Digital

VEJLEDNING

Persondataforordningen - Implementering i danske virksomheder

DI Digital
1787 København V.
3377 3377
digital.di.dk
digital@di.dk

DI Digital – et branchefællesskab i Dansk Industri for virksomheder inden for it, tele, elektronik og kommunikation

Udgivet af: DI Digital

Redaktion: Henning Mortensen

ISBN: 978-87-7144-083-6

0.05.16

Digital

VEJLEDNING

Persondataforordningen - Implementering i danske virksomheder

BAGGRUND

Der er i 2016 vedtaget nye regler for behandling af personoplysninger i form af EU-forordningen, General Data Protection Regulation, GDPR. Reglerne erstatter i Danmark lov om behandling af personoplysninger fra 2001, som har sit udspring i EU-direktiv 95/46/EC fra 1995.

Lovgivningen, som er mere end 20 år gammel, har vanskeligt ved at følge med den teknologiske udvikling. Den nye forordning skal ses som en modernisering af beskyttelsen af behandling af personoplysninger. Der er ved udformningen af forordningen taget hensyn til en række forskellige hensyn: Styrkelse af individernes ret til databeskyttelse, understøttelse af det frie flow af data og reduktion af administrative byrder for dataansvarlige. Forordningen balancerer altså flere forskellige hensyn.

Forordningen bygger på en række punkter videre på den eksisterende lovgivning, og der er således en række forhold, som i sin kerne er uforandret. Der introduceres også en række nye tiltag.

Blandt de nye tiltag skal især fremhæves:

- delvis harmonisering af reglerne såvel som fortolkning af reglerne på tværs af de europæiske lande
- fjernelse af anmeldelsesforpligtelsen til Datatilsynet, når der skal behandles personoplysninger
- tilknytning til kun ét datatilsyn i Europa
- nye rettigheder for de registrerede
- nye og skærpede forpligtelser for de dataansvarlige og databehandlerne
- mere samarbejde mellem de europæiske datatilsyn
- introduktion af betydelige bøder for ikke at efterleve forordningen.

Denne vejledning er bygget op således, at der først gives en overordnet gennemgang af de nye regler i forordningen, som er relevant for virksomhederne. På baggrund af denne gennemgang opstilles en tjekliste med grundlæggende spørgsmål og anbefalinger fra DI, som især de mindre og mellemstore virksomheder kan drage nytte af, når de skal i gang med at arbejde med forordningen.

Til vejledningen er knyttet en række bilag. At arbejde med forordningen er en compliance øvelse i form af efterlevelse af regler såvel som en teknisk og processuel sikkerhedsøvelse.

- I bilag 1 (Persondataforordningen formuleret som kontroller) er kravene til virksomhederne fra forordningen skrevet sammen som kontroller baseret på ISO27002. Formålet er at gøre lovgivningen mere operationel på baggrund af et kontrolframework i form af ISO27000, som måske i forvejen er kendt i virksomheden.
- I bilag 2 (Eksempel på Standard Operational Procedure – Backup) er gennemgået et meget overordnet eksempel på, hvordan kontrollerne fra forordningen kan omskrives i politikker, Standard Operational Procedures, SOP.
- I bilag 3 (Privatlivsfremmende teknologier) findes en konceptuel beskrivelse af nogle af de teknologier, som har fået en fremtrædende plads i forordningen bl.a. under sikkerhed og data protection by design, og som kan bruges til at understøtte sikkerheden såvel som compliance med reglerne.

Vejledningen har til formål at hjælpe virksomhederne i arbejdet med forordningen. Vejledningen kan ikke erstatte de konkrete vurderinger f.eks. i form af risikoanalyser, konsekvensanalyser og interesseafvejninger osv. som virksomhederne skal foretage.

PERSONDATAFORORDNINGENS OPBYGNING

Persondataforordningen er grundlæggende bygget op omkring en række temaer, som hver især har nogle implikationer for virksomhederne:

1. Indledningsvis fastsættes det, hvilke informationer der er omfattet af forordningen og hvilke personaer, der er omfattet af forordningen. Her sondres der mellem dem personoplysningerne vedrører, "de registrerede", dem der har ansvaret for behandling af data, "de dataansvarlige", og dem som faktisk udfører behandlingen af personoplysningerne på vegne af de dataansvarlige, "databehandler".

   De spørgsmål, som virksomhederne skal stille sig selv i denne forbindelse, er:

   - er informationerne, som virksomheden ønsker at behandle, omfattet af forordningen; er informationerne at betragte som personoplysninger?
   - er virksomheden omfattet af forordningen?
   - spiller virksomheden en rolle som dataansvarlig eller databehandler i forhold til de konkrete behandlinger?

2. Forordningen indeholder en opdeling af personoplysninger i forskellige kategorier. Nogle personoplysninger er almindelige mens andre er følsomme (race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssigt tilhørsforhold, genetiske data, biometriske data, helbredsoplysninger eller oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering). Ud fra kategorierne af personoplys-

Dataansvarlig

Den der afgør til hvilke formål og med hvilke hjælpemidler, der må foretages behandling af personoplysninger

Databehandler

Den der behandler personoplysninger på den dataansvarliges vegne

Personoplysning

Enhver form for information om en identificeret eller identificerbar fysisk person – f.eks. kunde- eller HR-oplysninger

Kategorier af personoplysninger

Det skal bestemmes, om der behandles almindelige eller følsomme personoplysninger

ningerne kan virksomheden fastslå, om den må behandle de pågældende oplysninger; om virksomheden har retligt grundlag for behandlingen.

De spørgsmål, virksomhederne skal stille sig selv i denne forbindelse, er:
- hvilke kategorier af personoplysninger ønsker virksomheden at behandle?
- har virksomheden et retligt grundlag for at behandle de ønskede kategorier af personoplysninger?

3. Der findes i forordningen en række principper som skal følges, hvis virksomhederne ønsker at behandle personoplysninger. Principperne inkluderer bl.a. at personoplysningerne skal behandles lovligt (f.eks. med samtykke), fair, transparent, at oplysningerne kun må behandles til et specifikt, eksplicit og legitimt formål, at der ikke må behandles flere oplysninger end nødvendigt, at oplysningerne skal være korrekte og opdaterede, at oplysningerne ikke må lagres længere end nødvendigt og at oplysningerne skal beskyttes via sikkerhedsforanstaltninger iværksat efter en risikovurdering.

   De spørgsmål, virksomhederne skal stille sig selv i denne forbindelse, er:
   - hvilke behandlinger ønsker virksomheden at foretage?
   - opfylder virksomheden principperne for behandling af oplysningerne?
   - er behandlingen nødvendig (proportional)?
   - kan virksomheden behandle oplysningerne på en mindre indgribende måde og stadig opnå formålet?

Behandling

Indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse

Samtykke

Frivillig, specifik, informeret og utvetydig viljestilkendegivelse der bekræfter, at personoplysninger må behandles

4. Efterfølgende fastslås det, at de registrerede har en række rettigheder i forhold til de personoplysninger som behandles. De registrerede har bl.a. generelt ret til at blive informeret om behandlingen og ret til at få rettet eller slettet personoplysninger. De har også ret til at få deres oplysninger udleveret, så de kan bæres videre til en anden tjenesteudbyder, og desuden har de i udgangspunktet ret ikke at blive profileret.

   Det spørgsmål, virksomhederne skal stille sig selv i denne forbindelse, er:
   - opfylder virksomheden og kan virksomheden løbende opfylde de registreredes rettigheder ved behandling af oplysningerne?

5. Den dataansvarlige har også en række pligter, som virksomheden skal opfylde for at kunne foretage behandlingen. Disse pligter indebærer, at de skal beskytte personoplysninger tilstrækkeligt og herunder i et vist omfang designe beskyttelse af personoplysninger ind i deres it-systemer. Disse tiltag skal baseres på en risikoanalyse, men kan også i en række tilfælde baseres på en konsekvensanalyse (Data Protection Impact Assessment, DPIA og Privacy Impact Assessment, PIA). DI har lavet en let tilgængelig skabelon for konsekvensanalyse, som virksomhederne

Konsekvensanalyse

Kortlægning af konsekvenser for privatlivet ved digital behandling af personoplysninger og iværksættelse af tiltag til beskyttelse og kontrol af beskyttelse af personoplysninger

med fordel kan anvende[1]. Virksomhederne skal også i en række tilfælde udpege en databeskyttelsesansvarlig, kunne dokumentere deres behandlinger og sikkerhedstiltag samt kunne reagere på sikkerhedshændelser og meddele disse til myndigheder og eventuelle berørte registrerede. Yderligere skal de have kontrol med databehandleren, og databehandleren skal selv efterleve en række krav i forordningen. Endelig skal virksomhederne være opmærksom på de regler der gælder for overførsel af personoplysninger til lande udenfor EU.

Det spørgsmål, virksomhederne skal stille sig selv i denne forbindelse, er:
- opfylder virksomheden sine forpligtelser (herunder vedrørende overførsel og sikkerhed) ved at behandle personoplysninger?

6. Ud over ovenstående generelle forhold, eksisterer der en række specifikke forhold, som virksomheden skal forholde sig til. Disse forhold træder i kraft i særlige tilfælde – f.eks. hvis den dataansvarlige eller databehandleren overfører personoplysninger ud af EU, hvis der inden for branchen er særlige adfærdskodeks eller certificeringer, som skal efterleves, eller hvis der er særlige regler for visse branchers behandling eller på nationalt plan.

   Det spørgsmål, virksomhederne skal stille sig selv i denne forbindelse, er:
   - er der særlige forhold der gør sig gældende for vores virksomheds behandling af personoplysninger?

7. Endelig indeholder forordningen en række forhold, som ikke vedrører virksomhederne direkte, men som har konsekvens for virksomhederne, og som det derfor kan være nyttigt at kende til. Disse forhold vedrører reglerne for de nationale tilsynsmyndigheder (datatilsyn), samarbejdet mellem tilsynsmyndighederne på tværs af lande indenfor EU, sanktioner som kan ramme virksomhederne. Disse regler er ikke genstand for behandling i denne vejledning.

Det er i forbindelse med ovenstående oversigt værd at notere sig, at forordningen vedrører behandlinger af personoplysninger og ikke ejerskab. Behandlinger er f.eks. indsamling, lagring og sletning. I forordningen fastslås det således, hvornår og hvordan man må behandle personoplysninger defineret som informationer, der kan tilknyttes en person - uanset og uafhængigt af et egentligt ejerskab af disse informationer. Det forhold, at en virksomhed kan sige at eje nogle personoplysninger eller køber nogle personoplysninger (f.eks. en kundedatabase), giver således i sig selv ingen ret til at behandle disse.

Det er også værd at notere sig, at de spørgsmål, der er skitseret ovenfor, er det helt afgørende, at virksomhederne kan besvare. Hvis virksomhederne kommer til at bryde forordningen, er der fastsat bøder, som i værste fald kan udgøre 4% af virksomhedens koncernomsætning eller 20 mio. EUR. Det største beløb vil altid blive lagt til grund for en eventuel strafudmåling overfor den pågældende virksomhed. Det er virksomheden, der straffes og bøden går i statskassen. Den registrerede kan

---

[1] http://di.dk/Virksomhed/Produktion/IT/itsikkerhed/personoplysninger/Pages/DIsskabelonforPrivacyImpactAssessment.aspx

sideløbende eventuelt anlægge en erstatningssag. Forordningen skal således ses som en anledning til at beskytte personoplysninger på en fornuftig måde – og eventuelt ses som en bredere anledning til at få styr på sikkerheden. Dette kan i det brede perspektiv opnås ved at lade sig inspirere af sikkerhedsstandarden ISO27001.

DE NYE TILTAG I HOVEDTRÆK

Persondataforordningen indeholder en række nye tiltag, som nedenfor gennemgås i hovedtræk.

Samtykke

For at behandlingen af personoplysninger kan være lovlig, skal der i en række sammenhænge indhentes samtykke til behandlingen fra de registrerede. Det er der ikke noget nyt i. Når det drejer sig om behandling af almindelige personoplysninger skal samtykket være frit, specifikt, informeret og utvetydigt. Det nye er, at samtykket skal være utvetydigt! Samtykket er utvetydigt, når de registrerede foretager en bekræftende handling, som tilkendegiver at de registrerede accepterer den konkrete behandling af personoplysningerne til det konkrete formål. Eksempler på et sådant samtykke inkluderer, at de registrerede klikker i en boks, vælger indstillinger, afgiver en erklæring eller på anden måde udviser en adfærd, der tilkendegiver samtykket.

Den dataansvarlige er forpligtet til at kunne dokumentere, at samtykket er givet. Hvis der behandles følsomme personoplysninger, skal samtykket være eksplicit.

Datas følsomhed

I det nuværende direktiv 95/46/EC tales der om almindelige og følsomme oplysninger. Den danske persondatalov har en opdeling i almindelige, følsomme og semifølsomme oplysninger. Den danske implementering stammer fra de hedengangne danske registerlove, hvor Folketinget ønskede at opretholde den danske klassifikation, da man implementerede EU-direktivet. I den kommende forordning er der alene tale om almindelige og følsomme oplysninger, hvilket betyder, at definitionen af semifølsomme oplysninger endegyldigt bortfalder.

Ret til hjælp fra dataansvarlig

Den registrerede har ret til at få hjælp til at udfolde sine rettigheder fra den dataansvarlige.

Oplysning

Der skal gives langt flere oplysninger om behandlingen, end virksomhederne er vant til i dag. De oplysninger, der skal gives, indeholder bl.a. den dataansvarliges kontaktinformation, formålet med behandlingen, lovligheden af behandlingen, evt. overførsel til tredjeparter, perioden for behandlingen (inkl. lagring), retten til at gøre indsigelse og begrænse behandlingen, muligheden for at trække samtykke tilbage, muligheden for at klage til datatilsynet og angivelse af om behandlingen indgår i en profilering.

Retten til at blive glemt

Der har været meget mediemæssig bevågenhed om retten til at blive glemt. I realiteten er reglerne ikke væsentligt anderledes end i dag. Den registrerede har i en

række tilfælde ret til at få slettet sine oplysninger. Den dataansvarlige skal, hvis oplysningerne er blevet offentliggjort af den dataansvarlige, og den dataansvarlige pålægges at slette disse personoplysninger, tage rimelige skridt til, at andre dataansvarlige, som også behandler disse oplysninger, sletter personoplysningerne eller links hertil.

Dataportabilitet

Der introduceres en helt ny rettighed, som indebærer, at de registrerede kan kræve at få udleveret deres personoplysninger i et struktureret, almindeligt anvendt og maskinlæsbart format således, at de registrerede kan sende disse personoplysninger til en anden dataansvarlig. Formålet er at gøre det let for den registrerede dels at få overblik over alle sine data og dels at kunne portere sine data til en konkurrerende serviceudbyder.

Retten til ikke at blive profileret

Det introduceres en helt ny rettighed til de registrerede, som skal sikre, at de ikke kan profileres. Profilering er afgørelser, der alene er baseret på automatiserede behandlinger, som har retsvirkning eller betydelige konsekvenser. Profilering må således ikke bruges til f.eks. kreditvurdering eller e-rekruttering. Der kan dog samtykkes til profileringen f.eks. til markedsføringsformål, ligesom der også er enkelte andre retlige grundlag for profilering.

Profilering

Automatisk behandling af personoplysninger, der har til formål at evaluere bestemte personlige forhold

Den dataansvarliges pligter

Den dataansvarlige har som i dag ansvaret for, at behandlingen af personoplysninger er i overensstemmelse med forordningen. Der introduceres dog en række nye forpligtelser for den dataansvarlige:

- Beskyttelsen af personoplysninger skal under en række forudsætninger designes ind i løsningen og slås til som standard (data protection by design og default). I bilag 3 (Privatlivsfremmende teknologier) gennemgås nogle tekniske bud på data protection by design - herunder pseudonymisering og kryptering, som fremstår som centralt tiltag i forordningen
- Der skal udarbejdes dokumentation for den behandling, som foretages. Dokumentationen er meget central i forordningen, og man kan sige, at hvis noget ikke er dokumenteret, er det ikke gjort
- Der skal, som i dag, tilvejebringes de fornødne sikkerhedsforanstaltninger
- Der skal foretages meddelelse til Datatilsynet (og under visse omstændigheder også til de registrerede), hvis der er sket en sikkerhedshændelse, som har kompromitteret personoplysninger
- Der skal under visse omstændigheder foretages en risikovurdering set fra de registreredes synspunkt ved at oplysningerne behandles - en såkaldt konsekvensanalyse
- Der skal i visse tilfælde udpeges en databeskyttelsesrådgiver
- Den obligatoriske anmeldelse til Datatilsynet af behandling af personoplysninger bortfalder generelt. Hvis der behandles personoplysninger, som kan udsætte de registrerede for særlige risici, skal

Data protection by design og default

Design af teknologisk løsning således at den reducerer graden af indgriben i datasubjekternes privatliv. Tiltagene skal slås til som standard

Databeskyttelsesrådgiver

En person, der har det som sin opgave at sikre beskyttelse af personoplysninger og efterlevelse af reglerne

der under en række forudsætninger alligevel foretages anmeldelse.

Databehandlerens forpligtelser

Som noget nyt får databehandleren sine egne forpligtelser. Databehandlerens forpligtelser har hidtil alene være reguleret i databehandleraftalen indgået mellem den dataansvarlige og databehandleren, men der introduceres altså nu i forordningen særlige forpligtelser. Der kan idømmes bøde, hvis de ikke efterleves.

Væsentligst er det, at databehandleren er forpligtet til at hjælpe den dataansvarlige med at efterleve en række af sine forpligtelser, og at databehandleren har en forpligtelse til at oplyse den dataansvarlige, hvis de vurderer, at en instruktion er ulovlig.

Overførsel til tredjelande

Der kan overføres personoplysninger til tredjelande ved anvendelse af standardkontrakter (Standard Contractual Clauses, SCC), Binding Corporate Rules (BCR) og via de aftaler, som EU-Kommissionen laver med andre lande (f.eks. USA) (tidligere Safe Harbour og i fremtiden Privacy Shield). I skrivende stund er det uklart, hvilket retligt grundlag som præcist kan anvendes, og virksomhederne anbefales at følge med i udviklingen.

One-stop-shop og sammenhængsmekanismen

Den dataansvarlige skal fremover som hovedregel alene interagere med datatilsynet i det EU-land, hvor virksomheden foretager beslutninger vedrørende behandlingen. Dermed får hver virksomhed som hovedregel ét datatilsyn som myndighed i stedet for 28.

Hvis eventuelle tvister har sit udspring i et andet EU-land, end der hvor virksomheden interagerer med sit datatilsyn, skal datatilsynene samarbejde via sammenhængsmekanismen, så der træffes afgørelser, som begge datatilsyn er tilfredse med. Hvis datatilsynene ikke kan blive enige om en afgørelse, eskaleres afgørelsen til samarbejdet mellem alle de europæiske datatilsyn, som således træffer afgørelsen. Formålet er at sikre en harmoniseret fortolkningspraksis på tværs af EU-landene.

Administrative bøder

Virksomhederne kan pålægges bøder for ikke at overholde forordningen. For manglende efterlevelse af den dataansvarlige eller databehandlerens pligter kan virksomhederne straffes med bøder på 2% af moderselskabets omsætning eller 10 mio. EUR, hvad der er højest. For manglende efterlevelse af principperne, de registreredes rettigheder, overførsel til lande udenfor EU uden retligt grundlag eller manglende efterlevelse af ordrer fra Datatilsynet kan virksomhedens straffes med bøder på 4% af moderselskabets omsætning eller 20 mio. EUR. Det største beløb vil altid blive lagt til grund for en eventuel strafudmåling overfor den pågældende virksomhed.

Harmonisering

Da forordningen blev lavet, var det et klart hensyn, at der skulle ske en harmonisering af reglerne indenfor EU. Dette skulle bl.a. sikres ved, at der er tale om en forordning, som er gældende som den står (i modsætning til et direktiv, som skal tilpasses national ret), og ved harmonisering af fortolkningspraksis gennem sammenhængsmekanismen. Der opnås med de nye regler således en vis grad af harmonisering.

I det politiske kompromis, som er blevet resultatet, har man imidlertid lavet ganske mange muligheder for at fastsætte national lovgivning dels for at fastsætte mere bestemte regler for anvendelsen af forordningen og dels ved i national lov at fastsætte retligt grundlag på særlige områder. National lovgivning og nærmere fastsatte nationale regler vil derfor underminere harmonisering på en række områder. Virksomhederne er derfor nødt til at være opmærksom på, om der er fastsat national lovgivning i de EU-lande, de opererer i, og dermed ikke alene fokusere på at efterleve forordningen.

DI ANBEFALINGER

I tilknytning til de nye regler og de spørgsmål virksomhederne bør stille sig selv for at afklare, om personoplysninger behandles på en fornuftig måde, har DI et par konkrete anbefalinger.

Selv om det kun i de færreste tilfælde er et eksplicit juridisk krav for virksomhederne at udpege en databeskyttelsesrådgiver (Data Protection Officer, DPO), vil det for mange virksomheder være en fordel, at der til enhver tid findes en person, som har ekspertise til at vurdere virksomhedens behandling af personoplysninger, og som kender virksomheden godt. Hvis man først skal ud og finde en databeskyttelsesrådgiver, når Datatilsynet kommer på inspektion, har man som hovedregel tabt sin sag på forhånd. Virksomhederne bør derfor udpege en person, som har ansvaret for behandling af personoplysninger. Virksomhederne bør samtidig give den pågældende person tilstrækkelig myndighed til at kunne udøve sit hverv. Det er vigtigt, at ledelsen sikrer, at den pågældende person samarbejder med virksomhedens it-sikkerhedschef. Mange af de tiltag, som skal iværksættes, kræver sikkerhedstekniske kompetencer. Hvis virksomheden ikke selv har kompetencerne, er det tilrådeligt at købe disse fra it-sikkerhedsleverandører og advokathuse. Det skal bemærkes, at det ikke bør være den samme part, som rådgiver og fører kontrol med efterlevelsen af lovgivningen – hverken i forhold til databeskyttelsesrådgiveren eller i forhold til andre typer af rådgivere.

Virksomhederne bør ofte gøre brug af en konsekvensanalyse for de it-projekter, hvor det er hensigten, at der skal behandles personoplysninger. Virksomheden vil generelt på en meget operationel måde kunne få et unikt overblik over sine behandlinger og sit flow af personoplysninger gennem virksomheden ved at anvende en konsekvensanalyse. Tilsvarende vil man få et overblik over de sikkerhedstiltag, man har taget, og få en plan over, hvad der eventuelt skal til at få gjort beskyttelsen

tilstrækkelig. DI har lavet en let tilgængelig skabelon for konsekvensanalyse[2], som virksomhederne med fordel kan anvende.

Konsekvensanalysen vil, hvis den anvendes rigtigt, også kunne give nogle gode råd til at designe sikkerheden ind i sine it-systemer (data protection by design). I forordningen nævnes en række abstrakte teknologibegreber som kryptering, pseudonymisering og anonymisering. Sådanne teknologier kaldes privatlivsfremmende teknologier, og de kan bidrage væsentlig til beskyttelsen af personoplysninger. DI anbefaler, at det undersøges, om virksomhederne i en konkret sammenhæng kan drage nytte af dem. Teknologierne er yderligere beskrevet i bilaget til DI's konsekvensanalyse og bilag 3 i denne vejledning.

DI anbefaler, at virksomhederne gennemgår deres databehandleraftaler i lyset af de nye regler i forordningen. Det vil være de færreste, som på baggrund af eksisterende aftaler er i compliance med den kommende forordning.

Der vil de kommende år komme en række fortolkningsbidrag til hvordan forordningens regler skal forstås og implementeres i praksis. Bl.a. vil Justitsministeriet og Datatilsynet løbende bidrage med fortolkninger. Når loven er trådt i kraft vil gruppen af europæiske datatilsyn, European Data Protection Board, ligeledes komme med fortolkningsbidrag. Reglerne for at overføre personoplysninger til lande udenfor EU er ligeledes under løbende forandring i disse år. Det er derfor vigtigt hele tiden at holde sig orienteret - f.eks. gennem DI - om hvilke retlige grundlag, som fortsat er gyldige.

DI anbefaler desuden, at virksomheden for at gøre arbejdet med at skabe compliance med forordningen mere operationelt implementerer de kontroller, som er beskrevet i bilag 1 til denne vejledning. Kontrollernes form tager udgangspunkt i ISO27001 og ISO27002, som er almindeligt kendte standarder for informationssikkerhed. Standarderne bør læses som inspiration til at arbejde med informationssikkerhed i virksomheden generelt - og altså ikke alene for at skabe compliance med GDPR.

Arbejdet med forordningen er ikke gjort med at lave sikkerhedstiltag, processer og kontroller. Det er vigtigt, at medarbejderne forstår, at deres daglige omgang med personoplysninger skal vi i overensstemmelse med loven. Derfor bør virksomhederne træne medarbejderne i organisationen i korrekt behandling af personoplysninger.

Når man hører om forordningens regler første gang, kan man få den opfattelse, at der er tale om en bureaukratisk papirtiger. Man skal huske på, at lovgiver har haft gode hensigter om at beskytte de registreredes fundamentale rettigheder med denne forordning, og at der i afvejningen også har været lagt vægt på virksomhedernes byrder. Ved at skabe compliance med forordningen får man også nogle forretningsmæssige muligheder:

---

[2] http://di.dk/Virksomhed/Produktion/IT/itsikkerhed/personoplysninger/Pages/DIsskabelonforPrivacyImpactAssessment.aspx

- Man kommer til at kende sine data på en helt ny måde og kan måske skabe nye forretningsmuligheder baseret på disse data
- Man får mulighed for at strømligne nogle processer og træffe nogle risikofunderede beslutninger, hvad der burde kunne skabe effektiviseringsmuligheder
- Endelig kommer man til at beskytte personoplysninger på den måde, som samfundet har besluttet er acceptabelt. Det er derfor vigtigt at fokusere på, om man kan få noget positiv forretning ud af det arbejde, man alligevel skal udføre.

TJEKLISTE

Nedenstående spørgsmål er relateret til de vigtigste hovedområder i persondataforordningen. Virksomheden bør gøre sig i stand til at besvare og dokumentere sine svar på disse spørgsmål.

1. Er virksomheden omfattet af forordningen?
2. Er informationerne, som virksomheden ønsker at behandle, omfattet af forordningen; er informationerne at betragte som personoplysninger?
3. Hvilke kategorier af personoplysninger ønsker virksomheden at behandle?
4. Hvilke behandlinger ønsker virksomheden at foretage?
5. Spiller virksomheden en rolle som dataansvarlig eller databehandler i forhold til de konkrete behandlinger?
6. Har virksomheden et retligt grundlag til at behandle de ønskede kategorier af personoplysninger?
7. Opfylder virksomheden principperne for behandling af oplysningerne?
8. Er behandlingen nødvendig (proportional)?
9. Kan virksomheden behandle oplysningerne på en mindre indgribende måde og stadig opnå formålet?
10. Opfylder virksomheden de registreredes rettigheder ved behandling af oplysningerne?
11. Opfylder virksomheden sine forpligtelser (herunder vedrørende overførsel og sikkerhed) ved at behandle personoplysninger?
12. Er der særlige forhold, der gør sig gældende, for virksomhedens behandling af personoplysninger?

Virksomhederne bør desuden overveje at følge de nedenstående konkrete anbefalinger fra DI:

1. Virksomheden bør udpege en ansvarlige for behandlingen af personoplysninger i virksomheden. Denne person bør i vid udstrækning samarbejde med den person som er ansvarlig for informationssikkerheden. Hvis virksomheden ikke selv har kompetencerne bør disse skaffes fra eksterne leverandører
2. Virksomheden bør overveje at gennemføre en konsekvensanalyse / data protection impact assessment for de it-systemer, som i væsentlig grad behandler personoplysninger
3. Virksomhederne bør overveje om de kan designe bedre beskyttelse af personoplysninger ind i deres it-systemer og herunder anvende privatlivsfremmende teknologier
4. Virksomheden bør gennemgå sine databehandleraftaler i lyset af reglerne i forordningen
5. Virksomheden bør løbende have klarhed over sit retlige grundlag for overførsel af personoplysninger til lande udenfor EU
6. Virksomhederne bør gennemgå de kontroller, som er nævnt i bilagene til denne vejledning
7. Virksomhederne bør træne medarbejderne i korrekt behandling af personoplysninger
8. Virksomhederne bør vurdere, om de gennem kortlægningen af deres data kan udvikle forretningen baseret på data, og om de kan effektivisere processer.

BILAG 1: PERSONDATAFORORDNINGEN FORMULERET SOM KONTROLLER

I dette bilag opstilles persondataforordningens krav til private virksomheder som kontroller på samme form, som de er formuleret i ISO27002. På den baggrund kan kontrollerne hænges op på et ledelsessystem for informationssikkerhed, et ISMS, som beskrevet i ISO27001. Hensigten er at gøre det lettere at arbejde med at komme i compliance med forordningen, fordi forordningens krav kan hænges op på et operationelt, kendt og i forvejen etableret kontrolframework.

De krav, som gennemgås, er de almindelige krav i GDPR, rettet mod private virksomheder. Vejledningen gennemgår ikke krav til offentlige myndigheder. Vejledningen gennemgår heller ikke krav fra anden national (sektor)lovgivning - f.eks. sundhedsloven eller arkivloven.

For hver kontrol angives der:

- Henvisning til artikel i persondataforordningen på formen Artikel X, stk. Y og eventuelt en henvisning til en forklarende tekst i præamblen P.Z.
- Henvisning til kontrol i ISO27001:
  - Hvis der henvises til en kontrol i standardens bilag A er formen: A.X.Y.Z
  - Der er mange steder behov for at henvise til flere kontroller i ISO27001
  - Hvis der henvises til juridisk compliance i henhold til kontrol A.18.1.4 vil der være en angivelse af om opgaven overvejende skal varetages af en tekniker, A.18.1.4 (t), eller en jurist, A.18.1.4 (j).

1. SCOPE

Formål

Det skal afklares, om virksomheden er omfattet af forordningen, og om de informationer, som skal behandles, er omfattet af forordningen.

1.1 Overordnede spørgsmål

- Er virksomheden omfattet af forordningen?

Kontroller

Artikel 3 (territorie) og 27 (repræsentanter) A.18.1.4 (j) (compliance med privatlivets fred og beskyttelse af personoplysninger)	Virksomheden skal afklare, om den er omfattet af GDPR

Implementeringsvejledning

Alle dataansvarlige og databehandlere, som har etableret sig i EU er omfattet - uanset om behandlingen finder sted i EU.

Virksomheder, der laver varer eller services rettet mod borgere i EU, defineret ved f.eks. sprog, valuta eller kunder indenfor EU er omfattet.

Virksomheder som registrerer adfærd (tracking, profilering og/eller præferencer) for registrerede der befinder sig i EU er omfattet.

Virksomheder, som omfattes af de to sidste bullets, skal udpege en repræsentant i EU.

1.2 Overordnede spørgsmål

- Er informationerne, som virksomheden ønsker at behandle, omfattet af forordningen; er informationerne at betragte som personoplysninger?

Kontroller

Artikel 4, stk. 1, litra 1 (personoplysninger) A.8.2.1 (klassifikation af information)	Virksomheden skal afklare, om den behandler personoplysninger i forordningens forstand

Implementeringsvejledning

Forordningen omfatter personoplysninger, som behandles automatiseret, eller anden behandling af personoplysninger, som indgår i et arkiv.

Personoplysninger er alle informationer relateret til en identificeret eller identificerbar person - herunder inklusiv pseudonymisering, eksklusiv anonymisering.

En identificerbar person er en person, som kan identificeres (direkte eller indirekte) under henvisning til:

- en identifier som f.eks. navn, ID-nummer, lokationsdata eller
- en online identifier af alle slags (f.eks. IP, cookie, RFID) eller
- andre faktorer, som er specifikke for personen (fysisk, genetisk, mentalt, økonomisk, kulturelt eller socialt)

Identifikatorer

I forordningens præambel 30 og 64 samt §4, stk. 1, litra 1 beskrives identifikatorer, som noget der kan bruges til at identificere en person og der nævnes bl.a. specifikt IP-adresser, cookies og RFID. I det omfang disse identifikatorer faktisk kan bruges til at identificere en fysisk person må det antages at de er omfattet af forordnings definition af personoplysninger. Specielt cookies er dog også reguleret i ePrivacy-direktivet, jvf. henvisningen i artikel 95 til direktiv 2002/58/EF

2. BEHANDLING AF PERSONOPLYSNINGER

Formål

Det skal afklares, om virksomheden kan finde et retligt grundlag til at foretage de behandlinger af de kategorier af personoplysninger, som den ønsker. Desuden skal virksomhedens rolle i forhold til behandlingen afklares. Endelig skal virksomheden afklare hvilken myndighed, virksomheden skal interagere med.

2.1. Overordnede spørgsmål

- Hvilke kategorier af personoplysninger ønsker virksomheden at behandle?

Kontroller

Artikel 6 (almindelige oplysninger) og 9 (følsomme oplysninger) A.8.2.1 (klassifikation af information)	Virksomheden skal afklare, hvilke kategorier af personoplysninger den ønsker at behandle

Implementeringsvejledning

I GDPR findes der to kategorier af personoplysninger. Der findes almindelige personoplysninger og følsomme oplysninger.

De almindelige oplysninger er de oplysninger, som ikke er følsomme.

De følsomme oplysninger omfatter race, politiske holdninger, religiøse eller filosofiske overbevisninger, tilhørsforhold til fagforening, behandling af genetiske eller biometriske data som unik identifier, sundhed, sexliv og seksuel orientering.

Desuden udgør strafferetlige oplysninger en særlig kategori af almindelige personoplysninger, som kræver særlig beskyttelse.

I dansk retspraksis har de almindelige oplysninger hidtil været opdelt i almindelige oplysninger og almindelige fortrolige oplysninger. Der vil muligvis i lyset af GDPR være behov for at justere retspraksis på dette område.

Endelig skal virksomhederne være opmærksom på, at de semifølsomme oplysninger som defineret i lov om behandling af personoplysninger ikke følger direkte af direktiv 95/46/EC og i hvert fald ikke følger af GDPR og dermed bortfalder – med mindre der i fremtiden fastsættes national lovgivning for disse kategorier. Der er tale om strafferetlige oplysninger, oplysninger om sociale forhold og andre rent private oplysninger.

2.2 Overordnede spørgsmål

- Hvilke behandlinger ønsker virksomheden at foretage?

Kontroller

Artikel 4, stk. 1, litra 2 (behandling) A.8.1.3 (accepteret brug af aktiver)	Virksomheden skal afklare hvilke behandlinger, den ønsker at foretage af de forskellige personoplysninger

Implementeringsvejledning

Behandling skal forstås bredt, som f.eks. indsamling, registrering, systematisering, opbevaring, tilpasning eller ændring, selektion, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring samt blokering, sletning eller tilintetgørelse.

2.3 Overordnede spørgsmål

- Spiller virksomheden en rolle som dataansvarlig eller databehandler i forhold til de konkrete behandlinger?

Kontroller

Artikel 4, stk. 1, litra 7 (dataansvarlig) A.18.1.4 (j) (compliance med privatlivets fred og beskyttelse af personoplysninger)	Virksomheden skal afklare, for hvilke behandlinger den eventuelt er dataansvarlig
Artikel 4, stk. 1, litra 8 (databehandler) A.18.1.4 (j) (compliance med privatlivets fred og beskyttelse af personoplysninger)	Virksomheden skal afklare, for hvilke behandlinger den eventuelt er databehandler

Implementeringsvejledning

Virksomhederne skal være opmærksomme på, at de kan have begge roller i alle behandlinger eller have den ene rolle i forhold til nogle behandlinger og den anden rolle i forhold til andre behandlinger.

Virksomheden er dataansvarlig, hvis den bestemmer formålet med behandlingen og de midler, hvormed behandlingen foretages.

Virksomheden er databehandler, hvis den handler efter instruks fra den dataansvarlige.

2.4 Overordnede spørgsmål

- Har virksomheden et retligt grundlag for at behandle de ønskede kategorier af personoplysninger?

Kontroller

Artikel 6 (almindelige oplysninger), 9 (følsomme oplysninger, herunder sundhedsoplysninger), 85 (journalistiske, akademiske, kunstneriske og litterære formål), 86 (offentlighedens interesse), 87 (nationalt identifikationsnummer), 88 (arbejdsretlige regler), 89 (offentlighedens interesse, videnskabelige, historiske og statistiske formål) og 90 (religion) A.18.1.4 (j) (compliance med privatlivets fred og beskyttelse af personoplysninger)	Virksomheden skal afklare, om den kan finde et retligt grundlag for at behandle de ønskede kategorier af personoplysninger. I den forbindelse skal det også afklares, om særlige nationale regler på en række områder skal efterleves
Artikel 4, stk. 1, litra 16 (main establishment), 60 (one-stop-shop og sammenhængsmekanismen) og 55 (Datatilsynets kompetence) A.6.1.3 (kontakt til myndigheder)	Virksomheden bør afklare hvilket datatilsyn i Europa, som virksomheden hører under

Implementeringsvejledning

Virksomheden må behandle almindelige personoplysninger, hvis principperne for god databehandlingsskik er opfyldt (principperne gennemgås i kontrollerne nedenfor) og hvis en af nedenstående forudsætninger er opfyldt:

- Der er indhentet et lovligt samtykke
- Det er nødvendigt for gennemførelsen af en kontrakt, som de registrerede er en del af
- Den dataansvarlige skal overholde en retlig forpligtelse
- Hvis det sker for at varetage vitale interesser for de registrerede eller andre
- Hvis det følger af væsentlig offentlig interesse eller national lovgivning
- Interesseafvejning, hvor den dataansvarliges legitime interesse overstiger de registreredes interesser.

Virksomheden må behandle følsomme personoplysninger, hvis en af nedenstående forudsætninger er opfyldt:

- Der er indhentet et eksplicit samtykke
- Det retlige grundlag for behandlingen er fastsat i medfør af arbejdsretlige regler eller kollektive overenskomster
- Hvis det sker for at varetage vitale interesser for de registrerede eller andre
- Hvis behandlingen foretages af organisationer, som led i deres eget naturlige virke
- Hvis de pågældende oplysninger allerede er offentliggjort af de registrerede selv
- Hvis det sker som led i fremsættelse af juridiske krav
- Hvis det følger af væsentlig offentlig interesse eller national lovgivning
- Hvis det sker af hensyn til forskellige sundhedsmæssige formål
- Hvis det sker i forbindelse med videnskabelig eller historisk forskning eller til statistiske formål.

Foruden disse overordnede forudsætninger for behandling af personoplysninger fastslås der særskilt retligt grundlag til behandling i særlige situationer forskellige steder i GDPR og disse skal specificeres yderligere i national lovgivning:

- Journalistiske formål
- Akademiske, kunstneriske og litterære formål
- Behandling af nationalt identifikationsnummer
- Arbejdsretlige regler
- Offentlighedens interesse
- Videnskabelig eller historisk forskning eller til statistiske formål
- Kirker og religiøse foreninger
- Nationale regler på sundhedsområdet

Retsinformationssystemer, markedsføringsbureauer, arkiver og kreditoplysningsbureauer har hidtil haft mulighed for at behandle oplysninger på et særligt retligt grundlag i persondataloven. Dette videreføres ikke uændret i GDPR, og det må afventes at se, om der indføres national lovgivning på disse områder.

GDPR introducerer begrebet om one-stop-shop, som betyder, at hver virksomhed tilknyttes ét europæisk datatilsyn; nemlig datatilsynet i det land, hvor virksomheden har placeret det selskab, som foretager beslutninger vedrørende behandling af personoplysninger. Virksomhederne bør foretage en vurdering af, hvilket lands datatilsyn de hører under.

3. PRINCIPPER

Formål

Det skal afklares, om virksomhederne efterlever principperne for god databehandlingsskik, når de behandler personoplysninger.

3.1 Overordnede spørgsmål

- Opfylder virksomheden principperne for behandling af oplysningerne?
- Er behandlingen nødvendig (proportional)?
- Kan virksomhederne behandle oplysningerne på en mindre indgribende måde og stadig opnå formålet?

Kontroller

Artikel 5 (principper) A.8.2.3 (håndtering af aktiver)	Den dataansvarlige virksomhed skal bestemme, hvilke personoplysninger der må behandles hvordan
Artikel 5, stk. 1, litra a (lovlig) og artikel 6, stk. 1, litra a (samtykke) og Artikel 7 (samtykke) og 8 (samtykke for børn) A.18.1.4 (j) (compliance med privatlivets fred og beskyttelse af personoplysninger) A.12.1.1 (dokumenterede driftsprocedurer)	Hvis behandlingen har et retligt grundlag i form af samtykke, skal samtykket dokumenteres
Artikel 5, stk. 1, litra a (lovlig) og artikel 6, stk. 1, litra f (interesseafvejning) A.18.1.4 (j) (compliance med privatlivets fred og beskyttelse af personoplysninger) A.12.1.1 (dokumenterede driftsprocedurer)	Hvis behandlingen sker ud fra en interesseafvejning af de den dataansvarliges berettigede interesse og de registreredes interesse, skal denne interesseafvejning eksplicit dokumenteres
Artikel 5, stk. 1, litra a (lovlig) og Artikel 6, stk. 1, litra b (kontrakt) eller litra c (retlig	Hvis behandlingen har et retligt grundlag i en kontrakt eller en retlig forpligtelse, skal dette doku-

forpligtelse) A.18.1.4 (j) (compliance med privatlivets fred og beskyttelse af personoplysninger) A.12.1.1 (dokumenterede driftsprocedurer)	menteres
Artikel 5, stk. 1, litra a (lovlig) og Artikel 6 (almindelige oplysninger), 9 (følsomme oplysninger, herunder sundhedsoplysninger), 85 (journalistiske, akademiske, kunstneriske og litterære formål), 86 (offentlighedens interesse), 87 (nationalt identifikationsnummer), 88 (arbejdsretlige regler), 89 (offentlighedens interesse, videnskabelige, historiske og statistiske formål) og 90 (religion) A.18.1.4 (j) (compliance med privatlivets fred og beskyttelse af personoplysninger) A.12.1.1 (dokumenterede driftsprocedurer)	Hvis virksomheden på anden måde finder retligt grundlag for behandlingen, skal dette dokumenteres
Artikel 5, stk. 1, litra a (lovlighed, rimelighed og gennemsigtighed) A.18.1.4 (j) (compliance med privatlivets fred og beskyttelse af personoplysninger)	Virksomheden skal sikre sig, at behandlingen er rimelig/fair
Artikel 5, stk. 1, litra a (lovlighed, rimelighed og gennemsigtighed) A.18.1.4 (j) (compliance med privatlivets fred og beskyttelse af personoplysninger)	Virksomheden skal sikre sig, at behandlingen er gennemsigtig
Artikel 5, stk. 1, litra b (formålsbegrænsning) A.18.1.4 (j) (compliance med privatlivets fred og beskyt-	Virksomheden skal sikre sig, at behandlingen begrænses til et udtrykkeligt angivet og legitimt formål

telse af personoplysninger)	
Artikel 5, stk. 1, litra b (formålsbegrænsning) A.18.1.4 (j) (compliance med privatlivets fred og beskyttelse af personoplysninger)	Virksomheden skal sig, at behandling ikke sker til andre uforenelige formål
Artikel 5, stk. 1, litra c (dataminering) A.18.1.4 (j) (compliance med privatlivets fred og beskyttelse af personoplysninger) A.12.1.1 (dokumenterede driftsprocedurer)	Virksomheden skal sikre sig, at der kun behandles personoplysninger, som er tilstrækkelige, relevante og begrænset til hvad der er nødvendigt i forhold til formålet; herunder at man ikke kunne opnå formålet ved en mindre indgribende behandling
Artikel 5, stk. 1, litra d (rigtighed) (se også artikel 16-21) A.12.1.1 (dokumenterede driftsprocedurer)	Virksomhedens skal sikre sig, at personoplysninger er korrekte og ajourførte
Artikel 5, stk. 1, litra d (rigtighed) (se også artikel 16-21) A.12.1.1 (dokumenterede driftsprocedurer)	Virksomheden skal sikre sig, at ukorrekte personoplysninger slettes eller rettes
Artikel 5, stk. 1, litra e (opbevaringsbegrænsning) A.12.1.1 (dokumenterede driftsprocedurer)	Virksomheden skal sikre sig, at personoplysninger kun lagres i en form, hvor de kan bruges til at identificere den registrerede, så længe som det er nødvendigt for formålet
Artikel 5, stk. 1, litra f (integritet og fortrolighed) (se også artikel 32) A.5.1.1 (politikker for informationssikkerhed) A.6.1.5 (informationssikkerhed ved projektstyring) A.14.1.1 (analyse og specifikation af informationssikkerhedskrav) A.14.2.5 (principper for ud-	Virksomheden skal iværksætte de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger således, at personoplysninger kan behandles lovligt, er sikret fortrolighed, integritet, tilgængelighed og modstandskraft og ikke fortabes, tilintetgøres eller beskadiges (sikkerhedstiltagene uddybes nedenfor under virksomhedens forpligtelser).

vikling af sikre systemer)	

Implementeringsvejledning

Det er den dataansvarlige, som henset til formålet afgør, hvilke behandlinger der må finde sted på hvilke personoplysninger. Det er i den forbindelse den dataansvarlige, som har ansvaret for behandlingerne. Formålet må ikke være for bredt defineret, men skal i overvejende grad søges at være så præcist som muligt.

Først og fremmest skal den dataansvarlige dokumentere, på hvilket juridisk grundlag behandlingen foregår. Dette grundlag bør den dataansvarlige dokumentere, så der ikke kan herske tvivl om det. Hvis den dataansvarlige ønsker at bruge personoplysningerne til et andet formål, skal det vurderes, om de to formål er kompatible. Det afgøres ved at vurdere sammenhængen mellem de to formål, relationen mellem den dataansvarlige og den registrerede, datas følsomhed, de mulige konsekvenser for den registrerede, sikkerhedsforanstaltningerne, og om den registrerede skal informeres.

Når behandlingen foretages skal den begrænses til det, som er fair overfor den registrerede, hvilket betyder, at den registrerede skal have kendskab til behandlingens eksistens og have mulighed for at udøve sine rettigheder.

Den dataansvarlige skal sikre, at behandlingen er transparent. Det gøres ved at give den registrerede oplysninger om den dataansvarliges identitet og kontaktinformation, behandlingsformålet, lovligheden af behandlingen, kategorierne af modtagerne af data, om der sker overførsel til tredjelande, perioden for behandlingen, om der sker profilering samt om den registreredes rettigheder (bl.a. om retten til at trække samtykke tilbage, begrænse behandlingen, rette personoplysninger og retten til at klage over behandlingen). Oplysningerne skal så vidt muligt gives i almindeligt sprog eller via standardiserede ikoner.

De personoplysninger, der behandles, skal være korrekte og opdaterede, og ukorrekte oplysninger bør slettes eller rettes. Virksomhederne skal dog som udgangspunkt ikke rette oplysninger bare for at rette; sletning skal kun ske efter behov. Desuden kan der i mange tilfælde være behov for at de fejlbehæftede oplysninger ikke slettes, men i stedet suppleres med de rette oplysninger og en note om, at de er rettet så virksomheden kan bevare historikken på en sag.

Personoplysninger skal slettes, når der ikke længere er behov for dem i forhold til formålet. Der kan alternativt foretages anonymisering, så data efterfølgende falder udenfor forordningen. I givet fald bør virksomheden sikre sig, at det i praksis er umuligt at henføre data til personer.

Virksomhederne skal iværksætte passende sikkerhedstiltag til at beskytte personoplysningers fortrolighed, tilgængelighed og integritet, som det også nævnes i ISO27001. Desuden skal it-systemerne udvise en passende modstandskraft mod angreb udefra. Det må antages, at denne modstandskraft opnås ved at efterleve ISO27001. De sikkerhedstiltag, der iværksættes, skal baseres på en risikovurdering. Tiltagene skal testes løbende, og det skal sikres, at der kan ske retablering. Det må forventes, at der vil komme mere præcise sikkerhedskrav i takt med at retspraksis

udvikler sig og i takt med, at der kommer vejledninger til GDPR såvel nationalt som på europæisk plan, f.eks. a la Sikkerhedsbekendtgørelsen. Sikkerhedsbekendtgørelsen stiller krav om organisering, fysisk sikring, administration af autorisation og adgangskontrol, behandling og destruktion af ind- og uddatamateriale og medier, awareness, mobile arbejdspladser og logning. Den gælder formelt set kun for den offentlige sektor, men den private sektor anbefales at efterleve kravene. Der lægges i forordningen ikke op til, at virksomhederne skal efterleve ISO27001. Men mange af de metoder og tiltag, som skal iværksættes, er omtalt i standarden, hvorfor det kan anbefales at efterleve ISO27001 og ISO27002.

4. DE REGISTREREDES RETTIGHEDER

Formål

Det skal afklares, om virksomheden gør de registrerede i stand til at kunne udleve deres rettigheder.

4.1 Overordnede spørgsmål

- Opfylder virksomheden de registreredes rettigheder ved behandling af oplysningerne?

Kontroller

Artikel 12, stk. 2 (gennemsigtighed) A.12.1.1 (dokumenterede driftsprocedurer)	Den dataansvarlige virksomhed skal hjælpe de registrerede således, at de kan udøve deres rettigheder
Artikel 12, stk. 3 (gennemsigtighed) A.12.1.1 (dokumenterede driftsprocedurer)	Den dataansvarlige skal kunne håndtere henvendelser fra de registrerede og besvare disse indenfor en måned
Artikel 13, stk. 1 og 2, Artikel 14, stk. 1 og 2 (oplysningspligt) Artikel 15, stk. 1 (indsigtsret) A.12.1.1 (dokumenterede driftsprocedurer) A.6.1.1 (ansvar) A.18.1.4 (j) (compliance med privatlivets fred og beskyttelse af personoplysninger) A.8.2.1 (klassifikation af information)	Den dataansvarlige skal tilvejebringe de registrerede oplysninger om de behandling, der foretages, uanset om personoplysningerne er indhentet fra de registrerede selv (*) eller erhvervet fra tredjepart (**). Udover at den dataansvarlige skal give de registrerede oplysningerne, kan de registrerede også selv kræve indsigt til enhver tid. Oplysningsforpligtelsen omfatter som minimum: - Den dataansvarliges identitet og kontaktinformation, ditto evt. databeskyttelsesrådgiveren - Behandlingsformålet og retsgrundlaget - Legitime interesse hos den dataansvarlige, hvis behandling er baseret på interesseafvejning - Kategorierne af personoplysningerne (**) - Kategorierne af modtagerne af personoplysninger - Evt. overførsel til tredjelande

A.13.2.1 (politikker og procedurer for informationsoverførsel)	- Perioden for behandlingen (inkl. lagring) - Retten til at få indsigt, rette eller slette personoplysninger, begrænse behandling, gøre indsigelse mod behandling og retten til dataportabilitet - Muligheden for at trække samtykke tilbage - Muligheden for at klage til Datatilsynet - Kilden til personoplysningerne (**) - Personoplysningerne behandles som led i en kontrakt (*) - Evt. profilering - Anvendelse af personoplysningerne til et nyt formål (*)
Artikel 16 (berigtigelse), Artikel 17 (sletning) og Artikel 18 (begrænsning) A.12.1.1 (dokumenterede driftsprocedurer)	Den dataansvarlige skal sikre, at de registrerede kan få rettet og slettet personoplysninger. Den dataansvarlige skal desuden sikre, at behandlingen kan begrænses efter ønske fra den registrerede.
Artikel 19 (underretningspligt) A.12.1.1 (dokumenterede driftsprocedurer)	Den dataansvarlige skal videregive den registreredes ønske om rettelse eller sletning til tredjeparter, som evt. måtte have fået adgang til data
Artikel 20 (dataportabilitet) A.12.1.1 (dokumenterede driftsprocedurer)	Den dataansvarlige skal kunne videregive personoplysninger vedrørende den registrerede i et struktureret, almindeligt anvendt og maskinlæsbart format til den registrerede selv eller til en anden dataansvarlig på opfordring fra den registrerede
Artikel 21 (indsigelse) A.12.1.1 (dokumenterede driftsprocedurer) A.18.1.4 (j) (compliance med privatlivets fred og beskyttelse af personoplysninger)	Den dataansvarlige skal kunne håndtere en indsigelse mod behandling af personoplysninger
Artikel 22 (profilering) A.12.1.1 (dokumenterede driftsprocedurer) A.18.1.4 (j) (compliance med privatlivets fred og beskyttelse af personoplysninger)	I udgangspunktet må den dataansvarlige ikke foretage profilering. Hvis det er nødvendigt for indgåelse af en kontrakt, er hjemlet i national lovgivning eller hvis den registrerede samtykker, kan der dog foretages profilering.

Implementeringsvejledning

Den dataansvarlige skal hjælpe den registrerede med at udleve sine rettigheder. Dette indebærer bl.a., at der skal kommunikeres i et letforståeligt sprog og eventuelt med anvendelse af standardiserede ikoner. Den dataansvarlige skal hjælpe de registrerede gratis, med mindre der er tale om mange gentagne henvendelser.

Den registrerede kan få rettet oplysningerne og under en række forudsætninger - f.eks. ved at trække samtykke tilbage - få oplysningerne slettet. Hvis den dataansvarlige har videregivet oplysningerne, skal den dataansvarlige meddele et eventuelt ønske om sletning og fjernelse af links til oplysningerne til den part oplysningerne er videregivet til. Hvis oplysningerne er upræcise eller ulovlige, kan den registrerede gøre indsigelse mod behandling og begrænse denne.

Den registrerede har ret til at få sine oplysninger udleveret i et struktureret, almindeligt anvendt og maskinlæsbart format. Hensigten er, at den registrerede skal kunne overflytte sine oplysninger til en anden dataansvarlig. I det omfang det er teknisk muligt, har den registrerede desuden ret til at bede den dataansvarlige overføre oplysningerne til en ny dataansvarlig.

Den registrerede har ret til ikke at blive profileret. Profilering skal forstås som en afgørelse der alene er baseret på automatiserede behandlinger, der har retsvirkning eller betydelige konsekvenser. Profilering må kun ske i medfør af samtykke, ved indgåelse af en kontrakt eller i medfør af national lovgivning. Der må gerne samtykkes til markedsføringsformål.

Der påhviler især den dataansvarlige en række oplysningsforpligtelser. Hvis den dataansvarlige har personoplysningerne direkte fra den registrerede, skal der informeres om følgende: den dataansvarliges identitet og kontaktinformation, formålet med og lovligheden af behandlingen, kategorierne af dem som får adgang til at behandle oplysningerne, hvorvidt der sker overførsel til tredjelande, perioden for behandlingen, retten til at få rettet oplysninger eller begrænse behandlingen, gøre indsigelse, muligheden for dataportabilitet, muligheden for at trække samtykke tilbage, muligheden for at klage til datatilsynet, hvorvidt oplysningerne behandles som led i opfyldelsen af en kontrakt, hvorvidt der foretages en automatiseret beslutning (profilering) på baggrund af oplysningerne og eventuelle nye formål, hvorefter oplysningerne behandles. Hvis oplysningerne er indsamlet fra tredjepart skal der også oplyses om, hvilke kategorier af personoplysninger som behandles, og hvilken kilde oplysningerne stammer fra. Til gengæld skal der ikke oplyses om nye formål eller om oplysningerne behandles som led i en kontrakt.

5. VIRKSOMHEDENS FORPLIGTELSER

Formål

Det skal afklares, om virksomheden efterlever de forpligtelser, som den pålægges af forordningen.

5.1 Overordnede spørgsmål

- Opfylder virksomheden sine forpligtelser ved at behandle personoplysninger?

Kontroller

Artikel 24, stk. 1 (ansvar) A.5.1.1 (politikker for informationssikkerhed) A.5.1.2 (gennemgang af politikker for informationssikkerhed) A.18.2.2 Overensstemmelse med sikkerhedspolitikker og -standarder	Den dataansvarlige har ansvaret for at efterleve og dokumentere efterlevelse af persondataforordningens regler
Artikel 24, stk. 2 (databeskyttelsespolitikker) A.5.1.1 (politikker for informationssikkerhed) A.5.1.2 (gennemgang af politikker for informationssikkerhed)	Den dataansvarlige bør fastlægge databeskyttelsespolitikker, -procedurer og kontroller
Artikel 25, stk. 1 (databeskyttelse gennem design) og stk. 2 (standardindstillinger) A.5.1.1 (politikker for informationssikkerhed) A.6.1.5 (informationssikkerhed ved projektstyring) A.14.1.1 (analyse og specifikation af informationssikkerhedskrav) A.14.2.5 (principper for udvikling af sikre systemer)	Den dataansvarlige skal under hensyn til bl.a. formålet, behandlingerne, risici, og konsekvenser for de registrerede, omkostninger og det aktuelle tekniske niveau vurdere, om der skal designes sikkerhedsforanstaltninger (f.eks. pseudonymisering), der understøtter forordningens principper for behandling og forordningen i almindelighed, ind i it-løsningen Sikkerhedsforanstaltningerne skal slås til som standard.
Præambel 78 (data protection by design i udbud) A.15.1.1 (informationssikkerhedspolitik for leverandørforhold) A.15.1.2 (håndtering af sikkerhed i leverandøraftaler) A.13.2.2 (aftaler om informations-	Den dataansvarlige bør vurdere, om der skal stilles særlige designkrav om understøttelse af forordningens principper til it-leverandører

overførsel)	
Artikel 28, stk. 1 (databehandler) A.15.1.1 (informationssikkerheds-politik for leverandørforhold) A.15.1.2 (håndtering af sikkerhed i leverandøraftaler) A.13.2.1 (politikker og procedurer for informationsoverførsel) A.13.2.2 (aftaler om informations-overførsel)	Den dataansvarlige skal i aftalen med databehandlerne sikre sig, at de kan implementere de rette tekniske og organisatoriske foranstaltninger
Artikel 28, stk. 2 (databehandler) A.15.1.1 (informationssikkerheds-politik for leverandørforhold) A.15.1.2 (håndtering af sikkerhed i leverandøraftaler) A.13.2.1 (politikker og procedurer for informationsoverførsel) A.13.2.2 (aftaler om informations-overførsel)	Den dataansvarlige skal sikre sig at databehandleren ikke bruger underdatabehandlere uden godkendelse
Artikel 28, stk. 3 (databehandler) A.9.2.2 (brugeradgang) A.9.4.1 (adgangsbegrænsning) A.12.1.1 (dokumenterede driftsprocedurer) A.13.2.2 (aftaler om informations-overførsel) A.15.1.1 (informationssikkerheds-politik for leverandørforhold) A.15.1.2 (håndtering af sikkerhed i leverandøraftaler) A.16.1.3 (rapportering af informationssikkerhedssvagheder)	Den dataansvarlige overfor databehandlere i en kontrakt sikre sig: - at der kun behandles personoplysninger efter instruktion fra den dataansvarlige - at kun autoriseret personale kan tilgå personoplysninger - at der kan tilvejebringes den fornødne information til brug for risikovurderinger og implementering af sikkerhedstiltag - at der kan gives bistand således, at den dataansvarlige kan hjælpe de registrerede med at forfølge deres rettigheder - at den fornødne dokumentation til at belyse databrud og gennemføre en konsekvensanalyse kan fremskaffes - at alle personoplysninger kan slettes eller tilbageleveres til den dataansvarlige - at al relevant dokumentation for efterlevelse af kravene i denne artikel er tilgængeligt Databehandlere skal orientere de dataansvarlige, hvis de vurderer, at den instruktion til behandling, de modtager, er ulovlig
Artikel 30, stk. 1 (fortegnelse over behandlingsaktiviteter) A.12.1.1 (dokumenterede driftspro-	Den dataansvarlige skal kunne dokumentere: - Navn og kontaktinformation på dataansvarlig

cedurer)	- Beskrivelse af formålet med behandlingen - Beskrivelse af kategorier af registrerede, personoplysninger og evt. modtagere - Overførsler - Periode for behandling - Sikkerhedstiltag - Processer for samarbejde med Datatilsynet
Artikel 30, stk. 2 (fortegnelse over behandlingsaktiviteter) A.12.1.1 (dokumenterede driftsprocedurer)	Databehandlere skal kunne dokumentere: - Navn og kontaktinformation på dataansvarlig - Kategorier af behandlinger, som foretages på vegne af den dataansvarlige - Overførsler - Sikkerhedstiltag - Processer for samarbejde med Datatilsynet
Artikel 32, stk. 1 og stk. 2 (behandlingssikkerhed) A.5.1.1 (politikker for informationssikkerhed) A.6.1.5 (informationssikkerhed ved projektstyring) A.14.1.1 (analyse og specifikation af informationssikkerhedskrav) A.14.2.5 (principper for udvikling af sikre systemer)	Virksomheden skal gennemføre en risikoanalyse med fokus på behandlingen af personoplysninger og på den baggrund iværksætte passende tekniske og organisatoriske sikkerhedstiltag
Artikel 32, stk. 1, litra a (behandlingssikkerhed) A.10.1.1 (politik for anvendelsen af kryptografi) A.9.4.1 (begrænset adgang til informationer)	Virksomhederne bør vurdere om sikkerhedstiltag skal inkludere kryptering og pseudonymisering
Artikel 32, stk. 1, litra b (behandlingssikkerhed) A.5.1.1 (politikker for informationssikkerhed) A.14.1.1 (analyse og specifikation af informationssikkerhedskrav) A.14.2.5 (principper for udvikling af sikre systemer)	Evne til at sikre en vedvarende høj informationssikkerhed og robusthed gennem alskens relevante sikkerhedstiltag som vurderes nødvendige på baggrund af risikovurderingen
Artikel 32, stk. 1, litra c (behandlingssikkerhed) A.12.3.1 (backup af information) A.17.1.1 (planlægning af informati-	Personoplysninger skal kunne genskabes indenfor rimelig tid

onssikkerhedskontinuitet) A.17.1.2 (implementering af informationssikkerhedskontinuitet)	
Artikel 32, stk. 1, litra d (behandlingssikkerhed) A.14.2.8 (systemsikkerhedstest) A.14.2.9 (systemgodkendelsestest) A.12.7.1 (kontroller i forbindelse med audit af informationssystemer) A.15.2.1 (overvågning og gennemgang af leverandørydelser) A.18.2 (gennemgang af informationssikkerhed)	Sikkerhedstiltag skal testes og evalueres
Artikel 32, stk. 4 (behandlingssikkerhed) A.5.1.1 (politikker for informationssikkerhed) A.14.1.1 (analyse og specifikation af informationssikkerhedskrav) A.14.2.5 (principper for udvikling af sikre systemer)	Medarbejdere hos dataansvarlige og databehandlere må kun behandle personoplysninger efter instruks
Artikel 33, stk. 1 og stk. 3 (sikkerhedsbrud til tilsynsmyndighed) A.16.1.1 (ansvar og procedurer) A.16.1.5 (håndtering af informationssikkerhedsbrud) A.6.1.3 (kontakt med myndigheder)	Den dataansvarlige skal have procedurer for at kunne håndtere databrud: - Meddelelse til Datatilsynet indenfor 72 timer - Meddelelsen skal indeholde type af databrud, kategorier af berørte data, antal af registrerede, antal af registreringer, kontaktinformation på databeskyttelsesrådgiveren, konsekvenser for de registrerede og en beskrivelse af de korrigerende tiltag
Artikel 33, stk. 5 (sikkerhedsbrud til tilsynsmyndighed) A.16.1.7 (indsamling af beviser) A.12.4 (logning og overvågning)	Den dataansvarlige skal indsamle dokumentation (forensics) af databruddet
Artikel 33, stk. 2 (sikkerhedsbrud til tilsynsmyndighed) A.16.1.3 (rapportering af informationssikkerhedssvagheder)	Databehandlere, som opdager et databrud, skal straks orientere den dataansvarlige
Artikel 34 (sikkerhedsbrud meddeles til de registrerede)	Den dataansvarlige skal vurdere risici for de registrerede, og hvis der er høj risiko, skal de

A.16.1.5 (håndtering af informationssikkerhedsbrud)	registrerede som udgangspunkt orienteres om bruddet
Artikel 35, stk. 1 (konsekvensanalyse) A.6.1.5 (informationssikkerhed ved projektstyring) A.14.1.1 (analyse og specifikation af informationssikkerhedskrav) A.14.2.5 (principper for udvikling af sikre systemer)	Den dataansvarlige skal under hensyntagen til omfanget og følsomheden af personoplysninger, formålet og de involverede teknologier vurdere, om der i forhold til it-projekter er behov for at gennemføre en konsekvensanalyse
Artikel 36, stk. 1 (forudgående høring) A.6.1.3 (kontakt til myndigheder)	Hvis konsekvensanalysen indikerer høj risiko ved behandlingen af personoplysninger for de registrerede, skal den dataansvarlige foretage anmeldelse til Datatilsynet
Artikel 37 (databeskyttelsesrådgiver) A.6.1.1 (ansvar)	Virksomheden skal overveje, om der skal udpeges en person, som har til opgave at sikre efterlevelse af reglerne om behandling af personoplysninger, en databeskyttelsesrådgiver (DPO)

Implementeringsvejledning

Det er den dataansvarlige, som har pligten til at efterleve og dokumentere sin efterlevelse af reglerne i forordningen. Det betyder, at det er den dataansvarlige, som kan straffes og som risikerer at tabe sit gode navn og rygte i offentligheden og hos samarbejdspartnere, hvis reglerne brydes.

Den dataansvarlige bør derfor lave politikker og procedurer for behandlingen, sikre at alt dokumentation løbende er på plads og gennem kontroller sikre, at de faktisk virker i praksis og har den ønskede effekt.

Det betyder konkret, at personoplysninger bør klassificeres og håndteres i overensstemmelse med fastlagte procedurer, at behandlingen dokumenteres, at de rette sikkerhedstiltag baseret på en risikovurdering er iværksat og at sikkerheden designes ind i it-systemerne, at sikkerhedsbrud skal håndteres i overensstemmelse med fastlagte procedurer, at det bør gennemføres "konsekvensanalyser" (data protection impact assessments) i vid udstrækning, og at der udpeges en ansvarlige for efterlevelsen af reglerne, databeskyttelsesrådgiver, DPO.

Databehandlerne får som noget nyt i forordningen en række direkte forpligtelser, som tidligere alene var indeholdt i databehandleraftalen. Det betyder, at også databehandleren kan straffes og risikerer at tabe sit gode navn og rygte i offentligheden og hos samarbejdspartnere, hvis reglerne brydes. Disse pligter omfatter bl.a., at de skal garantere, at de implementerer de rette tekniske og organisatoriske sikkerhedstiltag, at de indhenter samtykke fra de dataansvarlige, når de indgår nye underdatabehandleraftaler, at der er indgået en kontrakt om behandlingen, at de kun

behandler oplysninger under instruktion fra den dataansvarlige, at kun autoriseret personale har adgang til oplysningerne, og at de kan hjælpe den dataansvarlige med at efterleve forordningen herunder opfylde de registreredes rettigheder.

6. SÆRLIGE FORHOLD

Formål

En række regler i forordningen er afhængige af forhold, der gør sig gældende i specifikke situationer – f.eks. kun for virksomheder, der udveksler personoplysninger med lande udenfor EU, eller kun for virksomheder, der skal efterleve national lovgivning eller sektorspecifik lovgivning. Virksomhederne skal være opmærksomme på, om særlige forhold vedrørende behandling af personoplysninger gør sig gældende indenfor deres forretningsområde.

Det overordnede spørgsmål på dette område er:

- Er der særlige forhold der gør sig gældende for virksomhedens behandling af personoplysninger?

6.1 Overordnede spørgsmål

- Overføres der personoplysninger til lande udenfor EU?

Kontroller

Artikel 44 (overførsel) A.18.1.4 (j) (compliance med privatlivets fred og beskyttelse af personoplysninger)	Den dataansvarlige skal afklare, om der overføres personoplysninger til lande udenfor EU
Artikel 44 (overførsel) A.18.1.4 (j) (compliance med privatlivets fred og beskyttelse af personoplysninger)	I de tilfælde, hvor den dataansvarlige overfører personoplysninger til lande udenfor EU, skal det retlige grundlag være slået fast
Artikel 46 (overførsel) A.15.1.2 (håndtering af sikkerhed i leverandøraftaler)	I de tilfælde, hvor der er indgået aftale om behandling af personoplysninger med en databehandler udenfor EU, skal der foreligge en lovlig databehandleraftale
Artikel 46 og Arti-	Den dataansvarlige bør kontrollere, at den dataansvarlige

kel 47 (overførsel) A.15.2.1 (overvågning og gennemgang af leverandørydelser)	overholder persondataforordningen og de sikkerhedskrav, som er beskrevet i databehandleraftalen

Implementeringsvejledning

Der er i forordningen en række muligheder for at få et retligt grundlag til at overføre personoplysninger til lande udenfor EU.

For det første har EU Kommissionen besluttet at betragte en række lande som sikre, i medfør af den lovgivning de har. Det er især national lovgivning vedrørende behandling af personoplysninger, som vurderes. EU Kommissionen vedligeholder en liste over disse godkendte såkaldte sikre tredjelande.

For det andet er det muligt at overføre oplysninger til virksomheder i lande udenfor EU i medfør af bilaterale aftaler mellem EU Kommissionen og det pågældende land. Aftalerne omfatter ikke hele landet, men kan omfatte virksomheder i det pågældende land, som så gennem selvevaluering demonstrerer et tilstrækkeligt sikkerhedsniveau. Indtil efteråret 2015 var den mest kendte retlige grundlag Safe Harbour aftalen mellem EU Kommissionen og USA. Den aftale blev erklæret ulovlig ved EU Domstolen i efteråret 2015. I foråret 2016 (skrivende stund) er en ny aftale ved at blive forhandlet, kaldet Privacy Shield.

Desuden kan en dataansvarlig overføre personoplysninger til en databehandler, der bl.a. befinder sig i såkaldte tredjelande, under anvendelse af kontrakter. Kontrakterne skal godkendes af de nationale datatilsyn. Imidlertid har EU Kommissionen udformet en standard kontrakt (standard contractual clauses eller model clauses), som kan anvendes til at skabe retligt grundlag for overførsel af personoplysninger. Hvis standard kontrakten anvendes uden ændringer, kræves der ikke godkendelse af datatilsynet. Denne standardkontrakt er pt. det mest udbredte retlige grundlag til overførsel af personoplysninger.

Endelige findes der særlige kontrakter til overførsel af personoplysninger indenfor koncerner. Dette er især relevant, hvis der f.eks. skal overføres HR-oplysninger for danske ansatte til et HR-system hos et moderselskab i USA. Disse bindende virksomhedsregler kaldes for Binding Corporate Rules, BCR.

For det tredje kan der i mere afgrænsede tilfælde skabes retligt grundlag for at overføre personoplysninger til lande udenfor EU. Dette involverer samtykke fra den registrerede, hvis det er nødvendigt for at overholde en kontrakt, hvis det er i den registreredes interesse, hvis det er i offentlighedens interesse og der er tilvejebragt et nationalt retligt grundlag, hvis det er nødvendigt for opfyldelsen af et juridisk krav eller hvis der er tale om en enkeltstående overførsel.

Som nævnt er reglerne under forandring i skrivende stund, og det anbefales derfor, at virksomhederne holder sig orienteret om reglernes udvikling.

6.2 Overordnede spørgsmål

- Er virksomheden i compliance med national fortolkning/implementering af forordningens regler?

Kontroller

Der er mange steder, hvor forordningen åbner op for fastsættelse af nationale fortolkninger af lovgivningen A.18.1.4 (j) (compliance med privatlivets fred og beskyttelse af personoplysninger)	Den dataansvarlige skal afklare, om der forefindes national fortolkning/implementering af persondataforordningen, som virksomheden skal være i compliance med

Implementeringsvejledning

Der findes mange steder i persondataforordningen mulighed for, at der nationalt kan fastsættes implementering af reglerne. Derfor vil der ikke på alle områder være tale om en harmonisering af reglerne mellem EU-landene på trods af, at der er tale om en forordning.

6.3 Overordnede spørgsmål

- Er virksomheden i compliance med anden regulering end persondataforordningen, som vedrører behandling af personoplysninger?

Kontroller

Der er mange steder, hvor forordningen åbner op for fastsættelse af national lovgivning A.18.1.4 (j) (compliance med privatlivets fred og beskyttelse af personoplysninger)	Den dataansvarlige skal afklare, om der forefindes national lovgivning, som opstiller særlige regler for behandling af personoplysninger, og som virksomheden skal være i compliance med

Implementeringsvejledning

Der findes mange steder i persondataforordningen muligheder for at fastsætte national lovgivning - f.eks. på sundhedsområdet, i forhold til den offentlige sektors anvendelse af personoplysninger, i forhold til mediers anvendelse af personoplysninger og i forhold til arbejdsmarkedet.

BILAG 2: EKSEMPEL PÅ STANDARD OPERATIONAL PROCEDURE - BACKUP

Omskrivningen af GDPR til kontroller, som kan tilknyttes kontrollerne i ISO27002, og dermed hænges op på et ledelsessystem for informationssikkerhed, ISMS, baseret på ISO27001, fremgår af bilag 1. Disse GDPR-kontroller, skal, når de hænges op på ISMS, indføres i de Standard Operational Procedures (SOP)/politikker/procedurer/retningslinjer, som ISMS'et har givet anledning til. På den måde får de direkte effekt i de daglige processer.

Nedenfor har vi taget et simpelt eksempel - en SOP for backup - og demonstreret, hvordan GDPR-kontrollen for genskabelse af personoplysninger er hængt op på ISO-kontrollen, som operationaliseres i SOP'en for backup.

Kilderne

GDPR, Artikel 32, stk. 1, delvist litra c: "... den dataansvarlige... [skal gennemføre] passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til... risici, herunder bl.a.... evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse"

ISO/IEC 27002:2013, Control 12.3.1: "Backup copies of information, software and system images should be taken and tested regularly in accordance with an agreed policy"

DI's beskrivelse af kontrollen og mapping af de to kilder: "Virksomheden skal sikre, ... at personoplysninger kan genskabes indenfor rimelig tid".

Konsekvensen

På de følgende sider er en stiliseret udgave af en SOP for backup præsenteret. Den tekst, som er markeret med rødt er suppleret ind i SOP'en som følge af GDPR.

En række af de forhold, der omtales i SOP'er, men som ikke følger direkte af denne kontrol, er også relevant i en GDPR sammenhæng – f.eks. hvem der har adgang til at læse data, hvis backupservicen er lagret i et land udenfor EU.

SOP - BACKUP

Baggrundsinformation

Organisationens navn:	XXXXXX A/S
Formål:	Formålet med denne Standard Operational Procedure er at sikre, at der tages backup, og at denne testes løbende, så virksomheden er beskyttet mod tab af data.
Målgruppe:	XXXXXX
Afgrænsning/Scope:	XXXXXX
Referencer:	ISO/IEC 27002:2013, Control 12.3.1 GDPR, Artikel 32, stk. 1, litra c

Formalia

Klassifikation af SOP:	XXXXXX
Version:	1.0
Udarbejdet af:	XXXXXX
Revideret af:	XXXXXX
Ledelsesgodkendt af:	Navn: XXXXXX Dato: XXXXXX
Næste revision:	XXXXXX
Distribueret til:	XXXXXX

Projekt eller systemtilknytning

Projektets/systemets navn:	XXXXXX
Projektleder /systemejer:	XXXXXX
Ansvarlig for personoplysninger:	XXXXXX

Procedurer

Der tages backup af information, software og systembilleder...

Der er på det konkrete system følgende kategorier af personoplysninger...

Der foretages registreringer af backupkopierne...

Der er lavet dokumenterede gendannelsesprocedurer...

Omfanget (fuldstændig eller datostyret) og hyppigheder...

Backupkopierne opbevares hos...

Følgende aktører har adgang til data...

Backupinformationen er underlagt følgende beskyttelsesforanstaltninger...

Backup testes på følgende måde...

Backup'en kan indlæses indenfor følgende estimerede tidsrum...

Backup'en indeholder klassificeret information, herunder personoplysninger, hvorfor følgende kryptering er anvendt...

Driftsprocedurer overvåger backup-en og rapporterer uregelmæssigheder...

Opbevaringsperioden er...

BILAG 3: PRIVATLIVSFREMMENDE TEKNOLOGIER

Beskyttelsen af personoplysninger kan forbedres ved at designe sin teknologi således, at den reducerer graden af indgriben i de registreredes privatliv. Dette kaldes Privacy by Design (PbD) - eller i forordningen: data protection by design. Som en del af dette design kan man supplere med teknologier, som er privatlivsfremmende. Disse teknologier kaldes Privacy Enhancing Technologies (PET). Beslutninger om hvilket design og hvilke teknologier der skal vælges kan baseres på en konsekvensanalyse (Data Protection Impact Assessment, DPIA og Privacy Impact Assessment, PIA).

Det skal bemærkes, at der ikke findes globalt accepterede definitioner af disse tre begreber.

I forordningens præambel 78 nævnes dog at databeskyttelse gennem design bl.a. henviser til "minimering af behandlingen af personoplysninger" og "pseudonymisering af personoplysninger så hurtigt som muligt". Det nævnes også i præambel 83 at kryptering kan begrænse risici, og i præambel 28 at pseudonymisering kan mindske risikoen, ligesom pseudonymisering og kryptering eksplicit fremhæves i artikel 32. Det er dog tanken at pseudonymisering og kryptering skal suppleres af andre databeskyttelsesforanstaltninger, jf. præambel 28. Det eneste ord, som er eksplicit defineret i forordningen, er pseudonymisering, hvor det i artikel 4, nr. 5 hedder: " behandling af personoplysninger på en sådan måde, at personoplysningerne ikke længere kan henføres til en bestemt registreret uden brug af supplerende oplysninger, forudsat at sådanne supplerende oplysninger opbevares separat og er underlagt tekniske og organisatoriske foranstaltninger for at sikre, at personoplysningerne ikke henføres til en identificeret eller identificerbar fysisk person".

PbD og PET må anvendes ud fra en konkret vurdering. I dette bilag skitseres et par muligheder overordnet.

Data protection by design

Der er tale om data protection by design, når man designer sin teknologi således, at den reducerer graden af indgriben i de registreredes privatliv. Et banalt eksempel er, når et it-system designes således, at adgangen til indsamlede personoplysninger teknisk begrænses til kun at omfatte ansatte med en given rolle i en virksomhed istedet for alle virksomhedens medarbejdere. Jo færre, der har adgang til data, jo mindre er risikoen for, at data kan blive brugt til et formål, der er uforeneligt med de registreredes interesser, og jo bedre er adgangsbegrænsningen set fra den pågældende registreredes synspunkt.

Det vigtigste designprincip er, hvor det er muligt, at designe løsningen således, at den slet ikke behandler personoplysninger. Dette kan f.eks. ske ved at anonymisere jvf. nedenfor.

Et andet centralt designprincip er at overveje at overdrage retten til at skabe sammenhæng mellem de registrerede personoplysninger og identiteten til den registrerede. Hermed afskærer virksomheden sig selv fra at identificere det den registrerede, som personoplysningerne vedrører, men den registrerede kan skabe sammenhængen, når den registrerede skønner, at det er i vedkommendes egen interesse.

Man kan lade sig inspirere til designprincipper ved at følge DI's skabelon til konsekvensanalyser[3] eller ved at besvare nogle af de spørgsmål der er i Tjeklisten til nærværende vejledning.

Et designprincip, som har fået særskilt plads i forordningen, er Data Protection by Default, hvor alle de gode databeskyttelsestiltag, man har indbygget i en applikation og vil give mulighed for at de registrerede kan gøre brug af, slås til som standard, og ikke overlades til den registrerede selv at slå til.

Privacy Enhancing Technologies

De privatlivsfremmende teknologier dækker principielt over alle teknologier, som giver forbedringer af privatlivsbeskyttelsen i et it-system. Således vil f.eks. rollebaseret adgangskontrol, hvor adgang til personoplysninger begrænses til alene at være den gruppe medarbejdere, der har en given rolle, kunne anskues som en privatlivsfremmende teknologi. Rigtig mange teknologier ville derfor kunne falde i denne kategori og bør anvendes for at skabe sikkerhed og for at komme i compliance med forordningen. Overordnet kan man tal om bl.a. nedenstående grupper af teknologier:

Data Loss Prevention
Kan forhindre e-mails med specifikke data eller syntakser i at forlade virksomheden, som f.eks. CPR-numre, kontonumre eller lignende.

Data Discovery
Giver mulighed for at afdække persondata på virksomhedens netværk der ikke er ligger på de rette systemer.

Identity and Access Governance
Kan give overblik over brugerroller og deres adgange til systemer og data og omfatter bl.a. "Priviledged Account Management" som skal forhindre it-folk i at have for brede beføjelser og "Role Mining", der kan afdække om der er nogle ukendte mønstre i fordelingen af roller og rettigheder.

Log management
Gør det muligt at redegøre for, hvem der har haft adgang til hvilke data hvornår.

Backup
Backup sikrer at data kan genskabes – f.eks. efter man har været udsat for en sikkerhedshændelse. Retten til at blive glemt som omtalt i forordningen kan dog være en udfordring, da det kan være vanskeligt at slette specifikke data fra backup systemet.

Shadow-it discovery
Virksomhedens ansvar dækker også over informationer der placeres på systemer udenfor it-afdelingens kontrol. Denne type services kan afdække den totale mængde af it-services der anvendes i organisationen.

---

3 http://di.dk/Virksomhed/Produktion/IT/itsikkerhed/personoplysninger/Pages/DIsskabelonforPrivacyImpactAssessment.aspx.

Information Lifecycle Management
Sletning af data der ikke skal anvendes mere er en væsentlig praktisk udfordring. Med denne type software kan man sætte regler op for datas "udløbsdato".

Pseudonymization
Identificerende data erstattes af koder i kombination med en nøgle, således at data ikke kan henføres til en person uden anvendelse af nøglen, hvilket som nævnt i forordningen bidrager til at reducere risiko.

Encryption
Kodning af data således at data kun kan læses af den, som er besiddelse af nøglen.

Anonymization
Konvertering af dele af data således at de data som kan henføres til en person slettes eller gøres permanent ulæsbare; f.eks. gennem kryptering, hvor dekrypteringsnøglen slettes.

Virtual or partial identities
En identitet, som ikke kan tilknyttes en konkret fysisk person. Der kan eventuelt på samme it-system laves en kombination af flere virtuelle identiteter uden linkability. I en række sammenhænge kan den dataansvarlige nøjes med at kende bestemte karakteristika ved en fysisk person - f.eks. over 18 år, gyldigt adgangskort eller studerende/pensionist. En række identitetsudbydere kan sikre dette for den registrerede. Identitetsudbyderen skal kende til den registreredes rigtige identitet.

Et par af teknologierne fortjener en uddybelse på grund af den særlige rolle de spiller i forordningen.

Anonymisering

Anonymisering er en meget vidtgående PET. Det betyder, at personoplysninger endegyldigt fraknyttes den registreredes identitet således, at der ikke igen på nogen måde kan etableres forbindelse. I dette tilfælde vil der således typisk ikke længere være tale om personoplysninger i lovens forstand, men altså blot om data. De pågældende data falder derfor udenfor lovens anvendelsesområde.

Det faktum, at der ikke kan genetableres en forbindelse mellem data og identitet, kan være en udfordring - f.eks. hvis der opstår mistanke om, at data kan tilknyttes et kriminelt forhold eller hvis en registreret ikke kan forfølge sine rettigheder. Det vil ikke være muligt at opklare, hvilken registreret der står bag kriminalitet eller har krav på at få opfyldt en rettighed, når data er anonymiseret. Omvendt giver anonymisering den bedst tænkelige beskyttelse af privatlivets fred.

Anonymisering kan være ganske udfordrende at etablere i praksis. Hvis de umiddelbart identificerende oplysninger som f.eks. navn og adresse fjernes fra et datasæt, kan der sagtens blandt de resterende oplysninger være mulighed for at identificere en registreret, f.eks. ved at isolere nogle data, ved at koble data på tværs af datasæt eller ved at finde en stor sandsynlighed for at to sæt data hører sammen. Anonymisering foregår ud fra to grundlæggende teknikker. Den ene mulighed er at randomizere data f.eks. ved at tilføje uægte data til ægte data for en registreret eller ved at bytte om på data således, at et gennemsnit over det samlede datasæt fastholdes. Den anden mulighed er at generalisere, f.eks. således at visse data ikke bliver præcist gengivet, men falder i intervaller.

Anonymisering brugt i forbindelse med kommunikation kaldes kommunikationsanonymisering. Det betyder, at et it-system ikke registrerer oplysning som f.eks. IP-adresse, MAC-adresse, e-mailadresse og cookie-ID. På den måde kan den registrerede øge sin sandsynlighed for, at virksomheden ikke ved, hvilken part der har indgået i kommunikationen. It-systemet kan tilbyde dette. Den registrerede kan dog også selv foretage tiltag, som anonymiserer vedkommendes egne data i kommunikationsflowet.

En anden afart kaldes transaktionsanonymisering. Ideen er at to parter skal kunne indgå en transaktion uden at den registreredes identitet er kendt. Begrebet har været anvendt i forbindelse med anonyme online betalinger. En registreret kan i sin bank få udstedt en virtuel pengeseddel, som er anonym ligesom fysiske trykte pengesedler. Pengesedlen kan den registrerede bruge i en onlinebutik. Onlinebutikken kan af banken få verifikation for, om pengesedlen er ægte, og ikke er brugt tidligere, og kan herefter gennemføre transaktionen med den registrerede uden at kende den registreredes identitet. Når dette kan gennemføres skyldes det en avanceret krypteringsmekanisme baseret på zero-knowledge-proof, som vi ikke vil komme nærmere ind på her.

Pseudonymisering

Pseudonymisering betyder, at personoplysninger fraknyttes den registreredes identitet, men istedet tilknyttes en nøgle, som så kan tilknyttes en identitet. Fordelen er, at personoplysningerne ikke umiddelbart kan tilknyttes den registrerede. Alene den, der kontrollerer nøglerne, kan identificere den registrerede. Det fjerner en række risici og gør databehandlingen mere sikker set fra den registreredes synspunkt.

F.eks. kunne man forestille sig, at en registreret går til sin praktiserende læge for at blive undersøgt for en sygdom, hvis diagnose skal stilles på baggrund af en blodprøve. Den registrerede identificerer sig overfor lægen, som autentificerer den registrerede. Herefter tages blodprøven, som tilknyttes en nøgle af lægen. Blodprøven kan så sendes hvorsomhelst hen, uden at nogen ved hvem den tilhører - herunder til et vilkårligt laboratorium, der skal analysere prøven. Resultatet af blodprøveundersøgelsen kommer tilbage til lægen, der på baggrund af nøglen tilknytter prøvens resultat til den registrerede og stiller diagnosen. Fordelen for den registrerede er, at alene den praktiserende læge ved, hvad hans diagnose er; laboratoriets ansatte ved det ikke og har ikke mulighed for at finde ud af det.

I et mere ekstremt tilfælde kunne man forestille sig, at den registrerede selv fik nøglen, således at det kun var den registrerede selv, der kunne se sin diagnose. I de tilfælde, hvor den registrerede selv administrerer nøglen, kunne der måske være mulighed for, at den registrerede selv var dataansvarlig i lovens forstand, og dermed vil en række forhold blive lettere for virksomheden.

Pseudonymisering rummer rigtig mange muligheder for at forbedre databeskyttelsen set fra den registreredes synspunkt, herunder muligheden for at give den registrerede selv kontrol over sine egne personoplysninger.

Kryptering

Kryptering er en byggesten, der bruges i flere af ovenstående løsninger. Kryptering er en proces, som omdanner oprindelig information til information, der er ulæselig

for tredjepart. Dette foregår som regel ved at bruge en offentlig og privat nøgle. Hvis Alice vil sende en fortrolig besked til Bob, bruger hun Bobs offentlige nøgle til at kryptere den med. Der er alene Bob, der har kontrol med sin private nøgle, og dermed er det alene Bob, der kan læse beskeden.

Kryptering er uendelig meget mere kompliceret og kan bruges i langt flere sammenhænge end skitseret ovenfor. Noget af det, som er særligt lovende, er, at man under særlige forudsætninger kan foretage databehandling på krypterede data uden at disse dekrypteres, og dermed uden at en registrerets identitet afsløres. Det vil være alt for omfattende i denne sammenhæng at komme igennem krypteringens muligheder. Men hovedbudskabet er, at hvis man kerer sig om at beskytte personoplysninger, er det en rigtig god ide at se på, om kryptering kan bringes i anvendelse på en eller anden måde.

Et par bemærkninger om lovgivning

Det er værd at notere sig, at pseudonymisering aldrig og anonymisering ikke altid betyder, at data i juridisk forstand ikke er personoplysninger. Det er f.eks. ikke nok alene at fjerne direkte identificerbar information som navn og adresse fra et datasæt. Der skal mere til, f.eks. en proces for generalisering (altså fjernelse af de enkelte records) med kontrol af at man ikke f.eks. indirekte kan slutte sig frem til de registreredes identitet, for at opnå det resultat at man ikke længere behandler personoplysninger. Psedonymisering og anonymisering skal derfor ses som metoder til at forbedre de registreredes sikkerhed. Har man anonymiseret korrekt, falder de anonymiserede data imidlertid udenfor forordningens anvendelsesområde.

Kilder

Der findes to vigtige kilder til det videre arbejde med privatlivsfremmende teknologier:

- Artikel 29-gruppens ”Opinion 05/2014 on Anonymisation Techniques”, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.
- IT- og Telestyrelsens “Nye digitale sikkerhedsmodeller”, http://digitaliser.dk/resource/781482.