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	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

fred og beskyttelse af personoplysninger)	
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)	Hvis behandlingen har et retligt grundlag i form af samtykke, skal samtykket dokumenteres

A.18.1.4 (j) (compliance med privatlivets fred og beskyttelse af personoplysninger) A.12.1.1 (dokumenterede driftsprocedurer)	
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 forpligtelse) 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 en kontrakt eller en retlig forpligtelse, skal dette dokumenteres
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)	Hvis virksomheden på anden måde finder retligt grundlag for behandlingen, skal dette dokumenteres

A.12.1.1 (dokumenterede driftsprocedurer)	
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 beskyttelse af personoplysninger)	Virksomheden skal sikre sig, at behandlingen begrænses til et udtrykkeligt angivet og legitimt formål
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)	Virksomhedens skal sikre sig, at personoplysninger er korrekte og ajourførte

A.12.1.1 (dokumenterede driftsprocedurer)	
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 udvikling af sikre systemer)	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).

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) A.13.2.1 (politikker og procedurer for informationsoverførsel)	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 - 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)	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.

A.12.1.1 (dokumenterede driftsprocedurer)	
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 informationsoverførsel)	Den dataansvarlige bør vurdere, om der skal stilles særlige designkrav om understøttelse af forordningens principper til it-leverandører
Artikel 28, stk. 1 (databehandler) A.15.1.1 (informationssikkerhedspolitik for leverandørforhold) A.15.1.2 (håndtering af sikkerhed i leverandøraftaler) A.13.2.1 (politikker og procedurer for informationsoverførsel)	Den dataansvarlige skal i aftalen med databehandlerne sikre sig, at de kan implementere de rette tekniske og organisatoriske foranstaltninger

A.13.2.2 (aftaler om informationsoverførsel)	
Artikel 28, stk. 2 (databehandler) A.15.1.1 (informationssikkerhedspolitik 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 informationsoverførsel)	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 informationsoverførsel) A.15.1.1 (informationssikkerhedspolitik 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 driftsprocedurer)	Den dataansvarlige skal kunne dokumentere: - Navn og kontaktinformation på dataansvarlig - 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 informationssikkerhedskontinuitet) A.17.1.2 (implementering af informationssikkerhedskontinuitet)	Personoplysninger skal kunne genskabes indenfor rimelig tid
Artikel 32, stk. 1, litra d (behandlingssikkerhed)	Sikkerhedstiltag skal testes og evalueres

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)	
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) A.16.1.5 (håndtering af informationssikkerhedsbrud)	Den dataansvarlige skal vurdere risici for de registrerede, og hvis der er høj risiko, skal de registrerede som udgangspunkt orienteres om bruddet
Artikel 35, stk. 1 (konsekvensanalyse)	Den dataansvarlige skal under hensyntagen til omfanget og følsomheden af personoplysninger, formålet og de involverede teknologier vurdere, om der i forhold til it-

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)	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 Artikel 47 (overførsel) A.15.2.1 (overvågning og gennemgang af leverandørydelser)	Den dataansvarlige bør kontrollere, at den dataansvarlige 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	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

beskyttelse af personoplysninger)	

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...