

## Baggrundspapir

### EU's Digital Omnibus, november 2025 Med fokus på forslagene til ændringer i GDPR

---

#### Opsummering

På baggrund af Draghi-rapporten har EU Kommissionen lagt op til en justering af GDPR mhp. at lette byrder for erhvervslivet i EU og fremme innovation – herunder brugen af AI – i EU.

Rådet for Digital Sikkerhed (Rådet) finder overordnet, at databeskyttelsesforordningen har bidraget meget væsentligt til at fremme informationssikkerheden hos dataansvarlige i hele EU. Sikkerhedskravene i artikel 32 samt kravene i artikel 25 om at designe de fundamentale databeskyttelsesprincipper fra artikel 5 ind i digitale løsninger har været en væsentlig årsag hertil. Disse krav har sparet europæiske virksomheder for mange penge i tabte omkostninger relateret til cybersikkerhedshændelser og ved øget tillid til digitaliseringen i både den offentlige og private sektor.

Omvendt har vi nu syv års erfaringer med GDPR, og Rådet finder, at der er betydelige muligheder for at spare de dataansvarlige for unødige omkostninger og lette adgangen til brug af teknologi, således at innovationen indenfor EU kan styrkes, og uden at de registreredes rettigheder berøres væsentligt.

Rådet finder videre, at databeskyttelsesforordningen har haft både negative og positive konsekvenser for virksomheder i EU. Rådet finder derfor, at Draghis kritik er lidt for ensidig. Rådet har indledningsvis i **første hovedafsnit** identificeret en række kilder, som analyserer og præciserer de økonomiske effekter af GDPR for de omfattede organisationer. Konklusionen er, at organisationernes omkostninger til processer, teknologier, konsulenter m.v. kan henføres til tiltag, som alligevel skulle gennemføres i de organisationer, der ønskede sig god informationssikkerhed. Foranstaltningerne har resulteret i undgåede databrud, har givet øget forretning gennem tillid og generelt har haft en positiv effekt i afkast. Det er på den baggrund uklart, hvad GDPR isoleret set faktisk har "kostet" organisationerne i nettotab.

Rådet har herefter i **andet hovedafsnit** gengivet EU Kommissionens forslag til justeringer af GDPR.

Rådet finder, at flere af EU Kommissionens forslag er ganske nyttige. Omvendt tager EU Kommissionen ikke fat på de byder, som er størst for de dataansvarlige. Rådet finder derfor behov for, at Omnibussen skal udvides, når der nu alligevel tages hul på at justere forordningen.

Rådet har gengivet sin holdning til Kommissionens forslag i **tredje hovedafsnit** og er især skeptisk overfor to af EU Kommissionens forslag:

- Hvis ændringen af definitionen af personoplysninger vedtages, skaber det øget compliancemæssig usikkerhed hos de dataansvarlige og flere omkostninger til at vurdere, hvilke data der falder indenfor, og hvilke data der falder udenfor forordningen. Videre skabes der en betydelig usikkerhed for de registrerede ved, at oplysninger nogen kan henføre til dem, måske falder i de forkerte hænder og/eller anvendes til andre formål, end de registrerede er bekendt hermed – herunder til formål, som er i modstrid med deres interesser.

- Når formålsforenelighedstesten sættes ud af kraft for viderebehandlinger i samfundets interesse, til videnskabelige eller historiske forskningsformål, kan den dataansvarlige administrativt uden samtykke eller uden et specifikt demokratisk vedtaget retligt grundlag behandle de personoplysninger, de er i besiddelse af, hvis den dataansvarlige kan argumentere for, at behandlingen opfylder et af de tre nævnte formål. Der er konstant pres på, at dataansvarlige i både den offentlige og private sektor anvender personoplysninger til nye formål. Hvis der ikke længere skal laves en formålsforenelighedstest, vil der ske et "function creep", hvor de personoplysninger, den dataansvarlige er i besiddelse af, benyttes til alle mulige formål, uden at den registrerede har indflydelse herpå – herunder f.eks. langt mere overvågning af de registrerede. Det vil underminere de registreredes rettigheder og tillid til digitaliseringen.

Rådet finder som nævnt, at der er et langt større rum end EU Kommissionen lægger op til for at modificere databeskyttelsesforordningen. GDPR fejler når compliance bliver symbolsk og håndhævelsen er fragmenteret. Rådet foreslår derfor en håndhævelses- og proportionalitetsreform med det formål at forbedre konkurrenceevnen ved at reducere byrder for europæiske organisationer uden væsentlig effekt på de registreredes rettigheder. Rådet har i **fjerde hovedafsnit** lavet et katalog med forslag til at justere GDPR til fordel for europæiske organisationer uden at underminere de registreredes rettigheder.

- Rådet anbefaler, at der sker en forskydning af en del af ansvaret for behandling fra den dataansvarlige til databehandlerne. Det er i langt de fleste tilfælde en illusion, at det er den dataansvarlige, der instruerer databehandleren, navnlig for så vidt angår de store teknologileverandører og andre leverandører af standardydelser, f.eks. hosting og drift, support mv. Den dataansvarlige står i den sammenhæng ofte i et paradoks, at den dataansvarlige kan tage imod en tjeneste fra databehandleren eller finde en anden databehandler (hvis ydelser i mange tilfælde vil lide af samme retlige mangler som den oprindelige, i hvert fald for så vidt angår de store teknologileverandører). Derfor bør ansvaret for en lang række af forordningens bestemmelser flyttes fra den dataansvarlige til databehandleren, som er den aktør, der reelt har indflydelse på arkitektur, funktionalitet, programmering, behandlingssikkerhed, anvendelse af underdatabehandlere, tredjelandsoverførsler og andre forhold vedrørende deres applikationer eller tjenester.

Rådet foreslår helt konkret at der introduceres en definition i artikel 4 for "*Systemiske databehandlere*", som

- a) leverer standardiserede behandlinger til >X dataansvarlige i EU, eller
- b) fastlægger væsentlige tekniske og organisatoriske rammer, som den dataansvarlige ikke realistisk kan ændre.

Desuden skal der introduceres en ny artikel 28a, hvor der indføres selvstændige krav til de systemiske databehandlere:

- a) gennemføre og opdatere DPIA'er for deres *standardtjenester*,
- b) dokumentere tredjelandsoverførsler,
- c) levere "compliance packs" til kunder.

Ligesom man på andre områder køber et produkt, som leverandøren garanterer, er lovligt, skal man også kunne gøre dette på det digitale område uden at have dyb specialiseret faglig viden. Det vil lempe byrderne for de dataansvarlige enormt. Som et særligt eksempel på en kolossal omkostningsbesparelse for dataansvarlige kan nævnes tilsyn, hvor nuværende retningslinjer lægger op til, at de dataansvarlige skal have indsigt i hele databehandlerens "behandlingskæde", hvilket ofte er umuligt, navnlig for så vidt angår de store teknologileverandører, som anvender et utal af interne og eksterne underdatabehandlere.

- Det er spild af ressourcer, at millioner af dataansvarlige i EU er pligtige til at lave de samme vurderinger af de samme løsninger fra IT-leverandørerne. Rådet foreslår derfor, at der under EU Kommissionen nedsættes et organ, som i samarbejde med EDPB vurderer og løbende fører tilsyn med de (f.eks. 100) mest udbredte databehandlaftaler i EU. Det vil lempe byrderne for de dataansvarlige enormt.
- Databeskyttelse gennem design er ikke slået ordentligt igennem med GDPR. Mange IT-leverandører har ikke den fornødne fokus på området, og den gældende praksis er elastisk i metermål grundet tilbageholdenhed med at pålægge krav om et sikkert design. Rådet foreslår derfor, at der strammes op på dette område, således at IT-leverandørerne dokumenterer designvalget for deres tjenester og dermed skaber mere gennemsigtighed om, f.eks. hvorfor kryptering eller pseudonymisering er tilvalgt eller fravalgt. Igen er dette ikke en byrde, som bør påhvile kunden, den dataansvarlige, fordi de ikke har indflydelse herpå. Tilsvarende fsva. udarbejdelsen af konsekvensanalyser.
- Mange virksomheder handler kun med andre virksomheder. I det omfang der handles mellem virksomheder, og hvor en fysisk persons kontaktoplysninger fremgår af transaktionerne mellem virksomhederne, kan disse personoplysninger som regel ikke siges at være relateret til personen som individ – men kun til personen som professionel repræsentant for sin virksomhed. Personoplysninger, som udveksles i transaktioner mellem virksomheder (B2B), bør derfor undtages forordningen.

I dette sidste hovedafsnit af nærværende papir findes mange flere forslag til justeringer, som Rådet finder, EU Kommissionen bør arbejde videre med, og som kan spare de dataansvarlige for omkostninger uden at berøre de registreredes rettigheder væsentligt.

### **GDPRs økonomiske fordele og ulemper**

GDPR har aldrig være elsket af de dataansvarlige. Blandt andet fordi reglerne er svære at forstå, og fordi der har været en oplevelse af, at det er bureaukratisk og omkostningstungt at implementere reglerne. I september 2024 udkom på EU Kommissionens foranledning den såkaldte Draghi-rapport<sup>1</sup>, som bl.a. kritiserede GDPR på en række områder:

- *Fragmenteret og inkonsekvent implementering i medlemsstaterne*  
Draghi kritiserer, at GDPR implementeres forskelligt på tværs af EU-lande, hvilket skaber retlig usikkerhed og hæmmer virksomhedernes mulighed for at skalere på tværs af EU.
- *”Heavy gold-plating” af GDPR-regler i flere medlemsstater*  
Nogle lande lægger ekstra nationale krav oven på EU-reglerne, hvilket gør den praktiske efterlevelse tungere end nødvendigt, og øger byrderne for virksomheder.
- *For komplekst og administrativt tungt regelsæt*  
Draghi har offentligt argumenteret for, at GDPR’s ”primary law” bør radikalt forenkles for at sikre både innovation og effektiv håndhævelse.
- *GDPR som barriere for europæisk innovation og AI-kapacitet*  
Rapporten sætter fokus på, at den nuværende udformning af GDPR begrænser Europas evne til at

---

<sup>1</sup> [https://commission.europa.eu/topics/competitiveness/draghi-report\\_en](https://commission.europa.eu/topics/competitiveness/draghi-report_en)

konkurrere globalt inden for AI og dataintensive teknologier — både pga. usikkerhed og compliance-omkostninger.

Der er således en markant kritik af de omkostninger og barrierer, som GDPR skaber – især for EU's erhvervs- liv. EU Kommissionen har på den baggrund lagt op til en let revision af GDPR.

Det er imidlertid vanskeligt at fastslå, hvilke omkostninger GDPR reelt har. Forskellige undersøgelser peger i forskellige retninger.

På den ene side er det klart, at GDPR har medført både etableringsomkostninger og løbende driftsomkostninger hos de dataansvarlige. PwC lavede i 2020 en undersøgelse, som viste, at 88% af internationale virksomheder bruger mere end 1 mio. USD for at efterleve GDPR<sup>2</sup>. Et estimat af implementeringsomkostningerne tilbage i fra 2018 lavet af IAPP og Forbes viste, at amerikanske Fortune 500 virksomheder brugte 7,8 mia. \$ på at forberede sig på GDPR, mens britiske FTSE 350 virksomheder brugte 1,1 mia. \$ på at forberede sig<sup>3</sup>. Forskellen skyldes, at europæiske virksomheder generelt var bedre forberedt på reglerne, eftersom de europæiske databeskyttelsesregler blev introduceret i form af databeskyttelsesdirektivet fra 1995. En analyse fra 2017 viser, at de forskellige brancher betaler meget forskellige beløb på at blive compliant med de persondataretlige regler: Den finansielle sektor og sundhedssektoren rammes meget hårdere end andre, fordi reguleringen er meget mere omfattende i disse sektorer<sup>4</sup>. Samme analyse viser også, at omkostningerne ved non-compliance er dobbelt så store som omkostningerne ved compliance.

Det, som driver omkostningerne op, er bl.a.:

- Juridiske omkostning – herunder udpegelse af DPO'er brug af advokathuse, udvidelse af juridiske afdelinger, brug af juridisk rådgivning, brug af andre konsulenter m.v. Dette er den største omkostning.
- Opbygning af teknisk infrastruktur – f.eks. anvendelse af kryptering, etablering af adgangskontrol og analyse af logning.
- Driftsmæssige opgaver – som f.eks. håndtering af indsigts- og slettebegøring
- Certificeringer og auditering.
- Bøder for non-compliance.
- Reduceret innovation og færre investeringer i europæisk digitalisering.
- Større omkostninger ved at handle med data og generelt mindre handel grundet barrierer for data-overførsel.

På den anden side har der gennem hele digitaliseringen været en tendens til have fokus på at udvikle funktionalitet og skabe effektivisering, mens der har været mindre fokus på sikkerhed og databeskyttelse. Både leverandører og kunder synes at have underinvesteret i informationssikkerhed, fordi der har været fokus på at få tjenester hurtigt på markedet fra leverandørerne og på at hente effektiviseringsgevinster fra kunderne. Dette illustreres bl.a. gennem en tysk undersøgelse, hvor 30% af respondenterne vurderer, at GDPR forsinket optaget af ny teknologi – formodentlig fordi man er nødt til at arbejde med sikkerhed og databeskyttelse<sup>5</sup>. Når der så faktisk bruges penge på sikkerhed og databeskyttelse viser en fransk undersøgelse, at de

---

<sup>2</sup> <https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/privacy-reset.html>

<sup>3</sup> <https://www.forbes.com/sites/oliversmith/2018/05/02/the-gdpr-racket-whos-making-money-from-this-9bn-business-shakedown/>

<sup>4</sup> <https://www.globalscape.com/resources/infographics/data-compliance-costs>

<sup>5</sup> <https://www.zew.de/en/press/latest-press-releases/six-years-of-gdpr-companies-remain-critical>

omkostninger, der er brugt på compliance med databeskyttelsesreglerne, har bidraget til at undgå tab relateret til cybersikkerhed på mellem 585 mio. EUR og 1,4 mia. EUR<sup>6</sup>.

Databeskyttelsesforordningen har bidraget meget væsentligt til at fremme informationssikkerheden hos dataansvarlige i hele EU. Sikkerhedskravene i artikel 32 samt kravene i artikel 25 om at designe de fundamentale databeskyttelsesprincipper fra artikel 5 ind i digitale løsninger har været en væsentlig årsag hertil. De økonomiske fordele ved at være compliant med GDPR understøttes af mange forskellige kilder:

- I en undersøgelse fra CISCO fra 2025 angiver 86%, at privacy-lovgivning har en positiv effekt på deres organisation, og selv om der er compliance-omkostninger, vurderer 96% af respondenterne, at fordelene ved investeringerne er større end omkostningerne<sup>7</sup>.
- Samme undersøgelse viser, at 95% mener, at kunderne ikke vil handle, hvis data ikke er ordentligt beskyttet, at 99% mener at eksterne privacy-certificeringer er vigtige, når der vælges leverandør, at 97% mener, at organisationen har et ansvar for at bruge data etisk, og endelig at 90% mener at stærk privacy regulering er vigtigt, for at kunderne vil dele deres data<sup>8</sup>.
- En anden undersøgelse fra 2024 fra CISCO viser, at investeringer i databeskyttelse giver et afkast på 1,6x investeringen<sup>9</sup>.
- IBM's årlige "Cost of Data Breach" rapporter understøtter i flere af rapporterne dette: Jo mere organisationen har arbejdet med compliance, jo mindre bliver omkostningerne ved et databrud<sup>10</sup>.
- PwC har i 2021 beskrevet, hvordan organisationer kan få fordele af at gennemføre en "privacy first" forretningsstrategi, fordi det er afgørende for kunderne. Videre kan man reducere complianceomkostningerne gennem automatisering<sup>11</sup>.
- Organisationer med en høj grad af compliancefokus har generelt en højere datakvalitet (som f.eks. resultatet af dataflowanalyser), hvilket er en forudsætning for at kunne drage nytte af AI.

Mange af organisationernes omkostninger til processer, teknologier, konsulenter m.v. kan henføres til tiltag, som alligevel skulle gennemføres i de organisationer, der ønskede sig god informationssikkerhed. De foranstaltninger, som understøtter informationssikkerhed, understøtter nemlig også databeskyttelse. Hertil kommer, at foranstaltningerne har resulteret i af undgå databrud, har givet øget forretning gennem tillid og generelt har haft en positiv effekt i afkast. Det er på den baggrund uklart, hvad GDPR isoleret set faktisk har kostet.

Fra et europæisk perspektiv er der et naturligt fokus på GDPR. Men det er værd at nævne, at efter GDPR har mange andre lande og regioner etableret databeskyttelseslovgivning. Ifølge Cisco har mere end 160 lande<sup>12</sup> brugt GDPR som en skabelon for at lave deres egne databeskyttelseslovgivninger – herunder bl.a.:

- Japan: Act on the Protection of Personal Information (APPI) fra 2003 med justeringer, så den kom tæt på GDPR fra 2017 og 2022
- Canada: PIPEDA og Digital Charter Implementation Act fra 2000 med justeringer i 2020 og 2022

<sup>6</sup> Commission Staff Working document SWD(2025) 836 final, pp.34-35, <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2025:0836:FIN:EN:PDF>

<sup>7</sup> <https://blogs.cisco.com/security/unlocking-the-privacy-advantage-to-build-trust-in-the-age-of-ai>

<sup>8</sup> <https://www.cisco.com/c/en/us/about/trust-center/data-privacy-benchmark-study.html>

<sup>9</sup> [https://www.cisco.com/c/dam/en\\_us/about/doing\\_business/trust-center/docs/cisco-privacy-benchmark-study-2024.pdf](https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-privacy-benchmark-study-2024.pdf)

<sup>10</sup> <https://cdn.table.media/assets/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf>

<sup>11</sup> <https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/privacy-reset.html>

<sup>12</sup> <https://blogs.cisco.com/security/unlocking-the-privacy-advantage-to-build-trust-in-the-age-of-ai>

- Sydafrika: Protection of Personal Information Act (POPIA) fra 2013/2021
- Brasilien: Lei Geral de Proteção de Dados (LGPD) fra 2020
- Kina: Personal Information Protection Law (PIPL) fra 2021
- Indien: Digital Personal Data Protection Act (DPDP) fra 2023
- Sydkorea: Personal Information Protection Act (PIPA), justeret i 2023
- Mange andre: Argentina, Chile, New Zealand, Singapore, Sveits,....

Der er også databeskyttelseslovgivning med varierende indhold i forskellige amerikanske stater f.eks.:

- California Consumer Privacy Act (CCPA) fra 2020
- The Virginia Consumer Data Protection Act (VCDPA) fra 2021
- The Utah Consumer Privacy Act (UCPA) fra 2023
- The Florida Digital Bill of Rights (FDBR) fra 2024.

Ud over de generelle databeskyttelseslove finder der også sektor specifik lovgivning i mange lande. Fra USA kendes f.eks.:

- Children's Online Protection Act (COPPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Gramm-Leach-Bliley Act (GLBA)
- Video Privacy Protection Act (VPPA)

Man kan derfor tale om en multi-compliance byrde eller en overlap-omkostning, hvor den enkelte organisation skal tilpasse sig alle de forskellige regler, der er på de markeder, hvor de opererer. GDPR står således ikke alene men var startskuddet til en global tendens, hvor digitaliseringen resulterer i et øget behov for at regulere og skabe beskyttelse af individernes rettigheder i deres roller som borgere, forbrugere m.v. Hvis GDPR ændres, skal man være opmærksom på, at omkostningerne for europæiske virksomheder ved at være compliant med disse andre landes persondatarelige regler ikke påvirkes.

Hertil kommer positive effekter for compliance med anden, tilstødende regulering om informationsikkerhed, f.eks. NIS 2. På trods af, at beskyttelsesobjektet er et andet i NIS 2 og anden sikkerhedslovgivning, påvirker navnlig forpligtelserne i GDPR om informationsikkerhed direkte compliance med eksempelvis NIS 2. Hvis GDPR ændres, skal man derfor også være opmærksom på, at omkostningerne ved at være compliant med NIS 2 m.v. ikke påvirkes.

Ud over det økonomiske aspekt, som vi har fokuseret på overfor, fordi det er baggrunden for Omnibussen jf. Draghi-rapporten, kunne man også adressere privacy som en fundamentale rettighed i EU jf. Charteret, eller som mere dataetiske værdier om, hvorfor databeskyttelse er vigtigt for individernes autonomi og tilliden til digitaliseringen. Da økonomien er driveren for Omnibussen, vil Rådet ikke forfølge dette yderligere for indværende.

### **Opsummering af ændringer**

Omnibussen lægger op til ændring af en række forskellige retsakter, hvoraf Rådet alene adresserer de justeringer, der foretages i GDPR. Ændringerne, som Rådet forstår dem, er sammenfattet nedenfor.

*Ændring af definitionen af personoplysninger*

#### Artikel 4, stk. 1, litra 1

Hvis en given enhed, med de midler som den pågældende enhed med rimelighed kunne anvende, ikke kan identificere en fysisk person på baggrund af data, så er de pågældende data ikke personoplysninger for den pågældende enhed. Blot fordi en anden enhed, med de midler de måtte være i besiddelse af, kan identificere en fysisk person på baggrund af data, gør dette forhold ikke data til personoplysninger for den første enhed.

#### *Tilføjelse af definitioner*

Artikel 4, stk. 1, litra 1, suppleres med en række definitioner relateret til de ændringer, der følger af ændringen af ePrivacy-direktivet tillige med en definition af videnskabelig forskning.

#### *Præcisering af formålsbestemmelsen*

#### Artikel 5, stk. 1, litra b

Hvis personoplysninger viderebehandles i samfundets interesse, til videnskabelige eller historiske forskningsformål eller statistiske formål, skal der ikke fremadrettet foretages en formålsforenelighedstest jf. artikel 6, stk. 4. I stedet skal de nye formål automatisk betragtes som værende forenelige. Viderebehandling til nye formål kan i øvrigt ske med interesseafvejning.

#### *Ændringer vedr. behandlingen af biometriske oplysninger*

#### Artikel 9, stk. 2, litra l

Der må behandles biometriske data mhp. verifikation af datasubjektets identitet, forudsat at midlerne til verifikationen er under data subjektets kontrol.

#### *Liberalisering ifht. brugen af personoplysninger i AI*

#### Artikel 9, stk. 2, litra k

Når der udvikles AI-systemer eller AI-modeller med store datasæt, kan der forekomme følsomme personoplysninger i datagrundlaget til brug for træning, test og validering uanset, at de følsomme oplysninger ikke var formålet med behandlingen. For ikke at forhindre udvikling og brug af AI må det accepteres, at der kan forekomme følsomme personoplysninger under udvikling og drift af et AI-system og i en AI-model. Det er dog en snæver undtagelsesbestemmelse, og det er en betingelse, at der er iværksat passende tekniske og organisatoriske foranstaltninger til at forhindre behandlingen og forudsat at de følsomme oplysninger enten kan fjernes eller ikke figurere af output.

#### *Indskrænkninger i indsigtsretten*

#### Artikel 12, stk. 5

Indsigtsretten indskrænkes således, at indsigtbegæring kan afvises, hvis de forfølger et andet formål (f.eks. at skade den dataansvarlige) end at beskytte personoplysninger. Det påhviler den dataansvarlige at demonstrere, at indsigtbegæringen forfølger andre formål end databeskyttelse.

#### *Indskrænkninger i oplysningspligten*

#### Artikel 13, stk. 4

Der skal ikke ske oplysning i henhold til stk. 1-3, hvis personoplysninger er indsamlet i en klar og gennemsigtig relation mellem den registrerede og den dataansvarlige, og der ikke behandles oplysninger mellem parterne, som kan udgøre en høj risiko for de registrerede, og det må forventes, at den registrerede allerede er informeret om indsamlingen. I de tilfælde, hvor behandlingen ikke er data-intensiv, ikke er kompleks, og hvor der behandles en lille mængde personoplysninger, er det sandsynligt, at den registrerede er bekendt med behandlingen – f.eks. i relationen mellem en håndværker og en kunde eller mellem en forening og et medlem.

Der skal dog alligevel ske oplysning, hvis der sker videregivelse af oplysningerne til andre modtagere, hvis der sker tredjelandsoverførsler, hvis data anvendes til automatiserede afgørelser, eller hvis behandlingen kan udgøre en høj risiko for den registrerede.

#### *Præcisering af oplysning i forbindelse med forskning*

Artikel 13, stk. 5

Hvis personoplysninger behandles til forskningsformål og oplysningsforpligtelsen under stk. 1-3, er umulig eller kræver en uforholdsmæssig stor indsats, kan den dataansvarlige opfylde sin informationspligt ved en bred offentliggørelse af formålene med behandlingen.

#### *Præcisering vedr. automatiseret beslutning*

Artikel 22, stk. 1 og 2

Sætningen om at den registrerede som udgangspunkt har ret til ikke at være genstand for en automatiseret beslutning fjernes: Det forhold at en fysisk person kunne have truffet beslutningen betyder ikke, at den dataansvarlige ikke må benytte automatiske beslutninger. Fsva. behandling på baggrund af kontrakt tilføjes det, at det er irrelevant for beslutningen, at denne ikke behøvede at være foretaget automatiseret, men også kunne være foretaget af en fysisk person.

#### *Grænsen for indberetning af sikkerhedshændelser til databeskyttelsesmyndigheden hæves*

Artikel 33, stk. 1 m.fl.

Der skal alene rapporteres sikkerhedsbrud, som det er sandsynligt vil resultere i en høj risiko for de registrerede. Det ændrer i den nuværende tilstand, hvor alle brud skal rapporteres, med mindre det er usandsynligt, at de udgør en risiko for de registrerede.

Tidsfristen for anmeldelse hæves fra 72 til 96 timer.

Indberetningen af brud skal ske til en central portal. Portalen skal dække indrapportering af hændelser fra GDPR, NIS2, DORA, CER og eIDAS m.v.

Der skal laves en central template for indberetninger. Der skal laves en liste over, hvilke hændelser der kan udgøre en høj risiko for de registrerede. Kommissionen kan fastsætte en delegeret retsakt baseret på dette.

#### *Harmonisering af brugen af DPIA*

Artikel 35, stk. 4-6

Der skal laves én på tværs af medlemslandene harmoniseret liste over, hvornår der skal udarbejdes DPIA – og hvornår der ikke skal.

Der skal laves en fælles harmoniseret skabelon for at gennemføre DPIA.

Kommissionen kan vedtage disse som delegerede retsakter.

#### *Lempelser for brugen af pseudonymiserede data*

##### Artikel 41a

Det har hidtil været en udbredt opfattelse, at pseudonyme personoplysninger altid er personoplysninger. Med en EU-dom fra efteråret 2025 fortolker EU Domstolen det sådan, at pseudonyme oplysninger ikke i alle behandlingssituationer for alle aktører skal betragtes som PII. Det forhold, at der et sted findes ekstra data, som kunne kombineres med pseudonyme data, således at disse kunne blive personoplysninger, gør ikke nødvendigvis de pseudonyme data til personoplysninger for den dataansvarlige. I henhold til artikel 41a skal Kommissionen kunne fastsætte delegerede retsakter, som opstiller kriterier for vurdering af risikoen for re-identifikation og hvilke teknikker, der kan anvendes til pseudonymisering, hvorefter pseudonymiserede data, der opfylder kriterierne, ikke er personoplysninger.

#### *Behandling af personoplysninger på brugernes terminaludstyr*

##### Artikel 88a

Lagring og behandling af data på brugernes terminaludstyr skal som udgangspunkt ske med samtykke. Brugeren skal have mulighed for at afslå samtykke, og den dataansvarlige må herefter ikke bede om samtykke igen indenfor en periode på seks måneder.

Behandling kan ske uden samtykke, hvis den vedrører eksplicit definerede formål som følger: oprettelse af en kommunikationsforbindelse, eller at tilvejebringe en service som brugeren har bedt om, eller tilvejebringelse af aggregerede data til eget brug om registreredes brug af en online service, eller sikkerhedshensyn.

For den efterfølgende behandling skal der findes hjemmel i artikel 6. Hjemlen kan være interesseafvejning, hvor der bl.a. lægges vægt på, at behandlingen er nødvendig for den dataansvarlige, at den registreredes fundamentale rettigheder ikke overtrædes, at den registrerede har rimelige forventninger om behandlingen, at behandlingen af data er begrænset til, hvad der er nødvendigt, og at der ikke sker en overvågning af en stor del af den registreredes online aktiviteter.

##### Artikel 88b

Der skal skrives standarder for maskinlæsbar signalering af brugeres præferencer. De dataansvarlige skal indrette deres tjenester således, at de kan opsamle og efterleve brugernes præferencer. Browsers skal indrettes således, at brugere kan signalere deres samtykke præferencer via browseren.

#### *Præcisering af hjemmel for behandling af personoplysninger med AI*

##### Artikel 88c

Hvis det er nødvendigt for den dataansvarlige at behandle PII i et AI-system eller en AI-model, kan det ske med interesseafvejning. Der skal ved interesseafvejningen bl.a. lægges vægt på, om behandlingen er til den registreredes fordel, til fordel for samfundet, forbedrer modellen ved at fjerne bias og diskrimination, sikrer et præcist output, er i overensstemmelse med den registreredes forventninger, er gennemsigtig for den registrerede, og sikrer den registrerede ret til at gøre indsigelse mod behandlingen. Kort sagt: med mindre den registreredes interesser overstiger den dataansvarliges interesser.

Når en sådan behandling sker, skal der være foretaget dataminimering, beskyttelse mod afsløring af PII fra model eller system, sikres gennemsigtighed for den registrerede og en ubetinget ret til at gøre indsigelse mod behandlingen.

### **Holdning til ændringer**

Overordnet finder Rådet, at der er behov for en justering af GDPR. Der er nu etableret syv års erfaringer med retsakten, og en række af bestemmelserne er meget byrdefulde for de dataansvarlige, uden at de giver værdi for og understøtter de registreredes rettigheder.

Rådet finder imidlertid, at Omnibussen ikke får adresseret de mest byrdefulde områder, hvorfor der er behov for en udvidelse af ændringer. Videre finder Rådet, at en række af de ændringer, Omnibussen lægger op til, skaber flere byrder i form af complianceusikkerhed eller ikke har nogen effekt for de dataansvarlige. Rådet kommer derfor først med bemærkninger til udvalgte dele af den fremsatte Omnibus og kommer herefter med bemærkninger til udvidelse af Omnibussen.

#### *Ændring af definitionen af personoplysninger*

Ændringen af definitionen af personoplysninger skaber for det første nye byrder for de dataansvarlige, som sættes til at vurdere, om et givent stykke data kan anvendes til at identificere en fysisk person – herunder i sammenhæng med de midler som den dataansvarlige har adgang til. For det andet skabes en compliancerisiko i forbindelse med den pågældende vurdering. For det tredje skabes betydelige risici for den registreredes rettigheder ved, at ukendte aktører kan behandle de pågældende data i en anden kontekst. Det kan føre til tillidsbrud mellem den registrerede og den dataansvarlige og desuden føre til mistillid til digitaliseringen. Rådet kan derfor ikke anbefale en ændring i definitionen af personoplysninger.

Fremfor at ændre i definitionen af 'personoplysninger', som er kernen i GDPR og forordningens sammenhæng med EU's Charter om grundlæggende rettigheder, bør det fremhæves, at det foreliggende forslag relateret til brugen af pseudonymisering by design, er et langt bedre fundament for forenkling og udvikling af dataanvendelsen i EU, jf. nedenfor.

#### *Præcisering af formålsbestemmelsen*

Når formålsforenelighedstesten sættes ud af kraft for viderebehandlinger i samfundets interesse, til videnskabelige eller historiske forskningsformål, kan den dataansvarlige administrativt uden samtykke eller uden et specifikt demokratisk vedtaget retligt grundlag behandle de personoplysninger, de er i besiddelse af, hvis der kan argumenteres for at behandlingen opfylder et af de tre nævnte formål. De betyder bl.a., at offentlige myndigheder i vid udtrækning administrativt kan vedtage behandling af personoplysninger uden Folketingets eller den registreredes kontrol. Også her skabes betydelige risici for den registreredes rettigheder ved at data behandles i en anden kontekst. Det kan føre til tillidsbrud mellem den registrerede og den dataansvarlige og desuden føre til mistillid til digitaliseringen. Rådet kan derfor ikke anbefale en undtagelse til formålsforenelighedstesten.

#### *Ændringer vedr. behandlingen af biometriske oplysninger*

Det er Rådets opfattelse, at præciseringen er i overensstemmelse med praksis, og Rådet kan derfor tilslutte sig forslaget.

### *Liberalisering ifht. brugen af personoplysninger i AI og præcisering af hjemmel for behandling af personoplysninger med AI*

Det er i praksis vanskeligt i forbindelse med træning af AI-modeller at sikre sig, at datasæt for træning er helt saniteret for følsomme personoplysninger. Videre er det vigtigt for de europæiske samfund og for de enkelte dataansvarlige, at barriererne for brug af AI ikke bliver for høje. I lyset af de korrigerende foranstaltninger, der supplerer forslaget, kan Rådet tilslutte sig ændringsforslaget.

Også i relation til behandling af almindelige personoplysninger i AI-modeller og AI-systemer er det vigtigt for de europæiske samfund og for de enkelte dataansvarlige, at barriererne for brug af AI ikke bliver for høje. Rådet kan derfor under de angivne forudsætninger tilslutte sig, at personoplysninger kan behandles med interesseafvejning.

### *Indskrænkninger i indsigtretten*

Indsigtretten er fundamentet for, at den registrerede kan udøve sine rettigheder og kontrollere den dataansvarlige. Omvendt kan indsigtbegæring være særdeles byrdefulde for den dataansvarlige. Rådet kan tilslutte sig ideen i justere i indsigtretten, om end Rådet ville have foretrukket en model, hvor begrænsningen gik på, hvilke registreringer de registrerede havde ret til at få indsigt i – f.eks. efter konkret vurdering af undtage logoplysninger. Med den foreslåede ordning er der risiko for, at indskrænkningerne i indsigtretten kan forsøges misbrugt til ikke at give de registrerede indsigt, om end at bevisbyrden ligger på den dataansvarlige. Dette kan skabe unødvendigt bureaukrati og proces for både dataansvarlige og de registrerede.

### *Indskrænkninger i oplysningspligten*

Rådet kan tilslutte sig, at den dataansvarliges oplysning af den registrerede er unødvendig, når det er indlysende, at almindelige oplysninger behandles, og den registrerede må formodes allerede at være klar over det.

### *Præcisering af oplysning i forbindelse med forskning*

Rådet er skeptisk ved at lave undtagelser til oplysning af de registrerede, når deres personoplysninger anvendes til forskning. Rådet frygter, at de registrerede på forhånd vil "opte" ud af medvirken i forskningsprojekter.

### *Præcisering vedr. automatiseret beslutning*

Rådet bakker op om præciseringen af at det forhold, at en fysisk person kunne have truffet beslutningen ikke betyder, at den dataansvarlige ikke må benytte automatiske beslutninger.

### *Grænsen for indberetning af sikkerhedshændelser til databeskyttelsesmyndigheden hæves*

Rådet bakker op om forslaget om, at begrænse indberetningen af sikkerhedshændelser. Indberetningen er byrdefuld og giver kun værdi, når der kan læres af hændelserne, hvilket kræver en vis grad af risiko for de registreredes rettigheder. Rådet bakker ligeledes op om etableringen af en fælles indberetningsportal i EU på tværs af flere reguleringsmæssige tiltag.

### *Harmonisering af brugen af DPIA*

Rådet bakker om en harmonisering og ensretning på tværs af medlemslandene af, hvornår der skal gennemføres DPIA'er.

### *Lempelser for brugen af pseudonymiserede data*

Rådet har gennem mange år bakket op om pseudonymisering som en teknisk foranstaltning. Rådet er enig i, at pseudonyme data ikke altid skal betragtes som personoplysninger, og Rådet kan derfor tilslutte sig ændringsforslaget.

### *Behandling af personoplysninger på brugernes terminaludstyr*

Rådet bakker op om forslaget om lægge kravene til håndtering af lagring på brugernes terminaludstyr fra e-Privacydirektivet ind under GDPR – herunder også de skitserede lempelser i forhold til at lagre oplysninger på brugernes terminaludstyr til de angivne formål.

## **RfDS' forslag til ændringer**

Som nævnt finder Rådet ikke, at Omnibussen får adresseret de mest byrdefulde områder, hvorfor der er behov for en udvidelse af ændringer af GDPR, ifht. hvad EU Kommissionen lægger op til.

Der er række områder, som kræver rigtig meget tid og mange ressourcer i organisationerne, for at sikre en god beskyttelse af de registreredes fundamentale rettigheder:

- Vurdering af (for organisationen) nye teknologier og leverandører
- Instruks af databehandlere, vurdering af databehandleraftaler, gennemsigtighed af dataflow og anvendelse af underdatabehandlere
- Tredjelandsoverførsler
- Håndtering af indsigts- og slettebegæringer
- Vurdering af risici, sårbarheder, trusselsbilledet og implementering af mitigerende foranstaltninger
- Fortegnelse og god datakvalitet – herunder sletteprocedurer
- Databrud/hændelser
- Oplysning
- Awareness
- Kontroller
- Øvelser
- Standarder
- Justeringer af procedurer som følge af ændring af praksis
- Automatisering – herunder brug af AI
- Praksis vedrørende databeskyttelse gennem design og default
- Konsekvensanalyser

En række af disse tiltag kan tilpasses således, at de bidrager positivt til forretningen – f.eks. vurdering og håndtering af risiko, implementering af foranstaltninger og compliance (markeret med **grønt**). Andre af disse tiltag forbedrer grundlæggende ikke sikkerheden for de registreredes rettigheder væsentligt, samtidig med at de er byrdefulde for organisationerne (markeret med **rødt**). Rådet finder, at Omnibussen bør adressere de røde tiltag, hvis formålet med Omnibussen er at lempe byrder for organisationerne i lyset af Draghi-rapporten.

### *Undtagelse for behandling af personoplysninger i B2B-relationer*

Mange virksomheder (leverandører) handler kun med andre virksomheder (professionelle kunder) og ikke private forbrugere. De professionelle kunder i disse relationer optræder derfor i deres professionelle rolle som indkøbere på vegne af deres arbejdsgiver og ikke som privatpersoner. I relationen udveksles som regel personoplysninger i form af visitkortinformationer. Forordningens formål er at "beskytte fysiske personers grundlæggende rettigheder og frihedsrettigheder", men visitkortinformationer er grundlæggende oplysninger om professionelle kunder og leverandørers kontaktpersoner. Det synes således ikke nødvendigt at beskytte individernes rettigheder, når de optræder som kontaktpersoner hos virksomheder, fordi de agerer som virksomheder. Rådet konstaterer, at det vil spare mange virksomhederne i EU-landene for mange penge og andre ressourcer, hvis de ikke skal beskytte de professionelle personoplysninger. Rådet foreslår derfor, at artikel 2, stk. 2, tilføjes et nyt litra d, der affattes som følger: "under udøvelse af transaktioner mellem professionelle virksomheder i en B2B-relation".

*Instruks af databehandlere, vurdering af databehandleraftaler, gennemsigtighed af dataflow og anvendelse af underdatabehandlere*

Vurdering af IT-leverandører, deres applikationers virkemåde, deres tekniske integration med andre IT-leverandører, deres behandling og placering af data og selve instruktionen i at behandle personoplysninger er nogle af de forhold, som de dataansvarlige pålægges i databeskyttelsesforordningens artikel 28 – herunder f.eks.:

- Artikel 28, stk. 1, pålægger de dataansvarlige udelukkende at benytte databehandlere, der anvender tekniske og organisatoriske foranstaltninger, som skaber compliance med reglerne og som beskytter de registrerede.
- Artikel 28, stk. 2, pålægger de dataansvarlige en pligt til at godkende hele kæden af leverandører fra databehandleren og ned til den sidste underdatabehandler.
- Artikel 28, stk. 3, nr. 1, pålægger databehandleren kun at behandle personoplysninger under instruks fra den dataansvarlige – herunder også mht. tredjelandsoverførsler efter mulighederne i kapitel V.

De krav, der stilles i artikel 28, er for så vidt alle fornuftige, når det drejer sig om at beskytte den registreredes fundamentale rettigheder. Rådet har således stor sympati for den politiske vision bag kravene. I praksis har kravene dog ikke en gang på jord, når de kommer ud og skal anvendes af dataansvarlige i erhvervslivet. Det forhold at en dataansvarlig (f.eks. en SMV) skulle kunne pålægge sine leverandører (sine databehandlere) en instruks i, hvilken sikkerhed der skal implementeres, hvilke underdatabehandlere der må benyttes, og hvilke lande udenfor EU, som personoplysninger må kunne overføres til (alle krav således at den registreredes fundamentale rettigheder opretholdes), er en velmenende illusion. Ingen dansk dataansvarlig kan instruere store internationale softwareleverandører eller tjenesteudbydere i noget som helst.

Der bruges (for at være compliant) hos de dataansvarlige enorme mængder af ressourcer på hver især at lave en vurdering af de tjenester de bruger, få gennemgået og underskrevet databehandleraftaler og vurderet tredjelandsoverførsler. Men uanset den store mængde ressourcer, bliver løsningen altid den, som leverandøren/databehandleren har valgt. Resultatet ændrer således ikke ved den registreredes sikkerhed eller ved compliance. Det er blot bureaukratisk spild, som reducerer europæiske virksomheders konkurrenceevne. Chromebooksagen har vist, at selv når halvdelen af landets kommuner, KL og Datatilsynet står sammen, er det vanskeligt reelt at flytte på leverandøren, og sagen tog i øvrigt fire år at kortlægge. Hvordan skulle en enkelt lille dataansvarlig SMV så på nogen måde kunne instruere en leverandør? Der er en massiv

asymmetri i såvel tekniske og juridiske kompetencer som forhandlingspower mellem en dataansvarlig og en databehandler. Rådet foreslår derfor:

- Det er databehandleren, som gøres ansvarlig for, at det produkt eller den tjeneste, der leveres, er sikker(t) og i overensstemmelse med såvel de databeskyttelsesretlige regler som Charteret. Det svarer til, hvad der gør sig gældende i alle andre brancher: Fødevarer, medicin, biler, elektriske artikler m.v. skal være sikre for brugerne at anvende. Det er grundtanken i bl.a. produktansvarsreglerne og synes også at være et princip i f.eks. AI-forordningen, hvor der stilles forskellige krav til udbydere og ibrugtagere af kunstig intelligens. Ibrugtagerne (som i denne sammenhæng er sammenlignelige med de dataansvarlige) skal således sikre, at *brugen* af den pågældende AI-løsning er sikker. Udbyderne (som i denne sammenhæng er sammenlignelige med databehandlerne) skal sikre, at AI-løsningen *som sådant* er sikker at bruge.
- Den dataansvarlige kan stille krav til sin direkte leverandør (jf. nedenfor), men det er databehandleren, som har ansvaret for den øvrige del af værdikæden – herunder underdatabehandlerne. Det svarer til kravene i NIS2, hvor de vigtige og væsentlige enheder kun skal kontrollere deres leverandørers sikkerhed i eet led - og ikke i hele værdikæden. Udover, at NIS2's tilgang repræsenterer en mere pragmatisk tilgang til styring af leverandører, er det et problem, at to forskellige regelsæt – altså GDPR og NIS2 – tager udgangspunkt i to vidt forskellige tilgange til leverandørstyring. Det gør det reelt umuligt for de dataansvarlige at opbygge og vedligeholde arbejdsgange, som gavner leverandørstyring på tværs.
- Den dataansvarliges instruks gælder kun den direkte behandling af personoplysninger, men ikke hvilke teknologier, tjenester og underdatabehandlere i forskellige dele af verden, som skal udføre denne instruktion. Dette ansvar bør pålægges databehandleren, som har de bedste kompetencer, forbindelser og forhandlingsposition. Generelt er samspillet mellem tekniske, persondataretlige og kontraktretlige kompetencer til stede i større omfang hos databehandleren end hos de fleste dataansvarlige. Også dette svarer til, hvad der gør sig gældende i alle andre brancher: Man kan instruere sin automobilforhandler i, at man gerne vil have en elbil med tidssvarende sikkerhedsudstyr, men man kan ikke bestemme om de elektriske komponenter er produceret i Tyskland, Kina eller på Taiwan.
- Det er databehandleren, som står på mål for, at databehandleraftalen er lovlige, og indeholder de elementer, som kræves af artikel 25, 28, 32, m.v.
- Databehandlerne skal i GDPR pålægges tre måneders varsel til at skifte underdatabehandlere og ikke overlades et skøn herfor. Det er en igen en illusion, at en dataansvarlig SMV kan vurdere og reagere på, at en databehandler skifter underdatabehandler indenfor en periode på f.eks. 2 uger. I praksis er det i dag umuligt for de dataansvarlige at styre underleverandører, herunder fordi alle store teknologileverandører i databehandleraftalen giver sig selv ret til at udskifte underdatabehandlere efter for godt befindende, herunder evt. ved opdatering af en hjemmeside, som databehandleren vedligeholder, ofte uden at give nogen form for notits til den dataansvarlige.
- Rådet foreslår helt konkret, at der introduceres en definition i artikel 4 for "*Systemiske databehandlere*", som omfatter de leverandører der
  - a) leverer standardiserede behandlinger til >X dataansvarlige i EU, eller
  - b) fastlægger væsentlige tekniske og organisatoriske rammer, som den dataansvarlige ikke realistisk kan ændre.Desuden skal der introduceres en ny artikel 28a, hvor der indføres selvstændige krav til de systemiske databehandlere:
  - a) gennemføre og opdatere DPIA'er for deres *standardtjenester*,

- b) dokumentere tredjelandsoverførsler,
- c) dokumentere underdatabehandlere og lovligheden ved anvendelse af disse
- c) levere "compliance packs" til kunder med bl.a. beskriver til fortegnelsen over behandlingsaktiviteter.

Det er ikke alle dele af ansvaret for en behandling, som kan flyttes fra den dataansvarlige til en databehandler. Ansvarret skal placeres hos den aktør (dataansvarlig eller databehandler), som faktisk har indflydelse og beslutningskraft. Rådet foreslår derfor, at den dataansvarlige ved brug af en IT-leverandør alene kan holdes ansvarlig for:

- Artikel 5, 6, 9, kapitel III, 24, 30, 31, 33, 34, 35, 37, 38 og 39. Dataansvarlige, som selv leverer en IT-tjeneste (herunder et produkt med indlejret teknologi), omfattes af hele forordningen. Dataansvarlige som selv behandler personoplysninger uden brug af en IT-leverandør omfattes af hele forordningen. Det betyder selvsagt ikke, at den dataansvarlige ikke er ansvarlig for sikker og fornuftig brug af indkøbte tjenester. F.eks. vil den dataansvarlige fortsat være ansvarlig for kun at tildele adgangrettigheder m.v. i nødvendigt omfang og at tilgængelige sikkerhedskonfigurationer anvendes på en formålstjenestelig måde.

Det er et uendeligt spild af organisationers ressourcer, at hver enkelt dataansvarlig skal vurdere de samme top-100 databehandleraftaler fra store internationale IT-leverandører. Millioner af europæiske virksomheder og andre organisationer bruger hver især f.eks. tid på at vurdere og kontrollere databehandleraftaler med Microsoft om deres udbredte Office365 eller Azure-løsninger. Rådet foreslår derfor:

- Det skrives ind i GDPR, at der under EU Kommissionen nedsættes et EU-organ, som får til opgave at vurdere lovlighed og compliance af eksempelvis top-100 databehandleraftaler fra store internationale IT-leverandører (et fælleseuropæisk databehandlersekretariat). Vurderingen skal efterfølgende kontrolleres af EDPB, og den endelige konklusion skal meldes offentligt ud til brug for dataansvarlige i hele EU.
- Dette vil være en fordel for de dataansvarlige, som ikke skal lave hver deres vurdering. Det vil også være en fordel for databehandlerne, som har et sted forhandle med – i stedet for at skulle bevare spørgsmål fra millioner af kunder.
- Rådet foreslår helt konkret, at der indføres en artikel 43a, EU Register for Trusted Processors. Som skal vurdere "*Systemiske databehandlere*", som bl.a. skal omfatte en central vurdering af:
  - a) overholdelse af GDPR,
  - b) tredjelandsoverførsler og transfer impacts assessments,
  - c) anvendelse af underdatabehandlere,
  - d) konsekvensanalyser

Set fra de registreredes perspektiv sikre at der etableres en ensartet, høj standard for godkendelse af systemiske databehandlere og dermed en reelt bedre beskyttelse.

### *Tredjelandsoverførsler*

Der har i årevis været compliance-mæssig usikkerhed om, hvorvidt der findes et retlig grundlag for at overføre personoplysninger til lande udenfor EU blandt alle de overførselsmuligheder, der findes i databeskyttelsesforordningens kapitel V. De overførselsgrundlag, som har været lovlige den ene dag, er det ikke den anden dag. Leverandørerne skifter overførselsgrundlag igen og igen, som vi f.eks. har set det med Meta. Reglerne på dette område er ekstremt komplicerede og foranderlige. Det er byrdefuldt for en dataansvarlig SMV at følge med i dette område, hvorfor stort set alle opgiver, resignerer og den politiske vision i GDPR

igen bliver en velmenende illusion. Det bør være databehandlerens ansvar, om personoplysninger skal overføres, og hvis de overføres, at det sker på et lovligt retligt grundlag.

Den praksis, der har udviklet sig omkring udarbejdelse af Transfer Impact Assessments, skal justeres. Det er kun den part, som er ansvarlig for overførslen, som bør udarbejde en TIA. Hvis en dansk dataansvarlig altså selv eksporterer personoplysninger ud af EU (f.eks. ved at bruge en IT-leverandør, som er registreret udenfor EU) skal den dataansvarlige udarbejde TIA'en. Hvis en dansk dataansvarlig benytter en europæisk registreret IT-leverandør, der anvender underdatabehandlere udenfor EU, er det databehandleren som skal lave TIA'en og stå på mål for dens lovlighed.

#### *Håndtering af indsigts- og slettebegæringer*

Omnibussen adresserer og lemper allerede de dataansvarliges pligt til at håndtere indsigts- og slettebegæringer en smule. Praksis fra EU-domstolen har ændret dansk praksis ved give de registrerede indsigt i logfiler. Rådet mener, at hensigten med indsigtbegæringer bør være, at den registrerede kan forsvare sine rettigheder som fastsat i databeskyttelsesforordningen overfor den dataansvarlige. Der bør derfor være begrænsninger på, hvad den registrerede kan kræve indsigt i. Logning af hvilke medarbejdere, der har tilgået den registreredes oplysninger, kan f.eks. være relevant for, at den registrerede kan forsvare sine interesser, mens logs af at en IP-adresse har søgt på en babyrangle på en hjemmeside, næppe kan være relevant for, at den registrerede kan forfølge sine interesser. Derfor foreslår Rådet følgende:

- Det bør i GDPR fastslås, at EDPB får mulighed for at lave bindende vejledning om, hvad den registrerede kan få indsigt i, og hvad den registrerede ikke kan få indsigt i.

#### *Databrud/hændelser*

Omnibussen adresserer og lemper allerede de dataansvarliges pligt til at indberette databrud. Dette har længe stået på Rådets ønskeseddel, og Rådet bakker op om forslaget, ligesom Rådet bakker op om en fælles anmeldelsesplatform på tværs af lovgivninger – herunder – f.eks. NIS2 og DORA.

#### *Oplysning*

Omnibussen adresserer og lemper allerede de dataansvarliges pligt til at oplyse den registrerede, og Rådet er som nævnt enige heri. Det gavner ikke den registrerede at modtage oplysning, som de allerede er i besiddelse af. Meget af denne oplysning gavner i øvrigt ikke den registrerede, da de ikke sætter sig ind i oplysningen.

#### *Justeringer af procedurer som følge af ændring af praksis*

Praksis ændrer sig løbende på både de store linjer (f.eks. tredjelandsoverførsler) og i detaljen (f.eks. indsigt i logning). Det er byrdefuldt at følge med i for de dataansvarlige, og det er byrdefuldt hver gang nye procedurer skal skrives, og automatiserede processer skal ændres. Efter Omnibussen er der brug for ro på det databeskyttelsesretlige område i en årrække, så der ikke skal allokeres så mange ressourcer til denne del.

GDPR blev lavet som en forordning, men grundet vanskelighederne med at lave politiske kompromisser, fungerer den på en række områder som et direktiv med forskellige nationale implementeringer. Dette skaber vanskeligheder for dataansvarlige, der arbejder på tværs af de forskellige EU-medlemslande. Rådet opfordrer til enten at udvise national tilbageholdenhed med at udnytte mulighederne for national regulering, eller lade mere harmonisering indgå i Omnibussen. Som et alternativ kunne EDPB tildeles mere magt til at fastslå rammer for udformning af national lovgivning.

### *Praksis vedrørende databeskyttelse gennem design og default*

Rådet finder grundlæggende, at artikel 25 ikke udnyttes i tilstrækkelig grad. På den ene side kan man ikke kræve, at alle løsninger altid vælger det mest databeskyttende design, fordi andre faktorer som f.eks. brugervenlighed, økonomi, teknologiens stade m.v. spiller ind. På den anden side er brug for et større pres fra lovgiver eller gennem praksis for at designe databeskyttelse ind i fremtidige digitale løsninger. Rådet foreslår derfor:

- IT-leverandører får pligt til at lave en offentlig opsummerende design-rapport, hvor der argumenteres for teknologitilvalg og -fravalg ud fra en risikobaseret tilgang og ud fra principperne i artikel 32. Rapporten kan passende blive et bilag til databehandleraftalen på linje med bilaget om sikkerhedsforanstaltninger. Rapporten skal kun laves ved meget udbredte eller meget indgribende teknologier, og rapporten skal ikke overstige et omfang på fem sider, for så bliver den ikke læst og brugt.

### *Konsekvensanalyser*

Mange dataansvarlige bruger mange ressourcer på at lave konsekvensanalyser, herunder at screene for, om der efter GDPR er krav om konsekvensanalyse (også omtalt som "tærskelvurderinger"), som i sig selv er en øvelse, som de dataansvarlige anvender mange ressourcer på, navnlig internationale organisationer, som skal forholde sig til de såkaldte "blacklists" og "whitelists" på tværs af EU, som indikerer hvornår der altid hhv. aldrig skal gennemføres en konsekvensanalyse. Disse lister stemmer ofte ikke overens og kan i nogle tilfælde være decideret selvmodsige. Rådet er stor tilhænger af den politiske vision om at få vurderet konsekvenser for de registrerede ved, at der foretages behandlinger. I praksis kan det imidlertid konstateres, at selv om der efterhånden er lavet gode solide skabeloner fra datatilsynenes side, så er det et meget stort arbejde, som skal gennemføres. Rådet foreslår derfor:

- Artikel 35 justeres således, at pligten til at udarbejde konsekvensanalyser fortrinsvis påhviler IT-leverandørerne, fordi det er dem, der har indflydelse på arkitektur, funktionalitet, programmering og andre forhold vedrørende deres applikationer eller tjenester. Desuden laves en skabelon for konsekvensanalyser-light, hvor de dataansvarlige kun skal lave konsekvensanalyser for de forhold, de har indflydelse på (jf. ovenstående punkt: "Instruks af databehandlere...").
- Black- og whitelister konsolideres på tværs af EU, f.eks. gennem EDPB, så dataansvarlige ikke skal forholde sig til flere nationale black- og whitelister.