DATATILSYNET

JUSTITSMINISTERIET

DIGITALISERINGSSTYRELSEN

# Behandlingssikkerhed

# Databeskyttelse gennem design og standardindstillinger

Juni 2018

# Indhold

# 1. Forord

Databeskyttelsesforordningen finder anvendelse fra den 25. maj 2018. Denne vejledning er primært skrevet til dig, der som *dataansvarlig* eller *databehandler*[1] har brug for at vide, hvordan du tilvejebringer en tilstrækkelig behandlingssikkerhed (artikel 32), og hvordan du som *dataansvarlig* håndterer forordningens krav om databeskyttelse gennem design og standardindstillinger (artikel 25).

Vejledningen behandler således artikel 25 og 32 i databeskyttelsesforordningen. Denne fremgangsmåde er valgt ud fra to hovedhensyn. *For det første* har vi ønsket at lade vejledningen afspejle den praktiske virkelighed, som virksomheder og offentlige myndigheder opererer indenfor. *For det andet* er der et naturligt sammenspil mellem på den ene side forordningens krav til behandlingssikkerhed og på den anden side databeskyttelse gennem design og standardindstillinger. Dette illustreres bl.a. ved, at formålet med databeskyttelse gennem design og standardindstillinger er, at du som dataansvarlig - allerede som led i forberedelsen og iværksættelsen af persondatabehandlingen - etablerer nogle forhold, der egner sig til at sikre, at forordningen bliver overholdt, og at det nødvendige beskyttelsesniveau kan realiseres.

Den samlede behandling af de to bestemmelser sker i fuld respekt for, at der er tale om to *forskellige bestemmelser*. Det bemærkes i den forbindelse, at artikel 25, om databeskyttelse gennem design og standardindstillinger, er en nyskabelse, som er inspireret af Ann Cavoukians 7 principper herom, der omtales nedenfor i afsnit 5.1. Det fremhæves også, at artikel 25 ikke blot handler om at "indbygge" *behandlingssikkerhed* fra begyndelsen, men tillige indebærer, at systemer designes og standardindstillinger tilpasses på en sådan måde, at alle forordningens grundlæggende principper f.eks. princippet om dataminimering kan overholdes.

Vejledningen er opdelt i to dele, som kort introduceres nedenfor.

Del 1 – Behandlingssikkerhed (artikel 32)

Når du har ansvaret for en behandling[2] af personoplysninger, er det vigtigt at være opmærksom på, at du i tilstrækkelig grad beskytter de oplysninger, du har ansvaret for behandlingen af.

Får du ikke tilvejebragt den tilstrækkelige sikkerhed, risikerer du, at personoplysningerne havner i de forkerte hænder, hvilket *blandt andet* kan betyde, at oplysningerne anvendes til uautoriserede formål, manipuleres eller tilintetgøres. Udover uvedkommendes adgang til dine systemer kan en utilstrækkelig sikkerhed f.eks. medføre misbrug eller forkert håndtering af autoriserede brugere eller manglende kontrol/validering, manglende tilgængelighed grundet it-nedbrud, brand eller forkert håndtering af krypteringsnøgler.

[1] Se *vejledning om dataansvarlige og databehandlere*, der er tilgængelig på datatilsynets hjemmeside www.datatilsynet.dk, for en nærmere gennemgang af hvornår man er dataansvarlig og databehandler.

[2] F.eks. indsamling, registrering, videregivelse eller sletning

Som ansvarlig for behandlingen skal du derfor sikre, at der tilvejebringes et sikkerhedsniveau, der forhindrer, at der foretages behandlinger i strid med forordningen, herunder at uvedkommende får adgang til de oplysninger, du behandler, og anvender dem til uautoriserede formål, eller at der sker andre sikkerhedsbrud som følge af forkert håndtering af systemerne m.v.

Vejledningens Del 1 vil bringe dig igennem de krav, forordningen stiller, og de overvejelser, du forventes at skulle gøre dig. Afsnit 4 indeholder en praktisk "hjælpeguide" til din overholdelse af kravene til behandlingssikkerhed.

Del 2 – Databeskyttelse gennem design (artikel 25, stk. 1) og databeskyttelse gennem standardindstillinger (artikel 25, stk. 2)

Forordningen indfører også regler om databeskyttelse gennem design. Reglerne herom skal sikre, at de fornødne garantier i behandlingen integreres fra starten med henblik på at opfylde forordningens krav og beskytte de registreredes rettigheder.

Begrebet "gennem design" er således en tilgang til at indlejre databeskyttelse på et tidligt stadie i systemudviklingen. Herved sikres det bl.a., at databeskyttelse tænkes ind fra starten, når it-løsninger designes, udvikles, indkøbes eller tilpasses.

Derudover indfører forordningen også regler om databeskyttelse gennem standardindstillinger. Denne bestemmelse fastslår, at den dataansvarlige og databehandleren skal sørge for at afpasse indstillingerne på en sådan måde, at der som standard ydes den størst mulige grad af beskyttelse for den registrerede.

# DEL I

# 2. Hvad er behandlingssikkerhed (artikel 32)?

Behandlingssikkerhed reguleres i databeskyttelsesforordningens artikel 32 og handler overordnet om, at du som den ansvarlige for databehandlingen – dataansvarlig eller databehandler – tilvejebringer et tilstrækkeligt sikkerhedsniveau for den behandling af oplysninger, du foretager.

Forordningen kræver, at du skal fastlægge sikkerhedsniveauet ud fra en samlet vurdering af det aktuelle tekniske niveau, implementeringsomkostninger og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder.

Når du har taget hensyn hertil, skal du gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici, bl.a. afhængigt af, hvad der er relevant i forhold til de foranstaltninger, som forordningen selv nævner, jf. nedenfor under vejledningens afsnit 3.2.

Det er altså en forudsætning for at opnå den efter forordningen tilstræbte databeskyttelse, at der stilles nogle krav til dit sikkerhedsniveau, som modsvarer de risici, der er ved en given behandling af personoplysninger.

I praksis betyder det, at du skal have et *passende sikkerhedsniveau* for at forhindre, at du behandler oplysninger i strid med forordningen, herunder at de personoplysninger du behandler (f.eks. indsamler og opbevarer) enten hændeligt eller bevidst tilintetgøres, misbruges eller lignende.

# 3. Krav til behandlingssikkerhed

For at etablere en tilstrækkelig sikkerhed og forhindre, at der sker behandling i strid med databeskyttelsesforordningen, skal du som dataansvarlig eller databehandler vurdere de risici, som en behandling indebærer, og gennemføre foranstaltninger, der kan begrænse disse risici, som f.eks. kryptering.

Generelt bemærkes det, at personoplysninger klassificeres som almindelige personoplysninger (mindst sensitive) og følsomme personoplysninger (mest sensitive). Generelt kan man sige, at beskyttelsesbehovet er større, des mere sensitive personoplysninger, der behandles. Herudover afhænger beskyttelsesbehovet af yderligere omstændigheder, herunder risicienes varierende sandsynlighed. Således kan risici være større grundet f.eks. den mængde af data, der behandles – flere data betyder potentielt større udbytte ved uvedkommendes adgang, hvorfor flere givet vil forsøge at få (adgang til) disse data, hvilket vil øge sandsynligheden for succesfuld hacking.

Det er dig, der skal gøre dig overvejelser om beskyttelsesbehovet for de oplysninger, der behandles.

Hvis forskellige typer af personoplysninger behandles sammen, skal du indrette sikkerhedsforanstaltningerne efter de mest sensitive oplysninger. Selve måden, du behandler oplysningerne på, kan også spille en rolle for indretningen af dine sikkerhedsforanstaltninger, f.eks. hvis du foretager profilering på baggrund af almindelige personoplysninger.

## 3.1 Passende sikkerhedsniveau

Forordningen kræver, at en behandling af personoplysninger skal have et *passende* sikkerheds*niveau*. Hvornår et sådant "passende sikkerhedsniveau" er etableret vil bero på en konkret vurdering. Som vejledende pejlemærke kan nævnes, at et passende sikkerhedsniveau vil afhænge af, *hvilke* og *hvor store* risici der er for sikkerhedsbrud og dermed for, at fysiske personers rettigheder og frihedsrettigheder krænkes.

Risikoen er teknisk defineret som en given trussel, dennes indvirkning på den fysiske persons rettigheder og sandsynligheden for, at truslen realiseres. For at etablere et passende sikkerhedsniveau bør du derfor starte med at afdække, hvilke risici, der er forbundet med din behandling. Afsnit 4.1.1 nedenfor, der omhandler identifikation og vurdering af risici kan være en praktisk hjælp til, hvordan du kan gribe denne opgave an.

**Eksempler på risici, som en behandling af personoplysninger generelt kan udgøre:**

- *hændelig eller ulovlig tilintetgørelse,*
- *hændeligt eller ulovligt tab,*
- *hændelig eller ulovlig ændring eller*
- *uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet, og som kan føre til fysisk, materiel eller immateriel skade.*

**Eksempler på andre konkrete trusler, der kan medføre risiko ved behandling af personoplysninger:**

- *phising,*
- *spear phishing,*
- *malware,*
- *ransomware,*
- *tab af krypteringsnøgle,*
- *utilstrækkelig (for svag) kryptering*
- *tab af backups,*
- *manglende procedure for genoprettelse,*
- *uvedkommende adgang*
- *manglende intern viden i organisationen om håndtering af persondata og it-systemer m.v.*

Ovenstående eksempler udgør ikke udtømmende lister over potentielt relevante risici. Du kan anvende listerne som inspiration i relation til hvilke risici, der navnlig er relevante at imødegå, når du skal fastsætte sikkerhedsniveauet.

For så vidt angår uvedkommende adgang bemærkes det, at en sådan adgang både kan være en uvedkommende ekstern adgang, men det kan også være en uvedkommende intern adgang for medarbejdere, der ikke har behov for adgang. I den forbindelse bemærkes det endvidere, at alene de medarbejdere i den dataansvarliges eller databehandlers organisation, der har behov for adgang til oplysningerne, skal have adgang til oplysningerne. Adgangen skal derfor være begrænset hertil.

Endeligt skal det bemærkes, at et sikkerhedsbrud ikke *nødvendigvis* medfører, at databeskyttelsesforordningens regler er tilsidesat, hvis det i øvrigt vurderes, at den pågældende virksomhed eller myndighed har opretholdt et passende sikkerhedsniveau.

## 3.2. Risikovurdering/risikobaseret tilgang

Efter databeskyttelsesforordningen har fået virkning, er sikkerhedsbekendtgørelsen[3], som foreskriv hvilke sikkerhedsregler offentlige myndigheder skulle iagttage, ophævet. Bekendtgørelsen var udstedt i medfør af persondataloven.

At sikkerhedsbekendtgørelsen er ophævet betyder, at du som dataansvarlig myndighed ikke længere er bundet af udmøntningen af sikkerhedskravene heri. Forordningen foreskriver samtidig ikke, hvilke præcise foranstaltninger der skal træffes for at imødegå forordningens krav. Du er

[3] Bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning, som ændret ved bekendtgørelse nr. 201 af 22. marts 2001.

således blevet sat mere "fri", i forhold til hvordan du ønsker at løse opgaven med at skabe et tilstrækkeligt sikkerhedsniveau ud fra en vurdering af de risici, behandlingen udgør, bl.a. når der skal udvikles nye systemer. Hvis en eller flere af de foranstaltninger, der var en del af sikkerhedsbekendtgørelsen – efter en konkret vurdering – fortsat er relevante, vil det være oplagt at fortsætte med at gøre brug af dem. Det kunne f.eks. være kravene om autorisation, kontrol med afviste adgangsforsøg eller logning.

Der er med forordningen i stedet kommet fokus på en risikobaseret tilgang[4]. Den risikobaserede tilgang til sikkerhed er i forvejen kendt fra eksempelvis informationssikkerhedsstandarderne ISO 27001 og ISO/IEC 29134: 2017, som beskrives nærmere straks nedenfor. Denne risikobaserede tænkning kendetegnes ved implementeringen af processer, der tager højde for løbende identifikation af både risici og muligheder samt den efterfølgende overvågning, måling, evaluering og analyse af disse. Er du en privat dataansvarlig, foretog du sikkert allerede inden den 25. maj 2018 risikobaserede overvejelser for at fastlægge det rette sikkerhedsniveau. Det gjorde du ganske givet også, hvis du er en offentlig myndighed, selvom du var bundet af udmøntningen af sikkerhedsbekendtgørelsen, da der ikke deri var tale om en udtømmende regulering af, hvilke sikkerhedsforanstaltninger du skulle implementere i din organisation.

Det er ikke desto mindre alligevel vigtigt, at du er opmærksom på, at de risikovurderinger, du hidtil har foretaget, ikke nødvendigvis er dækkende i forhold til forordningens risikobaserede tilgang, idet risici kan handle om mange ting. Forordningen har f.eks. *ikke* fokus på risici for organisationens aktiver/værdier, men derimod udelukkende fokus på risici for fysiske personers rettigheder og frihedsrettigheder. Dette indebærer, at andre (eller flere) konsekvenser og sandsynligheder kan komme i spil, når risici vurderes i henhold til forordningen.

Udgangspunktet er således, at behandling af personoplysninger, er forbundet med risici for fysiske personer. Princippet er herefter, at der under selve udformningen og under iværksættelsen af en behandling skal etableres et sikkerhedsniveau, som passer til disse risici ved hjælp af passende tekniske og organisatoriske foranstaltninger, som du gennemfører. De foranstaltninger, som du etablerer, skal således søges målrettet mod de afdækkede risici.

De konsekvenser, der kan være for de registrerede, og som følgelig skal indgå i din risikovurdering er især (men ikke udelukkende):

- Fysisk skade
- Materiel skade
- Immateriel skade
- Forskelsbehandling
- Identitetstyveri
- Identitetssvig

[4] Risikoorientering er i det hele taget en del af forordningen.

- Økonomiske konsekvenser, herunder finansielle tab
- Skade på omdømme
- Sociale konsekvenser
- Indflydelse på privatliv
- Skade på menneskelig værdighed
- Skade på legitime interesser
- Begrænsning/krænkelse af fundamentale rettigheder og frihedsrettigheder
- Forhindring i udøvelse af kontrol med egne personoplysninger

### 3.2.1. ISO/IEC 27001: 2013

Som eksempel på en risikobaseret tilgang, der allerede kendes i dag, kan nævnes informationssikkerhedsstandarden ISO 27001, der er en international standard til styring af informationssikkerhed. Denne standard er valgt som statslig sikkerhedsstandard, hvorfor alle statslige myndigheder skal efterleve den, hvilket har været obligatorisk siden januar 2014, mens alle andre offentlige myndigheder skal efterleve principperne i den.

ISO 27001 er en normativ standard, hvilket vil sige, at den opstiller en række krav i forhold til forskellige aspekter af implementering af et ledelsessystem for informationssikkerhed. I ISO27000-serien indgår endvidere en række ikke-normative standarder med retningslinjer for, hvordan en organisation kan implementere og overholde de normative standarder[5].

ISO27001 standarden tager udgangspunkt i den enkelte myndighed eller virksomhed og lægger op til, at der implementeres netop de foranstaltninger, der er passende for den enkelte myndighed eller virksomhed. Standarden indeholder endvidere en (ikke udtømmende) liste af mulige kontroller, der kan indføres for at opnå et passende sikkerhedsniveau. Derudover er det relevant at nævne, at standarden kan anvendes sammen med andre rammeværk for informationssikkerhed som f.eks. COBIT (Control Objective for Information and Related Technology) og ISF Standard of Good Practice for Information Security.

Standarden kan således anvendes som et hjælpemiddel i din organisation i forbindelse med dit arbejde med at opfylde kravene i forordningens artikel 32 til behandlingssikkerhed.

[5] For mere information om denne samt yderligere ISO'er i ISO27000-serien, henvises til Digitaliseringsstyrelsens hjemmeside: www.digst.dk

### 3.2.2. ISO/IEC 29134: 2017

Et andet eksempel på en risikobaseret tilgang vi også allerede kender i dag, er informationssikkerhedsstandarden ISO 29134, der er en international standard til udarbejdelse af konsekvensanalyser vedrørende databeskyttelse (*Impact Assesment – DPIA*). Som det også er anført i Justitsministeriets betænkning nr. 1565 vedrørende databeskyttelsesforordningen (side 487), må det antages, at de europæiske tilsynsmyndigheder og Databeskyttelsesrådet vil tage standarden i betragtning i forbindelse med overvejelser omkring forordningens bestemmelser om behandlingssikkerhed og beskyttelse af fysiske personers rettigheder og frihedsrettigheder[6].

Standarden beskriver processen i en række trin, hvoraf et trin f.eks. vedrører identifikation af risici, mens et senere trin f.eks. vedrører beslutning om foranstaltninger. Standarden sætter bl.a. fokus på, at behandlingssikkerhed bliver iagttaget og indarbejdet i f.eks. design og implementeringen af it-løsninger.

### 3.2.3. Supplerende eksempel

Følgende eksempel belyser, hvilke overvejelser en kortlægning af risiko vil kunne give anledning til[7].

Det bemærkes, at ENISA allerede i 2016 udgav en engelsksproget relativt tilgængelig metodik til risikovurdering[8]. Denne giver en enkel tilgang for mikro-, små- og mellemstore virksomheder til at foretage og vurdere risikoen for den registreredes rettigheder.

På baggrund af den model kan man inddele graden af påvirkningen for de fysiske personer sådan:

| Påvirkningsgrad | Beskrivelse |
|---|---|
| Lav | De fysiske personer kan opleve få uhensigtsmæssigheder, der kan overkommes og imødegås uden større indsats (tid brugt på at genindtaste oplysninger, dårlig brugeroplevelse, irritation og lignende). |
| Medium | De fysiske personer kan opleve betydelige uhensigtsmæssigheder, som de kan overkomme med en indsats og overvindelse af nogle få besværligheder (ekstra omkostninger, manglende adgang til forretningsservices, frygt, mangel på forståelse, stress og mindre påvirkning af fysisk karakter og lignende). |
| Høj | De fysiske personer kan opleve betydelige konsekvenser, som kun kan overkommes med betydelig indsats og konsekvenser for den enkelte (Økonomiske konsekvenser, fejlkontering af midler, sortlistning eller nedgradering I kreditmuligheder, fysik skade på aktiver, påvirkning af arbejdssituation, stævning, dårligere helbred og lignende). |
| Meget høj | De fysiske personer kan opleve betydelige og indgribende konsekvenser, som det ikke er muligt eller kun vanskeligt muligt at overkomme. (Mistet erhvervsevne, langvarige fysiske og psykiske påvirkninger, død, og lignende.). |

[6] Se i den forbindelse Artikel 29-gruppens retningslinjer for konsekvensanalyse vedrørende databeskyttelse (DPIA) og bestemmelse af, om behandlingen "sandsynligvis indebærer en høj risiko" i henhold til forordning (EU) 2016/679 (WP 248 rev. 01).

[7] Eksemplerne stammer fra ENISAs publikation "Handbook on security of personal data processing" udgivet i december 2017.

[8] https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing

Eksemplet:
Virksomheden (V) driver en e-handelsplatform, hvor de sælger deres varer. Kunderne kan på platformen bladre mellem de tilbudte varer, lægge dem i den virtuelle indkøbsvogn, bestille og betale for disse.
For at kunne indgå ordren skal kunden indtaste kontaktoplysninger på e-handels platformen (for- og efternavn, modtageradresse, telefonnummer og e-mail adresse). Under selve bestillingsproceduren vil de nu registrerede kunder skulle indtaste deres betalingsoplysninger i en separat formular, der stilles til rådighed af en betalingsformidler. Såfremt bestilling og betaling går igennem, overføres ordren og betalingsoplysningerne til V's centrale ressourcestyrings system (ERP) og til kunderelations systemet (CRM) herudover involveres den serviceleverandør, der forstår transporten af varerne til kunden. Der benyttes et standardiseret e-handels-koncept, der er underkastet den for dette produkt definerede brugerpolitik og implementeret på den af systemleverandøren anbefalede måde.

| **Beskrivelse af behandlinger** | **E-handel: bestilling, betaling og leverering af varer** | |
|---|---|---|
| Hvilke persondata Behandles | **kontaktoplysninger på e-handels platformen (For- og efternavn, modtageradresse, telefonnummer og e-mail adresse) Betalingsdata (Kreditkort /bank information)** | |
| Behandlingens formål | **Bestilling, betaling og transport af varer** | |
| Datasubjekter | **kunder** | |
| Behandlingssystemer | **Ordre Styringssystem, (ERP, CRM og PORTAL)** | |
| Modtagere af data | **Eksternt** | **Betalingsservice leverandør** |
| | **Eksternt** | **Transportservice leverandør** |
| | **Internt** | **Kunderelations (CRM) system** |
| | **Internt** | **Centralt ressourcestyrings (ERP) system** |
| Dataansvarlige og databehandlere | **V , Betalingsformidler og Transportformidler** | |

I de behandlinger, der sker, vurderer V, at uautoriseret offentliggørelse og/eller ændring af de persondata, der behandles (inklusive de økonomiske transaktionsdata) vil kunne resultere i, at kunden kan opleve betydelige uhensigtsmæssigheder, som de kan overkomme med en indsats og overvindelse af nogle få besværligheder, såsom kontakt til banken eller returnering af en fejlagtigt modtaget vare. Risikoen for de registrerede vedrørende tab af konfidentialitet og integritet vurderes derfor af V som MEDIUM.

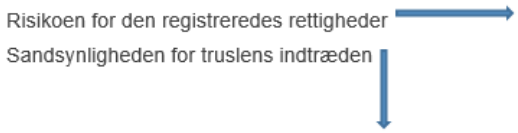
Tilgængeligheden på portalen og de bagvedliggende systemer vil alene påvirke de registrerede, så der opleves få uhensigtsmæssigheder, der kan overkommes og imødegås uden større indsats, f.eks. i form af genindtastning af oplysningerne eller genbesøg af siden på et andet tidspunkt. Risikoen for den registrerede for tilgængelighed vurderes derfor af V som LAV.

Sandsynligheden for trusler:
Virksomheden vurderer, at da systemet tilgås og baseres på brug over et netværk, som de ikke har kontrol over (internettet), at det er eksponeret for en vis mængde trusler, der kan ramme infrastrukturen, særligt i form af utilgængelighed. DDoS-angreb og lignende er relativt lette at iscenesætte, hvorfor der er en reel og potentiel sandsynlighed herfor. Da virksomheden imidlertid ikke er særligt eksponeret og i øvrigt har et setup med deres teleleverandør, der spærrer for IP-adresser, der gentagne gange rammer portalen, sætter de sandsynligheden til MEDIUM.

De korrigerende foranstaltninger omfatter bl.a. krav om, at programkoden til portalen skal testes, inden ændringer sættes i drift. Testen skal omfatte de ti mest gængse fejl i webprogrammering

fra OWASP 2017[9]. Desuden skal leverandøren sikre, at webserveren altid er opdateret og producere dokumentation for dette hver måned. Disse foranstaltninger bringer sandsynligheden for hacking af portalen ned på LAV.

På baggrund heraf har ENISA i "Handbook on security of personal data processing" udgivet i december 2017, Annex A, oplistet mulighederne for, hvilke sikkerhedsforanstaltninger der kan tages i brug til de forskellige udfald i skemaet nedenfor.




| | Lav | Medium | Høj / meget høj |
|---|---|---|---|
| Lav | | | |
| Medium | | X | |
| Høj | | | |

## 3.3. Passende tekniske og organisatoriske foranstaltninger

Forordningen stiller krav om, at du skal gennemføre passende *tekniske* og *organisatoriske* foranstaltninger for at sikre et sikkerhedsniveau, der passer til de konstaterede risici.

Forordningen fortæller dig ikke, hvilke præcise foranstaltninger, du skal træffe. Valget ligger i første række hos dig. Du er ansvarlig for, og du skal kunne påvise og dokumentere, at personoplysninger i din organisation behandles på en måde, der sikrer tilstrækkelig sikkerhed for de personoplysninger, du behandler. For at kunne gøre dette, er du nødt til at få de risici, der er forbundet med din behandling af personoplysninger frem i lyset. Det gør du ved hjælp af en risikoanalyse, hvor du også tager aktivt stilling til de risici, du har identificeret. Herefter gennemfører du de foranstaltninger, der er nødvendige for, at dit sikkerhedsniveau er tilstrækkeligt. Det er i den forbindelse et krav i fortegnelsen[10], at beskrive de tekniske og organisatoriske sikkerhedsforanstaltninger omhandlet i artikel 32, stk. 1.

Dette afsnit, samt følgende afsnit (afsnit 4) i vejledningen, sætter fokus på, hvordan du som dataansvarlig eller databehandler, skal gribe opgaven an med at finde passende tekniske og organisatoriske foranstaltninger og overholde kravene til behandlingssikkerhed.

Forordningen angiver i artikel 32, stk. 1, litra a-d, en række ikke-udtømmende eksempler på foranstaltninger, som det kan være relevant at indføre alt afhængigt af behandlingsaktiviteten og de

[9] https://www.owasp.org

[10] Du kan læse mere om fortegnelse i Datatilsynets og Justitsministeriets vejledning herom.

afdækkede risici ved behandlingen, og som derfor vil blive gennemgået i det følgende. I forlængelse heraf kan der også henvises til den internationale standard ISO IEC 29151: 2017 om persondatakontroller, som i høj grad supplerer ISO IEC 27001: 2013 i forhold til foranstaltninger/kontroller til beskyttelse af personoplysninger.

Nedefor finder du eksempler på de foranstaltninger, der kan tænkes anvendt. Du skal huske på, at foranstaltningerne skal/kan benyttes alt efter, hvad der er relevant.

| **Tekniske foranstaltninger** | **Organisatoriske foranstaltninger** |
|---|---|
| - *Antivirus herunder nye typer antivirus, der også kan detektere nye vira*<br>- *Firewall*<br>- *Antispam og -phishing filtre*<br>- *IDPS (system overvågning og alarmering ved ens perimetersikring)*<br>- *Endpointsecurity*<br>- *Kryptering*<br>- *Logging*<br>- *Pseudonymisering / anonymisering*<br>- *Sårbarhedsskanning og penetrationstests*<br>- *Løbende opdatering af software, herunder vedligeholdelse af systemer ved patching*<br>- *IAM systemunderstøttelse*<br>- *Adgangskontrol baseret på multifaktor autentifikation*<br>- *Klassifikation af data f.eks. almindelige, fortrolige, hemmelige og tophemmelige*<br>- *Netværkssegmentering og isolering*<br>- *Mobile device management, system der kan sikre og gennemtvinge sikkerhedspolitikker på mobile enheder* | - *IT-sikkerhedspolitik*<br>- *ISMS (information security management system)*<br>- *Fortegnelse over informationsaktiviteter*<br>- *Risikovurdering*<br>- *Træning af medarbejdere og løbende awareness*<br>- *Løbende identifikation af regler og praksis*<br>- *Identity and access governance* |

### 3.3.1. *Pseudonymisering og kryptering (eksempel 1)*

Det første eksempel på en foranstaltning, som forordningen nævner som relevant at gøre brug af (ofte i sammenhæng med yderligere relevante foranstaltninger) i forhold til sikkerhed i behandlingsmæssige sammenhænge, er *pseudonymisering og kryptering* af personoplysninger.

Ved pseudonymiserede oplysninger forstås, at du behandler personoplysningerne på en sådan måde, at de ikke længere kan henføres til en bestemt (identificerbar) fysisk person uden at gøre brug af supplerende oplysninger. Det er i denne sammenhæng en forudsætning, at de supplerende oplysninger opbevares separat. Det er endvidere en forudsætning, at de supplerende, se-

parat opbevarede oplysninger selvstændigt er underlagt tekniske og organisatoriske foranstaltninger for at sikre, at de pseudonymiserede oplysninger ikke umiddelbart (stående alene) kan henføres til en identificeret eller identificerbar fysisk person. Men kan f.eks. erstatte et personnummer med en "kode", som kan genfindes på en separat liste, hvor man kan se koblingen mellem personnummeret og koden. Det må dog ikke være muligt for uvedkommende at genskabe sammenhængen mellem person og kode.

Pseudonymiserede oplysninger kan give en bedre beskyttelse af den enkelte registrerede, da det ikke umiddelbart er muligt at genkende vedkommende, og dermed kan pseudonymisering gøre det lettere for dig at opfylde din databeskyttelsesforpligtelse efter forordningen.

Kryptering skal f.eks. forstås således, at udvalgte (person)oplysninger (evt. enkelte identificerende parametre) ved hjælp af en hemmelig krypteringsnøgle gøres ulæselige.

For at tilgå de krypterede oplysninger i et læseligt format skal du være i besiddelse af den korrekte krypteringsnøgle. Hvis du benytter en tilstrækkelig "stærk" kryptering og implementerer krypteringsforanstaltninger behørigt, kan det mindske risikoen for manglende fortrolighed, integritet, uafviselighed og autentifikation.

Det vil fortsat væres sådan, at du ikke må sende følsomme (og fortrolige) personoplysninger ukrypteret over netværk, som den dataansvarlige ikke har fuld kontrol over, f.eks. ukrypterede e-mail på internettet. I disse situationer skal du således anvende en sikker løsning, herunder f.eks. Digital Post eller bruge en forbindelse, der krypterer det overførte indhold under hele transporten.

### 3.3.2. *Sikring af vedvarende fortrolighed, integritet, tilgængelighed og robusthed (eksempel 2)*

Det andet eksempel på en foranstaltning, som forordningen nævner direkte, er *evnen til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester*.

Med "integritet" menes oplysningernes ægthed, hvilket bl.a. vil sige muligheden for at validere, om data på dine systemer er korrekte, pålidelige, nøjagtige og/eller fuldstændige. Der tænkes ikke på sandhedsværdien som sådan af de data, du behandler – f.eks. gemmer på din back-up. Teknisk set handler integritet om, at de data, du har gemt i systemet, forbliver uændret, sådan som de er gemt, medmindre du har til hensigt at ændre dem. Som eksempler på sikkerhedsforanstaltninger i forhold til integritet kan nævnes elektronisk signatur, individuelle fortrolige adgangskoder og VPN-forbindelser.

Med "tilgængelighed" menes bl.a. hvorvidt behandlingssystemer og –tjenester og den data, der ligger i disse, er tilgængelige ved anmodning fra en autoriseret bruger. Det kan også være reetableringen ved f.eks. hændelig eller ulovlig tilintetgørelse af oplysninger. Det kan eksempelvis opfyldes ved at sikre en velfungerende backup eller dublerede systemer, hvis det er relevant. Det er normalt en forudsætning, at der (samtidig) er fastsat organisatoriske processer for, hvordan disse opgaver udføres, og hvordan f.eks. backup testes.

Med ”robusthed” menes bl.a. evnen til at sikre den tekniske og organisatoriske modstandsdygtighed i dine behandlingssystemer og –tjenester. Det kan f.eks. gøres ved at sikre dem imod skadelige hændelser, herunder udfald ved dublerede diske, køling, nødstrømsanlæg, automatisk brandslukning m.v.

Med ”vedvarende” menes, at evnen til at sikre den nævnte fortrolighed, integritet, tilgængelighed og robusthed er en løbende teknisk og organisatorisk forpligtelse.

Der kan igen henvises til den internationale standard ISO 29151: 2017 om persondatakontroller, som i høj grad supplerer ISO IEC 27001: 2013 i forhold til foranstaltninger/kontroller til beskyttelse af personoplysninger.

### 3.3.3. *Rettidig genopretning af tilgængeligheden af og adgangen til personoplysninger (eksempel 3)*

Som det tredje eksempel på en foranstaltning, som forordningen nævner, er *evnen til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*

Det ligger heri, at din organisation har et beredskab for, hvordan adgangen til personoplysninger genoprettes i tilfælde af fysiske eller tekniske hændelser.

Af fysiske hændelser kan eksempelvis nævnes brand eller overgravede datakommunikationskabler. Tekniske hændelser kan eksempelvis være hacking eller krypto-ransomware. Ved krypto-ransomware krypterer en angriber dine filer, med krav om betaling for at få dekrypteringsnøglen. Når en malware har inficeret én computer i din organisation, kan den spredes til andre på netværket, så det bliver svært/umuligt at arbejde på normal vis.

Det er derfor vigtigt, at din organisation har planlagt, hvordan it-driften i tilfælde af sådanne hændelser kan genoprettes inden for et nærmere bestemt tidsrum (og hvordan det bedst undgås, at du bliver ramt af f.eks. tekniske hændelser). Det kan f.eks. være, at der tages regelmæssige sikkerhedskopier, at du begrænser brugen og installationen af browser-plugins (udvidelses programmer der nok giver funktionalitet men også kan benyttes til afvikling af kode der kan kompromittere ens sikkerhed), eller at du kan etablere en overgang til alternative datakommunikationslinjer m.v.

Du kan ved øvelser og tests demonstrere din evne til rettidig genoprettelse.

### 3.3.4. *Procedureregler (eksempel 4)*

Som det fjerde og sidste eksempel på en mulig relevant foranstaltning nævner forordningen *en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.*

Her sigtes der til, at du med jævne mellemrum tester/afprøver, vurderer og evaluerer – afhængigt af, om det er relevant – firewalls, krypterede forbindelser, krypterede lagringer, foranstaltninger

imod forsøg på overbelastelses- eller ”denial of service” angreb, foranstaltninger imod forsøg på at gætte adgangsgivende faktorer, adgangskontrol, brugeradministrationsprocesser og meget andet.

Til eksempel kan du finde inspiration til en model for processer for arbejdet med it-sikkerhed i ISO IEC 27001:2013, anneks A, og for en gennemgang i katalogform over hvilke mulige sikkerheds-foranstaltninger, der kan benyttes, beskriver ISO IEC 29151: 2017 flere af disse.

### 3.3.5. *Organisatoriske foranstaltninger (eksempel 5)*

Organisatoriske foranstaltninger kan – sammen med tekniske foranstaltninger – også være en del af din løsning for at leve op til artikel 32. Ifølge forordningen skal du foretage en afvejning, når du skal vurdere, hvilke passende sikkerhedsforanstaltninger, du skal indføre, idet du bl.a. skal tage hensyn til det aktuelle tekniske niveau og implementeringsomkostninger, jf. ordlyden i artikel 32, stk. 1.

**Eksempler på organisatoriske foranstaltninger du kan foretage:**
*Du skal – forudsat at du efter en konkret vurdering finder det nødvendigt for at opnå et passende sikkerhedsniveau – etablere organisatoriske løsninger, såsom undervisning af ansatte, løbende besvarelse af datarelaterede sikkerhedsspørgsmål f.eks. for så vidt angår medarbejdere, der i stor grad foretager behandling af personoplysninger, eller øvrige lignende interne it-sikkerhedsprocedure.*

*Viser det sig, at de implementeringsomkostninger, der er forbundet med, at du f.eks. skal bringe et ældre system – der ikke på alle områder helt modsvarer det aktuelle tekniske niveau – op på et passende sikkerhedsniveau, er uforholdsmæssigt store, kan du også imødekomme behovet for større sikkerhed ved hjælp af organisatoriske foranstaltninger. Der er således ingen forpligtelse til at efterkomme sikkerhedskravene alene rent teknisk, hvis der efter en konkret vurdering fra den dataansvarlige findes tilstrækkelige organisatoriske løsninger, der også kan bidrage til at sikre det aktuelle tekniske niveau. Du kan f.eks. søge at begrænse antallet af medarbejdere, som har adgang til følsomme personoplysninger. Kan der således etableres et passende sikkerhedsniveau for allerede ibrugtagne ældre systemer også gennem interne procedurer, undervisning af ansatte eller tilsvarende organisatoriske foranstaltninger, vil dette i princippet kunne være tilstrækkeligt.*

Lovforslaget til databeskyttelsesloven indeholder en ”værktøjskasse” med en række konkrete eksempler på sikkerhedsforanstaltninger, som du kan bruge for at sikre overholdelse af loven og forordningen samt finde eksempler til, hvor du kan søge inspiration[11].

Som en del af den dataansvarliges ”værktøjskasse”, nævnes i lovforslaget følgende eksempler på foranstaltninger (hvoraf enkelte er direkte inspireret af forordningens ordlyd, jf. ovennævnte):

[11] Se lovforslag L 68 punkt 2.3.3.3 i de almindelige bemærkninger.

- Tekniske og organisatoriske foranstaltninger til sikring af, at behandlingen er i overensstemmelse med forordningen. Se til inspiration afsnit 3.2 ovenfor.

- Foranstaltninger til sikring af, at det er muligt efterfølgende at undersøge og fastslå om og af hvem, der er behandlet personoplysninger (logning).

- Frivillig udpegning af databeskyttelsesrådgiver, jf. databeskyttelsesforordningens artikel 37, stk. 4[12].

- Fastsættelse af interne regler om organisatoriske forhold og fysisk sikring, herunder sikkerhedsorganisation, administration af adgangskontrolordninger og autorisationsordninger samt kontrol med autorisationer.

- Foranstaltninger til sikring af, at alene personer, som den dataansvarlige autoriserer hertil, fordi det er nødvendigt, kan få adgang til personoplysninger.

- Fastsættelse af retningslinjer for den dataansvarliges tilsyn med overholdelsen af de gennemførte sikkerhedsforanstaltninger, herunder løbende opfølgning og revision.

- Fornøden instruktion fra den dataansvarliges side til de medarbejdere, som behandler personoplysningerne.

- Foranstaltninger – på steder, hvor der foretages behandling af personoplysninger – med henblik på at forhindre uvedkommendes adgang til oplysningerne.

- Pseudonymisering af personoplysninger.

- Kryptering af personoplysninger.

- Sikring af vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester i forbindelse med behandling af personoplysninger.

- Sikring af sikkerheden i behandlingen, etablering af mekanismer for regelmæssig revision, vurdering og evaluering af effektiviteten af tekniske og organisatoriske foranstaltninger.

- Registrering af afviste adgangsforsøg og tekniske foranstaltninger, der kan sikre blokering for yderligere forsøg, hvis det er nødvendigt.

Det kan i øvrigt bemærkes, at Registerudvalget i sin betænkning nr. 1345, som blev afgivet i 1997, fandt, at sikkerhedsforanstaltninger grundlæggende bør indeholde følgende elementer: Fysisk sikkerhed, organisatoriske forhold, systemtekniske forhold, samt uddannelse og instruktion. I den forbindelse er det værd at nævne, at hver enkelt medarbejder i din organisation er/kan være en potentiel risiko i forhold til overholdelse af forordningen og udløsning af eventuelle sanktioner. Det

[12] For mere information om databeskyttelsesrådgivere henvises til vejledning om Databeskyttelsesrådgivere, der er tilgængelig på Datatilsynets hjemmeside: www.datatilsynet.dk

er derfor vigtigt, at alle medarbejdere forstår, hvordan de skal behandle oplysningerne lovligt, og at de har et ansvar over for deres arbejdsgiver på dette område.

Udvalget peger i betænkningen endvidere navnlig på følgende foranstaltninger, der – alt efter omstændighederne – kan komme på tale: Sikring af bygninger og lokaler, formel autorisation af brugerne, adgangskoder (password), benyttelsesstatistik, logning af transaktioner, registrering af uautoriserede adgangsforsøg, kryptering, regler for udskrifter, regler for destruktion, uddannelse samt tilsyn.

# 4. Praktisk ”hjælpe-guide” til din overholdelse af kravene til behandlingssikkerhed

## 4.1 Vejledende trin

Som en hjælp til, hvordan du som dataansvarlig skal gennemføre foranstaltninger, der sikrer et passende sikkerhedsniveau, er der udarbejdet nedenstående vejledende trin, som kan hjælpe dig med, hvordan du skal gribe opgaven an.[13]

Det er i den forbindelse værd at bemærke, at du som dataansvarlig selv bestemmer den nærmere fremgangsmåde og systematik, og at nedenstående blot er et forslag til, hvordan opgaven kan gribes an.

Overvejelser om behandlingssikkerhed og foranstaltninger er endvidere noget, som du skal gøre med regelmæssige mellemrum for at kunne imødegå ændringer i risikobilledet som følge af bl.a. tekniske og organisatoriske forandringer hos dig (både om dataansvarlig og evt. databehandler) samt ændrede trusler fra omverdenen og internt i din organisation.

### 4.1.1 *Trin 1: Identifikation og vurdering af risici*

Som første trin er det en fordel, at du har et kendskab til, hvordan personoplysningerne i din organisation behandles, hvilke midler der aktuelt anvendes ved den behandling, der foretages, samt hvilken konkret kontekst behandlingen foregår i.

Du skal med andre ord vide, hvilke personoplysninger du har, hvor de befinder sig, hvordan du behandler dem, og hvordan de udveksles mellem dine systemer.

Herunder kan det f.eks. være relevant at undersøge/klarlægge følgende:

- Hvilke systemer bruges i din organisation
- Hvem er ansvarlig for systemerne (er du selv det, eller er der f.eks. en leverandør?)
- Hvordan fungerer systemet (formål og funktionalitet)
- Trækkes personoplysningerne fra andre systemer og i så fald hvilke?

[13] Se ligeledes betænkning nr. 1565 om databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning, s. 486-490.

Når du har taget stilling til ovenstående, kan du bruge dette som udgangspunkt til at søge at identificere, hvilke risici din behandling udgør for de registrerede.

Det kan i den forbindelse være, at der skal foretages en mere detaljeret kortlægning af risiciene, idet der skal foretages en konsekvensanalyse[14], hvis der sandsynligvis er *høj* risiko for fysiske personers rettigheder og frihedsrettigheder.

Når du skal udfolde risikobilledet, kan der f.eks. søges hjælp og vejledning i anneks B i standard ISO/IEC DIS 29134 *Information technology – Security techniques – Privacy impact assesment – Guidelines*. Heri findes mange eksempler på mulige risici og trusler, som det kan være relevant at overveje og tage stilling til[15].

**Eksempler på risici:**

*Ved en helt almindelige datatransmission (transmission af oplysninger fra én aktør til en anden) kan der være risiko for, at uvedkommende får kendskab til de personoplysninger, der transmitteres. Det kan f.eks. ske ved aflytning af datatransmissionen, hvorved en ondsindet person "opsnapper" data enten hos afsender eller modtager, eller via netværket mellem de to parter.*

*I forhold til Cloud Computing kan der være risiko for tab af kontrol med data, idet der ved benyttelse af Cloud løsninger overlades kontrol til Cloud-udbyderen på en række områder, som kan have betydning for sikkerheden, f.eks. at oplysninger tilgås af uvedkommende, når de opbevares i "skyen" eller at der forekommer fysiske eller tekniske hændelser, der gør at man ikke selv kan tilgå oplysningerne. Det er derfor væsentligt, at du i databehandleraftalen får fastlagt netop det niveau af kontrol og mulighed for auditering, der er nødvendigt for din behandling.*

Ønsker du yderligere vejledning i udredning af risici, kan i øvrigt henvises til Artikel 29-gruppen, der har udgivet en række udtalelser[16], som bl.a. adresserer risici i forbindelse med nyere teknologier som f.eks. Cloud Computing, Internet of Things, biometri f.eks. ansigtsgenkendelse og geolokalisering i forbindelse med smarte mobile enheder.

### *4.1.2 Trin 2: Identifikation af mulige foranstaltninger*

Når du har udredt alle de aktuelle risici, skal du vurdere disse med henblik på, hvilke foranstaltninger der kan være relevante at træffe for at imødegå netop disse risici for at opnå et passende sikkerhedsniveau.

Hvilke foranstaltninger der vil være mest hensigtsmæssige, afhænger af de konkrete aktuelle omstændigheder og situationen ved den aktuelle behandling, ligesom det afhænger af de identificerede risici.

---

[14] Se vejledning om konsekvensanalyse, der er tilgængelig på Datatilsynets hjemmeside: www.datatilsynet.dk.

[15] Herudover har Artikel 29 gruppen udgivet en vejledning om konsekvensanalyse og indholdet af en sådan analyse

[16] Se bl.a. WP250: https://webshop.ds.dk/da-dk/standard/ds-iso-iec-291512017 om retningslinjer for anmeldelse af brud på persondatasikkerheden, som indeholder eksempler på brud på persondatasikkerheden samt artikel 29 gruppens vejledning om konsekvensanalyser vedrørende databeskyttelse (DPIA), wp248, der er tilgængelig på Datatilsynets hjemmeside: www.datatilsynet.dk.

Når du skal identificere, hvilke foranstaltninger du skal gennemføre for at imødegå de identificerede risici, kan det være en hjælp at søge vejledning i f.eks. ISO29151[17] eller ISO 27001-standardens anneks A, som indeholder en omfattende liste af kontroller. Disse kontrolmål og kontroller modsvarer foranstaltninger, der kan træffes.[18]

### *4.1.3 Trin 3: Gennemgang af, hvilke kortlagte foranstaltninger der imødegår relevante risici, så et passende sikkerhedsniveau opnås*

I praksis imødegås en identificeret risiko ved en kombination af flere foranstaltninger, som komplementerer hinanden og tilsammen reducerer de(n) identificerede risici/risiko.

Ud over risikoen er det relevant at have følgende overvejelser med, når der skal træffes de rette foranstaltninger:

- hvordan behandlingen af personoplysninger aktuelt foregår (f.eks. hvem der behandler dem, og hvilken behandling der foretages),
- hvilke midler, der aktuelt anvendes ved behandlingen,
- den konkrete kontekst, som behandlingen foretages i.

Det kan være hensigtsmæssigt at have øje for enkle/simple grundprincipper ved udvælgelse af kortlagte foranstaltninger, såsom isolation og adskillelse af dine data samt forsvar i dybden[19] (mere end f.eks. "blot" at have adgangskode på dine it-systemer).

**Eksempler på relevante foranstaltninger:**

*Udspringer risikoen f.eks. af antallet af personer, der har adgang til en (stor) mængde (følsomme) oplysninger, kan du opdele adgangen efter hvad den enkelte mere specifikt har behov for, og/eller begrænse den enkeltes muligheder for behandling (læse, ændre, udtrække, samkøre, slette m.v.).*

*Du kan også foretage logning af behandling af personoplysninger (for at kunne finde ud af, hvem der gør hvad, og om der er uvedkommende på netværket), kombineret med kontrol af om en konkret tilgang til oplysningerne har været inden for reglerne for tilgang.*

[17] https://www.iso.org/standard/62726.html

[18] Til yderligere inspiration kan der endvidere igen peges på publicerede udtalelser fra Artikel-29 gruppen og Datatilsynets IT-sikkerhedstekster. Endvidere kan publikationer fra Center for Cybersikkerhed og Digitaliseringsstyrelsen også anvendes til inspiration, herunder f.eks. *Cyberforsvar der virker*.

[19] Ved "forsvar i dybden" forstås etableringen af flere niveauer/lag af beskyttelsesbarrierer, så en fejl i en funktion således forhindres i at sprede sig til et andet systemniveau.

### *4.1.4 Trin 4: Implementering af de foranstaltninger, som det besluttes at gennemføre*

I dette trin træffer du (på baggrund af ovenstående) beslutning om, hvilke foranstaltninger, som skal gennemføres for at etablere et sikkerhedsniveau, der passer til risiciene for fysiske personers rettigheder og frihedsrettigheder.

Herefter skal du implementere foranstaltningerne i din organisation.

# DEL II

# 5. Databeskyttelse gennem design

## *5.1. Introduktion*

Grundtanken om, at et højt databeskyttelsesniveau bedst sikres ved at indlejre databeskyttelse på et tidligt stadie i systemudviklingen, blev oprindeligt udviklet i 90'ernes Canada af Ann Cavokian, der kortlagde begrebet ud fra følgende syv bærende principper:

**1. Proaktiv ikke reaktiv databeskyttelse**
Foranstaltninger skal forebygge risici fremfor blot at afhjælpe dem.

**2. Databeskyttelse som standardindstilling**
Den registrerede bør ikke selv skulle slå databeskyttelsesfremmende indstillinger til; beskyttelsen skal være indbygget fra starten.

**3. Databeskyttelse som en integreret del af design**
Databeskyttelse skal tænkes ind i systemers arkitektur fra starten.

**4. Fuld funktionalitet**
Både fuld funktionalitet og fuld sikkerhed skal sikres. Der bør ikke være et modsætningsforhold mellem databeskyttelse og sikkerhed.

**5. Databeskyttelse i hele livscyklussen**
Databeskyttelse skal sikres kontinuerligt, over hele domænet og i hele systemets levetid.

**6. Synlighed og gennemsigtighed**
Teknologier og forretningsmodeller bør være gennemsigtige, og de målsætninger, der er blevet signaleret, bør være verificerbare.

**7. Respekt for brugerens privatliv**
Den registreredes interesser skal sættes i fokus ved at opretholde høje privatlivs-standarder, tilvejebringe passende notifikation og tilbyde brugervenlige indstillinger.

Det er blandt andet i dette lys, at der nu i forordningens artikel 25 er indsat en bestemmelse om databeskyttelse gennem design og standardindstillinger.

## 5.2. Definition af databeskyttelse gennem design

Databeskyttelse gennem design indebærer ifølge forordningen, at *du som dataansvarlig* allerede fra tidspunktet, hvor midlerne (f.eks. et nyt it-system) for behandlingen fastlægges, skal gennemføre passende tekniske og organisatoriske foranstaltninger, som er designet med henblik på at sikre en effektiv implementering af *de grundlæggende databeskyttelsesprincipper*, der fremgår af databeskyttelsesforordningens artikel 5.

Kort sagt skal du på forhånd have designet og indrettet din it-mæssige og organisatoriske forretningsunderstøttelse af behandlinger sådan, at forordningens krav og beskyttelseshensyn varetages som en integreret del i hele behandlingsforløbet.

## 5.3. Rækkevidde

### 5.3.1. Betydning for eksisterende it-systemer

Forordningen kræver ikke, at ældre og allerede eksisterende systemer skal re-designes.

Kan der etableres et passende databeskyttelsesniveau, og kan den registreredes rettigheder opfyldes for allerede ibrugtagne ældre systemer, eventuelt gennem indførelsen af interne procedurer, undervisning af ansatte eller tilsvarende organisatoriske foranstaltninger, vil dette (i princippet) være tilstrækkeligt.

Hvis det konstateres, at it-systemet ikke opfylder kravene i andre af forordningens bestemmelser – såsom artikel 32 om behandlingssikkerhed eller principperne for behandling af personoplysning i artikel 5 – vil dette kræve, at systemet ændres, eller at yderligere organisatoriske foranstaltninger gennemføres efter den 25. maj 2018.

**Eksempel: Ikke re-design af eksisterende it-systemer, supplerende organisatoriske tiltag**

*En kommune løser en konkret forvaltningsopgave ved brug af en selvbetjeningsløsning på internettet. Idet der er tale om en kompleks opgave med underliggende økonomiske beregninger, foretages behandlingerne af de indsamlede oplysninger i flere af hinanden uafhængige it-systemer.*

*Oplysningerne om det tidsrum, oplysningerne opbevares i, fremgår ikke i den eksisterende fragmenterede it-understøttelse eller i den indsigt, der hidtil er givet efter persondatalovens § 31. Kommunen har derfor lavet en organisatorisk gennemgang af de it-tekniske sletteregler i de omfattede systemer og en procedure der tilsikrer, at de relevante oplysninger om slettereglerne gives til alle de registrerede, der efter den 25. maj 2018 udøver indsigtsret efter forordningens artikel 15, stk. 1, litra d.*

*Kommunen behøver derfor ikke af denne grund re-designe it-understøttelsen. Kommunen kunne også vælge at ændre teksten på internetformularen, så den inkluderede oplysningerne omkring, hvordan sletning sker, og derved opfylde oplysningspligten efter forordningens artikel 13 og 14.*

For dataansvarlige og databehandlere, der allerede inden den 25. maj 2018 har påbegyndt behandlinger omfattet af persondataloven, er der for den eksisterende portefølje, i reglerne om forpligtelsen til at skulle træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven,[20] allerede varetaget betydelige områder, som er sammenfaldende med de designfeatures, forordningen kræver.

a) Begrebets rækkevidde

Begrebet "databeskyttelse gennem design" er formuleret bredt. Det betyder, at du som dataansvarlig både forventes at tage højde for de tekniske indretninger (såsom it-systemer, infrastruktur og brugergrænseflader) og de forretningsgange, der præger din organisation. Der er med andre ord lagt op til, at du skal anlægge en helhedstænkning i forhold til organisationens samlede databehandlingsmiljø.

**Eksempel: En mulig måde at tilgodese helhedstænkning i et projektudviklingsforløb**
*Virksomheden (V) har besluttet, at indkøbe et nyt integreret CRM-system til oplysninger om V's kunder og disses engagement med V.*

*V foretager alle forretningsprocesændringer og indkøb af it-understøttelse som projekter i en projektmodel. V har i denne projektmodel allerede i præprojekt-fasen inkluderet en overvejelse om, hvilke behandlinger af personoplysninger, der vil skulle ske, og hvilke eksisterende behandlinger der vil blive berørt af ændringerne - både i de egentlige forretningsprocesser, men også i den organisatoriske og it-mæssige understøttelse. Resultaterne heraf er indlejret i det projektgrundlag, der udarbejdes, og der er lavet en ændringsprocedure, der håndterer om ændringerne indvirker på de behandlinger der er i scope.*

*Ved at inkludere de databehandlinger, der skal foretages som en naturlig del af forretningsudviklingen i en projektmodel, og ved at inkludere denne så tidligt som muligt, kan der skabes den helhedstænkning af opgaveløsningen som bestemmelsen lægger op til.*

[20] Lov om behandling af personoplysninger § 41, stk. 3

b) Tidsramme

Passende tekniske og organisatoriske foranstaltninger skal både gennemføres på tidspunktet, hvor der træffes beslutning om, hvordan behandlingen skal foretages (i forberedelsesfasen), på tidspunktet hvor den første behandling begynder og på tidspunktet for efterfølgende behandlinger.

**Eksempel**

*Det anførte eksempel ovenfor om V's anskaffelse af et CRM-system afspejler det faktum, at virksomheden inkluderer it-understøttelsen og den indbyggede sikkerhed på et tidligt stadie i projektforløbet, en mulig tilgang til løsningen af kravet om at indtænke beslutningen om sikkerheden allerede på tidspunktet for tilrettelæggelsen af hvordan behandlingen skal foretages.*

c) Gennemførelse af foranstaltninger

Princippet om databeskyttelse gennem design sigter ikke mod at etablere et nyt og selvstændigt sikkerhedskrav, forstået på den måde, at det alene er et krav om, at alle forordningens krav og garantier for den registreredes rettigheder overholdes, ved at der for behandlingen "fra fødsel til grav" er indbygget de organisatoriske og tekniske foranstaltninger, der er nødvendige til overholdelsen heraf.

Kravet om databeskyttelse gennem design indebærer, at du som dataansvarlig har en generel *overvejelses- og håndteringsforpligtelse*. Det betyder, at du allerede i forberedelsesfasen skal overveje, indtænke og håndtere indbygningen i løsningen af de foranstaltninger, der er relevante for at sikre, at databeskyttelsesforordningen overholdes.

Eksempler på foranstaltninger, der kan indbygges og udgøre databeskyttelse gennem design, kan være, men er ikke begrænset til:

- Minimeringen af persondatabehandlingen (artikel 5, stk. 1, litra c),
- Pseudonymisering af personoplysninger så hurtigt som muligt (artikel 4, nr. 5, jfr. artikel 5, stk. 1, litra e),
- Transparens hvad angår personoplysningernes funktion og behandling (artikel 5, stk. 1, litra a),
- Kryptering af data i transit eller hvile (artikel 5, stk.1, litra f jfr. artikel 32, stk. 1, litra b) og
- Sikring af infrastrukturen mod uautoriseret indtrængen (artikel 5, stk.1, litra f jfr. artikel 32, stk. 1, litra b)
- Effektive organisatoriske kontroller til autorisation og styring af adgangsrettigheder (artikel 5, stk.1, litra f jfr. artikel 32, stk. 1, litra b)
- Udladelse af visning af oplysninger i brugergrænseflader, når disse ikke er nødvendige for en given behandling (artikel 5, stk. 1, litra f

Der kan hentes inspiration til både mulige it-designprincipper og privatlivsfremmende foranstaltninger i ENISAs rapport fra 2014 om "*privacy and dataprotection by design*" eller i ISO 29151:2017 kodeks for beskyttelse af personhenførbar information, eller i designstrategier f.eks.

Hoepmann[21], der på dataniveau omhandler principper som ”skjul, minimer, separer og aggreger” og på det processuelle niveau; ”informer, kontroller, håndhæv og dokumentér”.

Hvilke foranstaltninger, der er nødvendige at gennemføre, vil dog afhænge af de konkrete omstændigheder. Momenter, der efter forordningens artikels 25’s ordlyd kan indgå i en sådan konkret afvejning, er:

- Det aktuelle tekniske niveau,
- Implementeringsomkostningerne,
- Behandlingens karakter og omfang,
- Sammenhæng og formål med behandlingen,
- Hvilke risici en behandling kan indebære for de registreredes rettigheder og frihedsrettigheder

**Eksempel: Aktuelt teknisk niveau**
*Det aktuelle tekniske niveau refererer til det, der er teknisk muligt på tidspunktet for vurderingen (men også teknisk muligt at gennemføre i praksis). Det vil sige, at den dataansvarlige ikke behøver overveje rent teoretiske, ikke endnu kommercielt tilbudte, tekniske løsninger. Løsninger, der er gængse, lettilgængelige - også i forholdet til implementering - skal overvejes og benyttes, hvis den samlede løsning tilsiger det (alene ud fra dette ene kriterium).*

Bestemmelsen er formuleret med udgangspunkt i en risikobaseret og helhedsorienteret tilgang til databeskyttelse. Det betyder dels, at den dataansvarlige overlades en stor grad af fleksibilitet for både vurderingen af, hvordan vægtningen foretages, men også for, hvordan behandlingen rent faktisk understøttes i at overholde hele forordningen. Dette vil kunne være et valgt miks mellem de mulige tekniske og organisatoriske foranstaltninger.

Den dataansvarlige er ikke underlagt en forpligtelse til at efterkomme kravene alene ved hjælp af rent tekniske foranstaltninger – også organisatoriske foranstaltninger vil kunne anvendes. Uanset hvilken samlet løsning du vælger at gøre brug af, it-systemunderstøttelse, organisatoriske foranstaltninger, fysisk eller netværksmæssig sikkerhed, forudsætter overholdelse af forordningen, at sådanne foranstaltninger efter en konkret vurdering anses for at være egnede til at sikre, at kravene til databeskyttelse gennem design[22] efterkommes. Der vil altså for en hver given behandling nok være en nedre grænse for ”hvor få” designfeatures, der er tilstrækkelige for, at reglen er overholdt.

For at tilgodese påvisningen af overholdelse af forordningen, jf. også princippet i artikel 24, stk. 1, fordres en dokumentation for alle de vurderinger som denne risiko-baserede tilgang er udtryk for. Den dataansvarlige kan med fordel føre en form for ”logbog”, der indeholder beskrivelserne

[21] Jaap-Henk Hoepmann Privacy Design Strategies 2012

[22] Artikel 25, stk. 1

og konklusionerne af de afvejninger, der er foretaget. Disse kan være en del af arbejdet efter ISO 27001, hvis dette rammeværk anvendes, men der er ikke noget formkrav til dokumentationen.

## 5.4. Formål med databeskyttelse gennem design

Bestemmelsens formål er at tænke databeskyttelse ind allerede i designfasen af it-systemet.

Ved at tilskynde dataansvarlige til at anlægge en helhedstænkning omkring deres tekniske platforme og forretningsgange banes vejen for, at databeskyttelse bliver en integreret del af organisationen. På den måde sikres en proaktiv tilgang til databeskyttelse, hvorved dataansvarlige på et tidligt tidspunkt kan identificere og løse potentielle problemer. Databeskyttelse gennem design udgør således et væsentligt redskab til at minimere databeskyttelsesrisici og opbygge tillid samt skabe en lovmæssig forpligtelse til at indlejre forholdsreglerne så tidligt, at disse lettere kan gennemføres, end hvis de først skulle indføjes efter systemets færdigudvikling.

## 5.5. Kravet om databeskyttelse gennem design set i forhold til andre krav i databeskyttelsesforordningen

Databeskyttelsesforordningens art. 25 stk. 1, om databeskyttelse gennem design skal læses i sammenhæng med de øvrige bestemmelser i databeskyttelsesforordningen. Dette er en naturlig følge af, at der i medfør af bestemmelsen skal iværksættes tiltag, der fremmer en effektiv implementering af forordningens regler og dennes databeskyttelsesretlige principper samt de forudsætninger, der er nødvendige for at beskytte den registreredes rettigheder i tilstrækkeligt omfang.

Det betyder for det *første*, at den dataansvarlige på et generelt plan er forpligtet til at *håndtere* og *overveje*, hvordan alle forordningens bestemmelser kan efterleves gennem konkrete tekniske og organisatoriske tiltag.

For det *andet* er den dataansvarlige forpligtet til at anvende foranstaltninger, der er designet med henblik på en effektiv implementering af databeskyttelsesprincipperne i artikel 5. Disse databeskyttelsesprincipper er nærmere bestemt; lovlighed, rimelighed og gennemsigtighed[23], formålsbegrænsning[24], dataminimering[25], korrekte og ajourførte[26], begrænsede opbevaringsperioder[27], foranstaltninger til at sikre datasikkerhed[28].

Alle disse princippers yderligere udfoldelse og detailregulering i andre bestemmelser skal også tilgodeses, f.eks. reglerne om hvad der er lovlig behandling efter artikel 6, samtykke efter artikel 7, behandling af særlige kategorier af personoplysninger efter artikel 9 (følsomme oplysninger) osv.

[23] Artikel 5, stk. 1, litra a.
[24] Artikel 5, stk. 1, litra b.
[25] Artikel 5, stk. 1, litra c.
[26] Artikel 5, stk. 1, litra d.
[27] Artikel 5, stk. 1, litra e.
[28] Artikel 5, stk. 1, litra f.

For det *tredje* indebærer henvisningen til de registreredes interesser, at hele forordningens kapitel III, om de registreredes rettigheder, vil skulle tages i betragtning og sikres gennem designet. Det betyder f.eks., at den registreredes ret til indsigt[29] skal sikres ved designet af systemunderstøttelse af behandlinger. For de behandlinger, der er omfattet heraf (gælder f.eks. ikke for behandling, der henhører under offentlig myndighedsudøvelse), skal muligheden for dataportabilitet[30] understøttes gennem designet, ligesom retten til begrænsning af behandling[31] skal tages i betragtning. Sådanne krav vil i visse tilfælde kunne sikres ved organisatoriske foranstaltninger. For eksempel vil en dataansvarlig, der kun sjældent modtager anmodninger om indsigt, ikke skulle indkøbe et nyt it-system alene for at håndtere sådanne anmodninger fra registrerede. Et sådant krav vil efter omstændighederne kunne løftes ved organisatoriske foranstaltninger, såsom indarbejdelsen af interne procedurer til håndtering af indsigtsforespørgsler.

For det *fjerde* skal den fornødne behandlingssikkerhed[32], som ligeledes er temaet for denne vejledning, også være indbygget i hele opsætningen og effektueringen af den konkrete behandling.

## *5.6. Databeskyttelse gennem design i praksis*

Det er væsentligt at se bestemmelsen som en betoning af vigtigheden i, at systemer til behandling af personoplysninger fra deres fødsel indeholder alle de features, der gør, at forordningens regler overholdes.

Herudover er der en kronologisk risikobaseret "sikkerhedsfortælling" i forordningen, nemlig at der allerede fra overvejelsen om at foretage en behandling bliver skabt en ramme, der gennem sit design sikrer forordningens overholdelse (artikel 25, stk. 1), at der ved sandsynligheden for en *høj* risiko for den registreredes rettigheder foretages en konsekvensanalyse (artikel 35), at der sker høring af tilsynsmyndigheden hvis den høje risiko ikke konkret kan imødegås (artikel 36), at der stedse er den fornødne behandlingssikkerhed (artikel 32), og at du som dataansvarlig sikrer og påviser dette (artikel 24, stk.1).

Alt dette kan umiddelbart forekomme relativt ukonkret eller uhåndterbart i den daglige opgavevaretagelse. Selv for dig, der arbejder med persondatabeskyttelse konkret, kan opgaven omkring, hvordan man forankrer forordningens beskyttelsesredskaber og garantier i en it-systemunderstøttelse forekomme lidt abstrakt.

Derfor kræver databeskyttelse gennem design en bred kompetencemæssig forankring i den enkelte dataansvarliges organisation, når nye systemer skal designes, udvikles, indkøbes og idriftsættes. Herudover kan det være godt at vide, at der eksisterer et samspil med genbrugelige komponenter som f.eks. afgrænset funktionalitet eller kode, mønstre som f.eks. the subscriber eller log-on pattern og udviklingsteknikker, der ligesom forordningens regler om certificering og adfærdskodeks på sigt kan skabe en sten at stå på - et afsæt der gør, at du får afprøvede og lettere

[29] Jf. artikel 15.
[30] Jf. artikel 20.
[31] Jf. artikel 18.
[32] Jf. artikel 32

veje til at benytte systemer, paradigmer, teknikker og hele værktøjskasser, der tilgodeser forordningens overholdelse.

### *5.6.1. Betydning for fremtidige it-systemers design*

Fremtidige IT-systemer, altså de der udvikles til ibrugtagning efter den 25. maj 2018, skal designes med henblik på effektiv implementering af databeskyttelsesprincipper – herunder dataminimering. Når du som dataansvarlig selv udvikler et system, vil dette bl.a. kunne sikres ved at indarbejde teknologier, der fremmer privatlivsbeskyttelse, såkaldte privatlivsfremmende teknologier (Privacy Enhancing Technologies PET's). Nogle af disse fremgår allerede af forordningens bestemmelse om databeskyttelse gennem design[33], nemlig dataminimering og pseudonymisering, men der er en mangfoldighed af forskellige PET´s til inspiration og genbrug, f.eks. har det Europæiske Agentur for Netværks- og Informationssikkerhed, ENISA (https://www.enisa.europa.eu/), udgivet både værktøjer til vurdering af front-end, platforme og systemer og i marts 2017 en gennemgang af et modus for anvendelsen af PET´s.

Mange såkaldte designmønstre (patterns) på området for it-sikkerhed og sikkerhedsarkitektur vil være PET´s.

**Eksempler på PET'S:**

- *Anonymisering og pesudonymisering af oplysninger*
- *Dataminimeringsforanstaltninger*
- *Adgangskontrol i form af access management*
- *Auditsporing*
- *Kryptering*
- *Projektmetoder der understøtter databeskyttelse*
- *Inputvalidering*
- *Sikkerhedsmønstre*
- *Kodemønstre*
- *Sikre netværks topografier*
- *Systemmæssig håndhævelse af databeskyttelse*

Hvis du indkøber et it-system eller en it-løsning, vil du kunne stille krav til leverandøren om, at systemets måde at realisere de forretningsmæssige mål designes i overensstemmelse med relevante bestemmelser i forordningen. Der vil også kunne ske en konkretisering i forhold til både funktionelle og non-funktionelle krav, der vedrører realiseringen af databeskyttelseshensyn, f.eks. anvendelse af kryptering og inputvalidering. Offentlige myndigheder og andre, der er omfattet af regler for udbud, vil skulle stille disse krav i udbudsfasen, hvor myndigheden, som led i arbejdet med kravsspecifikationen, vil skulle kunne relatere de forretningsmæssige krav til de behandlinger der foretages for i den relation at vurdere, hvilke krav om databeskyttelse disse afføder.

[33] Artikel 25, stk. 1.

Det er i den forbindelse væsentligt at fremhæve, at udbuddet og en kontraktlig pligt for en udviklingsleverandør til at levere et produkt, der lever op til databeskyttelsesforordningen, ikke fritager dig som dataansvarlig for de forpligtelser, du har efter forordningen.

### *5.6.2. Praktiske eksempler*

Det kan være nyttig med nogle praktiske eksempler. Inspiration kan hentes i Rådet for Digital sikkerheds vejledning om Databeskyttelse gennem Design eller artiklen herom i Revision og regnskabsvæsens nr. 12-2017, men også det norske Datatilsyn har udgivet en vejledning "Programvareutvikling med innebygd personvern[34].

**Eksempler på tekniske foranstaltninger:**

- *Krypteret, eventuelt signeret kommunikation*
- *CMS-systemer, der designes således, at der automatisk foretages en skanning i materiale, der uploades til en hjemmeside. Hvis systemet ved denne øvelse identificerer sammenhænge, der indikerer, at der kan være tale om personoplysninger (eks. et CPR nr.), vil systemet spørge brugeren, om der er tale om personoplysninger, og i bekræftende fald kunne blokere upload til hjemmesiden*
- *Sletningsmekanisme for behandlinger med hjemmel i samtykke, hvorved systemet automatisk sletter de personoplysninger, forordningen kræver, når den registreredes trækker sit samtykke tilbage*
- *Design af systemer, der automatisk sletter data efter et vist tidsrum eller andre objektivt fastsatte regler. Som eksempel kan nævnes et økonomisystem, der designes således, at det sletter, eller anonymiserer alle bogførte data 5 år efter registreringstidspunktet*
- *Design af systemer, der automatisk pseudonymiserer data, der ikke har været benyttet i et givet tidsrum*
- *Adgangskontrol-systemer, der baserer tilgangen til data på det minimale aktuelle behov for behandlingen.*

**Eksempler på organisatoriske foranstaltninger:**

- *Awareness hos medarbejdere – certificering af medarbejdere, der arbejder med personoplysninger*
- *Etablering af procedurer for behandling og kommunikation af personoplysninger*
- *Kontroller, audit og godkendelser*
- *ISO 27001*

# 6. Databeskyttelse gennem standardindstillinger

## *6.1. Definition af databeskyttelse gennem standardindstillinger*

Databeskyttelsesforordningen fastsætter et princip om databeskyttelse gennem *standardindstillinger*[35]. Det indebærer, at du som dataansvarlig skal sikre, at det kun er de personoplysninger, der er nødvendige til hvert specifikt formål med behandlingen, der bliver behandlet. Du skal også sikre, at personoplysninger ikke uden den registreredes indgriben stilles til rådighed for et ubegrænset antal personer.

Du skal altså særligt sikre dig imod, at oplysningerne er tilgængelige for enhver, hvilket implicerer overholdelse af de krav til datasikkerhed, som følger af forordningens regler om behandlingssikkerhed[36].

Standardindstillinger skal efter ordlyden af forordningen forstås bredt, således at det omfatter både tekniske og organisatoriske foranstaltninger. Standardindstillinger kan derfor forstås som både it-tekniske indstillinger og de almene forretningsgange, som understøtter databeskyttelse, herunder at adgang til personoplysninger – analoge såvel som digitale – er arbejdsbetingede og ikke lige tilgængelige for alle i din organisation.

**Eksempel**

*En virksomhed inden for forsikring indsamler i en hjemmesideblanket, i forbindelse med udstedelse af tilbud, oplysninger fra den mulige forsikringstager.*

*Alt efter hvilken forsikring, kunden ønsker, tilpasser blanketten indsamlingen af oplysninger til det minimalt nødvendige for at kunne afgive tilbuddet.*

*Hvis kunden ikke ønsker at benytte tilbuddet, slettes alle oplysningerne automatisk. Data kan ikke tilgås eller vises for nogen i virksomheden, før der fra kundens side aktivt vises interesse for at gå videre med tilbuddet.*

Forordningen udtrykker en pligt for dig som dataansvarlig til at sikre, at når f.eks. et softwareprogram, en onlinetjeneste, et it-system eller lignende anvendes til at behandle personoplysninger, skal de indstillingsmuligheder, som systemet mv. indeholder, som standard indstilles på en måde, der understøtter forordningens krav i artikel 25, stk. 2, om bl.a. formålsspecifik behandling af personoplysninger.

[35] Artikel 25, stk. 2.

[36] Artikel 32

Det betyder kort sagt, at konfigurerbare muligheder i systemet og alle standardindstillinger (defaults) en bruger stilles overfor, der vedrører indsamlingen af personoplysninger, skal indstilles til det minimalt nødvendige for behandlingen.

**Eksempler på databeskyttelse gennem standardindstillinger:**

- *Dynamisk rettighedsdeling.*
- *Slettet og sendt post slettes automatisk fra e-mail konto efter 30 dage.*
- *Ingen udgangspunktsindstillinger til ekstraydelser.*
- *Brug af op-in (aktivt tilvalg).*

## 6.2. Formål med databeskyttelse gennem standardindstillinger

Den grundlæggende idé bag bestemmelsen om databeskyttelse gennem standardindstillinger er, at du som dataansvarlig, ved at justere dine standard-konfigurationer, kan fremme persondatabeskyttelse. Denne fremgangsmåde sikrer, at privatlivsbeskyttelse er indlejret fra begyndelsen og aktiveret som standard.

## 6.3. Forholdet til andre krav i databeskyttelsesforordningen

Kravet om databeskyttelse gennem standardindstillinger (artikel 25, stk. 2) kan ses som et påkrævet supplement til kravet om databeskyttelse gennem design (artikel 25, stk. 1).

Ved at arbejde med princippet om databeskyttelse gennem design kan du som dataansvarlig indlejre privatlivs- og persondatabeskyttelse i it-design og -arkitektur fra start. Bestemmelsen om databeskyttelse gennem standardindstillinger operationaliserer de implementerede tiltag ved f.eks.at sikre, at du gør brug af den mest formålsbegrænsende indstilling som standard.

Sammenhængen mellem databeskyttelse gennem design og databeskyttelse gennem standardindstillinger kan illustreres ved, at en deling af personoplysninger, der ikke kan reguleres ved hjælp af standardindstillinger, *kan* være et tegn på, at du ikke har sikret databeskyttelse gennem design i den givne applikation.

## 6.4. Databeskyttelse gennem standardindstillinger i praksis

### 6.4.1. Betydning for fremtidige it-systemer

Fremtidige eller ændrede eksisterende it-systemers standardindstillinger skal udformes på en sådan måde, at der alene indsamles den datamængde, der er nødvendig, og at omfanget af behandlingen ikke er unødigt stort, samt at opbevaringstiden ikke er for lang.

For eksempel vil en fysisk person, der downloader en applikation (app) til sin smartphone, kunne forvente, at du som dataansvarlig som standard har sikret, at der ikke bliver indsamlet flere oplysninger om personen, end det er nødvendigt for at opnå formålet med app'en. I forlængelse heraf, vil denne person ligeledes kunne forvente, at du ikke som standard deler oplysninger om, hvorvidt personen f.eks. har været på en bestemt beværtning, løbet en tur, eller hvem vedkommende har været sammen med – medmindre denne deling er selve formålet med app'en.

### *6.4.2. Betydning for eksisterende it-systemer*

Eksisterende it-systemer, hvor standardindstillingerne ikke kan ændres, vil ikke mødes af de nye krav efter den 25. maj 2018, der følger af forordningen herom. Det forudsætter dog, at systemerne ikke forhindrer, at man lever op til databeskyttelsesforordningens krav, herunder eksempelvis kravene til behandlingssikkerhed i artikel 32 og de grundlæggende principper i artikel 5.

Når et it-system ændres, skal standardindstillinger opfylde forordningens krav.

Når et eksisterende it-systems standardindstillinger kan ændres, vil du som dataansvarlig, når forordningen træder i kraft den 25. maj 2018, være forpligtet til at tilpasse systemets standardindstillinger således, at disse understøtter forordningens krav om bl.a. formålsspecifik behandling.

# 7. Påvisning af overholdelse af kravene til behandlingssikkerhed

## *7.1. Godkendt adfærdskodeks eller certificeringsmekanisme*[37]

Forordningen foreskriver[38], at du som dataansvarlig gennemfører passende tekniske og organisatoriske foranstaltninger for at sikre og for at være i stand til at påvise, at behandling er i overensstemmelse med forordningen, herunder kravene til behandlingssikkerhed.

Overholdelse af et godkendt adfærdskodeks eller en godkendt certificeringsmekanisme kan bruges som element til at påvise, at du overholder kravene til behandlingssikkerhed.

En adfærdskodeks er i databeskyttelsesforordningens forstand et sæt retningslinjer, som skal bidrage til at sikre, at de virksomheder, der har tilsluttet sig kodeksen, anvender reglerne i databeskyttelsesforordningen korrekt.

En adfærdskodeks kan f.eks. gå ud på at specificere databeskyttelsesforordningens regler om behandlingssikkerhed. Overholdelse af en sådan kodeks kan på denne måde anvendes som element til at påvise, at man leverer på til forpligtelserne efter forordningen til behandlingssikkerhed.

Det er i denne forbindelse vigtigt, at være opmærksom på, at tilslutning til og overholdelse af en godkendt adfærdskodeks, ikke i sig selv er bevis på overholdelse af databeskyttelsesforordningen - heller ikke for så vidt angår de artikler i forordningen, som kodeksen måtte forholde sig til.

[37] Se vejledning om adfærdskodekser og certificering ordninger, der er tilgængelig på Datatlisynets hjemmeside: www.datatilsynet.dk

[38] Se forordningens artikel 24

**Eksempel på databehandlers overholdelse af godkendt adfærdskodeks**[1]

*Hvis du f.eks. er en virksomhed, der har specialiseret sig i at udbyde skræddersyede cloud-løsninger til dine kunder inden for en given branche, og du som databehandler opbevarer dine kunders oplysninger i clouden, kan du vælge at overholde en godkendt adfærdskodeks i henhold til databeskyttelsesforordningen (GDPR) vedrørende behandlingssikkerhed i cloud-løsninger – hvis en sådan findes – og dermed sikre dine kunders oplysninger bedst muligt. Du vil således kunne påvise overfor potentielle kunder (dataansvarlige), at du i din løsning kan stille de fornødne garantier i forhold til datasikkerhed.*

*Adfærdskodeksen kan f.eks. indeholde retningslinjer for, hvordan cloud-udbydere skal beskytte personoplysningerne mod, at disse bl.a. kan tilgås af uvedkommende, ligesom kodeksen f.eks. kan indeholde retningslinjer for, hvordan cloud-udbydere løbende skal teste effektiviteten af deres tiltag, samt retningslinjer for løbende ekstern kontrol og cloud-udbyderens opfølgning derpå, ligesom den kan indeholde retningslinjer for, hvordan cloud-udbydere hurtigst muligt kan genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse m.v.*

*En certificeringsmekanisme er en ordning, hvor en kvalificeret tredjepart (et certificeringsorgan) attesterer for, at en virksomhed eller en myndighed – der har anmodet om at blive certificeret – lever op til et foruddefineret sæt kriterier eller krav.*

*En certificeringsordning relaterer sig til behandlingsaktiviteterne, og kan således f.eks. vedrøre en virksomheds eller en myndigheds indsamling, registrering, pseudonymisering eller sletning af personoplysninger, men derimod ikke selve det it-system, hvori behandlingsaktiviteterne foregår. En certificeringsmekanisme kan således også bruges som element til at påvise overholdelse af kravene til behandlingssikkerhed.*

# 8. Opsummering

Efter at have læst denne vejledning skulle du gerne være blevet bekendt med nedenstående hovednedslag.

**Behandlingssikkerhed**

- Du skal som dataansvarlig eller databehandler vurdere de risici, som en behandling indebærer og gennemføre foranstaltninger, der kan begrænse disse risici.

- Forordningen kræver, at du tilvejebringer et "passende sikkerhedsniveau". Hvornår et sådant niveau er etableret beror på en konkret vurdering med udgangspunkt i **hvilke** og **hvor store** risici, der konkret er for sikkerhedsbrud og dermed for fysiske personers rettigheder og frihedsrettigheder.

- Forordningen sætter fokus på den risikobaserede tilgang (afsnit 3.2.), der kendetegnes ved indlejringen af processer, der tager højde for løbende identifikation af risici og muligheder samt den efterfølgende overvågning, måling, evaluering og analyse af disse.

- Du er blevet bekendt med, at informationssikkerhedsstandarder som ISO/IEC 27001:2013, ISO/IEC29134:2017 kan tjene som illustrerende eksempler på, hvad en risikobaseret tilgang indebærer.

**Databeskyttelse gennem design og standardindstillinger**

- Som dataansvarlig skal du allerede fra begyndelsen have designet og indrettet dig på en sådan måde, at forordningens krav og beskyttelseshensyn varetages.

- Du forventes at anlægge en helhedstænkning, hvorved du tager højde for såvel tekniske som organisatoriske foranstaltninger.

- Forordningen afkræver ikke, at eksisterende it-systemer *uden videre* re-designes. Dette vil bero på en konkret vurdering (se hertil afsnit 5.3.1.). Du er bekendt med, at dine indstillinger, som standard skal sikre, at kun de personoplysninger, der er nødvendige til hvert specifikt formål med behandlingen bliver behandlet. Du skal også sikre, at personoplysninger ikke uden den registreredes indgriben stilles til rådighed for et ubegrænset antal personer.

**Dato**
Juni 2018

Justitsministeriet
Slotsholmsgade 10
1216 København K

**Telefon**
72 26 84 00

**Email**
jm@jm.dk

**ISBN**
978-88-98564-35-7

**Foto**
Scanpix