Europaudvalget 2019
KOM (2019) 0374
Offentligt

EUROPA-
KOMMISSIONEN

Bruxelles, den 24.7.2019
COM(2019) 374 final

MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET OG RÅDET

Databeskyttelsesregler som en tillidsskabende katalysator i og uden for EU — status

Meddelelse fra Kommissionen til Europa-Parlamentet og Rådet

Databeskyttelsesregler som en tillidsskabende katalysator i og uden for EU — status

I. Indledning

Den generelle forordning om databeskyttelse[1] (i det følgende benævnt "forordningen") har fundet anvendelse i hele EU i over et år. Den er kernen i et sammenhængende og moderniseret EU-databeskyttelseslandskab, der også omfatter direktivet om databeskyttelse på retshåndhævelsesområdet[2] og databeskyttelsesforordningen for EU's institutioner og organer[3]. Denne ramme skal suppleres af e-databeskyttelsesforordningen, som i øjeblikket er under behandling i lovgivningsprocessen.

Effektive databeskyttelsesregler er afgørende for at sikre den grundlæggende ret til beskyttelse af personoplysninger. De er centrale for et demokratisk samfund[4] og et vigtigt element i en tid, hvor økonomien i stadig højere grad styres af data. EU ønsker at udnytte de mange muligheder, som de digitale omstillingsprocesser giver med hensyn til tjenesteydelser, beskæftigelse og innovation, og samtidig tackle de udfordringer, de medfører. Identitetstyveri, læk af følsomme oplysninger, forskelsbehandling af enkeltpersoner, indbygget forudindtagethed, deling af ulovligt indhold og udviklingen af indgribende overvågningsværktøjer er blot nogle eksempler på problemstillinger, der i stigende grad indgår i den offentlige debat, hvor det står klart, at borgerne forventer, at deres data beskyttes.

Databeskyttelse er blevet et reelt globalt fænomen, da mennesker verden over i stigende grad værdsætter beskyttelsen og sikkerheden af deres data. Mange lande har vedtaget eller er i færd med at vedtage omfattende databeskyttelsesregler baseret på principper, der ligger tæt op ad principperne i forordningen, hvilket resulterer i global konvergens af databeskyttelsesregler. Dette giver nye muligheder for at lette overførslen af oplysninger mellem kommercielle

---

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 (generel forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1): https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=CELEX%3A32016R0679.

2 Europa-Parlamentets og Rådets direktiv (EU) 2016/680 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger og om ophævelse af Rådets rammeafgørelse 2008/977/RIA (EUT L 119 af 4.5.2016, s. 89): https://eur-lex.europa.eu/legal-content/DA/ALL/?uri=celex:32016L0680. Direktivet skulle være gennemført i medlemsstaternes nationale lovgivning senest den 6.5.2018. I rapporterne om sikkerhedsunionen gøres der status over gennemførelsen.

3 Europa-Parlamentets og Rådets forordning (EU) 2018/1725 af 23. oktober 2018 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i Unionens institutioner, organer, kontorer og agenturer og om fri udveksling af sådanne oplysninger og om ophævelse af forordning (EF) nr. 45/2001 og afgørelse nr. 1247/2002/EF (EUT L 295 af 21.11.2018, s. 39): https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=CELEX%3A32018R1725. Den trådte i kraft den 11.12.2018.

4 I en skelsættende dom af 24.8.2017 anerkendte den indiske højesteret, at privatlivets fred var en grundlæggende rettighed, en "væsentlig facet af menneskets værdighed".

operatører eller offentlige myndigheder og forbedrer samtidig beskyttelsesniveauet for personoplysninger i EU og i hele verden.

Databeskyttelse tages mere alvorligt end nogensinde, og det har vidtrækkende konsekvenser for forskellige interessenter og sektorer. Kommissionen er fast besluttet på at sikre, at EU's gennemførelse af den nye databeskyttelsesordning bliver vellykket, og at støtte alle aspekter, således at den bliver fuldt operationel. I denne meddelelse gør Kommissionen status over de hidtidige resultater med hensyn til en konsekvent gennemførelse af databeskyttelsesreglerne i hele EU, det nye forvaltningssystems funktion, konsekvenserne for borgere og virksomheder og EU's indsats for at fremme global konvergens af databeskyttelsesordninger. Meddelelsen er en opfølgning på Kommissionens meddelelse om anvendelsen af forordningen fra januar 2018[5], og den er baseret på arbejdet i flerpartsgruppen[6], navnlig dens bidrag til den årige statusevaluering og drøftelserne under arrangementet afholdt af Kommissionen den 13. juni 2019[7] for at gøre status. Denne meddelelse er også et bidrag til den revision, som Kommissionen planlægger at gennemføre inden maj 2020[8].

EU's lovgivningsramme for databeskyttelse er en hjørnesten i den europæiske menneskecentrerede tilgang til innovation. Den er ved at blive en del af lovgivningsgrundlaget for en bredere vifte af politikker, herunder inden for sundhed og forskning, kunstig intelligens, transport, energi, konkurrence og retshåndhævelse. Kommissionen har konsekvent understreget betydningen af en korrekt gennemførelse og håndhævelse af de nye databeskyttelsesregler som fremhævet i Kommissionens meddelelse om anvendelsen af forordningen, der blev offentliggjort i januar 2018, og i Kommissionens vejledning i anvendelsen af Unionens databeskyttelseslovgivning i forbindelse med afholdelse af valg, der blev offentliggjort i september 2018[9]. På tidspunktet for udarbejdelsen af denne meddelelse var der gjort store fremskridt hen imod dette mål, selv om der helt klart er behov for en yderligere indsats, inden forordningen bliver fuldt operationel.

II. Et kontinent, én lovgivning: Databeskyttelsesrammen er indført i medlemsstaterne

Et af hovedformålene med forordningen var at fjerne et fragmenteret landskab med 28 forskellige nationale love, som fandtes under det tidligere databeskyttelsesdirektiv[10] og skabe

---

5 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) 43 final): https://eur-lex.europa.eu/legal-content/DA/TXT/?qid=1517578296944&uri=CELEX%3A52018DC0043.

6 Flerpartsgruppen vedrørende forordningen, der er oprettet af Kommissionen, inddrager civilsamfundet og repræsentanter for erhvervslivet, akademikere og fagfolk: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3537.

7 http://europa.eu/rapid/press-release_IP-19-2956_da.htm.

8 Forordningens artikel 97.

9 Kommissionens vejledning i anvendelsen af Unionens databeskyttelseslovgivning i forbindelse med afholdelse af valg (COM(2018) 638 final): https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:52018DC0638&from=EN.

10 Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger.

retssikkerhed for borgerne og virksomhederne i hele EU. Dette mål er i det store og hele opfyldt.

Harmonisering af lovgivningsrammen

Selv om forordningen gælder umiddelbart i medlemsstaterne, er de i henhold til forordningen forpligtet til at tage en række retlige skridt på nationalt plan, navnlig til at oprette og tildele beføjelser til de nationale databeskyttelsesmyndigheder[11], til at fastsætte regler om specifikke spørgsmål såsom foreningen af beskyttelsen af personoplysninger med ytrings- og informationsfrihed og til at ændre eller ophæve sektorspecifik lovgivning med databeskyttelsesaspekter. På tidspunktet for udarbejdelse denne meddelelse havde alle medlemsstater undtagen tre[12] ajourført deres nationale databeskyttelseslovgivning. Arbejdet med at tilpasse sektorlovgivningen er stadig i gang på nationalt plan. Efter forordningens indarbejdelse i aftalen om Det Europæiske Økonomiske Samarbejdsområde blev anvendelsen heraf udvidet til at omfatte Norge, Island og Liechtenstein, som også har vedtaget deres nationale databeskyttelseslovgivning.

En række interessenter ønsker imidlertid en endnu højere grad af harmonisering på visse områder[13]. Forordningen giver medlemsstaterne mulighed for yderligere at præcisere dens anvendelse på visse områder såsom aldersgrænsen for børns samtykke til onlinetjenester[14] eller behandlingen af personoplysninger på områder såsom lægemidler og folkesundhed. Der gælder to retsgrundlag for medlemsstaternes foranstaltninger i denne forbindelse:

i) En eventuel national præciserende lov skal opfylde kravene i chartret om grundlæggende rettigheder[15] (og må ikke gå ud over de begrænsninger, der er fastsat i forordningen, som bygger på chartret).
ii) Lovgivningen må ikke gribe ind i den frie udveksling af personoplysninger inden for EU[16].

I nogle tilfælde har medlemsstaterne indført yderligere nationale krav ud over kravene i forordningen, navnlig gennem mange sektorspecifikke love, og dette fører til fragmentering og skaber unødvendige byrder. Et eksempel på et yderligere krav indført af medlemsstaterne ud over kravene i forordningen er forpligtelsen i henhold til den tyske lovgivning til at udpege en databeskyttelsesansvarlig i virksomheder med 20 ansatte eller derover, som permanent er involveret i den automatiske behandling af personoplysninger.

En fortsat indsats i retning af større harmonisering

---

https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=celex:31995L0046.

11 F.eks. beføjelsen til at pålægge administrative bøder.

12 Pr. 23.7.2019 er Grækenland, Portugal og Slovenien stadig i færd med at vedtage deres nationale lovgivning.

13 Se rapporten fra flerpartsgruppen vedrørende forordningen af 13.6.2019: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=15670.

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

15 Artikel 8.

16 I overensstemmelse med artikel 16, stk. 2, i traktaten om Den Europæiske Unions funktionsmåde.

Kommissionen deltager i bilaterale dialoger med nationale myndigheder, hvor den navnlig har fokus på nationale foranstaltninger på følgende områder:

- databeskyttelsesmyndighedernes effektive uafhængighed, herunder ved at sikre tilstrækkelige finansielle, menneskelige og tekniske ressourcer
- nationale loves begrænsning af de registreredes rettigheder
- det forhold, at den nationale lovgivning ikke bør indføre krav, der går videre end forordningen, når der ikke er tale om en præcisering, f.eks. yderligere betingelser for behandling
- opfyldelsen af forpligtelsen til at forene retten til beskyttelse af personoplysninger med ytrings- og informationsfriheden under hensyntagen til, at denne forpligtelse ikke bør misbruges til at hæmme journalistisk arbejde.

Databeskyttelsesmyndighedernes samarbejde inden for rammerne af Det Europæiske Databeskyttelsesråd ("Databeskyttelsesrådet") er en vigtig drivkraft for en konsekvent anvendelse af de nye regler: Håndhævelsesforanstaltninger, der berører flere medlemsstater, er omfattet af Databeskyttelsesrådets samarbejds- og sammenhængsmekanisme[17], og Databeskyttelsesrådets retningslinjer bidrager til en harmoniseret forståelse af forordningen. Der er ikke desto mindre en forventning hos interessenterne om, at databeskyttelsesmyndighederne går videre i denne retning.

De nationale domstoles og EU-Domstolens arbejde bidrager også til at sikre en ensartet fortolkning af databeskyttelsesreglerne. Nogle nationale domstole har for nylig afsagt domme, der ugyldiggør bestemmelser i nationale love, som afviger fra forordningen[18].

III. Alle brikkerne i det nye forvaltningssystem er ved at falde på plads

Med forordningen blev der oprettet en ny forvaltningsstruktur, som sætter de uafhængige nationale databeskyttelsesmyndigheder i centrum som håndhævere af forordningen og interessenternes første kontaktpunkt. Selv om de fleste databeskyttelsesmyndigheder i det forløbne år har fået flere ressourcer, er der stadig store forskelle mellem medlemsstaterne[19].

Databeskyttelsesmyndighederne bruger deres nye beføjelser

Forordningen giver databeskyttelsesmyndighederne stærkere håndhævelsesbeføjelser. I modsætning til den frygt, som nogle interessenter gav udtryk for inden maj 2018, har de nationale databeskyttelsesmyndigheder en afbalanceret tilgang til håndhævelsesbeføjelser. De har fokuseret på dialog snarere end sanktioner, navnlig i forhold til mindre erhvervsdrivende, som ikke behandler personoplysninger som en kerneaktivitet. De er ikke samtidig ikke bange

---

[17] I henhold til forordningens artikel 60 skal databeskyttelsesmyndighederne samarbejde og nå til enighed om fortolkningen af forordningen i konkrete sager. I henhold til artikel 64 skal Databeskyttelsesrådet afgive udtalelser i visse tilfælde for at sikre en ensartet anvendelse af forordningen. Endelig gives Databeskyttelsesrådet beføjelse til at vedtage bindende afgørelser rettet til databeskyttelsesmyndighederne i tilfælde af uenighed mellem myndighederne.

[18] I Tyskland og Spanien.

[19] https://edpb.europa.eu/sites/edpb/files/files/file1/19_2019_edpb_written_report_to_libe_en.pdf.

for at bruge deres nye beføjelser effektivt, når det var nødvendigt, herunder ved at iværksætte undersøgelser om sociale medier[20] og pålægge administrative bøder fra nogle få tusinde euro til flere millioner, afhængigt af hvor alvorlige overtrædelserne af databeskyttelsesreglerne er.

Eksempler på bøder pålagt af databeskyttelsesmyndigheder[21]:

- 5 000 EUR til en sportsvæddemålscafé i Østrig på grund af ulovlig videoovervågning
- 220 000 EUR til et datamæglerfirma i Polen, som ikke havde oplyst kunderne om behandlingen af deres data
- 250 000 EUR til den spanske fodboldliga LaLiga på grund af manglende gennemsigtighed i designet af ligaens smartphoneapplikation
- 50 mio. EUR til Google i Frankrig på grund af betingelserne for at opnå samtykke fra brugere.

I forbindelse med gennemførelsen af undersøgelser er det vigtigt, at databeskyttelsesmyndighederne indsamler relevant dokumentation, overholder alle proceduremæssige skridt i den nationale lovgivning og sikrer en retfærdig procedure i ofte komplekse sager. Dette kræver tid og en betydelig indsats, hvilket forklarer, hvorfor de fleste af de undersøgelser, der er indledt efter forordningens ikrafttræden, stadig er i gang.

Når det er sagt, bør forordningens succes ikke måles på antallet af pålagte bøder, men på ændringer i kulturen og alle involverede aktørers adfærd. Databeskyttelsesmyndighederne råder i den forbindelse over andre værktøjer, idet de midlertidigt eller definitivt kan begrænse, herunder forbyde, behandling, eller påbyde suspension af overførsel af oplysninger til en modtager i et tredjeland[22].

Nogle databeskyttelsesmyndigheder har udviklet nye værktøjer såsom hjælpelinjer og værktøjer til virksomheder, mens andre har udviklet nye tilgange såsom reguleringsmæssige sandkasser[23] for at hjælpe virksomhederne med at opfylde deres forpligtelser. En række interessenter mener dog stadig, at de ikke har modtaget tilstrækkelig støtte og information, navnlig små og mellemstore virksomheder i nogle medlemsstater[24]. For at hjælpe med at rette op på denne situation yder Kommissionen tilskud til databeskyttelsesmyndigheder, så de kan nå ud til interessenter, navnlig borgerne og de små og mellemstore virksomheder[25].

---

[20] Den irske databeskyttelseskommission indledte f.eks. 15 formelle undersøgelser vedrørende multinationale teknologivirksomheders overholdelse af forordningen. Se s. 49 i den irske databeskyttelseskommissions årsberetning for 2018: https://www.dataprotection.ie/en/news-media/press-releases/dpc-publishes-annual-report-25-may-31-december-2018.

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

[22] Artikel 58, stk. 2, litra f) og j).

[23] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/09/ico-call-for-views-on-creating-a-regulatory-sandbox/.

[24] Se rapporten fra flerpartsgruppen vedrørende forordningen: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=15670&Lang=DA.

[25] 2 mio. EUR afsat til ni databeskyttelsesmyndigheder i 2018 til aktiviteter i 2018-2019: Belgien, Bulgarien, Danmark, Ungarn, Litauen, Letland, Nederlandene, Slovenien og Island: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/rec-rdat-trai-ag-2017;

Det Europæiske Databeskyttelsesråd er operationelt

Databeskyttelsesmyndighederne har intensiveret deres arbejde i Det Europæiske Databeskyttelsesråd[26]. Dette intensive arbejde har gjort det muligt for Databeskyttelsesrådet at vedtage ca. 20 retningslinjer om centrale aspekter i forordningen[27]. Databeskyttelsesrådets fremtidige arbejdsområder er præsenteret i et 2-årligt arbejdsprogram[28] som krævet i forordningen.

I grænseoverskridende sager er den enkelte databeskyttelsesmyndighed ikke længere blot en national myndighed, men er en del af en egentlig EU-dækkende proces, der omfatter alle faser lige fra undersøgelsen til afgørelsen. Et sådant tæt samarbejde er blevet almindelig praksis, og ved udgangen af juni 2019 var 516 grænseoverskridende sager således blevet behandlet gennem samarbejdsmekanismen.

Kommissionen bidrager aktivt til Databeskyttelsesrådets[29] arbejde for at fremme forordningens ånd og bogstav og sætter fokus på de generelle principper i EU-retten[30].

Hen imod skabelsen af en EU-databeskyttelseskultur

Det nye forvaltningssystem har endnu ikke nået sit fulde potentiale. Det er vigtigt, at Databeskyttelsesrådet strømliner sin beslutningstagning yderligere og udvikler en fælles EU-databeskyttelseskultur blandt dets medlemmer. Databeskyttelsesmyndighedernes muligheder for at samle deres indsats[31] på områder, der berører mere end én medlemsstat, f.eks. for at gennemføre fælles undersøgelses- og håndhævelsesforanstaltninger, kan bidrage til et sådant mål og samtidig sikre en bedre udnyttelse af de begrænsede ressourcer.

Mange interessenter ønsker, at de nationale databeskyttelsesmyndigheder samarbejder endnu tættere og anvender en mere ensartet tilgang[32]. De ønsker også større sammenhæng i databeskyttelsesmyndighedernes rådgivning[33] og en fuldstændig tilpasning af nationale retningslinjer til Databeskyttelsesrådets retningslinjer. Nogle forventer også yderligere præciseringer af centrale begreber i forordningen, f.eks. den risikobaserede tilgang, under særlig hensyntagen til små og mellemstore virksomheders problemer.

---

1 mio. EUR vil blive afsat i 2019: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/rec-rdat-trai-ag-2019.

26 Databeskyttelsesrådet har status som juridisk person og består af cheferne for de nationale tilsynsmyndigheder for databeskyttelse og Den Europæiske Tilsynsførende for Databeskyttelse.

27 https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_da.

28 https://edpb.europa.eu/our-work-tools/our-documents/publication-type/work-program_da.

29 Som deltager uden stemmeret.

30 Kommissionen har også bidraget til at lette oprettelsen af Databeskyttelsesrådet og støtter dets funktion gennem tilvejebringelse af kommunikationssystemet.

31 Forordningens artikel 62.

32 Se rapporten fra flerpartsgruppen vedrørende forordningen: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=15670. Nogle virksomheder mener f.eks., at de nationale lister over typer af behandlingsaktiviteter, for hvilke der kræves en konsekvensanalyse vedrørende databeskyttelse i henhold til forordningens artikel 35, kunne have været bedre harmoniseret.

33 Herunder mellem de forskellige myndigheder i delstater.

I den forbindelse er det af afgørende betydning, at interessenterne får bedre mulighed for at understøtte Databeskyttelsesrådets arbejde. Derfor glæder Kommissionen sig over den systematiske offentlige høring, som Databeskyttelsesrådet har foranstaltet om retningslinjer. Denne praksis bør sammen med tilrettelæggelsen af workshopper for interessenter i en tidlig fase i overvejelserne fortsættes og styrkes for at sikre gennemsigtigheden og relevansen af samt inddragelsen i Databeskyttelsesrådets arbejde.

IV. Borgerne gør brug af deres rettigheder, men der bør fortsat gøres en indsats for at øge bevidstheden

Et andet centralt formål med forordningen var at styrke den enkeltes rettigheder. Forordningen er bredt anerkendt af borgerrettighedsorganisationer og forbrugerorganisationer som et vigtigt bidrag til et retfærdigt digitalt samfund, der bygger på gensidig tillid.

En større bevidsthed om databeskyttelsesrettigheder

Borgerne i EU er i stigende grad opmærksomme på databeskyttelsesreglerne og deres rettigheder: 67 % af respondenterne i en Eurobarometerundersøgelse[34] fra maj 2019 kender forordningen, og 57 % ved, at der er en national databeskyttelsesmyndighed, som de kan henvende sig til for at få oplysninger eller indgive klager. 73 % har hørt om mindst én af rettighederne i henhold til forordningen. Et stort antal personer i EU tager dog fortsat ikke aktive skridt til at beskytte deres personoplysninger, når de går på nettet. F.eks. har 44 % ikke ændret standardindstillinger for beskyttelse af privatlivets fred på sociale netværk.

Borgerne udøver i stigende grad deres rettigheder

Som følge af denne øgede bevidsthed om rettigheder udøver borgerne dem mere intensivt gennem kundeforespørgsler og ved at henvende sig til databeskyttelsesmyndighederne hyppigere for at anmode om oplysninger eller indgive klager[35]. Virksomhederne angiver også, at anmodninger om adgang til personoplysninger er steget i flere sektorer, f.eks. bank- og telekommunikationssektoren. Borgerne har også oftere trukket deres samtykke tilbage og udøvet deres ret til at gøre indsigelse mod kommerciel kommunikation[36].

Nogle erhvervsdrivende rapporterede dog om borgere, der havde misforstået databeskyttelsesreglerne og f.eks. troede, at de skulle give samtykke til enhver behandling, eller at retten til sletning er absolut (selv om f.eks. personoplysninger nogle gange skal opbevares af de erhvervsdrivende på grund af retlige forpligtelser)[37]. Civilsamfundsorganisationerne klager over visse virksomheders og databeskyttelsesmyndigheders lange svartider.

En række ikkestatslige organisationer har navnlig indgivet klager på vegne af borgere, som har bemyndiget dem hertil og således gjort brug af den nye mulighed i henhold til

---

34 http://europa.eu/rapid/press-release_IP-19-2956_da.htm.
35 https://ec.europa.eu/commission/sites/beta-political/files/infographic-gdpr_in_numbers_1.pdf.
36 Se rapporten fra flerpartsgruppen vedrørende forordningen.
37 Se rapporten fra flerpartsgruppen vedrørende forordningen.

forordningen[38]. Anvendelsen af repræsentative søgsmål ville have været lettere, hvis flere medlemsstater havde gjort brug af muligheden i henhold til forordningen for at give ikkestatslige organisationer ret til at indgive klager uden en bemyndigelse[39].

Behovet for at fortsætte oplysningskampagnerne

Dialogen og oplysningskampagnerne med fokus på den brede offentlighed skal derfor fortsætte på nationalt plan og EU-plan. Med henblik herpå iværksatte Kommissionen i juli 2019[40] en ny onlinekampagne for at tilskynde borgerne til at læse databeskyttelseserklæringerne og optimere deres privatlivsindstillinger.

V. Virksomhederne tilpasser deres praksis

Forordningen har til formål at støtte virksomhederne i den digitale økonomi ved at tilbyde fremtidssikrede løsninger. Virksomhederne glæder sig generelt over forordningens ansvarlighedsprincip, der bevæger sig væk fra den tidligere byrdefulde ex ante-tilgang (ophævelse af anmeldelseskrav, skalérbare forpligtelser og en fleksibel databeskyttelse gennem princippet om beskyttelse af privatlivet ved hjælp af design og standardindstillinger, der gør det muligt at konkurrere på grundlag af privatlivsvenlige løsninger). Samtidig ønsker nogle virksomheder større retssikkerhed og yderligere eller klarere retningslinjer fra databeskyttelsesmyndighederne[41].

Forsvarlig dataforvaltning

Selv om virksomhederne melder om en række udfordringer i forbindelse med tilpasningen til de nye regler[42], understreger mange, at det også var en anledning til at gøre selskabsbestyrelserne opmærksom på spørgsmålet om databeskyttelse, bringe orden i eget hus med hensyn til de data, de er i besiddelse af, forbedre sikkerheden, være bedre forberedt på hændelser, mindske eksponeringen for unødvendige risici og opbygge mere tillidsfulde forhold til deres kunder og forretningspartnere. Med hensyn til gennemsigtighed påpeger en række virksomheder og civilsamfundsorganisationer den hårfine balance, der skal findes mellem at give borgerne alle de oplysninger, der kræves i henhold til forordningen, og give oplysningerne i et klart og enkelt sprog og i en form, som borgerne kan forstå. De erhvervsdrivende er i gang med at udvikle innovative løsninger i denne retning.

Generelt anførte virksomhederne, at de var i stand til at gennemføre de registreredes nye rettigheder, selv om det undertiden var en udfordring at overholde fristerne på grund af et øget

---

38 Forordningens artikel 80, stk. 1.

39 Forordningens artikel 80, stk. 2.

40 Den følger op på den tidligere kampagne, der havde til formål at udbrede informationsmateriale til borgere og virksomheder —tilgængelig her: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_da.

41 Se rapporten fra flerpartsgruppen vedrørende forordningen.

42 Opdatering af IT-systemet nævnes ofte som en af hovedudfordringerne, navnlig for gennemførelsen af principperne om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger, retten til sletning i backup osv.

antal anmodninger og deres mere omfattende karakter[43] og at kontrollere identiteten af den person, der fremsætter en anmodning.

Indvirkning på innovation

Forordningen giver ikke kun mulighed for, men tilskynder også til udvikling af nye teknologier under overholdelse af den grundlæggende ret til beskyttelse af personoplysninger. Dette er tilfældet på områder som kunstig intelligens.

Nogle virksomheder er begyndt at udvikle nye, mere privatlivsvenlige tjenester. F.eks. er søgemaskiner, der ikke sporer brugere eller bruger adfærdsbaseret annoncering, gradvist ved at vinde markedsandele i nogle medlemsstater. Andre virksomheder er i færd med at udvikle tjenester, der bygger på nye rettigheder til borgerne såsom portabilitet af deres personoplysninger. Et stigende antal virksomheder har fremmet respekten for personoplysninger som en konkurreparameter og et salgsargument. Denne udvikling er ikke begrænset til EU, men finder også sted i meget innovative økonomier i tredjelande[44].

Den særlige situation for mikrovirksomheder og små virksomheder med "lav risiko"

Selv om situationen varierer fra medlemsstat til medlemsstat, har mikrovirksomheder og små virksomheder[45], som ikke behandler personoplysninger som en kerneaktivitet, været nogle af de interessenter, der havde flest spørgsmål om anvendelsen af forordningen. Selv om deres bekymringer tilsyneladende til dels skyldes manglende kendskab til databeskyttelsesreglerne, bliver de også undertiden forværret af kampagner fra konsulentfirmaer, der ønsker at tilbyde rådgivning mod betaling, gennem spredningen af ukorrekte oplysninger, f.eks. om behovet for systematisk at indhente den enkeltes samtykke[46], og gennem yderligere krav, der pålægges på nationalt plan.

I denne forbindelse ønsker mikrovirksomheder og små virksomheder retningslinjer, der er skræddersyet til deres specifikke situation, med meget praktiske oplysninger. Nogle databeskyttelsesmyndigheder har allerede gjort dette på nationalt plan[47]. For at supplere nationale initiativer har Kommissionen udsendt informationsmateriale for at hjælpe disse virksomheder med at overholde de nye regler gennem en række praktiske skridt[48].

Brug af værktøjskassen i forordningen

---

43 Virksomhederne ønskede også retningslinjer fra Databeskyttelsesrådet om grundløse eller overdrevne anmodninger.

44 Ifølge en rapport offentliggjort af Israels branchesammenslutning for cybersikkerhed var delsektoren for databeskyttelse og privatlivets fred i sektoren for cybersikkerhed i 2018 den hurtigst voksende delsektor, til dels som følge af ikrafttrædelsen af den generelle forordning om databeskyttelse.

45 Som defineret i SMV-definitionen, tilgængelig på: https://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition_en.

46 Forordningen bygger nemlig ikke kun på samtykke, men indeholder flere retsgrundlag til behandling af personoplysninger.

47 F.eks. vejledningen udarbejdet af den franske databeskyttelsesmyndighed: https://www.cnil.fr/fr/la-cnil-et-bpifrance-sassocient-pour-accompagner-les-tpe-et-pme-dans-leur-appropriation-du-reglement.

48 https://ec.europa.eu/commission/sites/beta-political/files/ds-02-18-544-en-n.pdf.

Forordningen indeholder værktøjer til påvisning af overholdelse, f.eks. standardkontraktbestemmelser, adfærdskodekser og de nyligt indførte certificeringsordninger.

Standardkontraktbestemmelser er standardbestemmelser, som kan indsættes i en kontrakt, f.eks. mellem en dataansvarlig og en databehandling, og som fastsætter de kontraherende parters forpligtelser i henhold til forordningen. Forordningen udvider mulighederne for at anvende standardkontraktbestemmelser både ved internationale overførsler og inden for EU[49]. Med hensyn til internationale overførsler viser[50] deres brede anvendelse, at de er meget nyttige med hensyn til at hjælpe virksomhederne med at opfylde deres forpligtelser, og at de især er til fordel for virksomheder, der ikke har ressourcer til at forhandle individuelle kontrakter med hver enkelt af deres databehandlingsleverandører.

En række sektorer betragter også vedtagelsen af standardkontraktbestemmelser som en nyttig metode til at fremme harmonisering, navnlig når det er Kommissionen, der vedtager dem. Kommissionen vil samarbejde med interessenterne om at gøre brug af mulighederne i henhold til forordningen og ajourføre eksisterende bestemmelser.

Overholdelsen af adfærdskodekser er et andet operationelt og praktisk værktøj, som industrien råder over til at gøre det lettere at påvise overholdelsen af forordningen[51]. Disse kodekser bør udvikles af handelssammenslutninger og organer, der repræsenterer kategorier af dataansvarlige og databehandlere, og de bør beskrive, hvordan databeskyttelsesreglerne kan gennemføres i en bestemt sektor. Ved at afpasse forpligtelserne[52] med risiciene kan de også vise sig at være en meget nyttig og omkostningseffektiv måde, hvorpå små og mellemstore virksomheder kan opfylde deres forpligtelser.

Endelig kan certificering også være et nyttigt instrument til at påvise overholdelsen af specifikke krav i forordningen. Det kan øge retssikkerheden for virksomhederne og fremme forordningen generelt. De certificerings- og akkrediteringsretningslinjer[53], der for nylig blev vedtaget af Det Europæiske Databeskyttelsesråd, vil gøre det muligt at udvikle certificeringsordninger i EU. Kommissionen vil overvåge denne udvikling og, hvis det er relevant, gøre brug af beføjelsen i henhold til forordningen til at fastlægge kravene til certificering. Kommissionen kan også udstede en standardiseringsanmodning til EU's standardiseringsorganer om elementer, der er relevante for forordningen.

---

[49] Se forordningens artikel 28. Standardkontraktbestemmelser vedtaget af Kommissionen har gyldighed i hele EU. De bestemmelser, som en databeskyttelsesmyndighed har vedtaget i henhold til artikel 28, stk. 8, er derimod kun bindende for den myndighed, der har vedtaget dem, og kan således anvendes som standardkontraktbestemmelser for behandlingsaktiviteter, der er omfattet af den pågældende myndigheds kompetence, jf. artikel 55 og 56.

[50] De er rent faktisk det vigtigste redskab, som virksomhederne benytter til deres dataeksport.

[51] Det Europæiske Databeskyttelsesråd vedtog retningslinjer for adfærdskodekser den 4.6.2019. De præciserer procedurerne og reglerne for indgivelse, godkendelse og offentliggørelse af kodekser på både nationalt plan og EU-plan.

[52] Betragtning 98 i forordningen.

[53] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-certification_en; https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42018-accreditation-certification-bodies-under_en.

VI. Fremskridt i retning af opadgående konvergens på internationalt plan

Behovet for beskyttelse af personoplysninger er imidlertid ikke begrænset til EU. Som det fremgår af en nylig global undersøgelse om sikkerhed på internettet, vokser tillidsunderskuddet i hele verden, hvilket betyder at borgerne ændrer adfærd på internettet[54]. Et stigende antal virksomheder afhjælper disse bekymringer ved egenhændigt at udvide rettighederne i henhold til forordningen til deres kunder uden for EU.

Lande verden over har i stigende grad fokus på lignende udfordringer, og de er derfor i gang med at indføre nye databeskyttelsesregler eller modernisere de eksisterende regler. Disse love har ofte en række fælles træk med EU's databeskyttelsesordning såsom en overordnet lovgivning snarere end sektorspecifikke regler, individuelle rettigheder, der kan håndhæves, og en uafhængig tilsynsmyndighed. Der er tale om en reel global udvikling, fra Sydkorea til Brasilien, fra Chile til Thailand, fra Indien til Indonesien. Det stadig mere globale medlemskab af Europarådets konvention 108[55] — moderniseret for nylig[56] med et betydeligt bidrag fra Kommissionen — er endnu et klart tegn på denne tendens til opadgående konvergens.

Fremme af sikre og frie datastrømme gennem afgørelser om tilstrækkeligheden af beskyttelsesniveauet i tredjelande

Denne stigende konvergens giver nye muligheder for at lette overførslen af oplysninger og dermed samhandelen og samarbejdet mellem offentlige myndigheder og samtidig forbedre beskyttelsen af EU-borgernes personoplysninger, der overføres til tredjelande.

I forbindelse med gennemførelsen af den strategi, der blev fastlagt i Kommissionens meddelelse fra 2017 om udveksling og beskyttelse af personoplysninger i en globaliseret verden[57], intensiverede Kommissionen sit samarbejde med tredjelande og andre internationale partnere på grundlag af en række elementer til konvergens mellem systemer til beskyttelse af privatlivets fred, som blev videreudviklet. Dette omfattede en undersøgelse af muligheden for at træffe afgørelser om tilstrækkeligheden af beskyttelsesniveauet i samarbejde med udvalgte

---

54 Se "CIGI-Ipsos Global Survey on Internet Security and Trust" fra 2019. Ifølge denne undersøgelse var 78 % af de adspurgte bekymrede for deres privatliv på internettet. 49 % angav, at de lagde færre personoplysninger på internettet på grund af deres mistillid, 43 % angav, at de havde gjort mere for at sikre deres udstyr, og 39 % svarede, at de blandt andre forholdsregler anvendte internettet mere selektivt. Undersøgelsen blev gennemført i 25 lande: Australien, Brasilien, Canada, Egypten, Frankrig, Tyskland, Storbritannien, Hongkong, Indien, Indonesien, Italien, Japan, Kenya, Mexico, Nigeria, Pakistan, Polen, Rusland, Sydafrika, Republikken Korea, Sverige, Tunesien, Tyrkiet og USA.

55 Europarådets konvention af 28. januar 1981 til beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger (ETS nr. 108) og tillægsprotokollen til konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger vedrørende tilsynsmyndigheder og grænseoverskridende videregivelse af personoplysninger (ETS nr. 181) fra 2001. Dette er det eneste bindende multilaterale instrument inden for databeskyttelse. De seneste lande, der har ratificeret konventionen, omfatter Argentina, Mexico, Kap Verde og Marokko.

56 Protokol om ændring af konventionen om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger (ETS nr. 108) som vedtaget på det 128. møde i Ministerkomitéen i Helsingør, Danmark, den 17.-18.5.2018. Den konsoliderede udgave af den moderniserede konvention 108 findes på: https://rm.coe.int/16808ade9d.

57 Meddelelse fra Kommissionen til Europa-Parlamentet og Rådet om udveksling og beskyttelse af personoplysninger i en globaliseret verden (COM(2017) 7 final).

tredjelande[58]. Dette arbejde har skabt vigtige resultater, navnlig ikrafttrædelsen i februar 2019 af aftalen mellem EU og Japan om tilstrækkeligheden af beskyttelsesniveauet, som skabte verdens største område med frie og sikre datastrømme. Forhandlingerne om tilstrækkeligheden af beskyttelsesniveauet med Sydkorea er i en fremskreden fase, og det undersøges, om der kan indledes drøftelser med en række latinamerikanske lande såsom Chile og Brasilien, afhængigt af fuldførelsen af de igangværende lovgivningsprocesser. Udviklingen er også lovende i visse dele af Asien, f.eks. Indien, Indonesien og Taiwan, og i de østeuropæiske og sydlige nabolande, hvilket kan åbne døren for fremtidige afgørelser om tilstrækkeligheden af beskyttelsesniveauet.

Samtidig glæder Kommissionen sig over, at andre lande, der har indført overførselsinstrumenter, som med hensyn til tilstrækkeligheden af beskyttelsesniveauet svarer til forordningens, har anerkendt, at EU og lande, der er anerkendt af EU som lande med til tilstrækkeligt beskyttelsesniveau, sikrer et sådant fornødent beskyttelsesniveau[59]. Dette kan skabe et netværk af lande, hvor data kan flyde frit.

Sideløbende hermed er der et intenst arbejde i gang med andre tredjelande såsom Canada, New Zealand, Argentina og Israel for at sikre kontinuitet i henhold til forordningen om afgørelser om tilstrækkeligheden af beskyttelsesniveauet, der er vedtaget på grundlag af databeskyttelsesdirektivet fra 1995. EU's og USA's værn om privatlivets fred har vist sig at være et nyttigt redskab til at sikre transatlantiske datastrømme baseret på et højt beskyttelsesniveau med mere end 4 700 deltagende virksomheder[60]. Den årlige evaluering sikrer, at det regelmæssigt kontrolleres, om rammen fungerer korrekt, og at nye problemstillinger kan håndteres i tide.

Da der ikke er nogen standardtilgang til datastrømme, samarbejder Kommissionen også med interessenter og Databeskyttelsesrådet for at udnytte det fulde potentiale af forordningens værktøjskasse til internationale overførsler. Der er tale om instrumenter såsom standardkontraktbestemmelser, udviklingen af certificeringsordninger, adfærdskodekser eller administrative ordninger for offentlige organer. I den forbindelse er Kommissionen interesseret i udveksling af erfaringer og bedste praksis med andre systemer, der kan have udviklet en særlig ekspertise i anvendelsen af disse værktøjer. Kommissionen vil overveje at gøre brug af de tillagte beføjelser i forordningen med hensyn til disse overførselsværktøjer, navnlig standardkontraktbestemmelserne.

Ud over rent bilaterale værktøjer kunne det også være en god idé at undersøge, om ligesindede lande kunne etablere en multinational ramme på dette område på et tidspunkt, hvor datastrømme er en stadig vigtigere del af handel, kommunikation og sociale interaktioner. Et sådant instrument vil muliggøre fri udveksling af data mellem de kontraherende parter og samtidig sikre det fornødne beskyttelsesniveau på grundlag af fælles

---

[58] Forordningen har også skabt mulighed for at træffe afgørelser om tilstrækkeligheden af beskyttelsesniveauet i internationale organisationer som led i EU's bestræbelser på at lette udvekslingen af oplysninger med sådanne enheder.

[59] Dette er f.eks. den tilgang, der anvendes af Argentina, Colombia, Israel og Schweiz.

[60] Værnet om privatlivets fred har således i de første tre år flere deltagende virksomheder end dets forgænger, safe harbour-programmet, havde efter 13 år.

værdier og konvergerende systemer. Det kunne f.eks. udvikles på grundlag af den moderniserede konvention 108 eller være inspireret af initiativet "Data Free Flow with Trust", som Japan lancerede i begyndelsen af året.

Udvikling af nye synergier mellem handels- og databeskyttelsesinstrumenter

Kommissionen fremmer konvergensen af databeskyttelsesstandarder på internationalt plan og er samtidig fast besluttet på at imødegå digital protektionisme. Med henblik herpå har Kommissionen udarbejdet specifikke bestemmelser om datastrømme og databeskyttelse i handelsaftaler, som den systematisk sætter på dagsordenen i sine bilaterale og multilaterale forhandlinger såsom de nuværende forhandlinger om e-handel i WTO-regi. Disse horisontale bestemmelser udelukker rent protektionistiske foranstaltninger såsom tvungne datalokaliseringskrav og sikrer samtidig parternes reguleringsmæssige autonomi til at beskytte den grundlæggende ret til databeskyttelse.

Selv om dialoger om databeskyttelse og handelsforhandlinger skal følge forskellige spor, kan de supplere hinanden. Aftalen mellem EU og Japan om tilstrækkeligheden af beskyttelsesniveauet er det bedste eksempel på sådanne synergier, der letter samhandlen yderligere og således øger fordelene ved den økonomiske partnerskabsaftale. Denne form for konvergens, der er baseret på fælles værdier og høje standarder og understøttes af effektiv håndhævelse, er faktisk det stærkeste grundlag for udveksling af personoplysninger, hvilket i stigende grad anerkendes af vores internationale partnere[61]. Da virksomhederne i stigende grad opererer på tværs af grænserne og foretrækker at anvende regelsæt, der minder om hinanden, i alle deres forretningsaktiviteter verden over, bidrager denne konvergens til at skabe et miljø, der fremmer direkte investeringer, letter samhandelen og øger tilliden mellem handelspartnere.

Fremme af udveksling af oplysninger til bekæmpelse af kriminalitet og terrorisme på grundlag af fornødne garantier

Større overensstemmelse mellem databeskyttelsesordninger kan også i væsentlig grad lette den meget nødvendige udveksling af oplysninger mellem lovgivnings-, politi- og retsmyndighederne i EU og tredjelande og dermed bidrage til et mere effektivt og hurtigere retshåndhævelsessamarbejde[62]. Med henblik herpå overvejer Kommissionen at gøre brug af muligheden for at vedtage afgørelser om tilstrækkeligheden af beskyttelsesniveauet i henhold til direktivet om databeskyttelse på retshåndhævelsesområdet med henblik på at uddybe samarbejdet med de vigtigste partnere om bekæmpelsen af kriminalitet og terrorisme. Desuden kan "paraplyaftalen"[63] mellem EU og USA, som trådte i kraft i februar 2017, anvendes som model for lignende aftaler med andre vigtige sikkerhedspartnere.

---

[61] Som det f.eks. afspejles i henvisningen til begrebet "Data Free Flow with Trust" i erklæringen fra lederne på G20-topmødet i Osaka: https://www.consilium.europa.eu/media/40124/final_g20_osaka_leaders_declaration.pdf.

[62] Se meddelelsen fra Kommissionen til Europa-Parlamentet, Rådet, Det Europæiske Økonomiske og Sociale Udvalg og Regionsudvalget, Den europæiske dagsorden om sikkerhed (COM(2015) 185 final).

[63] Aftale mellem EU og USA om beskyttelse af personoplysninger, der overføres og behandles med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger, herunder terrorisme, i forbindelse

Andre eksempler på vigtigheden af høje databeskyttelsesstandarder som grundlag for et stabilt retshåndhævelsessamarbejde med tredjelande er overførslen af passagerlister (PNR)[64] og udvekslingen af operationelle oplysninger mellem Europol og vigtige internationale partnere. I denne forbindelse er eller vil der snart blive indledt forhandlinger om internationale aftaler med flere sydlige nabolande[65].

Stærke databeskyttelsesgarantier vil også være et væsentligt element i enhver fremtidig aftale om grænseoverskridende adgang til elektronisk bevismateriale i strafferetlige efterforskninger på bilateralt niveau (aftale mellem EU og USA) eller på multilateralt niveau (anden tillægsprotokol til Europarådets Budapestkonvention om IT-kriminalitet)[66].

Fremme af samarbejdet mellem databeskyttelsesmyndigheder

På et tidspunkt, hvor problemer med overholdelse af privatlivets fred eller sikkerhedshændelser kan påvirke et stort antal personer samtidigt i flere jurisdiktioner, kan tættere former for samarbejde mellem tilsynsmyndigheder på internationalt plan bidrage til at sikre både en mere effektiv beskyttelse af individuelle rettigheder og et mere stabilt erhvervsklima. På denne baggrund vil Databeskyttelsesrådet i tæt kontakt med Kommissionen arbejde på at lette retshåndhævelsessamarbejdet og den gensidige bistand mellem tilsynsmyndigheder i EU og i tredjelande, herunder ved at gøre brug af de nye beføjelser på dette område, der er fastsat i forordningen[67]. Dette kunne omfatte forskellige former for samarbejde i forbindelse med udvikling af fælles fortolkningsmæssige eller praktiske redskaber[68] til udveksling af oplysninger om igangværende undersøgelser.

Endelig agter Kommissionen også at intensivere sin dialog med regionale organisationer og netværk såsom Sammenslutningen af Sydøstasiatiske Nationer (ASEAN), Den Afrikanske Union, netværket af asiatiske privatlivsmyndigheder (APPA) eller det iberoamerikanske databeskyttelsesnetværk (RIPD), der spiller en stadig vigtigere rolle i udformningen af fælles databeskyttelsesstandarder, fremme af udvekslingen af bedste praksis og af samarbejdet mellem retshåndhævende myndigheder. Kommissionen vil også samarbejde med Organisationen for Økonomisk Samarbejde og Udvikling og inden for rammerne af det

---

med politisamarbejde og retligt samarbejde i straffesager: https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=celex:22016A1210(01) ("paraplyaftalen"). Paraplyaftalen er den første bilaterale internationale aftale på retshåndhævelsesområdet med et omfattende katalog af databeskyttelsesrettigheder og -forpligtelser i overensstemmelse med gældende EU-ret. Det er et vellykket eksempel på, hvordan retshåndhævelsessamarbejdet med en vigtig international partner kan styrkes ved at forhandle sig frem til et stærkt sæt databeskyttelsesgarantier.

64 I FN's Sikkerhedsråds resolution (SCR) 2396 af 21. december 2017 opfordres alle FN's medlemsstater til at udvikle kapaciteten til at indsamle, behandle og analysere PNR-oplysninger under fuld overholdelse af menneskerettighederne og de grundlæggende frihedsrettigheder. Se også meddelelse fra Kommissionen om den europæiske dagsorden om sikkerhed (COM (2015)185 final): https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:52015DC0185&from=DA.

65 https://ec.europa.eu/home-affairs/news/security-union-strengthening-europols-cooperation-third-countries-fight-terrorism-and-serious_en.

66 http://europa.eu/rapid/press-release_IP-19-2891_da.htm.

67 Se artikel 50 i forordningen om internationalt samarbejde om databeskyttelse. Denne bestemmelse dækker en lang række former for samarbejde, lige fra oplysninger om databeskyttelseslovgivningen til indbringelse af klager og efterforskningsbistand.

68 F.eks. fælles skabeloner for anmeldelser af brud.

økonomiske samarbejde i Asien-Stillehavsområdet med henblik på at skabe konvergens i retning af et højt databeskyttelsesniveau.

VII. Databeskyttelseslovgivning som en integreret del af en bred vifte af politikker

Beskyttelsen af personoplysninger er garanteret og integreret i en række af Unionens politikker.

Telekommunikationstjenester og elektroniske kommunikationstjenester

Kommissionen vedtog sit forslag til forordning om databeskyttelse inden for elektronisk kommunikation i januar 2017[69]. Forslaget har til formål at beskytte kommunikationshemmeligheden som fastsat i chartret om grundlæggende rettigheder, men også at beskytte personoplysninger, der kan være en del af en kommunikation, og slutbrugernes terminaludstyr.

Forslaget til forordning om e-databeskyttelse præciserer og supplerer forordningen ved at fastsætte specifikke regler til ovennævnte formål. Det moderniserer de nuværende EU-regler om databeskyttelse[70] for at afspejle den teknologiske og retlige udvikling. Det øger beskyttelsen af privatlivets fred ved at udvide anvendelsesområdet for de nye regler til at omfatte leverandører af "over-the-top"-kommunikationstjenester og skaber derved lige vilkår for alle elektroniske kommunikationstjenester. Europa-Parlamentet vedtog et mandat til at indlede triloger i oktober 2017, men Rådet er endnu ikke nået til enighed om en generel tilgang. Kommissionen er fortsat fuldt engageret i e-databeskyttelsesforordningen og vil støtte EU-lovgiverne i deres bestræbelser på at opnå en hurtig vedtagelse af den foreslåede forordning.

Sundhed og forskning

Fremme af udveksling af sundhedsoplysninger, som er følsomme oplysninger i henhold til forordningen, mellem medlemsstaterne er blevet en stadig vigtigere faktor af hensyn til samfundsinteresser på folkesundhedsområdet. Disse omfatter levering af sundhedsplejetjenester eller behandlinger, beskyttelse mod alvorlige grænseoverskridende sundhedsrisici og sikring af høje kvalitets- og sikkerhedsstandarder for sundhedspleje og lægemidler eller medicinsk udstyr. I forordningen fastsættes regler, der sikrer lovlig og pålidelig behandling og udveksling af helbredsoplysninger i hele EU. Disse regler gælder også for tredjeparters adgang til sundhedsoplysninger om patienter, herunder data i patientjournaler, e-recepter og på lang sigt omfattende elektroniske patientjournaler, og deres anvendelse til videnskabelige forskningsformål. På det specifikke område for kliniske forsøg

---

69 https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=CELEX%3A52017PC0010.

70 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 (Direktiv om databeskyttelse inden for elektronisk kommunikation) (EFT L 201 af 31.7.2002, s. 37).

har Kommissionen også udarbejdet specifikke spørgsmål og svar om samspillet mellem forordningen om kliniske forsøg[71] og den generelle forordning om databeskyttelse[72].

Kunstig intelligens

Da kunstig intelligens er ved at få strategisk betydning, er det afgørende at udforme globale regler for udviklingen og anvendelsen. Kommissionens fremme af udviklingen og indførelsen af kunstig intelligens er baseret på en menneskecentreret tilgang, hvilket betyder, at kunstig intelligens-applikationer skal respektere grundlæggende rettigheder[73]. I denne forbindelse er de regler, der er fastsat i forordningen, en generel ramme med specifikke forpligtelser og rettigheder, der er særlig relevante for behandlingen af personoplysninger i den kunstige intelligens. I forordningen fastsættes f.eks. retten til ikke at blive gjort til genstand for en afgørelse, som alene bygger på automatisk behandling, undtagen i visse situationer[74]. Den omfatter også specifikke gennemsigtighedskrav vedrørende brug af automatiske afgørelser, nemlig forpligtelsen til at oplyse om forekomsten af sådanne afgørelser og give relevante oplysninger og forklare betydningen af behandlingen, og hvilke konsekvenser den kan have for den enkelte[75]. Disse centrale principper i forordningen er blevet anerkendt af ekspertgruppen på højt plan vedrørende kunstig intelligens[76], Organisationen for Økonomisk Samarbejde og Udvikling[77] og G20[78] som særlig relevante for håndteringen af de udfordringer og muligheder, som kunstig intelligens giver. Det Europæiske Databeskyttelsesråd har identificeret kunstig intelligens som et af de mulige emner i sit arbejdsprogram for 2019-2020[79].

Transport

Udviklingen af opkoblede køretøjer og intelligente byer afhænger i stigende grad af behandling og udveksling af store mængder personoplysninger mellem flere forskellige parter, herunder køretøjer, bilproducenter, udbydere af telematiktjenester og offentlige myndigheder med ansvar for vejinfrastruktur. Dette miljø med flere aktører indebærer en vis kompleksitet med hensyn til fordelingen af rollerne og ansvarsområderne mellem de

---

71 https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=celex%3A32014R0536.

72 https://ec.europa.eu/health/sites/health/files/files/documents/qa_clinicaltrials_gdpr_en.pdf.

73 Kommissionens meddelelse af 8.4.2019 om opbygning af tillid til menneskecentreret kunstig intelligens: https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=COM%3A2019%3A0168%3AFIN.
Etiske retningslinjer for pålidelig kunstig intelligens fremlagt af højniveauekspertgruppen den 8.4.2019: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai. Se også OECD-Rådets henstilling om kunstig intelligens: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449, G20-principperne om kunstig intelligens, der blev godkendt som en del af erklæringen fra lederne på G20-topmødet i Osaka: https://www.g20.org/pdf/documents/en/annex_08.pdf, og G20-ministrenes erklæring om handel og den digitale økonomi: https://g20trade-digital.go.jp/dl/Ministerial_Statement_on_Trade_and_Digital_Economy.pdf.

74 Forordningens artikel 22.

75 Forordningens artikel 13, stk. 2, litra f).

76 https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence.

77 Rådets henstilling om kunstig intelligens: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

78 G20-ministrenes erklæring om handel og den digitale økonomi: https://g20trade-digital.go.jp/dl/Ministerial_Statement_on_Trade_and_Digital_Economy.pdf.

79 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-02-12plen-2.1edpb_work_program_en.pdf.

forskellige aktører, der er involveret i behandlingen af personoplysninger, og med hensyn til, hvordan det sikres, at alle aktørers behandling af personoplysninger er lovlig. Overholdelse af forordningen og e-databeskyttelseslovgivningen er afgørende for en vellykket udbredelse af intelligente transportsystemer inden for alle transportformer og for udbredelsen af digitale værktøjer og tjenester, der muliggør større mobilitet for personer og varer[80].

Energi

Udviklingen af digitale løsninger i energisektoren afhænger i stigende grad af behandlingen af personoplysninger. Den lovgivning, der blev vedtaget som led i pakken om ren energi for alle europæere[81], indeholder nye bestemmelser, der muliggør digitaliseringen af elektricitetssektoren, og regler om dataadgang, dataforvaltning og interoperabilitet, der gør det muligt at håndtere forbrugerdata i realtid med henblik på at opnå besparelser og fremme egenproduktion og deltagelse i energimarkedet. Overholdelse af databeskyttelsesreglerne er derfor af stor betydning for en vellykket gennemførelse af disse bestemmelser.

Konkurrence

Behandlingen af personoplysninger er i stigende grad et element, der skal tages højde for i konkurrencepolitikken[82]. Da databeskyttelsesmyndighederne er de eneste myndigheder, der har kompetence til at vurdere en overtrædelse af databeskyttelsesreglerne, samarbejder konkurrence- og forbruger- og databeskyttelsesmyndighederne, når det er nødvendigt, i krydsfeltet mellem deres respektive kompetencer, og det vil de også gøre fremover. Kommissionen vil fremme dette samarbejde og følge udviklingen nøje.

Valgsammenhæng

I sin vejledning i anvendelsen af Unionens databeskyttelseslovgivning i forbindelse med afholdelse af valg[83], der blev udsendt i september 2018 som en del af valgpakken[84], henledte Kommissionen opmærksomheden på regler af særlig betydning for de aktører, der er involveret i valg, herunder problemstillinger vedrørende mikromålretning af kommunikation mod vælgere. Denne vejledning blev bekræftet i en erklæring fra Det Europæiske Databeskyttelsesråd[85], og en række databeskyttelsesmyndigheder udstedte retningslinjer på nationalt plan. Valgpakken omfattede også en opfordring til de enkelte medlemsstater om at oprette et nationalt valgnetværk med deltagelse af nationale myndigheder med kompetence inden for valganliggender og myndigheder med ansvar for overvågning og håndhævelse af regler, f.eks. databeskyttelsesregler, om onlineaktiviteter af relevans for valget. Der blev også vedtaget nye foranstaltninger vedrørende indførelse af sanktioner for europæiske politiske partiers og fondes overtrædelse af databeskyttelsesreglerne. Kommissionen anbefalede

---

80 F.eks. ved at gøre det lettere at planlægge og anvende forskellige transportmidler under hele rejsen.

81 Navnlig elektricitetsdirektivet: https://eur-lex.europa.eu/legal-content/DA/ALL/?uri=CELEX%3A32009L0072.

82 F.eks. sag M.8788 — Apple/Shazam — og sag M.8124 — Microsoft/LinkedIn.

83 https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:52018DC0638&from=EN.

84 http://europa.eu/rapid/press-release_IP-18-5681_da.htm.

85 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections_en.pdf.

medlemsstaterne at anvende samme tilgang på nationalt plan. I evalueringen af valget til Europa-Parlamentet i 2019, som forventes udsendt i oktober 2019, vil der også blive taget hensyn til databeskyttelsesaspekter.

Retshåndhævelse

En virkningsfuld og ægte sikkerhedsunion kan kun opbygges i fuld overensstemmelse med de grundlæggende rettigheder, der er forankret i EU's charter og afledt EU-ret, herunder fornødne databeskyttelsesgarantier, for at muliggøre en sikker udveksling af personoplysninger med henblik på retshåndhævelse. Enhver begrænsning af den grundlæggende ret til beskyttelse af privatlivets fred og databeskyttelse underlægges en streng nødvendigheds- og proportionalitetstest.

VIII. Konklusion

På grundlag af de oplysninger, der er til rådighed til dato, og dialogen med interessenterne er det Kommissionens foreløbige vurdering, at forordningens første anvendelsesår generelt er forløbet godt. Som det fremgår af denne meddelelse, er der imidlertid behov for yderligere fremskridt på en række områder.

Gennemførelse og supplering af lovgivningsrammen:

- De tre medlemsstater, der endnu ikke har ajourført deres nationale databeskyttelseslovgivning, skal gøre dette hurtigst muligt. Alle medlemsstater bør afslutte tilpasningen af deres sektorlovgivning til forordningens krav.

- Kommissionen vil anvende alle de værktøjer, den har til rådighed, herunder traktatbrudsprocedurer, for at sikre, at medlemsstaterne overholder forordningen og begrænser fragmenteringen af databeskyttelsesrammen.

Et nyt forvaltningssystem, der udnytter sit potentiale fuldt ud:

- Medlemsstaterne bør afsætte tilstrækkelige menneskelige, finansielle og tekniske ressourcer til de nationale databeskyttelsesmyndigheder.

- Databeskyttelsesmyndighederne bør intensivere deres samarbejde, f.eks. ved at foretage fælles undersøgelser. Medlemsstaterne bør lette gennemførelsen af sådanne undersøgelser.

- Databeskyttelsesrådet bør videreudvikle en EU-databeskyttelseskultur og udnytte værktøjerne i forordningen fuldt ud for at sikre en harmoniseret anvendelse af reglerne. Det bør fortsætte sit arbejde med retningslinjer, navnlig for små og mellemstore virksomheder.

- Ekspertisen i Databeskyttelsesrådets sekretariat bør styrkes for at understøtte og lede Databeskyttelsesrådets arbejde mere effektivt.

- Kommissionen vil fortsat støtte databeskyttelsesmyndighederne og Databeskyttelsesrådet, navnlig ved at deltage aktivt i Databeskyttelsesrådets arbejde og henlede rådets opmærksomhed på EU-lovgivningens krav i forbindelse med gennemførelsen af forordningen.

- Kommissionen vil støtte interaktionen mellem databeskyttelsesmyndigheder og andre myndigheder, navnlig på konkurrenceområdet, idet den fuldt ud respekterer deres respektive kompetencer.

Støtte til og inddragelse af interessenter:

- Databeskyttelsesrådet bør forbedre den måde, hvorpå det inddrager interessenter i sit arbejde. Kommissionen vil fortsat yde finansiel støtte til databeskyttelsesmyndighederne for at hjælpe dem med at nå ud til interessenterne.

- Kommissionen vil fortsætte sine oplysningskampagner og samarbejdet med interessenterne.

Fremme af international konvergens:

- Kommissionen vil intensivere sin dialog om tilstrækkeligheden af beskyttelsesniveauet med relevante nøglepartnere yderligere, herunder på retshåndhævelsesområdet. Den sigter navnlig mod at afslutte de igangværende forhandlinger med Sydkorea i de kommende måneder. I 2020 vil den aflægge rapport om evalueringen af de 11 afgørelser om tilstrækkeligheden af beskyttelsesniveauet, der er vedtaget i henhold til databeskyttelsesdirektivet.
- Kommissionen vil fortsætte sit arbejde, bl.a. gennem teknisk bistand til udveksling af oplysninger og bedste praksis med de lande, der ønsker at vedtage moderne lovgivning om privatlivets fred, og fremme samarbejdet med tredjelandes tilsynsmyndigheder og regionale organisationer.
- Kommissionen vil samarbejde med multilaterale og regionale organisationer om at fremme høje databeskyttelsesstandarder som en drivkraft for handel og samarbejde (f.eks. inden for rammerne af initiativet "Data Free Flow with Trust", der blev lanceret af Japan i forbindelse med G20).

Ifølge forordningen[86] skal Kommissionen aflægge rapport om gennemførelsen i 2020. Dette vil være en lejlighed til at vurdere de fremskridt, der er gjort, og om de forskellige elementer i den nye databeskyttelsesordning efter to års anvendelse er fuldt operationelle. Med henblik herpå vil Kommissionen samarbejde med Europa-Parlamentet, Rådet, medlemsstaterne, Det Europæiske Databeskyttelsesråd, relevante interessenter og borgerne.

---

[86] Forordningens artikel 97.