalitet, herunder onlinesvindel, hvor der tilbydes falske lægemidler, der hævder at forebygge eller helbrede covid-19.

På denne baggrund skal beskyttelsen af privatlivets fred og fremme af overførsel af oplysninger mere end nogensinde gå hånd i hånd. EU står med sin databeskyttelsesordning, der kombinerer åbenhed over for internationale overførsler med et højt beskyttelsesniveau for enkeltpersoner, godt rustet til at fremme sikre overførsel af oplysninger. Persondataforordningen er allerede blevet et centralt referencepunkt på internationalt plan og har fået mange lande i hele verden til at overveje at indføre moderne regler for beskyttelse af privatlivets fred.

Det er i sandhed en universel tendens, der pågår, for blot at nævne nogle eksempler fra Chile til Sydkorea, fra Brasilien til Japan, fra Kenya til Indien, fra Tunesien til Indonesien og fra Californien til Taiwan. Denne udvikling er bemærkelsesværdig ikke blot i en mængdemæssig, men også kvalitativ synsvinkel: mange af de bestemmelser om privatlivets fred, der for nylig er blevet vedtaget, eller som er ved at blive vedtaget, er baseret på et sæt fælles garantier, rettigheder og håndhævelsesmekanismer, der deles af EU. I en verden, som alt for ofte er kendetegnet ved forskellige, endog afvigende, reguleringsmæssige tilgange, udgør denne tendens i retning af global konvergens en meget positiv udvikling, som giver nye muligheder for bedre

beskyttelse af enkeltpersoner i Europa, samtidig med at der sikres lettere overførsel af oplysninger, og operatørernes transaktionsomkostninger reduceres.

For at gribe disse muligheder og gennemføre den strategi, der er beskrevet i meddelelsen fra 2017 om udveksling og beskyttelse af personoplysninger i en globaliseret verden"[108], har Kommissionen i væsentlig grad optrappet sit arbejde vedrørende den internationale dimension af privatlivets fred ved at gøre fuld brug af den tilgængelige "værktøjskasse", jf. nedenfor. Dette omfattede aktivt samarbejde med vigtige partnere med henblik på at nå frem til en "afgørelse om et tilstrækkeligt beskyttelsesniveau", og der blev opnået vigtige resultater såsom skabelsen af verdens største område med frie og sikre overførsler af oplysninger mellem EU og Japan.

Ud over indsatsen for at sikre et tilstrækkeligt beskyttelsesniveau har Kommissionen arbejdet tæt sammen med databeskyttelsesmyndighederne i Databeskyttelsesrådet samt med andre interessenter for at udnytte det fulde potentiale i persondataforordningen for internationale overførsler. Dette vedrører modernisering af instrumenter såsom standardkontraktbestemmelser, udvikling af certificeringsordninger, adfærdskodekser eller administrative ordninger for dataudveksling mellem offentlige myndigheder, samt en præcisering af nøglebegreber vedrørende f.eks. det territoriale anvendelsesområde for EU's databeskyttelsesregler eller anvendelsen af såkaldte "undtagelser" til overførsel af personoplysninger.

Endelig har Kommissionen intensiveret sin dialog i en række bilaterale, regionale og multilaterale fora for at fremme en global kultur med respekt for privatlivets fred og udvikle en række elementer, der skal sikre konvergens mellem forskellige private systemer til beskyttelse af privatlivets fred. Kommissionen har i sin indsats kunnet støttet sig til aktiv støtte fra EU-Udenrigstjenesten og nettet af EU-delegationer i tredjelande og missioner ved internationale organisationer. Dette har også gjort det muligt at skabe større sammenhæng og komplementaritet mellem de forskellige aspekter af den eksterne dimension af EU's politikker – fra handel til det nye partnerskab mellem EU og Afrika.

7.2 Værktøjskassen for overførsler i persondataforordningen

I takt med at flere og flere private og offentlige operatører er afhængige af internationale overførsler af oplysninger som led i deres rutineoperationer, er der et stigende behov for fleksible instrumenter, der kan tilpasses forskellige sektorer, forretningsmodeller og overførselssituationer. For at afspejle disse behov giver persondataforordningen mulighed for en moderniseret værktøjskasse til at lette overførslen af personoplysninger fra EU til et tredjeland eller en international organisation, samtidig med at det sikres, at oplysningerne fortsat er omfattet af et højt beskyttelsesniveau. Denne kontinuitet i beskyttelse er vigtig i betragtning af, at det i dag er let at flytte data på tværs af grænserne, og den beskyttelse, der sikres ved persondataforordningen, ville være ufuldstændig, hvis den var begrænset til behandling inden for EU.

Med kapitel V i persondataforordningen bekræftede lovgiveren arkitekturen i de overførselsregler, der allerede eksisterede i henhold til direktiv 95/46: dataoverførsler kan finde sted, hvis Kommissionen har truffet en afgørelse om et tilstrækkeligt beskyttelsesniveau over for et tredjeland eller en international organisation, eller, hvis dette ikke er sket, hvis den dataansvarlige eller databehandleren i EU ("dataeksportør") har stillet tilstrækkelige garantier, f.eks. gennem en kontrakt med modtageren ("dataimportøren"). Desuden er de lovmæssige begrundelser for overførsler (såkaldte "undtagelser") fortsat tilgængelige i særlige situationer, hvor lovgiveren har besluttet, at afvejningen mellem interesser gør det muligt at overføre data på visse betingelser. Samtidig har reformen præciseret og forenklet de eksisterende regler, f.eks. ved at præcisere betingelserne for en afgørelse om tilstrækkeligt beskyttelsesniveau eller bindende virksomhedsregler, ved at begrænse godkendelseskravene til meget få, specifikke tilfælde og

[108] Meddelelse fra Kommissionen til Europa-Parlamentet og Rådet om udveksling og beskyttelse af personoplysninger i en globaliseret verden", (COM (2017) 7 final af 10.1.2017).

fuldstændigt ophæve anmeldelseskravene. Desuden er der indført nye overførselsværktøjer såsom adfærdskodekser eller certificeringsordninger, og mulighederne for at anvende eksisterende instrumenter (f.eks. standardkontraktbestemmelser) er blevet udvidet.

Den digitale økonomi i dag giver udenlandske operatører mulighed for (på afstand, men) direkte at deltage i EU's indre marked og konkurrere om europæiske kunder og deres personoplysninger. Hvis de specifikt er rettet mod europæere gennem udbud af varer eller tjenester eller overvågning af deres adfærd, bør de overholde EU-retten på samme måde som EU-operatører. Dette afspejles i persondataforordningens artikel 3, som udvider den direkte anvendelse af EU's databeskyttelsesregler til visse dataansvarliges eller databehandleres behandlingsaktiviteter uden for EU. Dette sikrer de nødvendige garantier og desuden lige vilkår for alle virksomheder, der opererer på EU-markedet.

Dens brede rækkevidde er en af grundene til, at virkningerne af persondataforordningen også er blevet mærkbare i andre dele af verden. Den detaljerede vejledning, der udsendes af Databeskyttelsesrådet efter en omfattende offentlig høring, er derfor vigtig for at hjælpe udenlandske operatører med at afgøre, om og hvilke behandlingsaktiviteter der er direkte underlagt dens garantier, herunder ved at give konkrete eksempler [109].

Udvidelsen af EU-databeskyttelseslovgivnings anvendelsesområde er imidlertid ikke i sig selv tilstrækkelig til at sikre, at den overholdes i praksis. Som Rådet også har fremhævet[110], er det afgørende at sikre, at udenlandske operatører overholder reglerne, og at de er omfattet af en effektiv håndhævelse. Udpegelsen af en repræsentant i EU (persondataforordningens artikel 27, stk. 1, stk. 2), som enkeltpersoner og tilsynsmyndigheder kan henvende sig til ud over eller i stedet for den ansvarlige virksomhed, der arbejder fra udlandet[111], bør spille en central rolle i denne forbindelse. Denne fremgangsmåde, som også tages mere og mere i brug i andre sammenhænge[112], bør følges mere energisk for at sende et klart budskab om, at manglende etablering i EU ikke fritager udenlandske operatører for deres ansvar i henhold til persondataforordningen. Hvis disse operatører ikke opfylder deres forpligtelse til at udpege en repræsentant[113], bør tilsynsmyndighederne gøre brug af den fulde håndhævelsesværktøjskasse i persondataforordningens artikel 58 (f.eks. offentlige advarsler, midlertidige eller endelige forbud mod behandling i EU, håndhævelse over for fælles dataansvarlige, der er etableret i EU).

Endelig er det meget vigtigt, at Databeskyttelsesrådet færdiggør sit arbejde med yderligere præcisering af forholdet mellem artikel 3 om den direkte anvendelse af persondataforordningen og reglerne om internationale overførsler i kapitel V[114].

Afgørelser om tilstrækkeligheden af beskyttelsesniveauet

Input fra interessenter bekræfter, at afgørelser om tilstrækkeligheden af beskyttelsesniveauet fortsat er et vigtigt værktøj for EU's operatører til at overføre personoplysninger til tredjelande på en sikker måde[115].

---

[109] Databeskyttelsesrådet, Retningslinjer 2/2018 om det territoriale anvendelsesområde for databeskyttelsesforordningen, 12.11.2019. Retningslinjerne omhandler flere af de punkter, der blev rejst under den offentlige høring, f.eks. fortolkningen af målretningen og overvågningskriterierne.

[110] Se Rådets holdning og resultater, stk. 34, 35 og 38.

[111] Se artikel 27, stk. 4, og betragtning 80 i persondataforordningen ("Den udpegede repræsentant bør være underlagt håndhævelsesforanstaltninger i tilfælde af manglende overholdelse fra den dataansvarliges eller databehandlerens side").

[112] Forslag til Europa-Parlamentets og Rådets direktiv om harmoniserede regler for udpegning af retlige repræsentanter med henblik på indsamling af bevismateriale i straffesager (COM(2018) 226 final), artikel 3. Forslag til Europa-Parlamentets og Rådets forordning om forebyggelse af udbredelse af terrorrelateret onlineindhold (COM(2018) 640 final), artikel 16, stk. 2, stk. 3.

[113] Ifølge ét indlæg til den offentlige høring er et af de hovedpunkter, der skal behandles, "effektiv håndhævelse og reelle konsekvenser for dem, der har valgt at ignorere dette krav [...]. Det bør navnlig tages i betragtning, at dette også stiller virksomheder, der er etableret i Unionen, ringere i konkurrencen end virksomheder, der ikke opfylder kravene, og som er etableret uden for EU og handler i Unionen." Se EU Business Partners, indlæg af 29. april 2020.

[114] Flere indlæg i den offentlige høring har rejst dette spørgsmål, f.eks. for så vidt angår videregivelse af personoplysninger til modtagere uden for EU, men omfattet af persondataforordningen.

Sådanne afgørelser sikrer den mest omfattende, enkle og omkostningseffektive løsning for dataoverførsler, da de sidestilles med overførsler inden for EU, hvilket sikrer sikker og fri udveksling af personoplysninger uden yderligere betingelser eller krav om tilladelse. Afgørelser om tilstrækkeligheden af beskyttelsesniveauet åbner derfor de kommercielle kanaler for EU-operatører og letter samarbejdet mellem offentlige myndigheder, samtidig med at der gives privilegeret adgang til EU's indre marked. Med udgangspunkt i praksis ifølge direktivet fra 1995 giver persondataforordningen udtrykkeligt mulighed for at træffe en afgørelse om tilstrækkelighed med hensyn til et bestemt område i et tredjeland eller til en bestemt sektor eller industri i et tredjeland (den såkaldte "delvise" tilstrækkelighed).

Persondataforordningen bygger på erfaringerne fra de seneste år og på de præciseringer, som Domstolen har givet, ved at udarbejde et detaljeret katalog over elementer, som Kommissionen skal tage hensyn til i sin vurdering. Tilstrækkelighedsstandarden kræver et beskyttelsesniveau, der er sammenligneligt (eller "i det væsentlige svarer til") det beskyttelsesniveau, der sikres i EU[116]. Dette indebærer en omfattende vurdering af det pågældende tredjelands system som helhed, herunder indholdet af beskyttelse af privatlivets fred, effektiv gennemførelse og håndhævelse samt regler om offentlige myndigheders adgang til personoplysninger, navnlig med henblik på retshåndhævelse og den nationale sikkerhed[117].

Dette afspejles også i den vejledning, der blev vedtaget af den tidligere artikel 29-Gruppe (og godkendt af Databeskyttelsesrådet), navnlig "referencen vedrørende et tilstrækkeligt beskyttelsesniveau", som yderligere præciserer de elementer, som Kommissionen skal tage hensyn til, når den foretager en tilstrækkelighedsvurdering, herunder ved at give et overblik over "væsentlige garantier" for offentlige myndigheders adgang til personoplysninger[118]. Sidstnævnte bygger navnlig på Den Europæiske Menneskerettighedsdomstols retspraksis. Selv om standarden "væsentlig ækvivalens" ikke indebærer en ordret kopiering ("fotokopi") af EU's regler, fordi midlerne til at sikre et sammenligneligt beskyttelsesniveau kan variere mellem forskellige privatlivssystemer, der ofte afspejler forskellige retstraditioner, kræver det ikke desto mindre et stærkt beskyttelsesniveau.

Denne standard er begrundet i, at en afgørelse om tilstrækkeligheden af beskyttelsesniveauet i alt væsentligt udvider fordelene ved det indre marked til et tredjeland, for så vidt angår den frie udveksling af data. Det betyder dog også, at der undertiden vil være relevante forskelle mellem det beskyttelsesniveau, der sikres i det pågældende tredjeland, og persondataforordningen, der skal udlignes, f.eks. gennem forhandling af yderligere garantier. Sådanne garantier bør behandles positivt, da de yderligere styrker den beskyttelse, der findes for enkeltpersoner i EU. Samtidig er Kommissionen enig med Databeskyttelsesrådet i betydningen af løbende at overvåge deres anvendelse i praksis, herunder effektiv håndhævelse fra tredjelandes databeskyttelsesmyndigheds side[119].

I persondataforordningen præciseres det, at afgørelser om tilstrækkeligheden af beskyttelsesniveauet er "levende instrumenter", som løbende bør overvåges og revideres med jævne mellemrum[120]. I

---

[115] Rådets holdning og resultater, stk. 17 Databeskyttelsesrådets bidrag, s. 5-6. Flere indlæg i den offentlige høring, herunder fra en række erhvervssammenslutninger (f.eks. den franske sammenslutning af store selskaber, Digital Europe, Global Data Alliance/BSA, Computer & Communication Industry Association (CCIA) eller det amerikanske handelskammer), har opfordret til at intensivere indsatsen, hvad angår afgørelser om tilstrækkelighed, især med vigtige handelspartnere.

[116] EU-Domstolens dom af 6.10.2015, sag C-362/14, Maximillian Schrems mod Data Protection Commissioner (herefter "Maximillian Schrems "), præmis 73, 74 og 96. Se ligeledes betragtning 104 i persondataforordningen, som henviser til standarden for grundlæggende ækvivalens.

[117] Artikel 45, stk. 2, og betragtning 104 i persondataforordningen. Se ligeledes *Schrems*, præmis 75, 91-91.

[118] Reference vedrørende et tilstrækkeligt beskyttelsesniveau, WP 254, rev. 01, 6.2.2018 (findes på: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108).

[119] Se Databeskyttelsesrådets bidrag, s. 5-6.

[120] I henhold til persondataforordningens artikel 45, stk. 4, og 5, overvåger Kommissionen løbende udviklingen i tredjelande og gennemgår regelmæssigt – mindst hvert fjerde år – afgørelser om tilstrækkeligheden af beskyttelsesniveauet. De giver også Kommissionen beføjelse til at ophæve, ændre eller suspendere en afgørelse om tilstrækkeligheden af beskyttelsesniveauet, hvis den finder, at det pågældende land eller den pågældende internationale organisation ikke længere sikrer et tilstrækkeligt beskyttelsesniveau. I henhold til persondataforordningens artikel 97, stk. 2, litra a), skal Kommissionen desuden forelægge en

overensstemmelse med disse krav fører Kommissionen regelmæssige drøftelser med de relevante myndigheder for proaktivt at følge op på nye udviklinger. Siden vedtagelsen af afgørelsen om EU's og USA's værn om privatlivets fred i 2016[121] har Kommissionen sammen med repræsentanter for Databeskyttelsesrådet foretaget tre årlige revisioner for at evaluere alle aspekter af rammens funktion[122]. Disse undersøgelser er baseret på oplysninger indhentet gennem udvekslinger med de amerikanske myndigheder samt input fra andre interessenter, f.eks. EU's databeskyttelsesmyndigheder, civilsamfundet og brancheorganisationer. De har gjort det muligt at forbedre den praktiske anvendelse af forskellige elementer i rammen. I et bredere perspektiv bidrog de årlige gennemgange til at etablere en bredere dialog med de amerikanske myndigheder om beskyttelse af privatlivets fred i almindelighed og de begrænsninger og garantier, der gælder med hensyn til den nationale sikkerhed i særdeleshed.

Som led i sin første evaluering af persondataforordningen skal Kommissionen også revidere de afgørelser om tilstrækkeligheden af beskyttelsesniveauet, der blev vedtaget i henhold til direktivet fra 1995[123]. Kommissionens tjenestegrene er gået i intens dialog med hvert af de 11 berørte lande og territorier med henblik på at vurdere, hvordan deres systemer for beskyttelse af personoplysninger har udviklet sig, siden afgørelsen om tilstrækkeligheden af beskyttelsesniveauet blev vedtaget, og om de opfylder den standard, der er fastsat i persondataforordningen. Behovet for at sikre kontinuitet i sådanne afgørelser, da de er et vigtigt redskab for handel og internationalt samarbejde, er en af de faktorer, der har fået flere af disse lande og territorier til at modernisere og styrke deres lovgivning om privatlivets fred. Dette er helt klart en positiv udvikling. Der drøftes yderligere beskyttelsesforanstaltninger med nogle af disse lande og territorier for at tage højde for relevante forskelle i beskyttelsen.

Da Domstolen imidlertid kan tænkes at give nærmere anvisninger i en dom, der forventes afsagt den 16. juli i en sag, og som kan være relevante for visse elementer af tilstrækkelighedsstandarden, vil Kommissionen særskilt aflægge rapport om evalueringen af de nævnte 11 afgørelser om tilstrækkeligheden af beskyttelsesniveauet, efter at Domstolen har afsagt dom i denne sag[124].

Kommissionen gennemførte også den strategi, der blev fastlagt i meddelelsen fra 2017 om udveksling og beskyttelse af personoplysninger i en globaliseret verden[125].

---

evalueringsrapport for Europa-Parlamentet og Rådet senest i 2020. Se også EU-Domstolens dom af 6.10.2015, sag C-362/14, Maximillian Schrems mod Data Protection Commissioner, præmis 76.

[121] Kommissionens gennemførelsesafgørelse (EU) 2016/1250 af 12. juli 2016 i henhold til Europa-Parlamentets og Rådets direktiv 95/46/EF om tilstrækkeligheden af den beskyttelse, der opnås ved hjælp af EU's og USA's værn om privatlivets fred. Denne afgørelse om tilstrækkeligheden af beskyttelsesniveauet er et specifikt tilfælde, som i mangel af en generel databeskyttelseslovgivning i USA er afhængigt af tilsagn fra deltagende virksomheder (som kan håndhæves under amerikansk lovgivning) om anvendelse af de databeskyttelsesstandarder, der er fastsat i denne ordning. Desuden bygger værnet om privatlivets fred på de specifikke udredninger og garantier, som den amerikanske regering har afgivet med hensyn til adgang til nationale sikkerhedsformål, som understøtter konstateringen af et tilstrækkeligt beskyttelsesniveau.

[122] Revisionen fandt sted i 2017 (Rapport fra Kommissionen til Europa-Parlamentet og Rådet om den første årlige evaluering af EU's og USA's værn om privatlivets fred (COM (2017) 611 final), 2018 (Rapport fra Kommissionen til Europa-Parlamentet og Rådet om den anden årlige evaluering af EU's og USA's værn om privatlivets fred (COM (2018) 860 final) og 2019 (Rapport fra Kommissionen til Europa-Parlamentet og Rådet om den tredje årlige evaluering af EU's og USA's værn om privatlivets fred (COM (2019) 495 final).

[123] Disse eksisterende afgørelser om tilstrækkeligheden af beskyttelsesniveauet vedrører lande, der er tæt integreret med Den Europæiske Union og dens medlemsstater (Schweiz, Andorra, Færøerne, Guernsey, Jersey, Isle of Man), vigtige samhandelspartnere (f.eks. Argentina, Canada og Israel) og lande, der har spillet en pionerrolle i udviklingen af databeskyttelseslove i deres område (New Zealand, Uruguay).

[124] Sag C-311/18, Data Protection Commissioner mod Facebook Ireland Limited, Maximillian Schrems ("Schrems II"), vedrører en anmodning om en præjudiciel afgørelse om de såkaldte standardkontraktbestemmelser. Der er dog visse elementer af tilstrækkelighedsstandarden, der også kan blive afklaret yderligere af Domstolen. Retsmødet i denne sag fandt sted den 9.7.2019, og dommen er blevet offentliggjort den 16.7.2020.

[125] Se fodnote 109 ovenfor. Kommissionen forklarede , at der vil blive taget hensyn til følgende kriterier ved vurderingen af, med hvilke lande der bør indledes en dialog om tilstrækkeligheden: i) omfanget af EU's (faktiske eller potentielle) handelsforbindelser med tredjelandet, herunder eksistensen af en frihandelsaftale eller igangværende forhandlinger ii) omfanget af strømmene af personoplysninger fra EU, der afspejler geografiske og/eller kulturelle bånd iii) tredjelandets

Dette arbejde har allerede givet betydelige resultater, der involverer vigtige partnere i EU. I januar 2019 vedtog Kommissionen sin afgørelse om tilstrækkeligheden af beskyttelsesniveauet for Japan, som er baseret på en høj grad af konvergens, herunder gennem specifikke beskyttelsesforanstaltninger, f.eks. med hensyn til videreoverførsel, og gennem oprettelsen af en mekanisme til at undersøge og løse borgeres klager vedrørende statens adgang til personoplysninger til retshåndhævelsesformål og til nationale sikkerhedsformål.

Som den første afgørelse om tilstrækkeligheden af beskyttelsesniveauet, der blev vedtaget i henhold til persondataforordningen, danner de rammer, der er aftalt med Japan, en nyttig præcedens for fremtidige afgørelser[126]. Dette omfatter det forhold, at det blev gengældt fra japansk side med en afgørelse om tilstrækkeligheden af beskyttelsesniveauet for EU. Tilsammen skaber disse gensidige afgørelser om tilstrækkelighed det største område med sikker og fri overførsel af oplysninger i verden og supplerer den økonomiske partnerskabsaftale mellem EU og Japan. Ordningen er hvert år til støtte for handel med varer for omkring 124 mia. EUR og for handel med tjenesteydelser for 42,5 mia. EUR.

Tilstrækkelighedsprocessen er også kommet langt i Sydkorea. Et vigtigt resultat heraf er Sydkoreas nylige lovgivningsreform, der førte til oprettelsen af en uafhængig databeskyttelsesmyndighed, der er udstyret med omfattende håndhævelsesbeføjelser. Dette illustrerer, hvordan en dialog om tilstrækkelighed kan bidrage til øget konvergens mellem EU's og et tredjelands databeskyttelsesregler.

Kommissionen er helt enig i opfordringen fra interessenter til at intensivere dialogen med udvalgte tredjelande med henblik på eventuelle nye afgørelser om tilstrækkeligheden af beskyttelsesniveauet[127]. Den er aktivt gået i gang med at undersøge denne mulighed med andre vigtige partnere på grundlag af den nuværende tendens til en opadgående global konvergens inden for databeskyttelsesstandarder. F.eks. er den omfattende lovgivning om privatlivets fred blevet vedtaget eller er langt fremme i lovgivningsprocessen i Latinamerika (Brasilien, Chile), og udviklingen tegner lovende i Asien (f.eks. Indien, Indonesien, Malaysia, Sri Lanka, Taiwan og Thailand), Afrika (f.eks. Etiopien og Kenya) samt i de østeuropæiske og sydlige nabolande (f.eks. Georgien og Tunesien). Hvor det er muligt, vil Kommissionen arbejde på at opnå omfattende afgørelser om tilstrækkelighed, der omfatter både den private og den offentlige sektor[128].

Desuden blev Kommissionens mulighed for at vedtage afgørelser om tilstrækkeligheden af beskyttelsesniveauet for internationale organisationer også indført i persondataforordningen. Nu, hvor nogle internationale organisationer er i færd med at modernisere deres databeskyttelsesordninger ved at indføre omfattende regler, samt mekanismer, der sikrer uafhængig kontrol og klageadgang, kunne denne mulighed undersøges for første gang.

---

pionerrolle inden for beskyttelse af privatlivets fred og databeskyttelse, der kunne tjene som model for andre lande i regionen og iv) de overordnede politiske forbindelser med tredjelandet, navnlig i forbindelse med fremme af fælles værdier og fælles mål på internationalt plan.

[126] Europa-Parlamentets beslutning af 13. december 2018 om tilstrækkeligheden af den beskyttelse af personoplysninger, der gives af Japan (2018/2979 (RSP)), punkt 27 Databeskyttelsesrådets bidrag, s. 5-6.

[127] Se f.eks. Europa-Parlamentet, beslutning af 12. december 2017 om udvikling af en digital handelsstrategi (2017/2065 (INI)), punkt 8 og 9 Rådets holdning og resultater vedrørende anvendelse af den generelle forordning om databeskyttelse (GDPR), 19.12.2019 (14994/1/19), punkt 17 Databeskyttelsesrådets bidrag, s. 5.

[128] Jf. også Rådets anmodning herom, se Rådets holdning og resultater vedrørende anvendelse af den generelle forordning om databeskyttelse (GDPR), 19.12.2019 (14994/1/19), punkt 17 og 40. Dette kræver dog, at betingelserne for en afgørelse om tilstrækkeligheden af beskyttelsesniveauet vedrørende dataoverførsler til offentlige myndigheder er opfyldt, herunder med hensyn til et uafhængigt tilsyn.

Tilstrækkelighed spiller ligeledes en vigtig rolle i sammenhæng med forholdet til Det Forenede Kongerige efter brexit, forudsat at de gældende betingelser opfyldes. Den udgør en faktor for fremme af handel, herunder digital handel, og er en afgørende forudsætning for et tæt og ambitiøst samarbejde om retshåndhævelse og sikkerhed[129]. I betragtning af betydningen af overførsel af oplysninger til Det Forenede Kongerige og landets nærhed til EU-markedet er en høj grad af konvergens mellem databeskyttelsesreglerne på begge sider af Kanalen desuden et vigtigt element for at sikre lige konkurrencevilkår. I overensstemmelse med den politiske erklæring om det fremtidige forhold mellem EU og Det Forenede Kongerige foretager Kommissionen i øjeblikket en tilstrækkelighedsvurdering i henhold til både persondataforordningen og direktivet om retshåndhævelse[130]. I betragtning af den selvstændige og ensidige karakter af en tilstrækkelighedsvurdering følger disse forhandlinger et særskilt spor i forhold til forhandlingerne om en aftale om det fremtidige forhold mellem EU og Det Forenede Kongerige.

Endelig har Kommissionen med tilfredshed bemærket, at andre lande er i færd med at indføre mekanismer til dataoverførsel, der minder om en afgørelse om tilstrækkeligheden af beskyttelsesniveauet. I den forbindelse anerkender de ofte EU og de lande, for hvilke Kommissionen har vedtaget en afgørelse om tilstrækkeligheden af beskyttelsesniveauet, som sikre destinationer for overførslers[131]. Det stigende antal lande, der drager fordel af EU's afgørelser om tilstrækkeligheden af beskyttelsesniveauet på den ene side og denne form for anerkendelse fra andre lande på den anden side, har potentiale til at skabe et netværk af lande, hvor data kan flyde frit og sikkert. Kommissionen anser dette for at være en velkommen udvikling, der yderligere vil øge fordelene ved en afgørelse om tilstrækkeligheden af beskyttelsesniveauet for tredjelande og bidrage til global konvergens. Denne type synergier kan også med fordel bidrage til at udvikle rammer for sikker og fri udveksling af data, f.eks. i forbindelse med initiativet "Data Free Flow with Trust" (se nedenfor).

Fornødne garantier

Persondataforordningen indeholder bestemmelser om en række andre overførselsinstrumenter ud over den omfattende løsning med en afgørelse om tilstrækkeligheden af beskyttelsesniveauet. Fleksibiliteten i denne "værktøjskasse" fremgår af persondataforordningens artikel 46, som regulerer dataoverførsler baseret på "passende garantier", herunder rettigheder, der kan håndhæves, og effektive retsmidler. For at sikre passende sikkerhedsforanstaltninger er der forskellige instrumenter til rådighed til at imødekomme både kommercielle aktørers og offentlige organers behov for overførsler.

- Standardkontraktbestemmelser

Den første gruppe af disse instrumenter vedrører aftalemæssige redskaber, der kan være enten skræddersyede, ad hoc-databeskyttelsesklausuler aftalt mellem en dataeksportør i EU og en dataimportør uden for EU, der er godkendt af den kompetente databeskyttelsesmyndighed (persondataforordningens artikel 46, stk. 3, litra a)), eller standardbestemmelser, som Kommissionen har godkendt (persondataforordningens artikel 46, stk. 2, litra c), d)[132]). De vigtigste af disse instrumenter er såkaldte

[129] Se forhandlingsdirektiverne i bilaget til Rådets afgørelse om bemyndigelse til at indlede forhandlinger med Det Forenede Kongerige Storbritannien og Nordirland om en ny partnerskabsaftale (ST 5870/20 ADD 1 REV 3), punkt 13 og 118.

[130] Se den reviderede politiske erklæring om rammen for de fremtidige forbindelser mellem Den Europæiske Union og Det Forenede Kongerige, som der var opnået enighed om på forhandlerniveau den 17. oktober 2019, punkt 8-10 (findes på https://ec.europa.eu/commission/sites/beta-political/files/revised_political_declaration.pdf).

[131] F.eks. fra Argentina, Colombia, Israel, Schweiz eller Uruguay.

[132] Standardkontraktbestemmelser for internationale overførsler kræver altid Kommissionens godkendelse, men kan udarbejdes af Kommissionen selv eller af en national databeskyttelsesmyndighed. Alle eksisterende standardkontraktbestemmelser falder ind under den første kategori.

standardkontraktbestemmelser, dvs. standardbestemmelser om databeskyttelse, som dataeksportøren og dataimportøren kan indarbejde i deres aftalemæssige ordninger (f.eks. en tjenesteydelseskontrakt, der kræver videregivelse af personoplysninger) på frivillig basis, og som fastsætter de krav, der er forbundet med de fornødne garantier.

Standardkontraktbestemmelser udgør langt den mest udbredte dataoverførselsmekanisme[133]. Tusindvis af virksomheder i EU er afhængige af standardkontraktbestemmelser for at levere en bred vifte af tjenester til deres kunder, leverandører, partnere og ansatte, herunder tjenesteydelser, der er af afgørende betydning for, at økonomien kan fungere. Deres brede anvendelse tyder på, at de er meget nyttige for virksomhederne i deres bestræbelser på at sikre deres overholdelse, og at de især er til fordel for virksomheder, der ikke har ressourcerne til at forhandle individuelle kontrakter med hver enkelt af deres samhandelspartnere. Gennem standardisering og forhåndsgodkendelse giver standardkontraktbestemmelser virksomhederne adgang til et værktøj, der er let at gennemføre for at opfylde databeskyttelseskravene i forbindelse med en overførsel.

De eksisterende standardkontraktbestemmelser[134] er blevet vedtaget og godkendt på grundlag af direktivet fra 1995. Disse standardkontraktbestemmelser forbliver i kraft, indtil de ændres, erstattes eller ophæves, om nødvendigt ved en kommissionsafgørelse (persondataforordningens artikel 46, stk. 5). Persondataforordningen udvider mulighederne for at anvende standardkontraktbestemmelser både i EU og i forbindelse med internationale overførsler. Kommissionen arbejder sammen med interessenterne for at udnytte disse muligheder og ajourføre eksisterende bestemmelser[135]. For at sikre, at den fremtidige udformning af standardkontraktbestemmelser er egnet til formålet, har Kommissionen indsamlet feedback om interessenternes erfaringer med standardkontraktbestemmelser gennem flerpartsgruppen vedrørende persondataforordningen og en særlig workshop, der blev afholdt i september 2019, men også via flere kontakter med virksomheder, der anvender standardkontraktbestemmelser, samt civilsamfundsorganisationer. Databeskyttelsesrådet ajourfører ligeledes en række retningslinjer, der kunne være relevante for revisionen af standardkontraktbestemmelser, f.eks. med hensyn til begreberne dataansvarlig og databehandler.

På grundlag af den modtagne feedback arbejder Kommissionens tjenestegrene i øjeblikket på at revidere standardkontraktbestemmelserne. I den forbindelse er der fundet en række områder, hvor der er behov for forbedringer, navnlig med hensyn til følgende aspekter:

1. Ajourføring af standardkontraktbestemmelserne i lyset af de nye krav, der er indført ved persondataforordningen, f.eks. vedrørende forholdet mellem dataansvarlig og databehandler i henhold til persondataforordningens artikel 28(navnlig databehandlerens forpligtelser), dataimportørens gennemsigtighedsforpligtelser (med hensyn til de påkrævede oplysninger til den registrerede) osv.
2. Håndtering af en række overførselsscenarier, som ikke er omfattet af de nuværende standardkontraktbestemmelser, f.eks. overførsel af data fra en databehandler i EU til en

[133] Ifølge rapporten IAPP-EY Annual Privacy Governance Report 2019 er de mest populære af disse værktøjer [for overførsler] – år for år – i helt overvældende omfang standardkontraktbestemmelser: 88 % af respondenterne i dette års undersøgelse berettede, at standardkontraktbestemmelser var den bedste metode til eksterritoriale dataoverførsler, efterfulgt af overensstemmelse med EU's og USA's værn om privatlivets fred (60 %). Med hensyn til data, der overføres fra EU til Det Forenede Kongerige (52 %), har 91 % af respondenterne til hensigt at bruge standardkontraktbestemmelser til dataoverførsel efter

[134] Der findes i dag tre standardkontraktbestemmelser, som Kommissionen har vedtaget vedrørende overførsel af personoplysninger til tredjelande: to for overførsler fra en dataansvarlig i EØS til en dataansvarlig uden for EØS og én for overførsler fra en dataansvarlig EØS til en databehandler uden for EØS. De blev ændret i 2016 efter Domstolens dom i Schrems I-sagen (C-362/14), der fjernede enhver begrænsning af de kompetente tilsynsmyndigheders beføjelser til at føre tilsyn med dataoverførsler. Se https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

[135] Se også Databeskyttelsesrådets bidrag, s. 6-7. Tilsvarende har Rådet opfordret Kommissionen til i nær fremtid at gennemgå og revidere [standardkontraktbestemmelserne] for at tage hensyn til dataansvarliges og databehandleres behov. Se Rådets holdning og resultater.

(under-)databehandler uden for EU, men også situationer, hvor den dataansvarlige befinder sig uden for EU[136].

3. Bedre hensyntagen til de faktiske forhold i forbindelse med databehandling i den moderne digitale økonomi, hvor sådanne operationer ofte involverer flere dataimportører og -eksportører, lange og ofte komplekse behandlingskæder, nye forretningsforbindelser osv. For at tage højde for sådanne situationer omfatter de løsninger, der undersøges i øjeblikket, f.eks. muligheden for, at flere parter underskriver standardkontraktbestemmelser, eller at nye parter får adgang i kontraktens løbetid.

Ved behandlingen af disse punkter overvejer Kommissionen også, hvordan den nuværende "arkitektur" kan gøres mere brugervenlig, f.eks. ved at erstatte flere sæt standardkontraktbestemmelser med et enkelt omfattende dokument. Udfordringen består i at finde en god balance mellem på den ene side behovet for klarhed og en vis grad af standardisering og på den anden side den nødvendige fleksibilitet, der gør det muligt for operatører med forskellige krav at anvende bestemmelserne i forskellige sammenhænge og for forskellige typer af overførsler.

Et andet vigtigt aspekt, der skal tages i betragtning, er, at der i lyset af de verserende retssager ved Domstolen[137], kan blive behov for yderligere at præcisere garantierne for udenlandske offentlige myndigheders adgang til oplysninger, der videregives på grundlag af standardkontraktbestemmelser, navnlig af hensyn til den nationale sikkerhed. Dette kan omfatte krav om, at dataimportøren eller dataeksportøren, eller begge, skal træffe foranstaltninger, og at databeskyttelsesmyndighedernes rolle i den forbindelse præciseres. Selv om revisionen af standardkontraktbestemmelserne er langt fremme, vil det være nødvendigt at afvente Domstolens dom for at tage hensyn til eventuelle yderligere krav i de reviderede bestemmelser, før et udkast til afgørelse om et nyt sæt standardkontraktbestemmelser kan forelægges for Databeskyttelsesrådet til udtalelse og derefter foreslås vedtaget gennem "udvalgsproceduren"[138].

Sideløbende hermed er Kommissionen i kontakt med internationale partnere, der er i færd med at udvikle lignende værktøjer[139]. Denne dialog, der gør det muligt at udveksle erfaringer og bedste praksis, kan i væsentlig grad bidrage til udvikling af yderligere konvergens i praksis og derved lette overholdelsen af reglerne om grænseoverskridende overførsler for virksomheder, der opererer på tværs af forskellige regioner i verden.

- Bindende virksomhedsregler

Et andet vigtigt instrument er de såkaldte bindende virksomhedsregler. Her er der tale om juridisk bindende politikker og ordninger, der gælder for medlemmerne af en koncern, herunder dennes ansatte (persondataforordningens artikel 46, stk. 2, litra b), og artikel 47). Anvendelsen af bindende virksomhedsregler tillader fri bevægelighed for personoplysninger mellem de forskellige koncernmedlemmer globalt – idet behovet for at indgå kontraktordninger mellem hver enkelt juridisk enhed undgås – samtidig med at det sikres, at det samme høje beskyttelsesniveau for personoplysninger overholdes i hele koncernen. De udgør en særlig god løsning for komplekse og store koncerner og for et tæt samarbejde

[136] Flere indlæg til den offentlige høring indeholder kommentarer til dette sidste scenario, og der er ofte udtrykt bekymring over, at et krav om, at databehandlere i EU sikrer passende garantier i deres forhold til dataansvarlige uden for EU, ville stille dem ringere i konkurrencen i forhold til udenlandske databehandlere, der tilbyder lignende tjenester.

[137] Se Schrems II-sagen.

[138] I overensstemmelse med artikel 46, stk. 2, litra c), i persondataforordningen skal standardkontraktbestemmelser vedtages efter undersøgelsesproceduren i artikel 5 i Europa-Parlamentets og Rådets forordning (EU) nr. 182/2011 af 16. februar 2011 om de generelle regler og principper for, hvordan medlemsstaterne skal kontrollere Kommissionens udøvelse af gennemførelsesbeføjelser (EUT L 55 af 28.2.2011, s. 13). Dette indebærer navnlig en positiv afgørelse fra et udvalg sammensat af repræsentanter for medlemsstaterne.

[139] Dette omfatter f.eks. det arbejde, der i øjeblikket udføres af ASEAN's medlemsstater for at udvikle "ASEAN-standardkontraktbestemmelser". Se ASEAN, Key Approaches for ASEAN Cross Border Data Flows Mechanism (findes på: https://asean.org/storage/2012/05/Key-Approaches-for-ASEAN-Cross-Border-Data-Flows-Mechanism.pdf).

mellem virksomheder, der udveksler data på tværs af flere jurisdiktioner. I modsætning til direktivet fra 1995 kan bindende virksomhedsregler anvendes af en gruppe af virksomheder, der udøver en fælles økonomisk aktivitet, men som ikke indgår i samme koncern.

Proceduremæssigt skal de bindende virksomhedsregler godkendes af de kompetente databeskyttelsesmyndigheder på grundlag af en ikkebindende udtalelse fra Databeskyttelsesrådet[140]. For at styre denne proces har Databeskyttelsesrådet gennemgået referencedataene for de bindende virksomhedsregler (fastsættelse af materielle standarder) for dataansvarlige[141] og databehandlere[142] i lyset af persondataforordningen og ajourfører disse dokumenter fortløbende på grundlag af tilsynsmyndighedernes praktiske erfaringer. Det har ligeledes vedtaget forskellige vejledninger for hjælpe ansøgere og for at strømline ansøgnings- og godkendelsesprocessen for bindende virksomhedsregler[143]. Ifølge Databeskyttelsesrådet er der i øjeblikket over 40 bindende virksomhedsregler på vej til godkendelse, hvoraf halvdelen forventes at blive godkendt inden udgangen af 2020[144]. Det er vigtigt, at databeskyttelsesmyndighederne fortsætter arbejdet med at strømline godkendelsesprocessen yderligere, da varigheden af sådanne procedurer ofte nævnes af interessenterne som en praktisk hindring for en bredere anvendelse af bindende virksomhedsregler.

Hvad angår bindende virksomhedsregler, der er godkendt af den britiske databeskyttelsesmyndighed, Information Commissioner Office, vil virksomheder kunne fortsætte med at anvende dem som en gyldig overførselsmekanisme i henhold til persondataforordningen efter udløbet af overgangsperioden under udtrædelsesaftalen mellem EU og Det Forenede Kongerige, men kun hvis de ændres, således at enhver forbindelse til Det Forenede Kongeriges retsorden erstattes med passende henvisninger til juridiske enheder og kompetente myndigheder i EU. Der bør indhentes godkendelse af nye bindende virksomhedsregler af en af tilsynsmyndighederne i EU.

- Certificeringsordninger og adfærdskodekser

Ud over at modernisere og udvide anvendelsen af de allerede eksisterende overførselsværktøjer er der ved persondataforordningen også indført nye instrumenter, hvilket har udvidet mulighederne for internationale overførsler. Dette omfatter, på visse betingelser, anvendelse af godkendte adfærdskodekser og certificeringsmekanismer (f.eks. datasikkerhedsmærkninger) med henblik på at sikre passende garantier. Dette er bottom-up-værktøjer, der giver mulighed for skræddersyede løsninger – som en generel ansvarlighedsmekanisme (se persondataforordningens artikel 40-42) og specifikt for internationale overførsler af oplysninger – og afspejler f.eks. de specifikke karakteristika og behov i en given sektor eller industri, eller med hensyn til overførsel af oplysninger. Adfærdskodekser kan også være en meget nyttig og omkostningseffektiv måde for små og mellemstore virksomheder at leve op til deres forpligtelser på i henhold til persondataforordningen.

Databeskyttelsesrådet har vedtaget retningslinjer, der skal fremme brugen af certificeringsmekanismer i EU, samtidig med at det fortsætter sit arbejde med at udvikle kriterier for godkendelse af disse som internationale overførselsværktøjer. Det samme gælder adfærdskodekser, hvor Databeskyttelsesrådet i øjeblikket arbejder på retningslinjer for anvendelsen af disse som overførselsværktøj.

I betragtning af betydningen af at give operatører en bred vifte af overførselsværktøjer, der er tilpasset deres behov, og det potentiale der ligger i navnlig certificeringsmekanismer, der gør det lettere at foretage

---

[140] Se https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en for en oversigt over de udtalelser, som Databeskyttelsesrådet har afgivet til dato.

[141] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614109.

[142] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614110.

[143] Disse dokumenter blev vedtaget (af den tidligere artikel 29-Gruppe) efter persondataforordningens ikrafttræden, men før overgangsperiodens udløb. Se WP263 (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623056); WP264 (https://edpb.europa.eu/sites/edpb/files/files/file2/wp264_art29_wp_bcr-c_application_form.pdf); WP265 (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623848).

[144] Databeskyttelsesrådets bidrag, s. 7.

dataoverførsler, samtidig med at der sikres et højt databeskyttelsesniveau, opfordrer Kommissionen indtrængende Databeskyttelsesrådet til så hurtigt som muligt at færdiggøre sin vejledning herom. Dette vedrører både materielle (kriterier) og proceduremæssige aspekter (godkendelse, overvågning osv.). Interessenter har udtrykt stor interesse for disse overførselsmekanismer og burde være i stand til at gøre fuld brug af persondataforordningen. Databeskyttelsesrådets retningslinjer vil også bidrage til at fremme EU's model for databeskyttelse på globalt plan og fremme konvergens, da andre systemer til beskyttelse af privatlivets fred anvender lignende instrumenter.

Der kan drages nyttige erfaringer fra eksisterende standardiseringsbestræbelser inden for privatlivets fred, både på europæisk og internationalt plan. Et interessant eksempel er den nyligt offentliggjorte internationale standard ISO 27701[145], som har til formål at hjælpe virksomheder med at leve op til krav om privatlivsbeskyttelse og med at håndtere risici i forbindelse med behandling af personoplysninger ved hjælp af informationsforvaltningssystemer for privatlivsbeskyttelse. Selv om certificering i henhold til standarden ikke opfylder kravene i persondataforordningens artikel 42 og 43, kan anvendelsen af informationsstyringssystemer bidrage til ansvarlighed, herunder i forbindelse med internationale dataoverførsler.

- Internationale aftaler og administrative ordninger

Persondataforordningen gør det også muligt at sikre de fornødne garantier for dataoverførsler mellem offentlige myndigheder eller organer på grundlag af internationale aftaler (artikel 46, stk. 2, litra a)) eller administrative ordninger (artikel 46, stk. 3, litra b)). Selv om begge instrumenter skal sikre samme resultat med hensyn til garantier, herunder tilgængelighed af rettigheder, som kan håndhæves, for registrerede og effektive retsmidler, er de forskellige med hensyn til deres retlige karakter og vedtagelsesproceduren.

I modsætning til internationale aftaler, som skaber bindende forpligtelser i henhold til folkeretten, er administrative ordninger (f.eks. i form af et aftalememorandum) typisk ikkebindende og kræver derfor forudgående tilladelse fra den kompetente databeskyttelsesmyndighed (se også betragtning 108 i persondataforordningen). Et tidligt eksempel er den administrative ordning for overførsel af personoplysninger mellem tilsynsmyndigheder inden for EØS og tilsynsmyndigheder uden for EØS, der samarbejder inden for rammerne af Den Internationale Børstilsynsorganisation (IOSCO), som Databeskyttelsesrådet afgav udtalelse[146] om i begyndelsen af 2019. Siden da har Databeskyttelsesrådet videreudviklet sin fortolkning af de "minimumsgarantier", som internationale (samarbejds-)aftaler og administrative ordninger mellem offentlige myndigheder eller organer (herunder internationale organisationer) skal sikre for at opfylde kravene i persondataforordningens artikel 46. Den 18. januar 2020 vedtog det et udkast til retningslinjer[147], der behandler medlemsstaternes anmodning om yderligere præcisering og vejledning om, hvad der kan betragtes som fornødne garantier for overførsler mellem offentlige myndigheder[148]. Udvalget anbefaler stærkt, at offentlige myndigheder anvender disse retningslinjer som referencepunkt for deres forhandlinger med tredjeparter[149].

---

[145] Listen over specifikke krav, der indgår i denne ISO-standard, findes på: https://www.iso.org/standard/71670.html.

[146] Det Europæiske Databeskyttelsesråd, Udtalelse 4/2019 om udkast til administrativ ordning for overførsel af personoplysninger mellem Det Europæiske Økonomiske Samarbejdsområde (EØS) og de finansielle tilsynsmyndigheder uden for EØS, 12.2.2019.

[147] Det Europæiske Databeskyttelsesråd, Retningslinjer 2/2020 om artikel 46 (2), litra a), og artikel 46 (3), litra b), i forordning (EF) nr. 2016/679 om overførsel af personoplysninger mellem myndigheder i EØS og offentlige myndigheder og organer uden for EØS (udkast findes på: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-22020-articles-46-2-and-46-3-b_en). Ifølge Det Europæiske Databeskyttelsesråd vil den kompetente tilsynsmyndighed basere sin undersøgelse på de generelle anbefalinger i disse retningslinjer, men kan også anmode om flere garantier afhængigt af den konkrete sag. Databeskyttelsesrådet fremsendte disse udkast til retningslinjer i offentlig høring, der sluttede den 18. maj 2020.

[148] Rådets holdning og resultater, punkt 20.

[149] Med hensyn til valget af instrument understreger Databeskyttelsesrådet samtidig, at offentlige myndigheder fortsat frit kan henholde sig til andre relevante værktøjer, der giver de fornødne garantier i overensstemmelse med persondataforordningens artikel 46. Med hensyn til valg af instrument understreger Databeskyttelsesrådet, at det bør vurderes nøje, om der skal gøres

Retningslinjerne demonstrerer, hvor fleksibel udformningen af sådanne instrumenter er, herunder vigtige aspekter som f.eks. tilsyn[150] og klageadgang[151]. Dette burde give de offentlige myndigheder mulighed for at overvinde vanskelighederne ved f.eks. at sikre, at de registreredes rettigheder kan håndhæves ved hjælp af ikkebindende ordninger. Et vigtigt element i sådanne ordninger er den kompetente databeskyttelsesmyndigheds fortsatte overvågning – understøttet af oplysnings- og registreringskrav – og suspension af overførsel af oplysninger, hvis der ikke længere kan sikres de fornødne garantier i praksis.

Undtagelser

Endelig præciseres det i persondataforordningen, at der anvendes såkaldte "undtagelser". Der er tale om særlige grunde til videregivelse af oplysninger (f.eks. udtrykkeligt samtykke[152], opfyldelse af en kontrakt eller af hensyn til vigtige samfundsinteresser), der er anerkendt ved lov, og som enheder kan henholde sig til, hvis der ikke findes andre overførselsværktøjer, og på visse betingelser.

For at præcisere anvendelsen af sådanne retlige grunde har Databeskyttelsesrådet udstedt specifikke retningslinjer[153] og har fortolket artikel 49 i en række tilfælde med hensyn til specifikke overførselsscenarier[154]. På grund af deres usædvanlige karakter mener Databeskyttelsesrådet, at undtagelserne skal fortolkes restriktivt i hvert enkelt tilfælde. Trods en streng fortolkning dækker disse begrundelser en bred vifte af overførselsscenarier. Dette omfatter navnlig overførsel af oplysninger både fra offentlige myndigheder og private enheder af hensyn til "vigtige samfundsinteresser", f.eks. mellem konkurrencemyndigheder, skatte- eller toldforvaltninger, finansielle tilsynsmyndigheder eller socialsikringsmyndigheder eller med henblik på folkesundhed (f.eks. i tilfælde af kontaktopsporing i forbindelse med smitsomme sygdomme eller for at nedbringe og/eller afskaffe doping inden for sport)[155]. Et andet område er grænseoverskridende samarbejde med henblik på strafferetlig håndhævelse, navnlig hvad angår grov kriminalitet[156].

---

brug af administrative ordninger, der ikke er juridisk bindende, for at tilvejebringe garantier i den offentlige sektor, i betragtning af formålet med behandlingen og arten af de foreliggende oplysninger. Hvis databeskyttelsesrettigheder og klageadgang for borgere i EØS ikke er forankret i tredjelandets nationale ret, bør indgåelsen af en juridisk bindende aftale fremmes. Uanset hvilken type retsakt der er tale om, skal de gældende foranstaltninger være effektive for at sikre passende gennemførelse, håndhævelse og tilsyn (punkt 67).

150 Dette kan f.eks. omfatte en kombination af intern kontrol (med en forpligtelse til at underrette den anden part om tilfælde af manglende overholdelse, med uafhængigt tilsyn gennem eksterne eller i det mindste ved hjælp af funktionelt uafhængige mekanismer, samt muligheden for at det overførende offentlige organ kan suspendere eller afslutte overførslen.

151 Dette kan for eksempel omfatte kvasiretlige, bindende mekanismer (f.eks. voldgift) eller alternative tvistbilæggelsesmekanismer, kombineret med muligheden for at den overførende offentlige myndighed kan suspendere eller afslutte overførslen af personoplysninger, hvis det ikke lykkes parterne at bilægge en tvist i mindelighed, plus et tilsagn fra det modtagende offentlige organ om at returnere eller slette personoplysningerne. Ved valget af alternative klagemekanismer, som er bindende og kan håndhæves, fordi der ikke er mulighed for at sikre en effektiv retlig prøvelse, anbefaler Databeskyttelsesrådet, at den kompetente tilsynsmyndighed høres, inden disse instrumenter indgås.

152 Dette er en ændring i forhold til direktiv 95/46, som kun krævede "utvetydigt" samtykke. Desuden gælder de generelle krav til samtykke i henhold til persondataforordningens artikel 4, stk. 11.

153 Det Europæiske Databeskyttelsesråd, Retningslinjer 2/2018 vedrørende undtagelser i artikel 49 i forordning (EF) nr. 2016/679, 25.5.2018 (findes på: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf).

154 Dette omfatter f.eks. internationale overførsler af sundhedsdata til forskningsformål i forbindelse med covid-19-udbruddet. Se Det Europæiske Databeskyttelsesråd, Retningslinjer 03/2020 om behandling af helbredsoplysninger med henblik på videnskabelig forskning i forbindelse med covid-19-udbruddet, 21.4.2020 (findes på: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf).

155 Se betragtning 112.

156 Se amicus curiae-indlæg fra Europa-Kommissionen på vegne af Den Europæiske Union til støtte for ingen af parterne i sag US mod Microsoft, s. 15: Generelt anerkender EU-lovgivningen såvel som medlemsstaternes lovgivning betydningen af at bekæmpe grov kriminalitet og dermed strafferetlig håndhævelse og internationalt samarbejde på det pågældende område, som et mål af almen interesse. [...] artikel 83 i TEUF identificerer flere kriminalitetsområder, der er særligt alvorlige og har grænseoverskridende dimensioner, såsom ulovlig narkotikahandel.(findes på: (findes på: https://www.supremecourt.gov/DocketPDF/17/17-2/23655/20171213123137791_17-2%20ac%20European%20Commission%20for%20filing.pdf).

Databeskyttelsesrådet har præciseret, at selv om den relevante samfundsinteresse skal anerkendes i EU-retten eller en medlemsstats nationale ret, kan dette også fastslås på grundlag af, at "en international aftale eller konvention, der anerkender et bestemt formål og indeholder bestemmelser om internationalt samarbejde til fremme af dette formål, kan være en indikator ved vurderingen af eksistensen af samfundsinteresser i henhold til artikel 49, stk. 1, litra d), når EU eller medlemsstaterne er part i den pågældende aftale eller konvention"[157].

Afgørelser truffet af udenlandske domstole eller myndigheder: ingen grund til overførsler

Ud over en positiv fastsættelse af grundene til overførsel af oplysninger præciseres det kapitel V i persondataforordningen ligeledes, i artikel 48, at retsafgørelser eller administrative myndigheders afgørelser uden for EU ikke i sig selv er legitime grunde til overførsler, medmindre de anerkendes eller kan håndhæves på grundlag af en international aftale (f.eks. en traktat om gensidig retshjælp). Enhver videregivelse fra den ansøgte instans til den udenlandske domstol eller myndighed som svar på en sådan dom eller afgørelse udgør en international overførsel af oplysninger, der skal baseres på et af de nævnte overførselsinstrumenter[158].

Persondataforordningen udgør ikke en "blokerende bestemmelse" og vil på visse betingelser tillade en overførsel som reaktion på en passende anmodning om håndhævelse fra et tredjeland. Det vigtige er, at det er EU-retten, der bør afgøre, om dette er tilfældet, og på grundlag af hvilke garantier sådanne overførsler kan finde sted.

Kommissionen redegjorde for, hvordan persondataforordningens artikel 48 fungerer, herunder den mulige anvendelse af undtagelsen vedrørende samfundsinteresser i forbindelse med en editionskendelse (warrant) af en udenlandsk retshåndhævende myndighed i Microsoft-sagen ved den amerikanske højesteret[159]. Kommissionen understregede i sit indlæg EU's interesse i at sikre, at retshåndhævelsessamarbejdet foregår "inden for en retlig ramme, hvorved der undgås lovkonflikter, og som bygger på [...] respekt for hinandens grundlæggende interesser, både med hensyn til privatlivets fred og retshåndhævelse"[160]. "[n]år en offentlig myndighed kræver, at en virksomhed, der er etableret i dens egen jurisdiktion, fremlægger elektroniske data, der er lagret på en server i en udenlandsk jurisdiktion, er det navnlig territorialprincippet og princippet om anerkendelse af domme under folkeretten, der finder anvendelse"[161].

[157] Det Europæiske Databeskyttelsesråd, Retningslinjer vedrørende undtagelser (fodnote 153 ovenfor), s. 10. Det Europæiske Databeskyttelsesråd præciserede yderligere, at selv om dataoverførsler baseret på undtagelsen om samfundsinteresser ikke må finde sted "i stor skala" eller "systematisk", men skal "begrænses til særlige situationer og [...] opfylder den strenge nødvendighedstest", er der ikke noget krav om, at de skal være "lejlighedsvise".

[158] Dette fremgår klart af ordlyden af persondataforordningens artikel 48 ("uden at det berører andre grunde til overførsel i henhold til dette kapitel") og den ledsagende betragtning 115 ("[O]verførsel af oplysninger bør kun tillades, hvis denne forordnings betingelser for overførsel til tredjelande er opfyldt. Det kan være tilfældet, bl.a. hvis videregivelse er nødvendig af hensyn til vigtige samfundsinteresser, der anerkendes i EU-retten eller medlemsstaternes nationale ret, som den dataansvarlige er omfattet af"). Det anerkendes også af Databeskyttelsesrådet, jf. Retningslinjer vedrørende undtagelser (fodnote 153 ovenfor, s. 5). Som for alle behandlinger skal også de øvrige garantier i forordningen overholdes (f.eks. at data overføres til et specifikt formål, er relevante, begrænset til, hvad der er nødvendigt for at imødekomme anmodningen osv.).

[159] Indlæg fra Microsoft (fodnote 156 ovenfor). Som Kommissionen har forklaret, betyder persondataforordningen, at traktater om gensidig retshjælp "foretrækkes" frem for overførsler, da sådanne traktater "giver mulighed for indsamling af bevismateriale ved samtykke, og er udtryk for en nøje forhandlet balance mellem de forskellige staters interesser, der har til formål at imødegå de konflikter om jurisdiktion, der ellers kan opstå." Se også Det Europæiske Databeskyttelsesråds Retningslinjer vedrørende undtagelser (fodnote 153 ovenfor), s. 5 ("I situationer, hvor der er en international aftale, f.eks. en traktat om gensidig retshjælp, bør virksomheder i EU generelt afvise direkte anmodninger og henvise den anmodende myndighed i tredjelandet til en eksisterende traktat om gensidig retshjælp eller aftale").

[160] Indlæg fra Microsoft (fodnote 156 ovenfor), s. 4.

[161] Indlæg fra Microsoft (fodnote 156 ovenfor), s. 6.

Dette afspejles også i Kommissionens forslag til forordning om europæiske editions- og sikringskendelser om elektronisk bevismateriale i straffesager[162], som indeholder en særlig bestemmelse om anerkendelse af domme, der gør det muligt at gøre indsigelse mod en editionskendelse, hvis overholdelsen af lovgivningen i et tredjeland forbyder videregivelse, navnlig med den begrundelse, at dette er nødvendigt for at beskytte de berørte personers grundlæggende rettigheder[163].

Det er vigtigt at sikre anerkendelse af domme i betragtning af, at retshåndhævelse – som f.eks. kriminalitet og navnlig cyberkriminalitet – i stigende grad er grænseoverskridende og derfor ofte rejser jurisdiktionsspørgsmål og skaber potentielle lovkonflikter[164]. Ikke overraskende er den bedste måde at behandle disse spørgsmål på gennem internationale aftaler, der fastsætter de nødvendige begrænsninger og garantier for grænseoverskridende adgang til personoplysninger, herunder ved at sikre et højt databeskyttelsesniveau hos den anmodende myndighed.

Kommissionen, der handler på vegne af EU, deltager i øjeblikket i multilaterale forhandlinger om anden tillægsprotokol til Europarådets konvention om IT-kriminalitet ("Budapestkonventionen"), der har til formål at styrke de eksisterende regler for at opnå grænseoverskridende adgang til elektronisk bevismateriale i strafferetlige efterforskninger, samtidig med at der sikres passende databeskyttelsesgarantier som en del af protokollen[165]. Ligeledes er der indledt bilaterale forhandlinger om en aftale mellem EU og USA om grænseoverskridende adgang til elektronisk bevismateriale med henblik på retligt samarbejde i straffesager[166]. Kommissionen regner med Europa-Parlamentets og Rådets støtte og Det Europæiske Databeskyttelsesråds vejledning under disse forhandlinger.

Mere generelt er det vigtigt at sikre, at når virksomheder, der er aktive på det europæiske marked, på basis af en legitim anmodning opfordres til at dele oplysninger med henblik på retshåndhævelse, kan de gøre dette uden at opleve lovkonflikter og i fuld respekt for EU's grundlæggende rettigheder. For at forbedre sådanne overførsler forpligter Kommissionen sig til at udvikle passende retlige rammer med sine internationale

---

[162] Europa-Kommissionen, Forslag til Europa-Parlamentets og Rådets forordning om europæiske editions- og sikringskendelser om elektronisk bevismateriale i straffesager (COM (2018) 225 final af 17.4.2018). Rådet vedtog sin generelle indstilling til den foreslåede forordning den 7.12.2018 (findes på: https://www.consilium.europa.eu/en/press/press-releases/2018/12/07/regulation-on-cross-border-access-to-eevidence-council-agrees-its-position/#). Se også EDPS, Udtalelse 7/19 om forslag vedrørende europæiske editions- og sikringskendelser om elektronisk bevismateriale i straffesager (findes på: https://edps.europa.eu/data-protection/ourwork/publications/opinions/electronic-evidence-criminal-matters_en).

[163] I den forklarende note, s. 21, præciseres det, at ud over at sikre anerkendelse af domme i forhold til tredjelandes suveræne interesser for derved at beskytte den pågældende person og undgå lovkonflikter for tjenesteydere, er gensidighed, dvs. sikring af respekt for EU's regler, herunder beskyttelse af personoplysninger (persondataforordningens artikel 48), en vigtig motivation for bestemmelsen om anerkendelse af domme. Se også erklæringen fra Artikel 29-Gruppen af 29.11.2017, aspekter vedrørende databeskyttelse og privatlivets fred i forbindelse med grænseoverskridende adgang til elektronisk bevismateriale (WP29-erklæringen) (findes på: file:///C:/Users/ralfs/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/20171207_e-Evidence_Statement_FINALpdf%20(1).pdf), p. 9.

[164] Se udtalelse fra Artikel-29-Gruppen (fodnote 163 ovenfor), s. 6.

[165] Se henstilling med henblik på Rådets afgørelse om bemyndigelse til at deltage i forhandlinger om anden tillægsprotokol til Europarådets konvention om IT-kriminalitet (CETS nr. 185), 5.2.2019 (COM (2019) 71 final). Jf. også EDPS, Udtalelse 3/2019 om deltagelse i forhandlingerne med henblik på anden tillægsprotokol til Budapestkonventionen om IT-kriminalitet, 2.4.2019 (findes på: https://edps.europa.eu/sites/edp/files/publication/19-04-02_edps_opinion_budapest_convention_en.pdf); Databeskyttelsesrådet, Bidrag til høringen om udkast til anden tillægsprotokol til Europarådets konvention om IT-kriminalitet (Budapestkonventionen), 13.11.2019 (findes på: https://edpb.europa.eu/sites/edpb/files/files/file1/edpbcontributionbudapestconvention_en.pdf).

[166] Se henstilling med henblik på Rådets afgørelse om bemyndigelse til at indlede forhandlinger med henblik på en aftale mellem EU og Amerikas Forenede Stater om grænseoverskridende adgang til elektronisk bevismateriale inden for strafferetligt samarbejde (COM (2019) 70 final af 5.2.2019). Se også EDPS, Udtalelse 2/2019 om forhandlingsmandatet til en aftale mellem EU og USA om grænseoverskridende adgang til elektronisk bevismateriale (findes på: https://edps.europa.eu/sites/edp/files/publication/19-04-02_edps_opinion_on_eu_us_agreement_on_e-evidence_en.pdf).

partnere for at undgå lovkonflikter og støtte effektive samarbejdsformer, navnlig ved at tilvejebringe de nødvendige garantier for databeskyttelse, og derved bidrage til en mere effektiv bekæmpelse af kriminalitet.

7.3 Internationalt samarbejde på databeskyttelsesområdet

Fremme af konvergens mellem forskellige systemer for privatlivsbeskyttelse betyder også, at man lærer af hinanden gennem udveksling af viden, erfaring og bedste praksis. Sådanne udvekslinger er afgørende for at imødegå de nye udfordringer, der i stigende grad er af global karakter og rækkevidde. Kommissionen har derfor intensiveret sin dialog om databeskyttelse og overførsel af oplysninger med en bred vifte af aktører og i forskellige fora på bilateralt, regionalt og multilateralt plan.

Den bilaterale dimension

Efter vedtagelsen af persondataforordningen har der været en stigende interesse for EU's erfaringer med udformning, forhandling og gennemførelse af moderne regler for beskyttelse af privatlivets fred. Dialogen med lande, der gennemlever lignende processer, har antaget forskellige former.

Kommissionens tjenestegrene er kommet med indlæg til en række offentlige høringer arrangeret af udenlandske regeringer, der overvejer lovgivning om beskyttelse af privatlivets fred, f.eks. af USA[167], Indien[168], Malaysia og Etiopien. I nogle tredjelande havde Kommissionens tjenestegrene den ære at få lov til at afgive forklaring til de kompetente parlamentariske organer, f.eks. i Brasilien[169], Chile[170], Ecuador, og Tunesien[171].

Endelig blev der i forbindelse med de igangværende reformer af databeskyttelseslovene afholdt særlige møder med regeringsrepræsentanter eller parlamentariske delegationer fra mange regioner i verden (f.eks. Georgien, Kenya, Taiwan, Thailand og Marokko). Dette omfattede tilrettelæggelse af seminarer og studiebesøg, f.eks. med repræsentanter for den indonesiske regering og en delegation af medarbejdere fra den amerikanske kongres. Dette gav mulighed for at præcisere vigtige begreber i persondataforordningen, forbedre den gensidige forståelse af anliggender om privatlivets fred og illustrere fordelene ved konvergens for at sikre et højt niveau af beskyttelse af individuelle rettigheder, handel og samarbejde. I nogle tilfælde har det også gjort det muligt at mane til forsigtighed med hensyn til visse fejlopfattelser af databeskyttelse, som kan føre til indførelse af protektionistiske foranstaltninger såsom krav om obligatorisk beliggenhed.

---

[167] Se indlægget fra GD Retlige Anliggender og Forbrugere af 9.11.2018 som svar på en anmodning om kommentarer fra offentligheden om en foreslået tilgang til beskyttelse af forbrugernes privatliv [sag nr. 180821780-8780-01] fra USA's National Telecommunications and Information Administration (findes på: https://ec.europa.eu/info/sites/info/files/european_commission_submission_on_a_proposed_approach_to_consumer_privacy.pdf).

[168] Se indlægget fra GD Retlige Anliggender og Forbrugere af 19.11.2018 om udkastet til lov om beskyttelse af personoplysninger i Indien 2018 til ministeriet for elektronik og informationsteknologi (findes på: https://eeas.europa.eu/delegations/india/53963/submission-draft-personal-data-protection-bill-india-2018-directorate-general-justice_en).

[169] Se plenarmødet den 17.4.2018 i det brasilianske senat (https://www25.senado.leg.br/web/atividade/sessao-plenaria/-/pauta/23384), mødet den 10.4.2019 i Det Blandede Udvalg om MP 869/2018 under den brasilianske kongres (https://www12.senado.leg.br/ecidadania/visualizacaoaudiencia?id=15392), og mødet den 26.11.2019 i det brasilianske Deputeretkammers særlige udvalg (https://www.camara.leg.br/noticias/616579-comissao-discutira-protecao-de-dados-no-ambito-das-constituicoes-de-outros-paises/).

[170] Se mødet den 29.5.2018 (https://senado.cl/appsenado/index.php?mo=comisiones&ac=asistencia_sesion&idcomision=186&idsesion=12513&idpunto=15909&sesion=29/05/2018&listado=1) og den 24.4.2019 (https://www.senado.cl/appsenado/index.php?mo=comisiones&ac=sesiones_celebradas&idcomision=186&tipo=3&legi=485&ano=2019&desde=0&hasta=0&idsesion=13603&idpunto=17283&listado=2) og Udvalget om Konstitutionelle Anliggender, Lovgivningsmæssige og Retlige Anliggender i det chilenske senat.

[171] Se mødet den 2.11.2018 i den tunesiske forsamling af repræsentanter for folket for rettigheder, frihedsrettigheder og eksterne forbindelser (https://www.facebook.com/1515094915436499/posts/2264094487203201/).

Siden vedtagelsen af persondataforordningen har Kommissionen også været i kontakt med flere internationale organisationer, bl.a. i lyset af betydningen af dataudveksling med disse organisationer på en række politikområder. Der er navnlig etableret en specifik dialog med De Forenede Nationer med henblik på at lette drøftelserne med alle involverede interessenter for at sikre problemfri overførsel af oplysninger og udvikle yderligere konvergens mellem de respektive databeskyttelsesordninger. Som led i denne dialog vil Kommissionen arbejde tæt sammen med Databeskyttelsesrådet om at få yderligere præciseret, hvordan offentlige og private operatører i EU kan overholde deres databeskyttelsesforpligtelser, når de udveksler oplysninger med internationale organisationer som FN.

Kommissionen er parat til fortsat at dele erfaringerne fra sin reformproces med interesserede lande og internationale organisationer, på samme måde som den lærte det fra andre systemer, da den udarbejdede sit forslag til nye databeskyttelsesregler i EU. Denne form for dialog er til gensidig gavn for EU og dets partnere, da den gør det muligt at opnå en bedre forståelse af den nuværende situation med hensyn til beskyttelse af privatlivets fred og udveksle synspunkter om nye retlige og teknologiske løsninger.

Det er også i denne ånd, at Kommissionen opretter et "databeskyttelsesakademi", der skal fremme udvekslinger mellem tilsynsmyndigheder i Europa og i tredjelande, og dermed forbedre samarbejdet i praksis.

Derudover er der behov for, at der udarbejdes hensigtsmæssige retsforskrifter med henblik på tættere samarbejde og gensidig bistand, bl.a. ved at tillade de nødvendige udvekslinger af oplysninger i forbindelse med undersøgelser. Kommissionen vil derfor gøre brug af de beføjelser, den har fået tillagt på dette område i medfør af persondataforordningens artikel 50, og navnlig anmode om bemyndigelse til at indlede forhandlinger om indgåelse af samarbejdsaftaler vedrørende håndhævelse med relevante tredjelande. I denne forbindelse vil den også tage hensyn til Databeskyttelsesrådets holdninger med hensyn til, hvilke lande der bør prioriteres i lyset af omfanget af overførsler af oplysninger, den håndhævende myndigheds rolle og beføjelser i tredjelandet vedrørende beskyttelse af privatlivets fred, samt behovet for samarbejde om håndhævelse af sager af fælles interesse.

Den multilaterale dimension

Ud over bilaterale udvekslinger deltager Kommissionen også aktivt i en række multilaterale fora for at fremme fælles værdier og skabe konvergens på regionalt og globalt plan.

Det stadig mere universelle medlemskab af Europarådets konvention 108, som er det eneste retligt bindende multilaterale instrument for beskyttelse af personoplysninger, er et klart tegn på denne tendens i retning af (stigende) konvergens[172]. Konventionen, som også er åben for ikkemedlemmer af Europarådet, er allerede ratificeret af 55 lande, herunder en række afrikanske og latinamerikanske stater[173]. Kommissionen bidrog væsentligt til det vellykkede resultat af forhandlingerne om modernisering af konventionen[174] og sikrede, at den afspejlede de samme principper som dem, der er forankret i EU's databeskyttelsesregler. De fleste EU-medlemsstater har nu undertegnet ændringsprotokollen, selv om der fortsat mangler underskrifter fra Danmark, Malta og Rumænien. Kun fire medlemsstater (Bulgarien, Kroatien, Litauen og Polen) har

[172] Hvad der er vigtigt, er, at den moderniserede konvention ikke blot er en traktat, der fastsætter strenge databeskyttelsesgarantier, men også skaber et netværk af tilsynsmyndigheder med værktøjer til håndhævelse af reglerne og, med konventionsudvalget, et forum for drøftelser, udveksling af bedste praksis og udvikling af internationale standarder.

[173] Se den fuldstændige liste over medlemmer: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures. Lande fra Afrika omfatter Kap Verde, Mauritius, Marokko, Senegal og Tunesien, fra Latinamerika Argentina, Mexico og Uruguay. Burkina Faso er blevet opfordret til at tiltræde konventionen.

[174] Se teksten til den moderniserede konvention: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf.

ratificeret ændringsprotokollen. Kommissionen opfordrer de tre resterende medlemsstater til at undertegne den moderniserede konvention og alle medlemsstaterne til hurtigt at ratificere konventionen, så den kan træde i kraft i den nærmeste fremtid[175]. Derudover vil den fortsætte med proaktivt at tilskynde tredjelande til tiltrædelse.

Overførsel af oplysninger og databeskyttelse er ligeledes for nylig blevet behandlet i G20 og G7. I 2019 anerkendte verdens ledere for første gang betydningen af databeskyttelse for at skabe tillid til den digitale økonomi og fremme udvekslingen af oplysninger. Med Kommissionens aktive støtte[176] tilsluttede lederne sig begrebet "Data Free Flow with Trust" (DFFT), som oprindeligt blev foreslået af Japans premierminister Abe i erklæringen fra G20-topmødet i Osaka[177] og G7-topmødet i Biarritz [178]. Denne tilgang afspejles også i Kommissionens meddelelse fra 2020 om en europæisk strategi for data[179] hvori den understreger sin intention om at fortsætte med at fremme dataudveksling med pålidelige partnere, samtidig med at misbrug bekæmpes, f.eks. (udenlandske) offentlige myndigheders uforholdsmæssige adgang til data.

I den forbindelse vil EU også kunne anvende en række værktøjer på forskellige politikområder, der i stigende grad tager hensyn til konsekvenserne for privatlivets fred: F.eks. giver EU's første rammer for screening af udenlandske investeringer, som vil finde fuld anvendelse fra oktober 2020, EU og dets medlemsstater mulighed for at screene investeringstransaktioner, der har indvirkning på "adgang til følsomme oplysninger, herunder personoplysninger, eller muligheden for at kontrollere sådanne oplysninger", hvis de påvirker sikkerheden eller den offentlige orden[180].

Kommissionen arbejder sammen med ligesindede lande i flere andre multilaterale fora for aktivt at fremme sine værdier og standarder. Et vigtigt forum er OECD's nyligt oprettede Working Party on Data Governance and Privacy (DGP), som har iværksat en række vigtige initiativer vedrørende databeskyttelse, dataudveksling og dataoverførsel. Dette omfatter evaluering af OECD's retningslinjer for beskyttelse af privatlivets fred fra 2013. Desuden bidrog Kommissionen aktivt til OECD-Rådets henstilling om kunstig intelligens[181] og sikrede, at EU's menneskecentrerede tilgang, dvs. at AI-applikationerne skal overholde de grundlæggende rettigheder og navnlig databeskyttelse, blev afspejlet i den endelige tekst. Hvad der er nok så vigtigt er, at henstillingen om kunstig intelligens – som efterfølgende er blevet indarbejdet i G20's principper for kunstig intelligens, der er knyttet som bilag til erklæringen fra lederne på G20-topmødet i Osaka[182] – fastsætter principperne om gennemsigtighed og forklarlighed med henblik på at gøre det muligt for dem, der

---

[175] Ifølge dens beslutning vedrørende ændringsprotokollen af 18.5.2018 tilskyndede Ministerkomitéen medlemsstater og andre af konventionens parter til ufortøvet at træffe de nødvendige foranstaltninger til at tillade protokollens ikrafttræden inden for tre år fra dens åbning for undertegnelse og til straks, men under ingen omstændigheder senere end ét år efter den dato, på hvilken protokollen er blevet åbnet for undertegnelse, at indlede ratificeringsprocessen i medfør af deres nationale lovgivning. Den anmodede ligeledes medlemmerne til halvårligt, og første gang ét år efter datoen for åbningen af protokollen for undertegnelse, at undersøge fremskridtene mod ratificering på basis af de oplysninger, som vil blive tilstillet generalsekretæren af hver af medlemsstaterne og andre af konventionens parter, senest én måned forud for denne undersøgelse. Se https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016808a3c9f.

[176] I forbindelse med topmødet mellem EU og Japan i april 2019 udtrykte kommissionsformand, Jean-Claude Juncker, sin støtte til Japans initiativ "Data Free Flow with Trust" og lanceringen af "Osaka-sporet" og forpligtede Kommissionen til at spille en aktiv rolle i begge initiativer.

[177] Se teksten til erklæringen fra lederne på G20-topmødet i Osaka: https://www.consilium.europa.eu/media/40124/final_g20_osaka_leaders_declaration.pdf.

[178] Se teksten til strategien fra lederne på G7-topmødet i Biarritz om en åben, fri og sikker digital omstilling: https://www.elysee.fr/admin/upload/default/0001/05/62a9221e66987d4e0d6ffcb058f3d2c649fc6d9d.pdf.

[179] Meddelelse fra Kommissionen til Europa-Parlamentet, Rådet, Det Europæiske Økonomiske og Sociale Udvalg og Regionsudvalget, En europæisk strategi for data (COM(2020) 66 final af 19.2.2020) (https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_da.pdf), s. 23-24.

[180] Artikel 4, stk. 1, litra d), i Europa-Parlamentets og Rådets forordning (EU) 2019/452 af 19. marts 2019 om et regelsæt for screening af udenlandske direkte investeringer i Unionen (EUT L 79 I af 21.3.2019).

[181] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

[182] G20-ministererklæring om handel og digital økonomi: https://g20trade-digital.go.jp/dl/Ministerial_Statement_on_Trade_and_Digital_Economy.pdf.

påvirkes negativt af et AI-system, at anfægte dens resultater på grundlag af klar og letforståelig information om de faktorer og den logik, der lå til grund for forudsigelsen, henstillingen eller beslutningen, og dermed nøje afspejle principperne i persondataforordningen med hensyn til automatisering af beslutningsprocessen[183].

Endelig optrapper Kommissionen sin dialog med regionale organisationer og netværk, der i stigende grad spiller en central rolle i udformningen af fælles databeskyttelsesstandarder[184], fremme udvekslingen af bedste praksis og samarbejdet mellem håndhævende myndigheder. Dette gælder navnlig Sammenslutningen af Sydøstasiatiske Nationer (ASEAN) – herunder i forbindelse med det igangværende arbejde med dataoverførselsværktøjer – Den Afrikanske Union, forummet Asia Pacific Privacy Authorities (APPA) og Ibero-American Data Protection Network, der alle har iværksat vigtige initiativer på dette område og udgør fora for en frugtbar dialog mellem tilsynsmyndigheder for privatlivets fred og andre interessenter.

Afrika er et godt eksempel, der illustrerer komplementariteten mellem de nationale, regionale og globale privatlivsdimensioner. Digitale teknologier er hastigt og gennemgribende ved at transformere det afrikanske kontinent. Dette kan fremskynde opfyldelsen af målene for bæredygtig udvikling ved at fremme økonomisk vækst, bekæmpe fattigdom og forbedre menneskers liv. En moderne databeskyttelsesramme, der tiltrækker investeringer og fremmer udviklingen af et konkurrencedygtigt erhvervsliv og samtidig bidrager til respekten for menneskerettigheder, demokrati og retsstatsprincippet, er et centralt element i denne omstilling. Harmoniseringen af databeskyttelsesreglerne i Afrika vil gøre det muligt at integrere digitale markeder, samtidig med at konvergens med globale standarder vil lette udvekslingen af data med EU. Disse forskellige aspekter af databeskyttelsen er indbyrdes forbundne og gensidigt forstærkende.

Der er nu en stigende interesse for databeskyttelse i mange afrikanske lande, og antallet af afrikanske lande, der har vedtaget eller er i færd med at vedtage moderne databeskyttelsesregler, har ratificeret konvention 108[185], eller Malabokonventionen[186], stiger fortsat[187]. Samtidig er lovrammen fortsat meget uensartet og fragmenteret på hele det afrikanske kontinent. Mange lande har stadig kun få eller ingen garantier for databeskyttelse. Foranstaltninger til begrænsning af overførsel af oplysninger er stadig udbredte og hæmmer udviklingen af en regional digital økonomi.

For at udnytte de gensidige fordele ved konvergerende regler for databeskyttelse vil Kommissionen samarbejde med sine afrikanske partnere både bilateralt og i regionale fora[188]. Den bygger på det arbejde, der er udført af EU-AU Digital

[183] Se persondataforordningens artikel 13, stk. 2, litra f), artikel 14, stk. 2, litra g), og artikel 22.

[184] Se f.eks. Den Afrikanske Unions *Convention on Cyber Security and Personal Data Protection* ("Malabokonventionen") og *Standards for Data Protection for the Ibero-American States*, der er udviklet af Ibero-American Data Protection Network.

[185] Europarådets konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=DW5jevqD.

[186] African Union Convention on Cyber Security and Personal Data Protection https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection. Desuden har flere af de regionale økonomiske fællesskaber (REC) udviklet databeskyttelsesregler, f.eks. Det Økonomiske Fællesskab af Vestafrikanske Stater (ECOWAS) og Det Sydlige Afrikas Udviklingsfællesskab (SADC). Se hhv. http://www.tit.comm.ecowas.int/wp-content/uploads/2015/11/SIGNED-Data-Protection-Act.pdf and http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/docs/SA4docs/data%20protection.pdf.

[187]

[188] Bl.a. gennem Policy and Regulation Initiative for Digital Africa (PRIDA), se oplysninger på: https://www.africa-eu-partnership.org/en/projects/policy-and-regulation-initiative-digital-africa-prida.

Economy Task Force inden for rammerne af New Africa-Europe Digital Economy Partnership[189]. Det er også til fremme af sådanne mål, at anvendelsesområdet for Kommissionens partnerskabsinstrument "Enhanced Data Protection and Data Flows" udvides til også at omfatte Afrika. Projektet vil blive mobiliseret for at støtte afrikanske lande, der har til hensigt at udvikle moderne databeskyttelsesrammer, eller som ønsker at styrke deres tilsynsmyndigheders kapacitet gennem uddannelse, vidensdeling og udveksling af bedste praksis.

Endelig er Kommissionen også fast besluttet på at bekæmpe digital protektionisme, som det for nylig blev fremhævet i datastrategien, samtidig med at konvergensen mellem databeskyttelsesstandarder på internationalt plan fremmes som et middel til at lette overførsel af oplysninger og dermed samhandelen[190]. Med henblik herpå har den udviklet specifikke bestemmelser om overførsel af oplysninger og databeskyttelse i handelsaftaler, som den systematisk stiller forslag om i sine bilaterale (senest med Australien, New Zealand og Det Forenede Kongerige) og multilaterale forhandlinger, som f.eks. de nuværende WTO-forhandlinger om e-handel. Disse horisontale bestemmelser udelukker rent protektionistiske foranstaltninger, såsom tvungne datalokaliseringskrav, samtidig med at parternes reguleringsmæssige autonomi bevares for at beskytte den grundlæggende ret til databeskyttelse.

Dialogerne om databeskyttelse og handelsforhandlinger skal følge forskellige spor, men de kan samtidig godt supplere hinanden. Konvergens, baseret på høje standarder og en effektiv håndhævelse, udgør faktisk det stærkeste grundlag for udveksling af personoplysninger, hvilket i stigende grad anerkendes af vores internationale partnere. Eftersom virksomheder i stigende grad opererer på tværs af grænserne og foretrækker at anvende lignende regelsæt i alle deres forretningsaktiviteter i hele verden, bidrager en sådan konvergens til at skabe et miljø, der fremmer direkte investeringer, samhandel og øger tilliden mellem handelspartnere. Synergier mellem samhandel og instrumenter for databeskyttelse bør således udforskes nærmere for at sikre fri og sikker overførsel af oplysninger, hvilket er afgørende for forretningsaktiviteter, konkurrencedygtighed og vækst for europæiske virksomheder, herunder SMV'er, i vores stadig mere digitaliserede økonomi.

[189] Se fælles meddelelse fra Europa-Kommissionen og Unionens Højtstående Repræsentant for Udenrigsanliggender og Sikkerhedspolitik "Frem mod en omfattende strategi for samarbejdet med Afrika" (findes på: https://ec.europa.eu/international-partnerships/system/files/communication-eu-africa-strategy-join-2020-4-final_en.pdf); Digital Economy Task Force, New Africa-Europe Digital Economy Partnership: Accelerating the Achievement of the Sustainable Development Goals (findes på: https://www.africa-eu-partnership.org/sites/default/files/documents/finaldetfreportpdf.pdf).

[190] https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf, s. 23.

Bilag I – Bestemmelser vedrørende fakultative specifikationer i national lovgivning

Genstand	Anvendelsesområde	Persondataforordningens artikler
Specifikationer vedrørende retlige forpligtelser og offentlige opgaver	Tilpasning af anvendelsen af bestemmelser med hensyn til behandling med henblik på overholdelse af en retlig forpligtelse eller en offentlig opgave, herunder i særlige behandlingssituationer i henhold til kapitel IX	Artikel 6, stk. 2, og artikel 6, stk. 3
Aldersgrænse for samtykke i forbindelse med informationssamfundstjenester	Fastsættelse af minimumsalderen mellem 13 og 16 år	Artikel 8, stk. 1
Behandling af særlige kategorier af oplysninger	Opretholdelse eller indførelse af yderligere betingelser, herunder begrænsninger, for behandling af genetiske data, biometriske data eller helbredsoplysninger.	Artikel 9, stk. 4
Undtagelse fra oplysningskrav	Indsamling eller videregivelse af oplysninger, der er udtrykkeligt lovfæstet eller med henblik på lovbestemt tavshedspligt	Artikel 14, stk. 5, litra c) og d)
Automatisk individuel beslutningstagning	Bemyndigelse til automatisk beslutningstagning som undtagelse fra det generelle forbud	Artikel 22, stk. 2, litra b)
Begrænsninger af den registreredes rettigheder	Begrænsninger i henhold til artikel 12 og 22, artikel 34 og tilsvarende bestemmelser i artikel 5, når det er nødvendigt og forholdsmæssigt for at sikre udtømmende opregnede vigtige mål	Artikel 23, stk. 1
Høring og godkendelseskrav	Krav om, at dataansvarlige skal høre eller indhente tilladelse fra databeskyttelsesmyndigheden for behandling af en opgave i samfundets interesse	Artikel 36, stk. 5
Udpegelse af en databeskyttelsesansvarlig i yderligere tilfælde	Udpegelse af en databeskyttelsesansvarlig i andre tilfælde end dem, der er omhandlet i artikel 37, stk. 1	Artikel 37, stk. 4

Begrænsninger i overførsler	Begrænsning af overførsler af specifikke kategorier af personoplysninger	Artikel 49, stk. 5
Klager og søgsmål fra organisationer på egne vegne	Bemyndigelse af organisationer for beskyttelse af privatlivets fred til at indgive klager og anlægge søgsmål uafhængigt af en bemyndigelse fra de registrerede	Artikel 80, stk. 2
Aktindsigt i officielle dokumenter	Afstemning af aktindsigt i officielle dokumenter med retten til beskyttelse af personoplysninger	Artikel 86
Behandling af nationalt identifikationsnummer	Særlige betingelser for behandling af det nationale identifikationsnummer	Artikel 87
Behandling i forbindelse med ansættelsesforhold	Mere specifikke regler for behandling af arbejdstageres personoplysninger	Artikel 88
Undtagelser for behandling til arkivformål i samfundets interesse, til forskningsmål eller til statistiske formål	Undtagelser fra den angivne registreredes rettigheder, i det omfang sådanne rettigheder sandsynligvis vil gøre det umuligt eller i alvorlig grad hindre opfyldelse af de specifikke formål	Artikel 89, stk. 2 og stk. 3
Afstemning af databeskyttelse med tavshedspligt	Særlige bestemmelser om databeskyttelsesmyndighedernes undersøgelsesbeføjelser over for dataansvarlige eller databehandlere, der er omfattet af tavshedspligt	Artikel 90

Bilag II – Oversigt over databeskyttelsesmyndighedernes ressourcer

Nedenstående tabel indeholder en oversigt over databeskyttelsesmyndighedernes ressourcer (personale og budget) pr. EU/EØS-land[191].

Ved sammenligning af tallene mellem medlemsstaterne er det vigtigt at huske på, at myndighederne kan have opgaver, der er pålagt dem ud over kravene i persondataforordningen, og at disse kan variere fra medlemsstat til medlemsstat. Forholdet mellem personale ansat af myndighederne pr. million indbyggere og myndighedernes budget pr. mio. EUR af BNP er kun medtaget for at tilvejebringe yderligere elementer i sammenligningen mellem medlemsstater af samme størrelse og bør ikke ses isoleret. De absolutte tal, forhold og udvikling over de seneste år bør ses i sammenhæng ved vurderingen af en given myndigheds ressourcer.

	PERSONALE (Fuldtidsækvivalenter)					BUDGET (EUR)				
EU/EØS-medlemsstater	**2019**	**Prognose 2020**	**% vækst 2016-2019**	**% vækst 2016-2020 (prognose)**	**Antal medarbejdere pr. mio. indbyggere (2019)**	**2019**	**Prognose 2020**	**% vækst 2016-2019**	**% vækst 2016-2020 (prognose)**	**Budget pr. mio. EUR af BNP (2019)**
Østrig	34	34	48 %	48 %	3,8	2 282 000	2 282 000	29 %	29 %	5,7
Belgien	59	65	9 %	20 %	5,2	8 197 400	8 962 200	1 %	10 %	17,3
Bulgarien	60	60	-14 %	-14 %	8,6	1 446 956	1 446 956	24 %	24 %	23,8
Kroatien	39	60	39 %	114 %	9,6	1 157 300	1 405 000	57 %	91 %	21,5
Cypern	24	22	ikke oplyst	ikke oplyst	27,4	503 855	ikke oplyst	114 %	ikke oplyst	23,0
Tjekkiet	101	109	0 %	8 %	9,5	6 541 288	6 720 533	10 %	13 %	29,7
Danmark	66	63	106 %	97 %	11,4	5 610 128	5 623 114	101 %	101 %	18,0
Estland	16	18	-11 %	0 %	12,1	750 331	750 331	7 %	7 %	26,8
Finland	45	55	114 %	162 %	8,2	3 500 000	4 500 000	94 %	150 %	14,6
Frankrig	215	225	9 %	14 %	3,2	18 506 734	20 143 889	-2 %	7 %	7,7
Tyskland	888	1002	52 %	72 %	10,7	76 599 800	85 837 500	48 %	66 %	22,3
Grækenland	33	46	-15 %	18 %	3,1	2 849 000	3 101 000	38 %	50 %	15,2
Ungarn	104	117	42 %	60 %	10,6	3 505 152	4 437 576	102 %	155 %	24,4
Island	17	17	143 %	143 %	47,6	2 272 490	2 294 104	167 %	170 %	105,2
Irland	140	176	169 %	238 %	28,5	15 200 000	16 900 000	223 %	260 %	43,8
Italien	170	170	40 %	40 %	2,8	29 127 273	30 127 273	46 %	51 %	16,3
Letland	19	31	-10 %	48 %	9,9	640 998	1 218 978	4 %	98 %	21,0
Litauen	46	52	-8 %	4 %	16,5	1 482 000	1 581 000	40 %	49 %	30,6
Luxembourg	43	48	126 %	153 %	70,0	5 442 416	6 691 563	165 %	226 %	85,7
Malta	13	15	30 %	50 %	26,3	480 000	550 000	41 %	62 %	36,3
Nederlandene	179	188	145 %	158 %	10,4	18 600 000	18 600 000	130 %	130 %	22,9
Norge	49	58	2 %	21 %	9,2	5 708 950	6 580 660	27 %	46 %	15,9
Polen	238	260	54 %	68 %	6,3	7 506 345	9 413 381	66 %	108 %	14,2
Portugal	25	27	-4 %	4 %	2,4	2 152 000	2 385 000	67 %	86 %	10,1
Rumænien	39	47	-3 %	18 %	2,0	1 103 388	1 304 813	3 %	22 %	4,9
Slovakiet	49	51	20 %	24 %	9,0	1 731 419	1 859 514	47 %	58 %	18,4
Slovenien	47	49	42 %	48 %	22,6	2 242 236	2 266 485	68 %	70 %	46,7
Spanien	170	220	13 %	47 %	3,6	15 187 680	16 500 000	8 %	17 %	12,2
Sverige	87	87	81 %	81 %	8,5	8 800 000	10 300 000	96 %	129 %	18,5
I ALT	**2 966**	**3 372**	**42 %**	**62 %**	**6,6**	**249 127 139**	**273 782 870**	**49 %**	**64 %**	**17,4**

Kilde til rådata: Databeskyttelsesrådets bidrag. Beregninger foretaget af Kommissionen.

[191] Undtagen Liechtenstein.