Retningslinjer

Retningslinjer 4/2019 om artikel 25

Databeskyttelse gennem design og databeskyttelse gennem standardindstillinger

Version 2.0

Vedtaget den 20. oktober 2020

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Versionsoversigt

Version 1.0	13. november 2019	Vedtagelse af retningslinjerne til offentlig høring
Version 2.0	20. oktober 2020	Retningslinjerne vedtaget af Det Europæiske Databeskyttelsesråd (EDPB) efter offentlig høring

Indholdsfortegnelse

Det Europæiske Databeskyttelsesråd har –

under henvisning til artikel 70, stk. 1, litra e), i Europa-Parlamentets og Rådets forordning 2016/679/EU 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 ("databeskyttelsesforordningen")

under henvisning til EØS-aftalen, særligt dennes bilag XI og protokol 37, som ændret ved Det Blandede EØS-Udvalgs afgørelse nr. 154/2018 af 6. juli 2018

under henvisning til artikel 12 og artikel 22 i procesreglementet –

VEDTAGET FØLGENDE RETNINGSLINJER:

Resumé

I en stadig mere digital verden har overholdelse af kravene til databeskyttelse gennem design og databeskyttelse gennem standardindstillinger en vigtig rolle med hensyn til at fremme privatlivets fred og databeskyttelse i samfundet. Det er derfor væsentligt, at dataansvarlige tager dette ansvar alvorligt og gennemfører databeskyttelsesforordningens forpligtelser ved udformning af behandlingsaktiviteterne.

Retningslinjerne giver generel vejledning om forpligtelsen til at sikre databeskyttelse gennem design og databeskyttelse gennem standardindstillinger som fastlagt i artikel 25 i databeskyttelsesforordningen. Databeskyttelse gennem design og databeskyttelse gennem standardindstillinger er en forpligtelse for alle dataansvarlige, uanset behandlingens omfang og kompleksitet. Den dataansvarlige må have indsigt i databeskyttelsesprincipperne og den registreredes rettigheder og frihedsrettigheder for at kunne opfylde kravene til databeskyttelse gennem design og databeskyttelse gennem standardindstillinger.

Den centrale forpligtelse er at gennemføre *passende* foranstaltninger og fornødne garantier, der sikrer *effektiv implementering* af *databeskyttelsesprincipperne* og dermed *registreredes rettigheder og frihedsrettigheder gennem design og gennem standardindstillinger*. Artikel 25 fastslår, at både design- og standardelementer bør tages i betragtning. Disse elementer vil blive uddybet nærmere i disse retningslinjer.

I artikel 25, stk. 1, fastslås det, at de dataansvarlige på et tidligt tidspunkt bør overveje at anvende databeskyttelse gennem design og databeskyttelse gennem standardindstillinger, når de planlægger en ny behandling. De dataansvarlige skal gennemføre databeskyttelse gennem design og databeskyttelse gennem standardindstillinger både *inden* behandlingen og *løbende* under behandlingen ved regelmæssigt at gennemgå effektiviteten af de valgte foranstaltninger og garantier. Databeskyttelse gennem design og databeskyttelse gennem standardindstillinger finder også anvendelse på eksisterende systemer, der behandler personoplysninger.

Retningslinjerne indeholder desuden en vejledning i, hvordan databeskyttelsesprincipperne i artikel 5 implementeres effektivt, opstiller vigtige design- og standardelementer og giver praktiske eksempler. Den dataansvarlige bør tage i betragtning, om de påtænkte foranstaltninger er hensigtsmæssige i forbindelse med den pågældende behandling.

Det Europæiske Databeskyttelsesråd udsteder desuden anbefalinger for, hvordan dataansvarlige, databehandlere og producenter kan samarbejde om at opnå databeskyttelse gennem design og databeskyttelse gennem standardindstillinger. Det tilskynder de dataansvarlige i industrien, hos databehandlerne og hos producenterne til at anvende databeskyttelse gennem design og databeskyttelse gennem standardindstillinger som et middel til at opnå en konkurrencefordel i markedsføringen af deres produkter over for dataansvarlige og registrerede. Det tilskynder desuden alle dataansvarlige til at anvende certificeringer og adfærdskodekser.

1 ANVENDELSESOMRÅDE

1. Retningslinjerne fokuserer på dataansvarliges gennemførelse af databeskyttelse gennem design og databeskyttelse gennem standardindstillinger på baggrund af forpligtelsen i artikel 25 i databeskyttelsesforordningen.[1] Andre aktører – således databehandlere og producenter af produkter, tjenesteydelser og applikationer, der ikke direkte er omfattet af artikel 25 (herefter benævnt "producenter") – kan også tænkes at finde disse retningslinjer nyttige til at udforme produkter og tjenester, som er i overensstemmelse med databeskyttelsesforordningen, og som giver dataansvarlige mulighed for at opfylde deres databeskyttelsesforpligtelser.[2] Betragtning 78 i databeskyttelsesforordningen tilføjer, at der i forbindelse med offentlige udbud bør tages hensyn til databeskyttelse gennem design og databeskyttelse gennem standardindstillinger. Selvom alle dataansvarlige har pligt til at integrere databeskyttelse gennem design og databeskyttelse gennem standardindstillinger i deres behandlingsaktiviteter, fremmer denne bestemmelse vedtagelsen af principperne, hvor offentlige forvaltninger bør gå forud med et godt eksempel De dataansvarlige er ansvarlige for at opfylde deres forpligtelser til databeskyttelse gennem design og databeskyttelse gennem standardindstillinger for den behandling, der foretages af de databehandlere og underkontraherede databehandlere. Dette bør de tage i betragtning, når de indgår kontrakter med disse parter.

2. Kravet i artikel 25 er, at datasvarlige skal have databeskyttelse integreret i behandlingen af personoplysninger og som standardindstilling, og dette gælder i hele behandlingscyklussen. Databeskyttelse gennem design og databeskyttelse gennem standardindstillinger er også et krav til behandlingssystemer, der fandtes før databeskyttelsesforordningen trådte i kraft. Dataansvarlige skal konsekvent ajourføre behandlingen i overensstemmelse med databeskyttelsesforordningen. Yderligere oplysninger om, hvordan man bibeholder et eksisterende system i overensstemmelse med databeskyttelsesforordningen, findes i underkapitel 2.1.4 i disse retningslinjer. Bestemmelsens centrale del er at sikre *tilstrækkelig* og *effektiv* databeskyttelse både gennem *design* og gennem *standardindstillinger*. Det vil sige, at dataansvarlige bør kunne påvise, at de i behandlingen anvender tilstrækkelige foranstaltninger og garantier, der sikrer, at databeskyttelsesprincipperne og de registreredes rettigheder og frihedsrettigheder rent faktisk gennemføres.

[1] De heri fastlagte fortolkninger finder tilsvarende anvendelse på artikel 20 i direktiv (EU) 2016/680 og artikel 27 i forordning 2018/1725.

[2] Dette er klart fastlagt i betragtning 78 i databeskyttelsesforordningen: "*Når producenter af produkter, tjenester og applikationer udvikler, designer, udvælger og bruger applikationer, tjenester og produkter, der er baseret på behandling af personoplysninger eller behandler personoplysninger, for at udføre deres opgaver, bør de tilskyndes til at tage højde for retten til databeskyttelse i forbindelse med udvikling og design af sådanne produkter, tjenester og applikationer og til under behørig hensyntagen til "det aktuelle tekniske niveau" at sørge for, at de dataansvarlige og databehandlerne er i stand til at opfylde deres databeskyttelsesforpligtelser*."

3. Kapitel 2 i retningslinjerne er fokuseret på en fortolkning af kravene i artikel 25 og undersøger de retlige forpligtelser, som bestemmelsen indfører. Kapitel 3 giver eksempler på anvendelse af databeskyttelse gennem design og databeskyttelse gennem standardindstillinger i forbindelse med specifikke databeskyttelsesprincipper.

4. Retningslinjerne omhandler i kapitel 4 muligheden for at fastlægge en certificeringsmekanisme til at påvise overholdelse af artikel 25, og i kapitel 5 hvordan artiklen kan håndhæves af tilsynsmyndigheder. Endelig indeholder retningslinjerne supplerende anbefalinger til interessenterne om vellykket gennemførelse af databeskyttelse gennem design og databeskyttelse gennem standardindstillinger. Det Europæiske Databeskyttelsesråd erkender udfordringerne for små og mellemstore virksomheder ("SMV'er") med fuldt ud at opfylde kravene til databeskyttelse gennem design og databeskyttelse gennem standardindstillinger og giver supplerende anbefalinger særligt til SMV'er i kapitel 6.

2 ANALYSE AF ARTIKEL 25, STK. 1 OG 2 – DATABESKYTTELSE GENNEM DESIGN OG DATABESKYTTELSE GENNEM STANDARDINDSTILLINGER

5. Formålet med dette kapitel er at udforske og vejlede om kravene til henholdsvis databeskyttelse gennem design i artikel 25, stk. 1, og databeskyttelse gennem standardindstillinger i artikel 25, stk. 2, i databeskyttelsesforordningen. Databeskyttelse gennem design og databeskyttelse gennem standardindstillinger er komplementære begreber, der gensidigt styrker hinanden. Registrerede har større fordel af databeskyttelse gennem standardindstillinger, hvis der sideløbende anvendes databeskyttelse gennem design – og omvendt.

6. Databeskyttelse gennem design og databeskyttelse gennem standardindstillinger er et krav til alle dataansvarlige, både i mindre og i multinationale virksomheder. Derfor kan det være mere eller mindre komplekst at gennemføre databeskyttelse gennem design og databeskyttelse gennem standardindstillinger, alt efter den enkelte behandlingsaktivitet. Uanset virksomhedens størrelse vil det dog i alle tilfælde være en fordel for den dataansvarlige og den registrerede at gennemføre databeskyttelse gennem design og databeskyttelse gennem standardindstillinger.

2.1 Artikel 25, stk. 1: Databeskyttelse gennem design

2.1.1 Den dataansvarliges forpligtelse til at gennemføre fornødne tekniske og organisatoriske foranstaltninger og fornødne garantier i databehandlingen

7. I henhold til artikel 25, stk. 1, skal den dataansvarlige gennemføre *passende* tekniske og organisatoriske *foranstaltninger*, der er designet med henblik på at implementere databeskyttelsesprincipperne, og integrere de *fornødne garantier* i behandlingen for at opfylde kravene og beskytte registreredes rettigheder. Både passende foranstaltninger og fornødne garantier skal beskytte registreredes rettigheder og sikre, at beskyttelsen af deres personoplysninger er integreret i behandlingen.

8. *Tekniske og organisatoriske foranstaltninger* og fornødne *garantier* kan tolkes i bred forstand som en metode eller et middel, som en dataansvarlig kan benytte i behandlingen. *Passende* betyder, at foranstaltningerne og de fornødne garantier bør være egnede til at nå det tilsigtede mål, dvs. de skal

effektivt implementere databeskyttelsesprincipperne[3]. Kravet om, at de er passende, er derfor tæt knyttet til kravet om effektivitet.

9. En teknisk eller organisatorisk foranstaltning og garanti kan være alt fra avancerede tekniske løsninger til grunduddannelse af personale. Alt efter sammenhængen og de risici, der er knyttet til den pågældende behandling, kan det f.eks. være at pseudonymisere personoplysninger[4], opbevare personoplysninger i et struktureret, almindeligt anvendt maskinlæsbart format, der giver de registrerede mulighed for at gribe ind i behandlingen, give information om opbevaring af personoplysninger, have systemer til at afsløre skadelig software, uddanne ansatte i grundlæggende "cyberhygiejne", etablere systemer til at beskytte privatlivets fred og informationssikkerhed, forpligte databehandlere kontraktligt til at anvende specifikke metoder til dataminimering osv.

10. For at fastlægge passende foranstaltninger kan det være til hjælp at henholde sig til standarder, bedste praksis og adfærdskodekser, som er anerkendt af organisationer og andre organer, der repræsenterer kategorier af dataansvarlige. Den dataansvarlige skal dog efterprøve, at foranstaltningerne er passende i forhold til den pågældende databehandling.

2.1.2 *Databeskyttelsesprincipperne* i artikel 5 (det følgende benævnt "principperne") er designet med henblik på effektivt at implementere databeskyttelsesprincipper og beskytte registreredes rettigheder og frihedsrettigheder

11. *Databeskyttelsesprincipperne* anføres i artikel 5 (herefter kaldet "principperne").*De registreredes rettigheder og friheder* er fysiske personers grundlæggende rettigheder, navnlig deres ret til beskyttelse af personoplysninger, som i artikel 1, stk. 2, angives som formålet med databeskyttelsesforordningen (herefter kaldet "rettighederne")[5]. Den præcise formulering af principperne findes i EU's charter om grundlæggende rettigheder. Det er afgørende, at den dataansvarlige har indsigt i betydningen af *principperne* og *rettighederne* som grundlag for den beskyttelse, der gives i databeskyttelsesforordningen, navnlig forpligtelsen til databeskyttelse gennem design og databeskyttelse gennem standardindstillinger.

12. Ved gennemførelse af de passende tekniske og organisatoriske foranstaltninger bør foranstaltningerne og garantierne *udformes* med henblik på reelt at implementere hvert af de nævnte principper og den resulterende beskyttelse af rettigheder.

Opnåelse af effektivitet

13. Effektivitet er kernen i begrebet databeskyttelse gennem design. Kravet om at implementere principperne effektivt betyder, at de dataansvarlige skal gennemføre de fornødne foranstaltninger og garantier for at beskytte principperne med henblik på at sikre registreredes rettigheder. Hver gennemført foranstaltning bør frembringe de forventede resultater af den databehandling, som den dataansvarlige påtænker at foretage. Denne bemærkning har to konsekvenser.

14. For det første betyder den, at artikel 25 ikke kræver gennemførelse af specifikke tekniske og organisatoriske foranstaltninger, men derimod, at de valgte foranstaltninger og garantier bør være specifikke for implementeringen af databeskyttelsesprincipperne i den pågældende behandling. I denne forbindelse bør foranstaltningerne og garantierne være udformet, så de er robuste, og den dataansvarlige bør kunne gennemføre yderligere foranstaltninger for at tilpasse omfanget af en øget

[3] "Effektivitet" er omhandlet nedenfor i underkapitel 2.1.2.
[4] Som defineret i artikel 4, stk. 5, i databeskyttelsesforordningen.
[5] Se betragtning 4 i databeskyttelsesforordningen.

risiko[6]. Hvorvidt foranstaltninger er effektive, vil derfor afhænge af sammenhængen for den pågældende databehandling og en vurdering af visse elementer, der bør tages i betragtning, når man fastlægger hjælpemidlerne til behandlingen. Disse elementer vil blive taget op i underkapitel 2.1.3 nedenfor.

15. Desuden bør de dataansvarlige kunne påvise, at principperne er blevet fastholdt.

16. De gennemførte foranstaltninger og garantier bør have den ønskede virkning i form af databeskyttelse, og den dataansvarlige bør have dokumentation for de gennemførte tekniske og organisatoriske foranstaltninger.[7] Til dette formål kan den dataansvarlige fastlægge passende centrale præstationsindikatorer (KPI'er) til at påvise effektiviteten. En central præstationsindikator er en målbar værdi, der vælges af den dataansvarlige og viser, hvor effektivt den dataansvarlige opfylder sin målsætning om databeskyttelse. Centrale præstationsindikatorer kan være *kvantitative*, f.eks. procentdel falske positive eller falske negative resultater, reduktion af antal, og reduktion af responstid, når registrerede udøver deres rettigheder, eller de kan være *kvalitative*, f.eks. evaluering af præstationer, brug af klassificeringsskalaer eller ekspertvurderinger. I stedet for centrale præstationsindikatorer kan de dataansvarlige tænkes at kunne påvise effektiv implementering af principperne ved at angive rationalet for deres vurdering af effektiviteten af de valgte foranstaltninger og garantier.

2.1.3 Elementer, som skal tages i betragtning

17. Artikel 25, stk. 1, angiver de elementer, som den dataansvarlige skal tage i betragtning ved fastlæggelse af foranstaltningerne for en given databehandlingsaktivitet. I det følgende vejleder vi i, hvordan disse elementer finder anvendelse i designprocessen, herunder design af standardindstillingerne. Alle disse elementer bidrager til at fastslå, om en foranstaltning er egnet til effektivt at implementere principperne. Disse elementer er således i sig selv ikke et mål, men faktorer, der skal medregnes i forbindelse med opfyldelse af målsætningen.

2.1.3.1 "det aktuelle tekniske niveau"

18. Begrebet "det aktuelle tekniske niveau" finder anvendelse i forskellig gældende EU-ret, f.eks. vedrørende miljøbeskyttelse og produktsikkerhed. I databeskyttelsesforordningen omtales "det

[6] "De grundlæggende principper, der gælder for dataansvarlige (dvs. legitimitet, dataminimering, formålsbegrænsning, gennemsigtighed, dataintegritet og datanøjagtighed), bør forblive de samme, uanset databehandlingen og risiciene for de registrerede. Det har dog altid været en integrerende del af anvendelsen af disse principper at tage behørigt hensyn til karakteren og omfanget af en sådan databehandling. I deres væsen er principperne således skalerbare." Artikel 29-arbejdsgruppen. "Statement on the role of a risk-based approach in data protection legal frameworks" (redegørelse for en risikobaseret tilgang til retsgrundlaget for databeskyttelse). WP 218, 30. maj 2014, s. 3. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf

[7] Se betragtning 74 og 78.

aktuelle tekniske niveau"[8] foruden i artikel 32 i forbindelse med sikkerhedsforanstaltninger[9][10] også i artikel 25. Dette benchmark udvides dermed til alle tekniske og organisatoriske foranstaltninger, som er integreret i databehandlingen.

19. I forbindelse med artikel 25 forpligter omtalen af "det aktuelle tekniske niveau" dataansvarlige til **at tage hensyn til eksisterende teknologiske fremskridt, der er på markedet**, når de fastlægger passende tekniske og organisatoriske foranstaltninger. Dataansvarlige skal have viden om og være ajour med teknologiske fremskridt, hvordan teknologi kan frembyde databeskyttelsesrisici og nye muligheder for behandlingsaktiviteten, og hvordan man gennemfører de foranstaltninger og garantier, som *sikrer effektiv implementering* af principperne og registreredes rettigheder på baggrund af ændringerne i det teknologiske landskab.

20. "Det aktuelle tekniske niveau" er et dynamisk begreb, der ikke kan fastlægges på et givet tidspunkt, men som *til stadighed* bør evalueres i forbindelse med teknologiske fremskridt. I lyset af teknologiske fremskridt kan en dataansvarlig tænkes at konkludere, at en foranstaltning, som engang resulterede i et passende beskyttelsesniveau, ikke længere gør det. Undladelse af at holde sig ajour med de teknologiske forandringer ville derfor kunne føre til manglende overholdelse af artikel 25.

21. Kriteriet "det aktuelle tekniske niveau" gælder ikke kun for teknologiske foranstaltninger, men også for organisatoriske. Manglende passende organisatoriske foranstaltninger kan sænke eller helt undergrave effektiviteten af en valgt teknologi. Som eksempel på organisatoriske foranstaltninger kan nævnes indførelse af interne politikker, up-to-date uddannelse i teknologi, sikkerhed og databeskyttelse, og politikker for IT-sikkerhedsforvaltning og -styring.

22. Eksisterende anerkendte rammer, standarder, certificeringer, adfærdskodekser osv. på forskellige områder kan være med til at angive "det aktuelle tekniske niveau" inden for det pågældende anvendelsesområde. Når sådanne standarder findes og sikrer en høj grad af beskyttelse af den registrerede i overensstemmelse med – eller ud over – lovkrav, bør de dataansvarlige tage dem i betragtning ved udformning og gennemførelse af foranstaltninger til databeskyttelse.

2.1.3.2 "omkostninger til iværksættelse"

23. Den dataansvarlige kan tage hensyn til omkostningerne til iværksættelse, når han vælger og anvender passende tekniske og organisatoriske foranstaltninger og fornødne garantier, der reelt implementerer principperne for beskyttelse af registreredes rettigheder. Omkostninger vil i denne sammenhæng sige ressourcer i almindelighed, herunder tid og menneskelige ressourcer.

24. Omkostningselementet indebærer ikke, at den dataansvarlige behøver bruge uforholdsmæssigt mange ressourcer, når der findes andre, mindre ressourcekrævende, men effektive foranstaltninger.

---

[8] Se den tyske forbundsforfatningsdomstols afgørelse "Kalkar" i 1978 https://germanlawarchive.iuscomp.org/?p=67, som kan være grundlag for en metodologi til objektiv definition af begrebet. På denne baggrund kan "det aktuelle tekniske niveau" fastslås at ligge mellem det teknologiske niveau for den "eksisterende videnskabelig viden og forskning" og de mere veletablerede "almindeligt anerkendte teknologiske normer". "Det aktuelle tekniske niveau" kan derfor fastlægges at være det teknologiske niveau for en markedsført tjeneste eller teknologi eller et produkt, som mest effektivt opfylder de udpegede målsætninger.

[9] https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security

[10] www.teletrust.de/en/publikationen/broschueren/state-of-the-art-in-it-security/

Omkostninger til iværksættelse er imidlertid en faktor, der skal tages i betragtning ved gennemførelse af databeskyttelse gennem design, men ikke som en grund til at undlade at gennemføre dem.

25. De valgte foranstaltninger skal således sikre, at den databehandling, der påtænkes af den dataansvarlige, ikke behandler personoplysninger i strid med principperne, uanset omkostningerne. Dataansvarlige bør være i stand til at styre de samlede omkostninger for effektivt at implementere alle principperne og dermed beskytte rettighederne.

2.1.3.3 "behandlingens karakter, omfang, sammenhæng og formål"

26. Dataansvarlige skal tage hensyn til behandlingens karakter, omfang, sammenhæng og formål, når de fastlægger de fornødne foranstaltninger.

27. Disse faktorer bør fortolkes svarende til deres rolle i andre bestemmelser i databeskyttelsesforordningen, såsom artikel 24, 32 og 35, med henblik på at integrere databeskyttelsesprincipperne i behandlingen.

28. Kort sagt kan begrebet **karakter** forstås som de iboende [11] karakteristika for behandlingen. Med **omfang** menes behandlingens udstrækning og dækningsområde. **Sammenhæng** vedrører de omstændigheder ved behandlingen, der kan påvirke den registreredes forventninger, mens **mål**et er formålene med behandlingen.

2.1.3.4 "risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder"

29. Databeskyttelsesforordningen benytter en sammenhængende risikobaseret tilgang i mange af sine bestemmelser i artikel 24, 25, 32 og 35 med henblik på at fastlægge tekniske og organisatoriske foranstaltninger til at beskytte enkeltpersoner og deres personoplysninger og overholde kravene i databeskyttelsesforordningen. De aktiver, der skal beskyttes, er altid de samme (enkeltpersoner via beskyttelse af deres personoplysninger) mod de samme risici (over for enkeltpersoners rettigheder og frihedsrettigheder), og der tages hensyn til de samme betingelser (behandlingens karakter, omfang, sammenhæng og formål).

30. Når de dataansvarlige foretager risikoanalysen med henblik på overholdelse af artikel 25, skal de identificere de risici for de registreredes rettigheder, som en overtrædelse af principperne udgør, og fastlægge deres sandsynlighed og alvor med henblik på at gennemføre foranstaltninger til effektivt at afbøde de identificerede risici. Systematisk og grundig evaluering af behandlingen er afgørende ved risikovurderinger. For eksempel vurderer en dataansvarlig de særlige risici, der er forbundet med manglende frit afgivet samtykke, hvilket udgør en overtrædelse af lovlighedskriteriet i forbindelse med behandlingen af personoplysninger om børn og unge under 18 år som en sårbar gruppe, medmindre der er andre retlige grunde. Den dataansvarlige gennemfører passende foranstaltninger til at håndtere og effektivt afbøde de identificerede risici, der er knyttet til denne gruppe af registrerede.

31. "EDPB Guidelines on Data Protection Impact Assessment (DPIA)" [12] (Databeskyttelsesrådets retningslinjer for konsekvensanalyse vedrørende databeskyttelse (DPIA)) er rettet mod at vurdere, om

[11] Som eksempel kan nævnes særlige kategorier af personoplysninger, automatisk beslutningstagning, ulige magtforhold, uforudsigelig behandling, vanskeligheder for den registrerede med at udøve sine rettighederne mv.

[12] Artikel 29-Gruppen: "Retningslinjer for konsekvensanalyse vedrørende databeskyttelse (DPIA) og bestemmelse af, om behandlingen "sandsynligvis indebærer en høj risiko" i henhold til forordning (EU)

en behandlingsaktivitet må forventes at medføre høj risiko for den registrerede eller ej, og giver også vejledning om, hvordan man vurderer databeskyttelsesrisici, og hvordan man foretager en risikovurdering for databeskyttelse. Disse retningslinjer kan desuden være nyttige ved risikovurdering i henhold til alle ovennævnte artikler, herunder artikel 25.

32. Den risikobaserede tilgang udelukker ikke brugen af basislinjer, bedste praksis og standarder. Disse kan udgøre et praktisk sæt værktøj, som dataansvarlige kan bruge til at imødegå lignende risici i tilsvarende situationer (behandlingens karakter, omfang, sammenhæng og formål). Ikke desto mindre gælder forpligtelsen i artikel 25 (samt artikel 24, 32 og 35, stk. 7, litra c), i databeskyttelsesforordningen) stadig om at tage hensyn til "*risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder, som behandlingen indebærer*" Selvom dataansvarlige støtter sig til de nævnte værktøjer, skal de derfor altid foretage en vurdering af databeskyttelsesrisici for behandlingsaktiviteten i det enkelte tilfælde og efterprøve effektiviteten af de påtænkte passende foranstaltninger og garantier. I så fald kan det desuden være nødvendigt at foretage en konsekvensanalyse vedrørende databeskyttelse (DPIA) eller ajourføre en eksisterende DPIA.

2.1.4 Tidsaspektet

2.1.4.1 På tidspunktet for fastlæggelse af midlerne til behandling

33. Databeskyttelse gennem design skal gennemføres "på tidspunktet for fastlæggelse af midlerne til behandling".

34. "*Midlerne til behandling*" spænder fra de generelle til de detaljerede designelementer i behandlingen, således arkitektur, procedurer, protokoller, layout og udseende.

35. Med "*tidspunktet for fastlæggelse af metoderne til behandling*" menes det tidsrum, hvor den dataansvarlige beslutter, hvordan behandlingen skal foregå, og hvordan den vil finde sted, og de mekanismer, der vil blive anvendt til at foretage behandlingen. Det er under denne beslutningsproces, at den dataansvarlige skal vurdere de passende foranstaltninger og garantier til effektivt at implementere principperne og registreredes rettigheder i behandlingen, og tage hensyn til elementer som det aktuelle tekniske niveau, omkostninger til iværksættelse, karakter, omfang, sammenhæng, formål og risici. Dette indbefatter tidspunktet for udbud og gennemførelse for databehandlingssoftware, -hardware og -tjenesteydelser.

36. Det er nødvendigt at tage hensyn til databeskyttelse gennem design og databeskyttelse gennem standardindstillinger tidligt for at få en vellykket implementering af principperne om registreredes rettigheder og at beskytte dem. Også ud fra et cost-benefit-perspektiv er det i de dataansvarliges interesse tidligst muligt at tage hensyn til databeskyttelse gennem design og databeskyttelse gennem standardindstillinger, da det kan være udfordrende og bekosteligt at ændre planer, der allerede foreligger, og behandlingsaktiviteter, som allerede er udformet.

2.1.4.2 På tidspunktet for selve behandlingen (vedligeholdelse og revision af databeskyttelseskrav)

37. Når behandlingen er påbegyndt, er den dataansvarlige fortsat forpligtet til at bibeholde databeskyttelse gennem design og databeskyttelse gennem standardindstillinger, dvs. fortsat effektivt at implementere principperne for at beskytte rettighederne, holde sig ajour med den seneste

2016/679.". WP 248 rev.01, 4. oktober 2017. ec.europa.eu/newsroom/document.cfm?doc_id=47711 – godkendt af Databeskyttelsesrådet

udvikling, revurdere risikoniveauet osv. Behandlingsprocessernes karakter, omfang, sammenhæng og risiko kan ændre sig i løbet af behandlingen; derfor skal den datasvarlige foretage en fornyet vurdering af sin databehandling ud fra regelmæssig gennemgang og vurdering af effektiviteten af de valgte foranstaltninger og garantier.

38. Også for eksisterende systemer gælder forpligtelsen til at vedligeholde, revidere og om nødvendigt ajourføre behandlingen. Eksisterende systemer, der er udformet inden ikrafttrædelsen af databeskyttelsesforordningen, skal derfor gennemgås og vedligeholdes for at sikre, at der gennemføres foranstaltninger og garantier, som effektivt implementerer principperne og registreredes rettigheder som beskrevet i disse retningslinjer.

39. Denne forpligtelse gælder også al behandling, der udføres af databehandlere. Databehandleres aktiviteter bør regelmæssigt gennemgås og vurderes af de dataansvarlige for at sikre, at de giver mulighed for til stadighed at overholde principperne, og at de giver den dataansvarlige mulighed for at overholde sine forpligtelser i denne henseende.

2.2 Artikel 25, stk. 2: Databeskyttelse gennem standardindstillinger:

2.2.1 Som standard behandles kun personoplysninger, der er nødvendige for hvert specifikt formål med behandlingen.

40. Med en "standardindstilling" som den sædvanligvis defineres inden for datalogien, menes den allerede eksisterende eller forudvalgte værdi af en konfigurerbar indstilling, der tildeles en softwareapplikation, et computerprogram eller en enhed. Sådanne indstillinger kaldes også "forudindstillinger" eller "fabriksindstillinger", navnlig for elektroniske anordninger.

41. Med udtrykket "som standard" ved behandling af personoplysninger menes således at vælge konfigurationsværdier eller databehandlingsmetoder, som er fastlagt eller foreskrevet i et behandlingssystem, f.eks. en softwareapplikation, -tjeneste eller -anordning, eller en manuel behandlingsprocedure, der berører mængden af indsamlede personoplysninger, omfanget af deres behandling, deres opbevaringsperiode og deres tilgængelighed.

42. Den dataansvarlige bør vælge og stå til ansvar for at gennemføre forudindstillinger og valgmuligheder på an sådan måde at, der som standard kun foretages behandling, der er strengt nødvendig for at opfylde det fastlagte lovlige formål. Her bør dataansvarlige støtte sig til deres vurdering af behandlingens nødvendighed med hensyn til retsgrundlaget i artikel 6, stk. 1. Det vil sige, at dataansvarlige ikke automatisk må indsamle flere oplysninger end nødvendigt, de må ikke behandle de indsamlede oplysninger mere, end hvad der er nødvendigt til deres formål med dem, og de må heller ikke opbevare oplysningerne længere end nødvendigt. Det grundlæggende krav er, at databeskyttelse er integreret i behandlingen som standard.

43. Den dataansvarlige skal på forhånd fastlægge, hvilke specificerede, klart angivne legitime formål personoplysningerne indsamles og behandles til.[13] Foranstaltningerne skal som standard være passende til at sikre, at der kun behandles personoplysninger, der er nødvendige til hvert specifikt formål med behandlingen. Databeskyttelsesrådets "Guidelines to assess necessity and proportionality of measures that limit the right to data protection of personal data" (retningslinjer for vurdering af

[13] Artikel 5, stk. 1, litra b), c), d) og e), i databeskyttelsesforordningen

nødvendigheden og proportionaliteten af foranstaltninger, som begrænser retten til databeskyttelse), kan være nyttige til at afgøre, hvilke data der skal behandles for at opfylde et givet formål.[14] [15] [16]

44. Hvis den dataansvarlige benytter tredjepartssoftware eller kommercielt software, bør den dataansvarlige foretage en risikovurdering af produktet og sørge for at funktioner, som ikke understøttes af retsgrundlaget eller ikke er forenelige med de tilsigtede formål med behandlingen, deaktiveres.

45. De samme overvejelser gør sig gældende for organisatoriske foranstaltninger, der støtter behandlingsaktiviteter. De skal indledningsvist være designet til kun at behandle den minimale mængde personoplysninger, som er nødvendig til de specifikke aktiviteter. Dette bør især overvejes ved tildeling af dataadgang til personale med forskellige roller og forskellige adgangsbehov.

46. Passende "tekniske og organisatoriske foranstaltninger" betyder i forbindelse med databeskyttelse gennem standardindstillinger det samme som diskuteret i ovenstående underkapitel 2.1.1, men finder specifikt anvendelse på princippet om dataminimering.

47. Den nævnte forpligtelse til kun at behandle personoplysninger, som er nødvendige til hvert specifikt formål, gælder for følgende elementer:

2.2.2 Dimensionerne af pligten til dataminimering

48. Artikel 25, stk. 2, angiver dimensionerne af den obligatoriske dataminimering ved standardbehandling ved at anføre, at forpligtelsen gælder mængden af indsamlede personoplysninger og omfanget af deres behandling, opbevaringsperiode og tilgængelighed.

2.2.2.1 "den mængde personoplysninger, der indsamles"

49. Dataansvarlige bør både tage hensyn til mængden af personoplysninger samt de typer af, kategorier af og detaljeringsgrader for personoplysninger, der kræves til behandlingsformål.. Deres designvalg bør tage hensyn til de øgede risici for principperne integritet, fortrolighed, dataminimering og opbevaringsbegrænsning ved indsamling af store mængder detaljerede personoplysninger og sammenligne dem med den risikoreduktion, der opnås ved at indsamle færre eller mindre detaljerede oplysninger om registrerede. Under alle omstændigheder må standardindstillingen ikke omfatte indsamling af personoplysninger, som ikke er nødvendige til det konkrete behandlingsformål. Med andre ord må der ikke indsamles overskydende personoplysninger, hvis visse kategorier af personoplysninger er unødvendige, eller hvis der ikke behøves detaljerede oplysninger, fordi det er tilstrækkeligt med mindre granulære data.

[14] EDPS. "Guidelines on assessing the necessity and proportionality of measures that limit the right to data protection" (retningslinjer for vurdering af nødvendigheden og proportionaliteten af foranstaltninger, som begrænser retten til databeskyttelse). 25. februar 2019. edps.europa.eu/sites/edp/files/publication/19-02-25_proportionality_guidelines_en.pdf

[15] Se også Den Europæiske Tilsynsførende for Databeskyttelse (EDPS). "Assessing the necessity of measures that limit the fundamental right to the protection of personal data:" (vurdering af nødvendigheden af foranstaltninger, der begrænser den grundlæggende ret til beskyttelse af personoplysninger): A Toolkit" (et sæt værktøjer) https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_en

[16] For flere oplysninger om nødvendighed, se Artikel 29-Gruppen: "Udtalelse 6/2014 om den dataansvarliges legitime interesser som omhandlet i artikel 7 i direktiv 95/46/EF". WP 217, 9. april 2014. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_da.pdf

50. Samme standardkrav gælder for tjenester, der er uafhængige af, hvilken platform eller anordning, der anvendes: Der må kun indsamles de personoplysninger, der er nødvendige til det givne formål.

2.2.2.2 "omfanget af deres behandling"

51. Behandlingsaktiviteter[17] for personoplysninger skal begrænses til det, der er nødvendigt. Mange behandlingsaktiviteter kan bidrage til et behandlingsformål. Det forhold, at visse personoplysninger er nødvendige for at opfylde et formål, betyder dog ikke, at der kan foretages databehandling af enhver art eller så ofte som muligt. Dataansvarlige bør også passe på ikke at udvide grænserne for "forenelige formål" (artikel 6, stk. 4) og være opmærksomme på, hvilken behandling der vil være inden for, hvad de registrerede med rimelighed forventer.

2.2.2.3 "deres opbevaringsperiode"

52. Indsamlede personoplysninger må ikke opbevares, hvis de ikke er nødvendige for behandlingen, og der ikke er noget andet foreneligt formål og retsgrundlag i henhold til artikel 6, stk. 4. Enhver opbevaring af oplysninger bør kunne begrundes objektivt som nødvendig af den dataansvarlige i overensstemmelse med ansvarlighedsprincippet.

53. Den dataansvarlige skal begrænse opbevaringsperioden til, hvad der er nødvendigt til formålet. Personoplysninger skal som standard slettes eller anonymiseres, hvis de ikke længere behøves til databehandlingen. Opbevaringsperioden vil derfor afhænge af formålet med den pågældende behandling. Denne forpligtelse er direkte forbundet med princippet om opbevaringsbegrænsning i artikel 5, stk. 1, litra e), og den skal gennemføres som standardindstilling – dvs. den dataansvarlige bør have integreret systematiske sletnings- eller anonymiseringsprocedurer i behandlingen.

54. Anonymisering[18] af personoplysninger er et alternativ til sletning, forudsat at der tages hensyn til alle relevante elementer i sammenhængen, og at risicienes sandsynlighed og alvor, inklusive risikoen for identifikation på ny, regelmæssigt vurderes.[19].

2.2.2.4 "deres tilgængelighed"

55. Den dataansvarlige bør begrænse, hvem der har adgang til personoplysninger, og hvilken form for adgang, på baggrund af en vurdering af nødvendighed, og bør desuden sikre sig, at personoplysningerne faktisk er tilgængelige for dem, som har brug for dem, når det er nødvendigt, f.eks. i nødsituationer. Adgangskontrol bør overholdes for hele datastrømmen under behandlingen.

56. Artikel 25, stk. 2, fastslår yderligere, at personoplysninger ikke må gøres tilgængelige for et ubegrænset antal fysiske personer uden den pågældendes indgriben. Den dataansvarlige skal som standardindstilling begrænse tilgængeligheden og give den registrerede mulighed for at gribe ind,

---

[17] Ifølge artikel 4, stk. 2, i databeskyttelsesforordningen omfatter dette indsamling, registrering, organisering, strukturering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse.

[18] Artikel 29-Gruppen: "Udtalelse 05/2014 om anonymiseringsteknikker". WP 216, 10. april 2014. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_da.pdf

[19] Se artikel 4, stk. 1, i databeskyttelsesforordningen, betragtning 26 i databeskyttelsesforordningen og Artikel 29-Gruppens "udtalelse 05/2014 om anonymiseringsteknikker". Se også underafsnittet "opbevaringsbegrænsning" i kapitel 3 i dette dokument, der omhandler nødvendigheden af, at den dataansvarlige sikrer effektiviteten af den/de gennemførte anonymiseringsteknik(ker).

inden personoplysninger om den registrerede offentliggøres eller på anden måde gøres tilgængelige for et ubegrænset antal fysiske personer.

57. At gøre personoplysninger tilgængelige for et ubegrænset antal personer kan føre til endnu større udbredelse af oplysningerne end oprindeligt påtænkt. Dette er særlig relevant i forbindelse med internettet og søgemaskiner. Derfor bør dataansvarlige som standard give registrerede mulighed for at gribe ind, før personoplysninger gøres tilgængelige på det åbne internet. Særligt for børn og sårbare grupper er dette vigtigt.

58. Afhængigt af retsgrundlaget for behandlingen kan muligheden for at gribe ind være forskellig alt efter baggrunden for behandlingen. F.eks. kan man anmode om samtykke til at gøre personoplysningerne offentligt tilgængelige, eller man kan have privatlivsindstillinger, der giver de registrerede mulighed for selv at styre offentlighedens adgang.

59. Selv om personoplysninger gøres offentligt tilgængelige med den registreredes tilladelse og viden, betyder det ikke, at andre dataansvarlige med adgang til personoplysningerne frit selv kan behandle dem til egne formål – de skal have deres eget retsgrundlag.[20]

3 IMPLEMENTERING AF DATABESKYTTELSESPRINCIPPERNE I BEHANDLINGEN AF PERSONOPLYSNINGER MED BRUG AF DATABESKYTTELSE GENNEM DESIGN OG DATABESKYTTELSE GENNEM STANDARDINDSTILLINGER

60. I alle faser af udformningen af behandlingsaktiviteterne – herunder indkøb, udbud, outsourcing, udvikling, støtte, vedligeholdelse, testning, opbevaring, sletning mv. – bør den dataansvarlige tage hensyn til og overveje de forskellige elementer i databeskyttelse gennem design og databeskyttelse gennem standardindstillinger. Dette illustreres af eksemplerne i dette kapitel i sammenhæng med implementeringen af principperne.[21] [22] [23]

61. Dataansvarlige skal implementere principperne for opnåelse af databeskyttelse gennem design og databeskyttelse gennem standardindstillinger. Disse principper omfatter gennemsigtighed, lovlighed, rimelighed, formålsbegrænsning, dataminimering, nøjagtighed, opbevaringsbegrænsning, integritet og fortrolighed samt ansvarlighed. Principperne er beskrevet i artikel 5 og betragtning 39 i databeskyttelsesforordningen. For at få fuldstændig indsigt i, hvordan man gennemfører databeskyttelse gennem design og databeskyttelse gennem standardindstillinger er det vigtigt at forstå betydningen af de enkelte principper.

62. I forbindelse med eksemplerne på, hvordan databeskyttelse gennem design og databeskyttelse gennem standardindstillinger kan gennemføres, har vi for hvert princip opstillet lister over **hovedelementerne i databeskyttelse gennem design og databeskyttelse gennem standardindstillinger**. Eksemplerne fremhæver det pågældende specifikke databeskyttelsesprincip og

[20] Jf. sagen Satakunnan Markkinapörssi Oy og Satamedia Oy mod Finland nr. 931/13

[21] Flere eksempler kan findes hos de norske databeskyttelsesmyndigheder: "Software Development with Data Protection by Design and by Default" (softwareudvikling med databeskyttelse gennem design og databeskyttelse gennem standardindstillinger). 28. november 2017 www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/?id=7729

[22] https://www.cnil.fr/en/cnil-publishes-gdpr-guide-developers

[23] https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf

kan også overlappe med andre nært beslægtede principper. Det Europæiske Databeskyttelsesråd understreger, at følgende hovedelementer og eksempler hverken er udtømmende eller bindende, men er tænkt som vejledende elementer for hvert princip. Dataansvarlige skal vurdere, hvordan de sikrer overholdelse af principperne i forbindelse med den pågældende konkrete behandling.

63. Dette afsnit er fokuseret på implementeringen af principperne, men den dataansvarlige bør desuden gennemføre *passende* og *effektive* måder at beskytte registreredes rettigheder på, også i henhold til kapitel III i databeskyttelsesforordningen, når dette ikke allerede er fastlagt i principperne.

64. Ansvarlighedsprincippet er overordnet: Det fastslår, at den dataansvarlige har ansvar for at vælge de nødvendige tekniske og organisatoriske foranstaltninger.

3.1 Gennemsigtighed[24]

65. Den dataansvarlige skal fra starten af klart og åbent angive over for den registrerede, hvordan han vil indsamle, bruge og dele personoplysninger. Gennemsigtighed drejer sig om, at registrerede får mulighed for at sætte sig ind i deres rettigheder i artikel 15 til 22 og om nødvendigt gøre brug af dem. Princippet er integreret i artikel 12, 13, 14 og 34. Foranstaltninger og garantier, som er indført for at støtte gennemsigtighedsprincippet, bør også støtte gennemførelsen af disse artikler.

66. Blandt de vigtigste design- og standardelementer vedrørende gennemsigtighedsprincippet kan være:

- Klarhed – Information skal affattes på et klart og enkelt sprog og være kortfattet og forståelig.
- Semantik – Kommunikationen bør have klar betydning for målgruppen.
- Tilgængelighed – Informationen skal være lettilgængelig for den registrerede.
- Sammenhæng – Information bør gives på det relevante tidspunkt og i en passende form.
- Relevans – Information bør være relevant og anvendelig for den pågældende registrerede.
- Universelt design – Information skal være tilgængelig for alle registrerede og anvende maskinlæsbare sprog for at fremme og automatisere læsbarhed og klarhed.
- Forståelighed – Registrerede bør have rimelig indsigt i, hvad de kan forvente af behandlingen af deres personoplysninger, navnlig når de registrerede er børn eller andre sårbare grupper.
- Mange kanaler – Information bør gives gennem mange forskellige kanaler og medier, ikke kun tekstmedier, for at informationen faktisk skal nå frem til den registrerede.
- Information på flere forskellige niveauer – Informationen bør gives på flere niveauer, så den ophæver modsætningen mellem fuldstændighed og indsigt og tager højde for rimelige forventninger hos de registrerede.

Eksempel[25]

En dataansvarlig er ved at udforme en politik for databeskyttelse på sit websted for at opfylde gennemsigtighedskravene. Privatlivspolitikken bør ikke indeholde en masse information, som er vanskelig at sætte sig ind i og forstå for den gennemsnitlige registrerede. Den skal være affattet klart og kortfattet, så det er let for brugere af webstedet at få indsigt i, hvordan deres personoplysninger

[24] En uddybet forklaring af begrebet gennemsigtighed er givet i Artikel 29-Gruppens: "Guidelines on transparency under Regulation 2016/679" (retningslinjer for gennemsigtighed i henhold til forordning 2016/679). WP 260 rev.01, 11. april 2018. ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025 – godkendt af Databeskyttelsesrådet

[25] Den franske databeskyttelsesmyndighed har offentliggjort flere eksempler, der illustrerer bedste praksis for at informere brugerne, foruden andre principper om gennemsigtighed: https://design.cnil.fr/en/

behandles. Den dataansvarlige giver derfor information på flere forskellige niveauer og fremhæver hovedpunkterne. Mere detaljerede oplysninger gøres let tilgængelige. Der er rullemenuer og links til andre sider for at udvide forklaringen af de forskellige emner og begreber, der anvendes i politikken. Den dataansvarlige sørger desuden for, at informationen gives ad flere kanaler og indeholder videoklip for at forklare hovedpunkterne i den skriftlige information. Synergi mellem de forskellige websider er afgørende for, at den flerstrengede tilgang ikke skaber mere forvirring, men mindsker den.

Det bør ikke være vanskeligt for registrerede at få adgang til privatlivspolitikken. Politikken for databeskyttelse gøres således tilgængelig og synlig på alle interne websider på det pågældende websted, så den registrerede altid kun er et klik fra informationen. Den information, der gives, udformes desuden i overensstemmelse med bedste praksis og standarder for universelt design, så den er tilgængelig for alle.

Derudover bør den nødvendige information gives i den rette sammenhæng og på et passende tidspunkt. Da den dataansvarlige foretager mange behandlingsaktiviteter ved hjælp af data indsamlet på webstedet, er en generel fortrolighedspolitik alene på webstedet ikke tilstrækkelig til, at den dataansvarlige opfylder gennemsigtighedskravene. Den dataansvarlige udformer derfor en informationsstrøm, der forsyner den registrerede med relevant information i passende sammenhænge, f.eks. med små uddrag af information eller pop-op-vinduer. Når den registrerede bliver bedt om at indtaste personoplysninger, kan den dataansvarlige f.eks. oplyse den registrerede om, hvordan personoplysningerne vil blive behandlet, og hvorfor de er nødvendige til behandlingen.

3.2 Lovlighed

67. Den dataansvarlige skal fastlægge et gyldigt retsgrundlag for behandlingen af personoplysninger. Foranstaltningerne og garantierne bør støtte kravet om at sikre, at hele processens livscyklus er i overensstemmelse med det relevante retsgrundlag for behandlingen.

68. De vigtigste elementer af design- og standardindstillinger med henblik på lovlighed kan være:
    - Relevans – Behandlingen skal være omfattet af det korrekte retsgrundlag.
    - Differentiering[26] – Retsgrundlaget skal være differentieret for de enkelte behandlingsaktiviteter.
    - Specificeret formål – Det passende retsgrundlag skal have klar sammenhæng med behandlingens specifikke formål.[27]
    - Nødvendighed – Behandlingen skal være ubetinget nødvendig, for at formålet er lovligt.
    - Selvstændighed – Den registrerede bør tildeles så megen selvstændighed som muligt vedrørende kontrollen over personoplysninger inden for rammerne af retsgrundlaget.
    - Opnåelse af samtykke – samtykket skal være frivilligt, specifikt, informeret og utvetydigt.[28] Der bør lægges særlig vægt på børns og unges evne til at give informeret samtykke.
    - Tilbagetrækning af samtykke – Hvis samtykke er retsgrundlaget, bør behandlingen gøre det let at trække samtykket tilbage. Samtykket skal være lige så let at trække tilbage som at give.

[26] Databeskyttelsesrådet: "Retningslinjer 2/2019 for behandling af personoplysninger i henhold til artikel 6, stk. 1, litra b), i GDPR i forbindelse med leveringen af onlinetjenester til registrerede" version 2.0, 8. oktober 2019. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_da.pdf

[27] Se afsnittet om formålsbegrænsning nedenfor.

[28] Se "Guidelines 05/2020 on consent under Regulation 2016/679" (retningslinje 05/2020 om samtykke i henhold til forordning (EF) nr. 2016/679). https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_da

Ellers er den dataansvarliges samtykkemekanisme ikke i overensstemmelse med databeskyttelsesforordningen.[29]

- Interesseafvejning – Når retsgrundlaget er legitime interesser, skal den dataansvarlige foretage en vægtet afvejning af interesser med særlig vægt på den skæve magtbalance, navnlig for børn under 18 år og andre sårbare grupper. Der skal være foranstaltninger og garantier for at afbøde de negative virkninger for de registrerede.
- Forhåndsbestemmelse – Retsgrundlaget skal være fastlagt, inden databehandlingen finder sted.
- Ophør – Hvis retsgrundlaget ikke længere finder anvendelse, skal også behandlingen ophøre.
- Tilpasning – I tilfælde af en gyldig ændring af retsgrundlaget for behandlingen skal den aktuelle behandling tilpasses efter det nye retsgrundlag.[30]
- Tildeling af ansvar – Hvis der skal være fælles dataansvar, skal parterne fordele deres respektive ansvarsområder i forhold til den registrerede på en klar og gennemsigtig måde, og de skal udforme foranstaltningerne for behandlingen i overensstemmelse med denne fordeling.

Eksempel

En bank har til hensigt at tilbyde en tjenesteydelse for at styrke effektiviteten af behandlingen af låneansøgninger. Ideen bag tjenesteydelsen er, at banken med kundens tilladelse skal kunne indhente oplysninger om kunden direkte fra skattemyndighederne. Med dette eksempel er der ikke taget stilling til behandling af personoplysninger fra andre kilder.

Personoplysninger om den registreredes finansielle situation er nødvendige for at tage skridt til at indgå en lånekontrakt på den registreredes anmodning.[31] Det anses imidlertid ikke for nødvendigt at indsamle personoplysninger direkte fra skattemyndighederne, da kunden kan indgå en kontrakt ved selv at give oplysningerne fra skattemyndighederne. Banken kan have en legitim interesse i at modtage dokumentation direkte fra skattemyndighederne, f.eks. for at sikre effektiv lånebehandling, men en sådan direkte adgang for banker til ansøgeres personoplysninger medfører risiko i forbindelse med brug eller potentielt misbrug af adgangsrettighederne.

Når den dataansvarlige implementerer princippet om lovlighed, vil han indse, at han ikke i denne sammenhæng kan benytte "nødvendigt for kontrakten" som grundlag for den del af behandlingen, der består i at indsamle personoplysninger direkte fra skattemyndighederne. Denne særlige behandling udgør en risiko for, at den registrerede bliver mindre inddraget i behandlingen af sine oplysninger og er desuden en relevant faktor i vurderingen af selve behandlingens lovlighed. Banken konkluderer, at denne del af behandlingen er nødt til at have hjemmel i et andet retsgrundlag. I den dataansvarliges hjemstat giver de nationale love banken mulighed for at indsamle oplysninger direkte fra skattemyndighederne mod forudgående samtykke fra den registrerede.

Banken lægger derfor oplysninger om behandlingen på onlineansøgningsplatformen på en måde, der gør det let for registrerede at forstå, hvilken behandling der er obligatorisk, og hvilken der er valgfri.

[29] Se "Guidelines 05/2020 on consent under Regulation 2016/679" (retningslinje 05/2020 om samtykke i henhold til forordning 2016/679), s. 24. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_da

[30] Hvis det oprindelige retsgrundlag er samtykke, se "Guidelines 05/2020 on consent under Regulation 2016/679" (retningslinje 05/2020 om samtykke i henhold til forordning (EF) nr. 2016/679). https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_da

[31] Se artikel 6, stk. 1, litra b), i databeskyttelsesforordningen

Som standard tillader valgmulighederne for behandling ikke at indhente oplysninger direkte fra andre kilder end den registrerede, og muligheden for at vælge direkte indhentning af informationer præsenteres på en måde, der ikke afholder den registrerede i at afstå. Ethvert samtykke til at indsamle oplysninger direkte fra andre dataansvarlige er midlertidig ret til indsigt i bestemte informationer.

Ethvert afgivet samtykke behandles elektronisk på en dokumenterbar måde, og registrerede får let mulighed for at kontrollere, hvad de har afgivet samtykke til, og til at trække samtykket tilbage.

Den dataansvarlige har vurderet disse krav til databeskyttelse gennem design og databeskyttelse gennem standardindstillinger på forhånd og har medtaget alle disse kriterier i dennes kravspecifikation for udbuddet til anskaffelse af platformen. Den dataansvarlige er opmærksom på, at hvis denne ikke inkluderer kravene til databeskyttelse gennem design og databeskyttelse gennem standardindstillinger i udbuddet, kan det enten være for sent eller meget dyrt at gennemføre databeskyttelse bagefter.

3.3 Rimelighed

69. Ifølge det overordnede rimelighedsprincip må personoplysninger ikke behandles på en måde, som er urimeligt skadelig, ulovligt diskriminerende, uventet eller vildledende for den registrerede. Foranstaltninger og garantier, som implementerer rimelighedsprincippet, støtter også registreredes rettigheder og frihedsrettigheder, navnlig retten til information (gennemsigtighed), retten til at gribe ind (adgang, sletning, dataportabilitet og berigtigelse) og retten til at begrænse behandlingen (retten til ikke at blive underlagt automatiske enkeltafgørelser, og til ikke-diskrimination af registrerede under sådanne processer).

70. Blandt de vigtigste design- og standardelementer vedrørende rimelighed kan være:
    - Autonomi – de registrerede bør have størst mulig autonomi til at afgøre, hvordan deres personoplysninger skal anvendes, i hvilket omfang og på hvilke vilkår.
    - Interaktion – Registrerede skal have mulighed for at kommunikere og til at udøve deres rettigheder vedrørende de personoplysninger, den dataansvarlige behandler.
    - Forventning – Behandlingen bør svare til de registreredes rimelige forventninger.
    - Ikke-diskrimination – Den dataansvarlige må ikke diskriminere registrerede urimeligt.
    - Ikke-udnyttelse – Den dataansvarlige må ikke udnytte registreredes behov eller sårbarheder.
    - Valgfrihed for forbrugerne – Den dataansvarlige må ikke "fastlåse" sine brugere urimeligt. Når en tjenesteydelse, der behandler personoplysninger, er omfattet af ejendomsrettigheder, kan den oprette et "lock-in" til tjenesteydelsen. Hvis det svækker de registreredes mulighed for at udøve deres ret til dataportabilitet i henhold til artikel 20, kan dette eventuelt anses for at være urimeligt.
    - Magtbalance – Et ligeligt magtforhold bør være en hovedmålsætning for relationen mellem den dataansvarlige og den registrerede. Ulige magtforhold bør undgås. Når dette ikke er muligt, bør det tages til efterretning og tages højde for med passende modforanstaltninger.
    - Dataansvarlige bør ikke flytte virksomhedens risici over på de registrerede.
    - Ikke-vildledende – Oplysninger og valgmuligheder vedrørende databehandling bør fremlægges objektivt og neutralt, så man undgår vildledende eller manipulerende formuleringer og design.
    - Respekt af rettigheder – Den dataansvarlige skal respektere de registreredes grundlæggende rettigheder, gennemføre passende foranstaltninger og garantier, og ikke overtræde disse rettigheder, medmindre det udtrykkeligt er begrundet i lovgivningen.

- Etik — Den dataansvarlige bør være opmærksom på behandlingens bredere konsekvenser for enkeltpersoners rettigheder og værdighed.
- Sandfærdighed – De dataansvarlige skal stille oplysninger til rådighed om, hvordan de behandler personoplysninger. De bør handle på den måde, som de har erklæret, og ikke vildlede de registrerede.
- Menneskelig indgriben – Den dataansvarlige skal integrere *kvalificeret* menneskelig indgriben, som er i stand til at udbedre afvigelser, som maskiner kan danne i forhold til retten til ikke at være underlagt automatiske individuelle afgørelser som angivet i artikel 22..[32]
- Rimelige algoritmer – Regelmæssigt vurdere, om algoritmerne virker i overensstemmelse med formålene, og tilpasse algoritmerne, så de afbøder systemiske fejl og sikrer rimelighed i behandlingen. Registrerede bør oplyses om, hvordan den behandling af personoplysninger foregår, som er baseret på algoritmer, der analyserer eller opstiller forudsigelser om dem – såsom arbejdsindsats, økonomisk situation, helbred, personlige præferencer, pålidelighed eller adfærd, geografisk placering og geografiske bevægelser.[33]

Eksempel 1

En dataansvarlig driver en søgemaskine, der primært behandler brugergenererede personoplysninger. Den dataansvarlige drager fordel af at have store mængder personoplysninger og at være i stand til at benytte disse personoplysninger til målrettede reklamer. Den dataansvarlige ønsker derfor at påvirke de registrerede til at tillade mere omfattende indsamling og brug af deres personoplysninger. Der skal indhentes samtykke ved at forelægge valgmulighederne for behandlingen for den registrerede.

Ved at implementere princippet om rimelighed, hvor der tages hensyn til behandlingens karakter, omfang, sammenhæng og formål, indser den dataansvarlige, at denne ikke må forelægge valgmulighederne på en måde, som presser den registrerede i retning af at tillade, at den dataansvarlige indsamler flere personoplysninger end hvis valgmulighederne blev præsenteret på en ligeværdig og neutral måde. Det vil sige, at den dataansvarlige ikke må fremlægge behandlingsmulighederne på en måde, som gør det svært for de registrerede at afstå fra at dele deres oplysninger eller gør det vanskeligt for dem at tilpasse deres databeskyttelsesindstillinger og begrænse behandlingen. Dette er eksempler på uheldige mønstre, som strider mod ånden i artikel 25. Standardindstillingerne for behandlingen bør ikke være for invasive, og valget af videre behandling bør forelægges på en måde, der ikke presser den registrerede til at give sit samtykke. Derfor fremlægger den dataansvarlige valget mellem at samtykke eller ej som to ligeværdige alternativer, og redegør nøje for konsekvenserne af hvert valg for den registrerede.

Eksempel 2

En anden dataansvarlig behandler personoplysninger til levering af en streamingtjeneste, hvor brugerne kan vælge mellem et almindeligt abonnement af standardkvalitet og et

[32] Se "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679" (retningslinjer for automatiserede enkeltafgørelser og profilering med henblik på forordning nr. 2016/679), https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826

[33] Se betragtning 71 i databeskyttelsesforordningen.

premiumabonnement af højere kvalitet. Som en del af premiumabonnementet får abonnenter prioriteret kundeservice.

Af hensyn til rimelighedsprincippet må den prioriterede kundeservice til premiumabonnenter ikke diskriminere almindelige abonnenters adgang til at udøve deres rettigheder i henhold til databeskyttelsesforordningens artikel 12. Dette betyder, at selvom premiumabonnenter får prioriteret service, må denne prioritering ikke resultere i, at der undlades passende foranstaltninger til at imødekomme anmodninger fra almindelige abonnenter uden unødig forsinkelse og under alle omstændigheder senest en måned efter modtagelse af anmodningerne.

Prioriterede kunder kan betale for bedre service, men alle registrerede skal have lige og ikke-diskriminerende muligheder for at håndhæve deres rettigheder og frihedsrettigheder som fastlagt i artikel 12.

3.4 Formålsbegrænsning[34]

71. Den dataansvarlige skal indsamle oplysninger til specificerede, udtrykkelige og legitime formål og må ikke viderebehandle oplysninger på en måde, som er uforenelig med de formål, de er indsamlet til.[35] Behandlingens design bør derfor udformes efter, hvad der er nødvendigt for at opfylde formålene. Hvis der skal foretages yderligere behandling, skal den dataansvarlige først sikre sig, at formålene med denne behandling er forenelige med de oprindelige, og designe behandlingen tilsvarende. Om et nyt formål er foreneligt eller ej, skal vurderes ud fra kriterierne i artikel 6, stk. 4.

72. Hovedelementerne i design- og standardindstillinger for formålsbegrænsning kan være:
- Forudbestemmelse – De legitime formål skal fastlægges, inden behandlingen designes.
- Specificitet – Formålene skal specificeres, og skal udtrykkeligt angive, hvorfor der behandles personoplysninger.
- Formålsorienteret – Behandlingens formål bør være vejledende for behandlingens design og fastlægge grænser for behandlingen.
- Nødvendighed – Formålet er bestemmende for, hvilke personoplysninger der er nødvendige til behandlingen.
- Forenelighed – Nye formål skal være forenelige med det oprindelige formål, som oplysningerne blev indsamlet til, og vejledende for relevante designændringer.
- Begrænsning af yderligere behandling – Den dataansvarlige bør ikke tilslutte datasæt eller foretage yderligere behandling til nye, uforenelige formål.
- Begrænsninger for videreanvendelse – Den dataansvarlige bør benytte tekniske foranstaltninger, herunder hashing og kryptering, til at begrænse muligheden for at ændre formålet med personoplysninger. Den dataansvarlige bør også anvende organisatoriske foranstaltninger, såsom politikker og kontraktlige forpligtelser, som begrænser videreanvendelsen af personoplysninger.

[34] Artikel 29-Gruppen har givet vejledning om, hvordan man skal opfatte princippet om formålsbegrænsning i henhold til direktiv 95/46/EF. Selvom udtalelsen ikke er vedtaget af Databeskyttelsesrådet, kan den alligevel være relevant, da princippets ordlyd er den samme som i databeskyttelsesforordningen. Artikel 29-Gruppens udtalelse 03/2013 om formålsbegrænsning, WP 203, 2. april 2013. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

[35] Artikel 5, stk. 1, litra b), i databeskyttelsesforordningen.

- Gennemgang – Den dataansvarlige bør regelmæssigt gennemgå, om behandlingen er nødvendig til de formål, oplysningerne er indsamlet til, og afprøve designet i forhold til formålsbegrænsningen.

Eksempel

Den dataansvarlige behandler personoplysninger om sine kunder. Behandlingens formål er at opfylde en kontrakt, dvs. at være i stand til at levere varer til den korrekte adresse og indhente betaling. De personoplysninger, som opbevares, er købshistorik, navn, adresse, e-mailadresse og telefonnummer.

Den dataansvarlige overvejer at anskaffe et (CRM-) produkt, der samler alle kundeoplysninger på ét sted, dvs. markedsføring og kundeservice. Med produktet kan man opbevare alle telefonopkald, aktiviteter, dokumenter, e-mails og markedsføringskampagner og således få et helhedsoverblik over kunden. Desuden analyserer CRM automatisk kundernes købekraft ved hjælp af offentligt tilgængelige oplysninger. Formålet med analysen er at målrette reklameaktiviteterne bedre. Disse aktiviteter er ikke en del af det oprindelige lovlige formål med behandlingen.

For at være i overensstemmelse med princippet om formålsbegrænsning skal den dataansvarlige kræve, at produktets leverandør kortlægger de forskellige behandlingsaktiviteter med personoplysninger og de formål, der er relevante for den dataansvarlige.

Efter at have fået resultaterne af kortlægningen vurderer den dataansvarlige, om det nye markedsføringsformål og det påtænkte reklameformål er forenelige med de oprindelige formål, der blev fastlagt ved indsamlingen af oplysningerne, og om der er tilstrækkeligt retsgrundlag for den pågældende behandling. Hvis vurderingen ikke er positiv, må den dataansvarlige ikke anvende de pågældende funktioner. I stedet kan den dataansvarlige vælge at give afkald på vurderingen og simpelthen ikke gøre brug af de beskrevne funktioner i produktet.

3.5 Dataminimering

73. Der må kun behandles personoplysninger, som er passende, relevante og begrænset til, hvad der er **nødvendigt** til formålet.[36] Derfor skal den dataansvarlige på forhånd afgøre, hvilke funktioner og parametre i behandlingssystemerne og deres støttefunktioner, der er tilladte. Dataminimering underbygger og realiserer nødvendighedsprincippet. Ved den videre behandling bør den dataansvarlige med mellemrum tage stilling til, om behandlede personoplysninger stadig er passende, relevante og nødvendige, eller om oplysningerne skal slettes eller anonymiseres.

74. Dataansvarlige bør som det første vurdere, om de overhovedet har brug for at behandle personoplysninger til deres relevante formål. Den dataansvarlige bør efterprøve, om de relevante formål kan opfyldes ved at behandle færre personoplysninger eller have mindre detaljerede eller aggregerede personoplysninger, eller helt uden at behandle personoplysninger[37]. En sådan efterprøvning bør finde sted inden behandlingen, men kan også finde sted på ethvert tidspunkt under behandlingen. Dette er også i overensstemmelse med artikel 11.

[36] Artikel 5, stk. 1, litra c), i databeskyttelsesforordningen.
[37] I betragtning 39 i databeskyttelsesforordningen hedder det: "... personoplysninger bør kun behandles, hvis formålet med behandlingen ikke med rimelighed kan opfyldes på anden vis."

75. Minimering kan også henvise til graden af identificering. Hvis behandlingens formål ikke kræver, at det endelige sæt oplysninger henviser til en identificeret eller identificerbar enkeltperson (som til statistik), men dette er tilfældet for den indledende behandling (f.eks. inden aggregering af oplysningerne), skal den dataansvarlige anonymisere personoplysningerne, så snart der ikke længere behøves identificering. Hvis identificering fortsat er nødvendig til brug for andre behandlingsaktiviteter, bør personoplysningerne pseudonymiseres for at mindske risiciene for de registreredes rettigheder.

76. Hovedelementerne for minimering i design- og standardindstillinger kan omfatte:
    - Undgåelse af oplysninger – Helt at undgå at behandle personoplysninger, når dette er muligt til det pågældende formål.
    - Begrænsning – Begrænsning af mængden af indsamlede personoplysninger til, hvad der er nødvendigt til formålet.
    - Adgangsbegrænsning – Udformning af databehandlingen på en måde, så færrest mulige personer behøver adgang til personoplysninger for at udføre deres opgaver, og begrænsning af adgangen i overensstemmelse med det.
    - Relevans – Personoplysninger bør være relevante for den pågældende behandling, og dette bør den dataansvarlige kunne påvise.
    - Nødvendighed – Hver kategori af personoplysningerne bør være nødvendig til det angivne formål og bør kun behandles, hvis formålet ikke kan opfyldes på anden måde.
    - Aggregering – Brug aggregerede oplysninger, når det er muligt.
    - Pseudonymisering – Personoplysninger skal pseudonymiseres, når det ikke længere er nødvendigt at have direkte identificerbare personoplysninger, og identifikationsnøgler skal opbevares separat.
    - Anonymisering og sletning – Når personoplysninger ikke – eller ikke længere – er nødvendige til formålet, skal de anonymiseres eller slettes.
    - Datastrøm – Datastrømmen bør gøres så effektiv, at der ikke oprettes flere kopier end nødvendigt.
    - "Det aktuelle tekniske niveau" – Den dataansvarlige bør anvende egnede tidssvarende teknologier til at undgå eller minimere data.

Eksempel 1

En boghandel vil øge sine indtægter ved at sælge bøger online. Boghandlens ejer vil oprette en standardformular til bestillingsprocessen. For at sikre, at kunderne giver alle de nødvendige oplysninger, gør boghandlens ejer alle formularens felter obligatoriske (alle felter skal udfyldes for at man kan afgive bestillingen). Webbutikkens ejer benytter indledningsvis en standardkontaktformular, som beder om kundens fødselsdato, telefonnummer og privatadresse. Ikke alle felterne i formularen er imidlertid nødvendige for at købe bøger og få dem leveret. I dette tilfælde er den registreredes fødselsdato og telefonnummer ikke nødvendig for købet, hvis denne forudbetaler for produktet. Det vil sige, at disse felter ikke må være obligatoriske i webformularen for at kunne bestille produktet, medmindre den dataansvarlige klart kan påvise, at felterne på anden måde er nødvendige, og hvorfor. Derudover er der situationer, hvor adressen er unødvendig. F.eks. kan kunden ved bestilling af en e-bog downloade den direkte til sin enhed.

Webbutikkens ejer beslutter derfor at oprette to webformularer: én til bestilling af bøger med et felt til kundens adresse, og én til bestilling af e-bøger uden felt til kundens adresse

Eksempel 2

Et offentligt transportselskab ønsker at indsamle statistiske oplysninger baseret på de rejsendes ruter. Dette er nyttigt til at træffe fornuftige valg om ændringer af planer for offentlig transport og korrekte togruter. Passagererne skal scanne billetten i en læser hver gang de går ind i eller ud af et transportmiddel. Efter at have foretaget en risikovurdering vedrørende passagerers rettigheder og frihedsrettigheder i forbindelse med indsamling af oplysninger om passagerers rejseruter fastslår den dataansvarlige, at man ud fra den enkelte rute kan identificere passagerer ved hjælp af billettens identifikationskode under omstændigheder, hvor de bor eller arbejder i tyndtbefolkede område. Den dataansvarlige undlader derfor at opbevare billettens identifikationskode, da den ikke er nødvendig for at optimere fartplanerne for offentlig transport og togruter. Når rejsen er forbi, opbevarer den dataansvarlige kun de enkelte rejseruter, så han ikke er i stand til at identificere rejser knyttet til en enkelt billet, men kun bibeholder oplysninger om separate rejseruter.

Hvis der er risiko for at identificere en person udelukkende ud fra vedkommendes rute med offentlig transport, foretager den dataansvarlige statistiske tiltag til at mindske risikoen, såsom at fjerne rutens start- og slutpunkt.

Eksempel 3

En kurérvirksomhed vil vurdere effektiviteten af sine leverancer ud fra leveringstider, planlagt arbejdsbelastning og brændstofforbrug. For at opfylde dette mål er kurérvirksomheden nødt til at behandle en række personoplysninger om både ansatte (chauffører) og kunder (adresser, forsendelser til levering, mv.). Denne behandlingsaktivitet medfører risici både vedrørende overvågning af ansatte – hvilket kræver særlige retlige garantier – og sporing af kundernes vaner ud fra kendskab til leverancerne over tid. Disse risici kan væsentligt mindskes med passende pseudonymisering af medarbejdere og kunder. Hvis pseudonymiseringsnøgler hyppigt udskiftes, og makroområder benyttes i stedet for detaljerede adresser, så kan man forfølge en effektiv dataminimering, og den dataansvarlige kan udelukkende fokusere på leveringsprocessen og ressourceoptimering uden at overtræde grænserne for adfærdsovervågning af enkeltpersoner (kunder eller medarbejdere).

Eksempel 4

Et hospital indsamler data om sine patienter i et hospitalsinformationssystem (en elektronisk patientjournal). Hospitalets personale behøver adgang til patientjournalerne for at registrere deres afgørelser om pleje og behandling af patienterne og for at dokumentere alle diagnosemæssige og plejerelaterede og behandlingsmæssige tiltag. Som standard gives kun adgang til de medlemmer af det lægelige personale, der behandler den pågældende patient på den specialafdeling, som vedkommende er tilknyttet. Hvis man involverer andre afdelinger eller diagnosticeringsenheder i behandlingen, udvider man gruppen af personer med adgang til patientens journal. Når patienten er udskrevet, og epikrisen er skrevet, reduceres adgangen til en lille gruppe medarbejdere på hver specialafdeling, som efter samtykke fra patienten besvarer anmodninger om lægelige oplysninger eller samråd fra andre ydere af medicinske tjenester.

3.6 Nøjagtighed

77. Personoplysninger skal være korrekte og ajourført, og der skal tages ethvert rimeligt skridt til, at personoplysninger straks slettes eller berigtiges, hvis de er ukorrekte med hensyn til de formål, de behandles til.[38]

78. Kravene bør ses i relation til risiciene og konsekvenserne forbundet med den faktiske anvendelse af oplysningerne. Ukorrekte personoplysninger kan udgøre en risiko for registreredes rettigheder og frihedsrettigheder, f.eks. hvis de fører til fejldiagnose eller til fejlagtig angivelse af behandling i en protokol, eller når et ukorrekt billede af personen kan føre til fejlafgørelser enten manuelt, ved brug af automatisk beslutningstagning eller med kunstig intelligens.

79. Blandt de vigtigste design- og standardelementer vedrørende nøjagtighed kan være:
    - Datakilde – Datakilder bør være pålidelige med hensyn til dataenes nøjagtighed.
    - Grad af nøjagtighed – Hvert element af personoplysningerne bør være så nøjagtigt som nødvendigt til de angivne formål.
    - Målbart korrekt – Mindskelse i antal falske positive/negative resultater, f.eks. skævheder i automatiserede afgørelser og kunstig intelligens.
    - Verifikation – Ud fra personoplysningernes karakter og under hensyn til, hvor ofte de kan ændre sig, bør den dataansvarlige verificere oplysningernes korrekthed i forhold til den registrerede. Dette bør ske inden behandlingen og på forskellige behandlingsstadier (f.eks. vedrørende alderskrav).
    - Sletning/berigtigelse – Den dataansvarlige skal straks slette eller berigtige urigtige oplysninger. Den dataansvarlige skal navnlig fremme dette, når de registrerede er eller var børn og senere ønsker at fjerne sådanne personoplysninger.[39]
    - Undgåelse af akkumulerede fejl – Dataansvarlige bør mindske virkningen af en akkumuleret fejl i behandlingskæden.
    - Adgang – Registrerede bør informeres om og have faktisk adgang til personoplysninger i overensstemmelse med databeskyttelsesforordningens artikel 12 til 15 for at kontrollere deres nøjagtighed og berigtige dem efter behov.
    - Vedvarende nøjagtighed – Personoplysninger bør være nøjagtige i alle faser af behandlingen, og der bør foretages kontrol af deres nøjagtighed ved kritiske trin.
    - Ajourføring – Personoplysninger skal ajourføres, hvis det er nødvendigt til formålet.
    - Datadesign – brug teknologisk og organisatorisk design for at mindske unøjagtighed, f.eks. kortfattede forudbestemte valg fremfor fritekstfelter

Eksempel 1

Et forsikringsselskab ønsker at anvende kunstig intelligens (AI) til at profilere købere af forsikringer og anvende det som grundlag for sine afgørelser ved beregning af forsikringsrisikoen. Når selskabet afgør, hvordan AI-løsninger bør udvikles, fastlægger det, hvordan betalingen skal ske, og skal derfor tage hensyn til databeskyttelse gennem design, når det vælger en AI-applikation fra en forhandler, og når det afgør, hvordan løsningerne skal programmeres.

De dataansvarlige bør råde over nøjagtige oplysninger, når de afgør, hvordan AI-løsningerne skal programmeres, så der kan opnås præcise resultater. De dataansvarlige bør derfor sikre, at de oplysninger, som bruges til at programmere løsningerne er korrekte.

[38] Artikel 5, stk. 1, litra d), i databeskyttelsesforordningen.
[39] Jf. betragtning 65.

Forudsat at de har et gyldigt retsgrundlag for at programmere AI-løsningerne ved hjælp af personoplysninger fra en stor pulje af eksisterende kunder, vælger de dataansvarlige en kundepulje, som er repræsentativ for befolkningen, for at undgå skævhed.

Kundeoplysningerne indsamles derefter fra det pågældende datahåndteringssystem, herunder oplysninger om forsikringstypen, f.eks. sundhedsforsikring, boligforsikring, rejseforsikring osv., samt data fra offentlige registre, som den dataansvarlige har lovlig adgang til. Alle oplysninger pseudonymiseres, inden de overføres til systemet, som skal oplære modellen for kunstig intelligens.

For at sikre at de oplysninger, som bruges til AI-oplæring, er så nøjagtige som muligt, indsamler den dataansvarlige kun oplysninger fra kilder med korrekte og ajourførte oplysninger.

Forsikringsselskabet tester, om AI'en er pålidelig og giver ikke-diskriminerende resultater, både under sin udvikling, og til slut inden produktet frigives. Når AI'en er færdigoplært og driftsklar, anvender forsikringsselskabet resultaterne til at understøtte vurderingerne af forsikringsrisici – dog uden at forlade sig alene på kunstig intelligens – til at afgøre, om der skal ydes en forsikring, medmindre afgørelsen træffes i overensstemmelse med undtagelserne i artikel 22, stk. 2, i databeskyttelsesforordningen.

Forsikringsselskabet vil desuden regelmæssigt gennemgå resultaterne fra AI'en for at fastholde pålideligheden og om nødvendigt justere algoritmen.

Eksempel 2

Den dataansvarlige er en sundhedsinstitution, som søger metoder til at sikre integriteten og nøjagtigheden af personoplysningerne i sine patientregistre.

I situationer, hvor to personer ankommer til institutionen samtidig og modtager samme behandling, er der risiko for at forveksle dem, hvis de kun kan skelnes på navnet. For at sikre nøjagtighed behøver den dataansvarlige en unik identifikator for hver person, dvs. flere oplysninger end bare navnet.

Institutionen anvender flere systemer, som indeholder personoplysninger om patienterne, og skal sikre, at oplysningerne om patienten er korrekte, nøjagtige og konsekvente i alle systemerne på ethvert tidspunkt. Institutionen har konstateret flere risici, som kan opstå, hvis der ændres oplysninger i ét system men ikke i de andre.

Den dataansvarlige beslutter at mindske risikoen ved hjælp af en hashing-teknik, der kan sikre integriteten af oplysningerne i behandlingsjournalen. Der oprettes kryptografiske tidsstempler til behandlingsjournalerne og den tilknyttede patient, så eventuelle ændringer kan konstateres, samkøres og om nødvendigt spores.

3.7 Opbevaringsbegrænsning

80. Den dataansvarlige skal sikre, at personoplysninger opbevares i en form, der ikke tillader identifikation af registrerede længere, end hvad der er nødvendigt til det formål, personoplysningerne behandles til.[40]

[40] Artikel 5, stk. 1, litra c), i databeskyttelsesforordningen.

Det er ubetinget nødvendigt, at den dataansvarlige nøjagtigt ved, hvilke personoplysninger virksomheden behandler, og hvorfor. Behandlingens formål skal være det afgørende kriterium for, hvor længe personoplysninger opbevares.

81. Foranstaltninger og garantier, der implementerer princippet om opbevaringsbegrænsning, skal supplere de registreredes rettigheder og frihedsrettigheder, navnlig retten til sletning og retten til at gøre indsigelse.

82. Blandt hovedelementerne i design- og standardindstillinger for opbevaringsbegrænsning kan være:
- Sletning og anonymisering – den dataansvarlige bør have klare interne procedurer og funktioner for sletning og/eller anonymisering.
- Effektiviteten af anonymisering/sletning – Den dataansvarlige skal sørge for, at det ikke er muligt at genidentificere anonymiserede oplysninger eller gendanne slettede oplysninger, og bør efterprøve, om det er muligt.
- Automatisering – Sletning af visse personoplysninger bør automatiseres.
- Kriterier for opbevaring – Den dataansvarlige skal fastlægge, hvilke oplysninger og hvilken opbevaringsperiode, der behøves til formålet.
- Begrundelse – den dataansvarlige skal kunne begrunde, hvorfor opbevaringsperioden er nødvendig til det pågældende formål og de pågældende personoplysninger, og skal kunne oplyse begrundelsen og retsgrundlaget for opbevaringsperioden.
- Håndhævelse af politikker for opbevaring – Den dataansvarlige bør håndhæve interne opbevaringspolitikker og foretage tests af, om organisationen fører sine politikker ud i praksis.
- Sikkerhedskopier/logfiler — Dataansvarlige skal bestemme, hvilke personoplysninger og hvilken opbevaringsvarighed der er nødvendig for sikkerhedskopier og logfiler.
- Datastrøm – Dataansvarlige bør være opmærksomme på strømmen af personoplysninger og opbevaringen af kopier deraf, og bør søge at begrænse den "midlertidige" opbevaring af dem.

Eksempel

Den dataansvarlige indsamler personoplysninger med det formål at administrere et medlemskab for den registrerede. Personoplysningerne skal slettes, når medlemskabet ophører, og der ikke er retsgrundlag for fortsat at opbevare oplysningerne.

Den dataansvarlige opstiller først en intern procedure for opbevaring og sletning af oplysninger. I henhold til denne procedure skal medarbejderne manuelt slette personoplysninger, når opbevaringsperioden er slut. Medarbejderen følger proceduren for regelmæssigt at slette og korrigere oplysninger fra alle enheder, sikkerhedskopier, logfiler, e-mails og andre relevante opbevaringsmedier.

For at gøre sletningen mere effektiv og mindre fejlbehæftet gennemfører den dataansvarlige i stedet et system, der sletter oplysningerne automatisk, pålideligt og mere regelmæssigt. Systemet konfigureres til at følge den givne procedure for sletning af oplysninger, som derefter gennemføres med regelmæssige forudbestemte intervaller for at fjerne personoplysninger fra alle virksomhedens opbevaringsmedier. Den dataansvarlige gennemgår og tester regelmæssigt opbevaringsproceduren og sikrer, at den er i overensstemmelse med den ajourførte opbevaringspolitik.

3.8 Integritet og fortrolighed

83. Princippet integritet og fortrolighed inkluderer beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse, og ved hjælp af passende tekniske eller

organisatoriske foranstaltninger. Sikkerheden af personoplysninger kræver passende foranstaltninger, der er udformet til at forhindre og håndtere databrud, garantere korrekt udførelse af databehandlingsopgaver, overensstemmelse med de øvrige principper, og fremme af effektiv udøvelse af enkeltpersoners rettigheder

84. Betragtning 78 fastslår, at en af foranstaltningerne til databeskyttelse gennem design og databeskyttelse gennem standardindstillinger kan bestå i at gøre det muligt for den dataansvarlige at *"tilvejebringe og forbedre sikkerhedselementer"*. Sammen med andre foranstaltninger til databeskyttelse gennem design og databeskyttelse gennem standardindstillinger antyder betragtning 78, at de dataansvarlige er ansvarlige for løbende at vurdere, om der til enhver tid benyttes passende behandlingsmidler, og vurdere, om de valgte foranstaltninger faktisk modvirker de eksisterende sårbarheder. Dataansvarlige bør desuden regelmæssigt gennemgå de foranstaltninger til informationssikkerhed, der omgiver og beskytter personoplysningerne, og proceduren for håndtering af databrud.

85. Blandt de vigtigste design- og standardelementer i integritet og fortrolighed kan være:
    - Et system til at forvalte informationssikkerhed (ISMS) – Hav et operativt middel til at forvalte politikker og procedurer for informationssikkerhed.
    - Risikoanalyse – Vurder risiciene over for sikkerheden af personoplysninger ved at tage hensyn til virkningen på enkeltpersoners rettigheder, og imødegå konstaterede risici. Inden for risikovurdering at udvikle og opretholde en omfattende, systematisk og realistisk "trusselsmodellering" og en analyse af angrebsfladen af den designede software for at reducere angrebsvektorer og mulighederne for at udnytte svage punkter og sårbarheder.
    - Sikkerhed gennem design – Tag hensyn til sikkerhedskrav tidligst muligt i systemets udformning og udvikling, integrer relevante tests løbende, og udfør dem.
    - Vedligeholdelse – Gennemgå og test regelmæssigt software, hardware, systemer og tjenester osv. for at afdække sårbarheder i de systemer, der ligger til grund for behandlingen.
    - Styring af adgangskontrol – Der bør kun være adgang for bemyndiget personale, som behøver adgang til de personoplysninger, der er nødvendige for deres behandlingsopgaver, og den dataansvarlige bør skelne mellem adgangsrettighederne for bemyndiget personale.
        - Adgangsbegrænsning (ansatte) – Tilrettelæg databehandlingen, så at kun et minimalt antal personer behøver adgang til personoplysninger for at udføre deres arbejdsopgaver, og begræns adgangen tilsvarende.
        - Adgangsbegrænsning (indhold) – For hver behandling, begræns adgangen til de attributter for hvert datasæt, der er nødvendige for at udføre den pågældende operation. Begræns desuden adgangen til data vedrørende de registrerede, som hører under den pågældende medarbejders ansvarsområde.
        - Opdeling af adgang – Udform databehandlingen på en sådan måde, at ingen behøver fuldstændig adgang til alle data, der er indsamlet om en registreret, endnu mindre alle personoplysninger om en given kategori af registrerede.
    - Sikre overførsler – Overførsler bør være sikret mod uautoriseret adgang og utilsigtede ændringer.
    - Sikker opbevaring – Opbevarede data bør være sikret mod uautoriseret adgang og uautoriserede ændringer. Der bør være procedurer til at vurdere risikoen ved central eller decentral opbevaring, og hvilke kategorier af personoplysninger, de gælder for. Nogle oplysninger kan behøve flere sikkerhedsforanstaltninger end andre.
    - Pseudonymisering – Personoplysninger og sikkerhedskopier/logfiler bør som sikkerhedsforanstaltning pseudonymiseres for at minimere risiciene for databrud, f.eks. ved hjælp af hashing eller kryptering.

- Sikkerhedskopier/logfiler – Sørg for at føre sikkerhedskopier og logfiler i det omfang, det er nødvendigt for informationssikkerheden. Brug revisionssporing og hændelsesovervågning som rutinemæssig sikkerhedskontrol. Disse skal være beskyttet mod uautoriseret og utilsigtet adgang og ændring, og regelmæssigt gennemgås, og hændelser bør straks håndteres.
- Katastrofeberedskab/driftskontinuitet – Opfyld kravene om katastrofeberedskab og driftskontinuitet til genoprettelse af personoplysninger efter større hændelser.
- Beskyttelse i henhold til risiko – Alle kategorier af personoplysninger bør være beskyttet med foranstaltninger, der er tilstrækkelige i forhold til risikoen for sikkerhedsbrud. Data, der indebærer særlige risici, bør om muligt holdes adskilt fra resten af personoplysningerne.
- Håndtering af sikkerhedshændelser – Hav rutiner, procedurer og ressourcer til at afsløre, håndtere, dæmme op for og indberette brud på datasikkerheden og lær af dem.
- Hændelseshåndtering – Den dataansvarlige bør have indført procedurer til håndtering af brud og hændelser for at gøre behandlingssystemet mere robust. Hertil hører underretningsprocedurer, således. håndtering af anmeldelser (til tilsynsmyndigheden) og oplysninger (til registrerede).

Eksempel

En dataansvarlig ønsker at uddrage store mængder personoplysninger fra en medicinsk database, der indeholder elektroniske (patient)journaler, til en særlig databaseserver i virksomheden for at behandle de uddragne data med henblik på kvalitetssikring. Virksomheden har vurderet, at overførsel af uddragene til en server, som er tilgængelig for alle virksomhedens medarbejdere, må forventes at medføre stor risiko for de registreredes rettigheder og frihedsrettigheder. Der er kun én afdeling i virksomheden, som behøver at behandle uddrag af patientoplysninger. Den dataansvarlige beslutter derfor at begrænse adgangen til den dedikerede server til ansatte i den pågældende afdeling. For yderligere at mindske risikoen vil oplysningerne blive pseudonymiseret, inden de overføres.

For at regulere adgangen og afbøde mulige skader som følge af malware beslutter virksomheden at segregere netværket og etablere adgangskontrol til serveren. Derudover opretter virksomheden et system til sikkerhedsovervågning og et system til afsløring og forhindring af indtrængen, som isoleres fra rutinemæssig brug. Der etableres et automatisk revisionssystem til at overvåge adgang og ændringer. Systemet genererer herudfra alarmer og automatiske advarsler, når der er konfigureret visse hændelser i forhold til anvendelsen. Den dataansvarlige sikrer, at brugere kun har adgang ud fra "need-to-know"-princippet og har det tilbørlige adgangsniveau. Uhensigtsmæssig brug kan opdages hurtigt og let.

Nogle af uddragene skal sammenholdes med nye uddrag og kræves derfor opbevaret i tre måneder. Den dataansvarlige beslutter at indlæse disse i separate databaser på samme server og anvende både gennemsigtig kryptering og kryptering på kolonneniveau til at opbevare dem. Nøgler til dekryptering af kolonnedata opbevares i særlige sikkerhedsmoduler, som kun kan anvendes af autoriseret personale, men ikke kan hentes ud.

Håndtering af kommende hændelser gør systemet mere robust og pålideligt. Den dataansvarlige ved, at der bør integreres effektive forebyggende foranstaltninger og garantier i alle nuværende og fremtidige aktiviteter med behandling af personoplysninger, og at dette kan medvirke til at forhindre lignende databrud i fremtiden.

Den dataansvarlige fastlægger disse sikkerhedsforanstaltninger både for at sikre nøjagtighed, integritet og fortrolighed, og for at forhindre spredning af malware fra cyberangreb og gøre løsningen robust. At have robuste sikkerhedsforanstaltninger bidrager til at styrke tilliden hos de registrerede.

3.9 Ansvarlighed[41]

86. Princippet om ansvarlighed fastslår, at den dataansvarlige er ansvarlig for, at alle ovennævnte principper overholdes, og kan påvise det.

87. Den dataansvarlige skal kunne påvise, at principperne er overholdt. Til dette kan den dataansvarlige påvise virkningerne af de foranstaltninger, der er truffet for at beskytte de registreredes rettigheder, og hvorfor foranstaltningerne anses for at være hensigtsmæssige og effektive. Herunder kan han for eksempel påvise, hvorfor en foranstaltning er passende til at sikre princippet om effektivt at begrænse opbevaring

88. For at kunne varetage ansvaret for at behandle personoplysninger bør den dataansvarlige både have tilstrækkelig viden og kapacitet til at gennemføre databeskyttelse. Dette indebærer, at den dataansvarlige har indsigt i databeskyttelsesforpligtelserne i henhold til databeskyttelsesforordningen og er i stand til at opfylde dem.

4 ARTIKEL 25, STK. 3, CERTIFICERING

89. I henhold til artikel 25, stk. 3, kan certificering i henhold til artikel 42 anvendes til at påvise overholdelse med databeskyttelse gennem design og databeskyttelse gennem standardindstillinger. Omvendt kan dokumenter, der påviser overensstemmelse med databeskyttelse gennem design og databeskyttelse gennem standardindstillinger, også være nyttige i en certificeringsproces. Dette betyder, at når en dataansvarlig eller databehandler er certificeret i henhold til artikel 42, skal tilsynsmyndighederne tage dette i betragtning i deres vurdering af overholdelsen af databeskyttelsesforordningen, navnlig hvad angår databeskyttelse gennem design og databeskyttelse gennem standardindstillinger.

90. Når den behandling, der foretages af en dataansvarlig eller databehandler, er certificeret i henhold til artikel 42, er det designprocesserne, der bidrager til at påvise overholdelsen af artikel 25, stk. 1 og stk. 2, dvs. processen til at fastlægge midlerne til behandling, og de forvaltningsmæssige, tekniske og organisatoriske foranstaltninger til at implementere databeskyttelsesprincipperne. Kriterierne for certificering af databeskyttelsen fastlægges af certificeringsorganerne eller af ejerne af certificeringsordningerne, og godkendes derefter af den kompetente tilsynsmyndighed eller af Det Europæiske Databeskyttelsesråd. For yderligere oplysninger om certificeringsmekanismer henvises til Det Europæiske Databeskyttelsesråds retningslinjer om certificering[42] og til anden relevant vejledning, som er offentliggjort på Det Europæiske Databeskyttelsesråds websted.

91. Selv i tilfælde, hvor en behandling er tildelt en certificering i henhold til artikel 42, er det stadig den dataansvarliges ansvar løbende at overvåge og forbedre overholdelsen af kriterierne for databeskyttelse gennem design og databeskyttelse gennem standardindstillinger i artikel 25.

5 HÅNDHÆVELSE AF ARTIKEL 25 OG KONSEKVENSERNE HERAF

92. Tilsynsmyndigheder kan vurdere overholdelsen af artikel 25 i henhold til procedurerne i artikel 58. De korrigerende beføjelser er angivet i artikel 58, stk. 2, og omfatter udstedelse af advarsler, udtalelse af

[41] Se betragtning 74, hvor dataansvarlige forpligtes til at godtgøre, at deres foranstaltninger er effektive.
[42] Databeskyttelsesrådet: "Retningslinjer 1/2018 vedrørende certificering og identifikation af certificeringskriterier i overensstemmelse med artikel 42 og 43 i forordningen" Version 3.0, 4. juni 2019. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_da.pdf

kritik, udstedelse af påbud om at overholde registreredes rettigheder, begrænsninger for eller forbud mod behandling, administrative bøder osv.

93. Databeskyttelse gennem design og databeskyttelse gennem standardindstillinger er desuden med til at fastlægge størrelsen af økonomiske sanktioner for overtrædelser af databeskyttelsesforordningen, jf. artikel 83, stk. 4.[43] [44]

6 HENSTILLINGER

94. Databehandlere og producenter anerkendes desuden som vigtige katalysatorer for databeskyttelse gennem design og databeskyttelse gennem standardindstillinger, skønt dette ikke er direkte omhandlet i artikel 25. De bør imidlertid være opmærksomme på, at dataansvarlige kun må behandle personoplysninger med systemer og teknologier, der har integreret databeskyttelse.

95. Ved databehandling på vegne af dataansvarlige eller levering af løsninger til dataansvarlige bør databehandlere og producenter udnytte deres ekspertise til at opbygge tillid hos deres kunder, også SMV'er, og vejlede dem i at designe/anskaffe løsninger, som integrerer databeskyttelse i behandlingen. Dette betyder igen , at produkter og tjenester bør være udformet, så de støtter de dataansvarliges behov.

96. Ved gennemførelse af artikel 25 bør man have for øje, at den primære designmålsætning er *effektivt at implementere* principperne og *beskytte* registreredes rettigheder i behandlingen. For at lette og styrke brugen af databeskyttelse gennem design og databeskyttelse gennem standardindstillinger retter vi følgende henstillinger til dataansvarlige, producenter og databehandlere:
    - Dataansvarlige bør være opmærksomme på databeskyttelse lige fra de *indledende planlægningsfaser* af en behandlingsaktivitet, også inden hjælpemidlerne til behandling er fastlagt.
    - Når den dataansvarlige har en databeskyttelsesansvarlig (DPO), opfordrer Databeskyttelsesrådet den databeskyttelsesansvarlige til aktivt at integrere databeskyttelse gennem design og databeskyttelse gennem standardindstillinger i indkøbs- og udviklingsprocedurerne og i hele behandlingscyklussen.
    - En behandlingsoperation kan blive *certificeret.* Muligheden for at få en behandlingsaktivitet certificeret giver den dataansvarlige merværdi, når han vælger behandlingssoftware, hardware, tjenester og systemer fra producenter eller databehandlere. Producenter bør derfor søge at påvise databeskyttelse gennem design og databeskyttelse gennem standardindstillinger i livscyklussen af deres udvikling af en behandlingsløsning. En certificering kan også være vejledende for de registrerede i valget mellem forskellige produkter og tjenesteydelser. At kunne få en proces certificeret kan være en konkurrencefordel for både producenter, databehandlere og dataansvarlige og styrker desuden de registreredes tillid til behandlingen af deres personoplysninger. Hvis der ikke er mulighed for certificering, bør dataansvarlige søge at få andre *garantier* for, at producenter og tjenesteleverandører

[43] Artikel 83, stk. 2, litra d), i databeskyttelsesforordningen fastsætter, at ved pålæggelse af bøder for overtrædelse af databeskyttelsesforordningen *skal der tages "behørigt hensyn" til "den dataansvarliges eller databehandlerens grad af ansvar under hensyntagen til tekniske og organisatoriske foranstaltninger, som de har gennemført i henhold til artikel 25 og 32".*

[44] Mere information om bøder findes i Artikel 29-Gruppen: Retningslinjer vedrørende anvendelse og fastsættelse af administrative bøder i overensstemmelse med forordning (EU) 2016/679). WP 253, 3. oktober 2017. ec.europa.eu/newsroom/just/document.cfm?doc_id=47889 – godkendt af Databeskyttelsesrådet

overholder kravene om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger.

- Dataansvarlige, databehandlere og producenter bør tage hensyn til deres forpligtelser til at give børn under 18 år og andre sårbare grupper særlig beskyttelse ved databeskyttelse gennem design og databeskyttelse gennem standardindstillinger.
- Producenter og databehandlere bør søge at fremme gennemførelsen af databeskyttelse gennem design og databeskyttelse gennem standardindstillinger for at støtte den dataansvarliges mulighed for at overholde forpligtelserne i henhold til artikel 25. Derimod bør dataansvarlige ikke vælge producenter eller databehandlere, som ikke tilbyder systemer, der giver den dataansvarlige mulighed for at overholde artikel 25 eller støtter ham i det, da dataansvarlige vil blive holdt til ansvar for manglende gennemførelse af artiklen.
- Producenter og databehandlere bør aktivt tage del i at sikre, at kriterierne for "det aktuelle tekniske niveau" opfyldes, og bør underrette dataansvarlige om enhver ændring af "det aktuelle tekniske niveau", som kan have betydning for de foranstaltninger, de har indført. Dataansvarlige bør indsætte dette krav som en kontraktbestemmelse for at sikre, at de bliver holdt ajour.
- Det Europæiske Databeskyttelsesråd anbefaler de dataansvarlige at kræve, at producenter og databehandlere påviser, hvordan deres hardware, software, tjenester og systemer gør det muligt for den dataansvarlige at opfylde kravene om ansvarlighed i overensstemmelse med databeskyttelse gennem design og databeskyttelse gennem standardindstillinger, f.eks. ved at anvende centrale præstationsindikatorer til at påvise effektiviteten af foranstaltningerne og garantierne til implementering af principperne og rettighederne.
- Databeskyttelsesrådet understreger nødvendigheden af at benytte en harmoniseret tilgang til effektivt at implementere principper og rettigheder. Tilsynet opfordrer sammenslutninger og organer, som udarbejder adfærdskodeks i medfør af artikel 40, til også at indføje sektorspecifik vejledning om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger.
- Dataansvarlige bør være rimelige over for registrerede og gennemskuelige med hensyn til, hvordan de vurderer og påviser effektiv gennemførelse af databeskyttelse gennem design og databeskyttelse gennem standardindstillinger, på samme måde som dataansvarlige påviser, at databeskyttelsesforordningen bliver overholdt i henhold til ansvarlighedsprincippet.
- Privatlivsbeskyttende teknologier, der har nået en modenhed svarende til det aktuelle tekniske niveau, kan anvendes som foranstaltning i henhold til kravene om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger, hvis dette er hensigtsmæssigt i en risikobaseret tilgang. Privatlivsbeskyttende teknologier dækker i sig selv ikke nødvendigvis forpligtelserne i artikel 25. De dataansvarlige skal vurdere, om foranstaltningen er hensigtsmæssig og effektiv til at implementere databeskyttelsesprincipperne og registreredes rettigheder.
- Eksisterende nedarvede systemer er underkastet samme forpligtelser som nye systemer til databeskyttelse gennem design og databeskyttelse gennem standardindstillinger. Hvis et nedarvet system ikke allerede opfylder databeskyttelse gennem design og databeskyttelse gennem standardindstillinger, og der ikke kan foretages ændringer for at opfylde forpligtelserne, er det nedarvede system simpelthen ikke i overensstemmelse med forpligtelserne i henhold til databeskyttelsesforordningen og må ikke anvendes til at behandle personoplysninger.

- Artikel 25 sænker ikke kravene til SMV'er. Følgende punkter kan fremme SMV'ers overholdelse af artikel 25:
    - Foretag risikovurderinger tidligt
    - Start med en lille behandling – tilpas senere dens omfang og avancerethed
    - Søg efter producenters og databehandleres garantier for databeskyttelse gennem design og databeskyttelse gennem standardindstillinger, såsom certificering og overholdelse af adfærdskodekser
    - Anvend partnere med gode resultater
    - Før dialog med databeskyttelsesmyndighederne
    - Læs vejledninger fra databeskyttelsesmyndighederne og Det Europæiske Databeskyttelsesråd
    - Følg adfærdskodekser, hvis de forefindes
    - Få faglig hjælp og rådgivning

På vegne af Det Europæiske Databeskyttelsesråd

Formanden

(Andrea Jelinek)