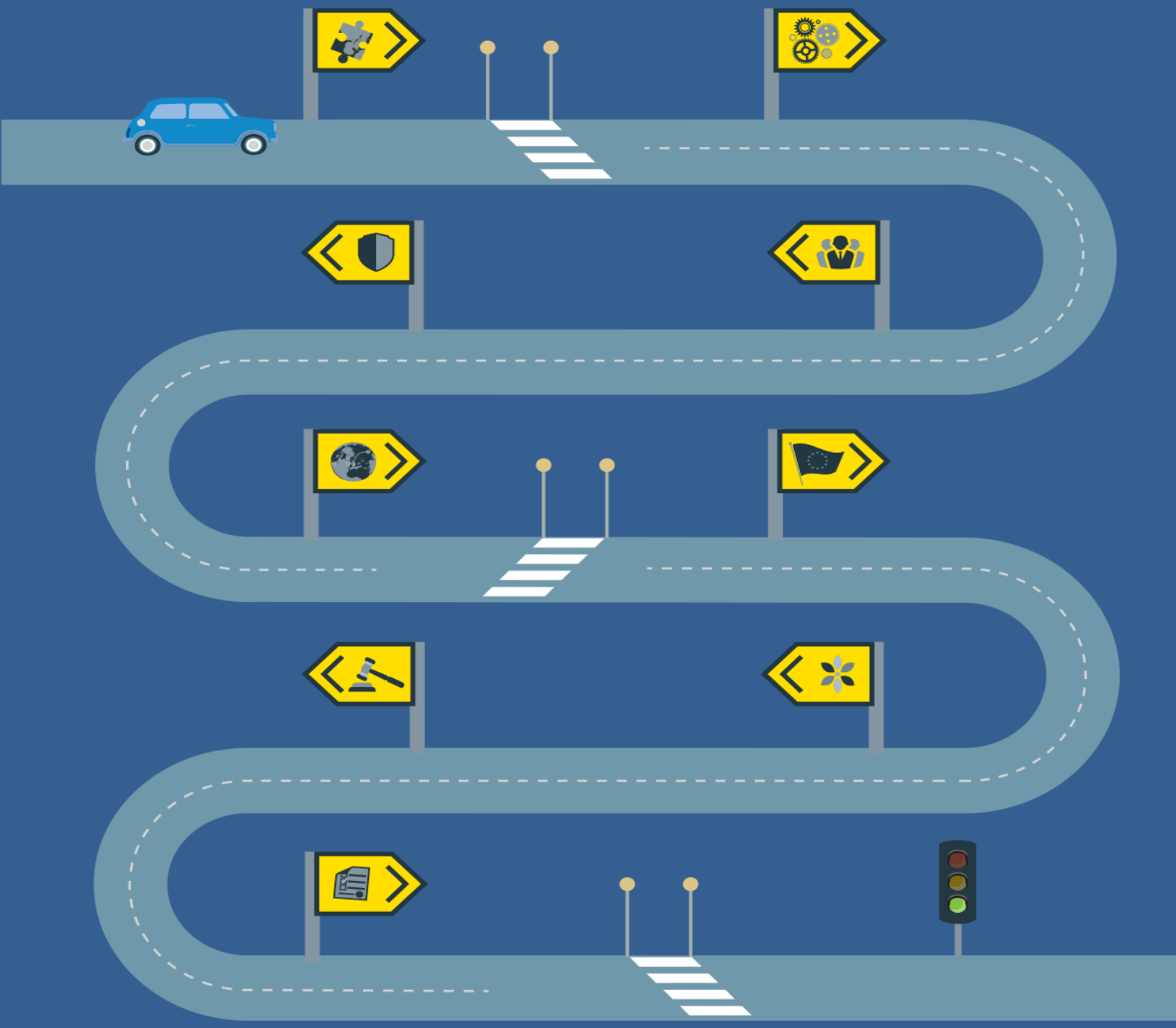
Bird&Bird&

Guide til den nye Persondataforordning

September 2016



Da Europa-Kommissionen offentliggjorde den nye Persondataforordning i januar 2012, affyrede den startskuddet til 4 års debat, forhandlinger og lobbyisme, som ikke tidligere er set i den Europæiske Union (EU). Denne guide opsummerer den forordning, som blev resultatet af denne proces – en lov, som giver Europas grundlæggende databeskyttelseslovgivning et grundigt eftersyn i en tid, hvor informationssystemer og digital handel understøtter vores tilværelse.

De ændringer, som den nye Persondataforordning varsler i 2018, er væsentlige og ambitiøse. Den mere end 200 sider lange forordning er en af de mest omfattende lovgivninger, som EU har vedtaget i de seneste år, og de nye principper som 'retten til at blive glemt', dataportabilitet, anmeldelsespligt ved sikkerhedsbrud og ansvarlighed (bare for at nævne nogle få eksempler) vil kræve en vis tilvænning. Selv dens juridiske form – en forordning og ikke et direktiv – gør Persondataforordningen til en usædvanlig lovgivning for jurister at analysere på.

Denne guide vil forsøge at opsummere de vigtigste ændringer, som den nye lovgivning introducerer, og at udpege de vigtigste forholdsregler, som virksomheder skal tage, når de forbereder sig på at skulle overholde den.

Vi har opdelt vores guide i kapitler, som i det store og hele følger forordningens opdeling, men hvert kapitel er underinddelt i temaer. Hvert underkapitel starter med et hurtigt resumé, en liste med de aktionspunkter, som vi foreslår, bliver prioriteret og vores vurdering af, i hvilken grad den analyserede del af Persondataforordningen vil medføre ændringer (i form af en trykmåler, der spænder fra grøn, som betyder en mindre ændring, til rød, der betyder en betydelig ændring). Vi har også i hvert underkapitel indsat vejskilte, der angiver, hvor du kan finde mere relevant kildemateriale i forordningen.

Europæisk lovgivning vedrørende personoplysninger har altid indeholdt en vis mængde jargon og fagudtryk, og den nye Persondataforordning er ingen undtagelse. For at hjælpe dem, som ikke kender disse udtryk i forvejen, har vi også indsat en ordliste.

Efterhånden som der kommer flere retningslinjer fra lovgiver, tilsynsmyndigheder og domstole om Persondataforordningen, og hvordan den skal implementeres, vil vi udgive opdateringer og vores egne retningslinjer. Kontakt os venligst, hvis du er interesseret i mere information. Indtil da håber vi, at du vil kunne bruge denne guide.

Jesper Langemark, partner

Nis Peter Dall, partner

Indholdsfortegnelse

Materielt og territorialt anvendelsesområde

» Resumé

- Sammenlignet med Direktiv 95/46/EC ("Persondatabeskyttelsesdirektivet"), som Persondataforordningen afløser, søger forordningen at udvide EU-persondatalovgivningens territoriale udstrækning.
  - Dataansvarlige og databehandlere, der er etableret i EU, er omfattet af forordningen, når personoplysninger bliver behandlet *"som led i aktiviteter"*, hvilket er bredt fortolket.
  - Persondataforordningen vil stadig finde anvendelse, selvom dataansvarlige og databehandlere ikke er etableret i EU, når: (1) en EU-borgers personoplysninger behandles i forbindelse med udbud af varer/tjenester; eller (2) hvis privatpersoners adfærd indenfor EU *"overvåges"*.
- Persondataforordningen tillader, at medlemsstaterne selv lovgiver på mange områder, selvom det er en forordning. Dette vil udfordre Persondataforordningens mål om ensartethed indenfor EU.
- Persondataforordningen blev endeligt vedtaget den 14. april 2016 og træder i kraft den 25. maj 2018.
- Der er visse aktiviteter, som Persondataforordningen ikke omfatter – herunder databehandling, der hører under "LEA"-direktivet på retshåndhævelsesområdet (the Law Enforcement Agencies Directive), databehandling med henblik på statens sikkerhed og databehandling, der udføres af privatpersoner udelukkende med personligt/privat formål.

☑ To-do liste

☐ Virksomheder, der ikke er etableret i EU, men som har EU-borgere som målgruppe, bør:

- forstå Persondataforordningens indvirkning; og
- fastlægge en strategi for, hvordan forordningen kan overholdes.

☐ Virksomheder, der arbejder indenfor områder, hvor "særlig"/sektorspecifik lovgivning er almindelig, bør:

- Vurdere, om det er nødvendigt med særlovgivning i medlemsstaten og søge at fremme sådan lovgivning; og
- Være opmærksom på, om sådan særlovgivning understøtter deres interesser.

Territorialt anvendelsesområde

Databehandlere og dataansvarlige, der er "etableret" i EU

Persondataforordningen finder anvendelse på alle virksomheder etableret i EU, hvor personoplysninger behandles "*som led i aktiviteter*", der udføres for sådanne virksomheder.

Hvis dette er tilfældet, gælder Persondataforordningen, uanset om selve persondatabehandlingen foretages indenfor eller udenfor EU.

Begrebet "*etablering*" blev vurderet af den Europæiske Unions Domstol i sagen *Weltimmo v NAIH (*C-230/14) fra 2015. Det blev bekræftet, at etablering er et bredt og fleksibelt begreb, som ikke er afhængig af juridisk form. En virksomhed kan være *"etableret"* der, hvor det udøver *"reel og faktisk aktivitet – også selvom den er minimal"* – via "*vedvarende foranstaltninger*" indenfor EU. Tilstedeværelsen af en enkelt repræsentant kan være tilstrækkelig. I denne sag blev Weltimmo betragtet som etableret i Ungarn, fordi der blev brugt en ungarsk hjemmeside til annoncering og salg af ungarske ejendomme (som dermed indebar, at salget blev betragtet som "*primært eller alene rettet mod dén medlemsstat*"), der blev brugt en lokal agent (som havde ansvaret for inkasso i Ungarn og som optrådte som repræsentant ved administrative og retlige procedurer), og der blev brugt en ungarsk postadresse og bankkonto – uagtet at Weltimmo var anmeldt som selskab i Slovakiet.

Virksomheder, som har salgskontorer i EU, som forestår markedsføring eller sælger reklamer, der er rettet mod EU-borgere, er sandsynligvis underlagt Persondataforordningen – eftersom den dermed forbundne behandling af personoplysninger anses for at være *"uløseligt forbundet"* med og dermed udført *"i sammenhæng med disse EU-virksomheders aktiviteter"* (*Google Spain SL, Google Inc. v AEPD, Mario Costeja González* (C-131/12)).

Virksomheder, der ikke er "etableret" i EU, som retter sig mod eller overvåger registrerede i EU

Virksomheder, der ikke er etableret i EU, er underlagt Persondataforordningen, hvis de behandler personoplysninger om registrerede, der befinder sig i EU, og behandlingsaktiviteterne vedrører:

- *"udbud af varer eller tjenester"* (uanset om betaling er påkrævet); eller
- "*overvågning*" af registreredes adfærd indenfor EU.

Det er ikke tilstrækkeligt, at en hjemmeside blot er tilgængelig for EU-borgere. Det skal være åbenbart, at virksomheden *"påtænker"*, at udbyde deres aktiviteter mod registrerede, der befinder sig i EU.

Kontaktoplysninger, der er tilgængelig i EU og anvendelse af den dataansvarliges lokale sprog er heller ikke tilstrækkelig. Dog vil anvendelse af europæisk sprog/valuta, muligheden for at afgive en ordre på dette andet sprog og henvisninger til brugere eller kunder fra EU være relevant.

EU-domstolen har i en anden sammenhæng undersøgt, hvornår en aktivitet (som fx udbud af varer eller tjenester) vil blive betragtet som "*rettet mod*" EU-medlemsstater (fx i "Bruxelles 1"-forordningen (44/2001/EC), der gælder for "*jurisdiktion…i civile og erhvervsmæssige anliggender*"). Kommentarerne til forordningen kan sandsynligvis bidrage til fortolkningen af det tilsvarende forhold i Persondataforordningen. Ud over de ovennævnte betragtninger tilføjer EU-domstolen, at en intention om at ville henvende sig til EU-kunder kan illustreres ved: (1) *"åbenbar"* bevis, som fx betaling til en søgemaskine, der giver en medlemsstats borgere lettere adgang, eller hvor udvalgte medlemsstater er nævnt ved navn; og (2) andre faktorer - eventuelt i forbindelse med hinanden - herunder den relevante aktivitets *"internationale karakter"* (fx visse turistaktiviteter), omtale af telefonnumre med international landekode, brug af top-level domænenavn ud over det, som tilhører det land, hvor den handlende er etableret (som fx .de eller .eu), beskrivelse af *"rejseplaner fra medlemsstater til stedet, hvor tjenesterne leveres"* og omtale af et *"internationalt klientel, der er sammensat af kunder, der er bosiddende i forskellige medlemsstater"*. Denne liste er "ikke

udtømmende" og spørgsmålet må afgøres fra gang til gang (*Pammer v Reederei Karl Schlüter GmbH & Co* og *Hotel Alpenhof v Heller* (Forenet sager *(*C-585/08) og (C-144/09)).

"Overvågning" indbefatter blandt andet sporing af privatpersoner online med henblik på at skabe profiler, herunder hvor dette anvendes til at analysere/forudsige personlige præferencer, adfærd og holdninger.

Virksomheder, der ikke er etableret i EU, og hvis behandlingsaktiviteter retter sig mod eller overvåger EU-borgere, skal udpege en repræsentant, der er bosiddende i EU.

I henhold til Databeskyttelsesdirektivet skal virksomheder, der henvender sig til registrerede i EU, kun overholde EU-reglerne, hvis behandlingen af oplysninger sker under benyttelse af "hjælpemidler", der befinder sig indenfor EU. Dette foranledigede nationale tilsynsmyndigheder, som søgte at opnå jurisdiktion, til at udvikle argumentation for, at det at anbringe cookies eller anmode brugere om at udfylde spørgeskemaer kunne sidestilles med at benytte "hjælpemidler", der befinder sig indenfor EU. Det vil nu blive lettere at påvise, at EU-lovgivningen gælder. (Selvom det kan blive ligeså vanskeligt som før at håndhæve lovgivningen, hvis virksomhederne ikke har en tilstedeværelse i EU).

Hvor EU-medlemsstaters nationale ret gælder i medfør af folkeretten

Som eksempler på dette angiver præambel 25 en medlemsstats diplomatiske eller konsulære repræsentation.

Undtagelser

Visse aktiviteter falder helt uden for Persondataforordningens anvendelsesområde (angivet nedenfor).

Derudover anerkender Persondataforordningen, at databeskyttelsesrettigheder ikke er absolutte og skal afvejes (proportionelt) med andre grundlæggende rettigheder – herunder *"frihed til at oprette og drive egen virksomhed"*. (For medlemsstaters mulighed for at indføre undtagelser, se afsnittet vedrørende begrænsninger og specifikke behandlingssituationer). Da Persondataforordningen er skærpet på mange områder og indfører mere pisk end gulerod, kan det måske være nyttigt for virksomheder at bide mærke i dette udsagn fra præambel (4).

Persondataforordningen gælder ikke for behandling af personoplysninger (disse generelle undtagelser er meget lig de tilsvarende bestemmelser i databeskyttelsesdirektivet):

- I forbindelse med aktiviteter, der falder uden for EU-lovgivningens anvendelsesområde (fx aktiviteter, der vedrører national sikkerhed).

- Der angår EU's fælles udenrigs- og sikkerhedspolitik.

- Som udføres af kompetente myndigheder med det formål at forebygge, efterforske, afsløre, eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner (fx hvor LEA-direktivet - Law Enforcement Agencies Directive),1 der oprindeligt er baseret på COM(2012) 10 og som i henhold til den politiske aftale af 15. december 2015 sammen med Persondataforordningen, nu gælder;

- Der udføres af EU-institutioner, hvor Forordning 45/2001/EC fortsat vil finde anvendelse i stedet for Persondataforordningen. Denne Forordning skal opdateres for at sikre overensstemmelse med Persondataforordningen; og

- Der udføres af en fysisk person *"som led i rent personlige eller familiemæssige aktiviteter"*. Dette inkluderer korrespondance og føring af en adressefortegnelse - men det dækker også sociale netværk og andre online aktiviteter, der foretages med sociale eller private formål. Dette udgør en mulig udvidelse af undtagelsen fra principperne, der blev fastslået i *Bodil Lindqvist* (C-101/01), før de sociale medier gjorde deres indtog. EU-domstolen anførte i denne sag, at det at offentliggøre oplysninger på Internettet, *"så oplysningerne er tilgængelige for en ubestemt mængde af mennesker",* ikke kunne falde under denne undtagelse, som domstolen anførte skulle begrænses til aktiviteter, der "*alene udføres i forbindelse med enkeltpersoners privat- eller familieliv"*. Bemærk også, at Persondataforordningen stadig vil være gældende for dataansvarlige og databehandlere, som *"tilvejebringer midlerne til behandling af personoplysninger"*, som falder indenfor denne undtagelse.

- Der udføres af en fysisk person *"som led i rent personlige eller familiemæssige aktiviteter"*. Dette inkluderer korrespondance og føring af en adressefortegnelse - men det dækker også sociale netværk og andre online aktiviteter, der foretages med sociale eller private formål. Dette udgør en mulig udvidelse af undtagelsen fra principperne, der blev fastslået i *Bodil Lindqvist* (C-101/01), før de sociale medier gjorde deres indtog. EU-domstolen anførte i denne sag, at det at offentliggøre oplysninger på Internettet, *"så oplysningerne er tilgængelige for en ubestemt mængde af mennesker",* ikke kunne falde under denne undtagelse, som domstolen anførte skulle begrænses til aktiviteter, der "*alene udføres i forbindelse med enkeltpersoners privat- eller familieliv"*. Bemærk også, at Persondataforordningen stadig vil være gældende for dataansvarlige og databehandlere, som *"tilvejebringer midlerne til behandling af personoplysninger"*, som falder indenfor denne undtagelse.

Det er anført, at Persondataforordningen skal gælde *"uden at det berører"* reglerne i E-handelsdirektivet (2000/31/EC), især mht. til de regler, der angår *"tjenesteydernes formidleransvar*" (og hvis intention er, at begrænse deres risiko for bødestraf og strafansvar, hvor de kun *hoster*, *cacher* eller optræder som "*ren videreformidler*"). Forholdet til E-handelsdirektivet er ikke ukompliceret - da direktivet anfører, at forhold vedrørende persondatabehandling er udenfor dens anvendelsesområde og

[1] Fuld titel: Direktiv *"om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger ved kompetente myndigheder med henblik på forebyggelse, efterforskning, afsløring eller retsforfølgning af straffelovsovertrædelser eller fuldbyrdelse af strafferetlige sanktioner og den fri udveksling af sådanne oplysninger."*

"alene reguleres" af relevant databeskyttelseslovgivning. Dette kan læses som værende overensstemmende, hvis det antages, at internettjenesteudbyderens ansvar for brugernes handlinger afgøres ud fra E-handelsdirektivet, men at andre forhold (som fx pligten til at slette og rette data eller en internettjenesteudbyders pligter i forhold til dennes egen brug af personoplysninger) afgøres af Persondataforordningen. Dette punkt er dog stadig uafklaret.

Forordningen versus national lovgivning

Persondataforordningen vil være direkte gældende i medlemsstaterne, forstået således at det ikke er nødvendigt at implementere den i national lovgivning.

Persondataforordningen giver dog i mange tilfælde medlemsstaterne mulighed for at lovgive om anliggender vedrørende persondatabeskyttelse. Herunder anliggender, hvor behandlingen af personoplysninger skal overholde retlige forpligtelser, vedrører opgaver, der er i offentlighedens interesse eller udføres af en offentlig myndighed. Mange af artiklerne angiver også, at deres bestemmelser kan blive nærmere fastsat eller begrænset af lovgivningen i medlemsstaterne.

Virksomheder, der arbejder på områder, hvor der ofte findes *"særregler"* (fx i sundhedssektoren eller den finansielle sektor) bør: (1) overveje, om de kunne drage nytte af sådanne *"særregler"*, som kunne præcisere eller liberalisere Persondataforordningen; og (2) søge at fremme sådan særlovgivning. De bør også holde øje med andre medlemsstater, der forsøger at indføre *"særregler"*, som kan vise sig at være restriktive eller uoverensstemmende på tværs af medlemsstaterne.

Hvor kan jeg læse mere?

Materielt anvendelsesområde	*Artikel 2* *Præambel 4 og 7-21.*
Geografisk anvendelsesområde	*Artikel 3* *Præambel 22-25*

Nye og væsentlig ændrede begreber

» Resumé

Persondataforordningen indfører væsentlige ændringer, herunder i forhold til de følgende begreber:

- **Gennemsigtighed og samtykke** – dvs. i forhold til de oplysninger, der skal afgives til de registrerede, og det samtykke fra de registrerede, der kræves for at være berettiget til at anvende deres personoplysninger. Persondataforordningens krav om, at samtykke skal være entydigt og ikke kan udledes af inaktivitet, betyder, at mange samtykkeerklæringer vedrørende behandling af persondata vil skulle tilrettes.
- **Børn og samtykke** – i relation til online - tjenester kræves der forudgående samtykke fra forældre for at anvende personoplysninger om barnet, hvis barnet er under 13 år. Medlemsstater kan frit indføre egne regler for børn fra 13 år og til og med 15 år. Hvis de vælger ikke at indføre egne regler, er forældres samtykke påkrævet for børn under 16 år.
- **Omfattede oplysninger** – definitionerne på "personoplysninger" og "følsomme oplysninger" er blevet udvidet, fx er genetiske og biometriske oplysninger nu inkluderet i sidstnævnte.
- **Pseudonymisering** – en teknik, der forøger graden af persondatabeskyttelse, og hvor oplysninger, der kan identificere en specifik person, opbevares separat og under sådanne tekniske og organisatoriske foranstaltninger, at det sikres, at personen ikke kan identificeres.
- **Brud på persondatasikkerheden** – nye regler om anmeldelse af sikkerhedsbrud bliver indført for alle dataansvarlige uanset branche.
- **Privacy by design og dokumentationskrav** – virksomheder skal implementere betydelige nye tekniske og organisatoriske foranstaltninger for at påvise, at de overholder Persondataforordningen.

√ To-do liste

X	Der skal ikke gøres noget.

Bestemmelserne i Persondataforordningen og de forpligtelser, forordningen medfører, er omfattende, men de følgende emner falder særligt i øjnene som helt nye eller ændrede begreber. Der findes nærmere information om hvert emne andre steder i guiden.

Samtykke

Betingelserne for at opnå samtykke er blevet skærpet:

- Den registrerede har til enhver tid ret til at tilbagekalde sit samtykke; og
- Der kræves separat samtykke for hver behandlingsaktivitet, og det formodes, at tvungen samtykke eller samtykke, som ikke klart kan skelnes fra andre forhold, ikke vil være gyldig. Det forventes, at der kommer yderligere vejledninger, men virksomheder skal gennemgå deres eksisterende samtykkeerklæringer for at sikre, at de giver udtryk for en frivillig handling.

Samtykke er ikke den eneste lovlige grund, der kan berettige behandling af personoplysninger. Der findes andre grunde fx hvis behandlingen er nødvendig for opfyldelse af en kontrakt, overholdelse af en retlig forpligtelse, eller hvis behandlingen er nødvendig af hensyn til vitale interesser.

Mere information om dette emne findes i afsnittene Samtykke, Børn og Særlige kategorier af oplysninger og lovlig behandling (under kapitlet vedrørende Principper).

Gennemsigtighed

Virksomheder skal afgive omfattende oplysninger til de registrerede om behandling af deres personoplysninger.

Persondataforordningen kombinerer de forskellige forpligtelser om gennemsigtighed, som er gældende rundt om i EU. Listen over de oplysninger, der skal afgives, fylder 6 sider i Persondataforordningen, og alligevel skal dataansvarlige lykkes med det, som EU-lovgivere ikke har kunnet gøre, nemlig at fremføre oplysningerne på en kortfattet, gennemskuelig, forståelig og lettilgængelig måde.

Persondataforordningen foreslår at man anvender standardiserede ikoner, og Kommissionen kan vælge at indføre disse på et senere tidspunkt via delegerede retsakter.

Mere information om dette emne findes i afsnittet Oplysningspligt (under kapitlet om Individets rettigheder).

Børn

Børn under 13 år kan aldrig selv afgive samtykke til behandling af deres personoplysninger i forbindelse med online-tjenester.

For børn mellem 13 og 15 år (inklusiv) er den generelle regel, at der skal indhentes samtykke fra forældre for at kunne behandle disse børns personoplysninger i forbindelse med online-tjenester, med mindre den enkelte medlemsstat lovgiver om at nedsætte aldersgrænsen – grænsen kan dog aldrig nedsættes til under 13 år.

Børn på 16 år og opefter kan selv afgive samtykke til behandling af deres personoplysninger.

Der findes ingen specifikke regler om forældresamtykke i forbindelse med offline behandling af personoplysninger: Medlemsstatens sædvanlige regler vil gælde i dette tilfælde.

Mere information om dette emne findes i afsnittet Børn (under kapitlet vedrørende Principper).

Personoplysninger/Følsomme oplysninger ("særlige kategorier af oplysninger")

Persondataforordningen gælder for oplysninger, som en levende person kan identificeres ud fra eller

gøres identificerbar (for enhver), uanset om det er direkte eller indirekte. Direktivets tekst mht. 'alle de midler, der med rimelighed kan tænkes anvendt' for at identificere en person bibeholdes.

Persondataforordningens præambler fremhæver, at visse kategorier af online-oplysninger kan være personoplysninger - online-identifikatorer, identifikatorer af enheder, cookies og IP-adresser nævnes som eksempler. Det forventes, at der kommer nærmere regler og juridisk vejledning, fx forventes det, at EU-domstolen vil komme med en præcisering i forhold til IP-adressers status i forbindelse med en henvisning fra den tyske højesteret, Bundesgerichtshof.

Det nuværende begreb følsomme oplysninger (som kaldes *"særlige kategorier"* i Persondataforordningen) bliver bibeholdt og udvidet til at dække genetisk data og biometrisk data. Som det er tilfældet i det nuværende Databeskyttelsesdirektiv, er sådanne data underlagt strengere betingelser end andre typer personoplysninger.

Hvor kan jeg læse mere?

Definitioner *Artikel 2* *Diverse (men hovedsageligt 24-32)*

Pseudoanonymisering

Et nyt begreb, som beskriver en teknik til at behandle personoplysninger på en sådan måde, at de 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, så det sikres, at de ikke kan anvendes til at identificere personen bag.

Pseudoanonymiserede oplysninger er stadig personoplysninger, men der opfordres til, at pseudoanonymisering anvendes, fx:

- Er det et forhold, der skal tages med i betragtning, når det vurderes, om behandlinger er "*i strid*" med formålet med den oprindelige indsamling og behandling af oplysningerne;
- Er der et eksempel på en teknik, der kan være med til at opfylde kravene til at implementere *"privacy by design and by default"* (jf. afsnittet Brud på persondatasikkerheden og anmeldelsespligt);
- Kan være med til at opfylde Persondataforordningens forpligtelser om persondatasikkerhed (jf. afsnittet Brud på persondatasikkerheden og anmeldelsespligt); og
- Hvis man ønsker at anvende personoplysninger til historisk eller videnskabelig research eller til statistiske formål, fremhæves brugen af pseudoanonymiserede oplysninger som en løsning.

Brud på persondatasikkerheden og anmeldelsespligt

Persondataforordningen indfører en anmeldelsespligt i forbindelse med brud på persondatasikkerheden, uanset hvilken branche man arbejder i.

Anmeldelsespligten (til tilsynsmyndighederne og til den registrerede) udløses potentielt af *"hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger"*.

Mere information om dette emne findes i afsnittet om Brud på persondatasikkerheden og anmeldelsespligt.

Datasikkerhed by design/ dokumentationskrav

Virksomheder skal kunne påvise, at de overholder Persondataforordningens principper, herunder implementere visse tekniske og organisatoriske foranstaltninger, der betegnes som "*databeskyttelse gennem design*" (fx brug af pseudoanonymiseringsteknikker), uddannelse af personale og udførelse af audit.

Hvis der udføres behandlinger, der indebærer en "høj risiko" (som fx overvågning, systematisk vurdering eller behandling af særlige kategorier af oplysninger), skal en detaljeret konsekvensanalyse ("DPIA") foretages og dokumenteres. Hvis DPIA'en viser, at der er en høj risiko for de registrerede, skal den dataansvarlige anmelde dette til tilsynsmyndigheden, og tilsynsmyndigheden skal høres i forhold til dennes vurdering af de forholdsregler, der foreslås i DPIA'en, til minimering af risikoen ved behandlingen.

Dataansvarlige og databehandlere kan beslutte at udpege en databeskyttelsesansvarlig ("DPO"). Dette er et krav for offentlige myndigheder, og i forhold til virksomheder, som er involveret i særligt følsomme aktiviteter. Virksomheder i samme koncern kan udpege en fælles databeskyttelsesrådgiver.

Mere information om dette emne kan findes i afsnittet Ansvarlig datastyring.

Individers udvidede rettigheder

Persondataforordningen fastlægger en lang række eksisterende og nye rettigheder for individer med hensyn til virksomheders behandling af deres personoplysninger.

Fx retten til at blive glemt, retten til dataportabilitet, retten til indsigelse mod visse behandlinger og mod automatiske individuelle afgørelser, herunder profilering.

Mere information om dette emne kan findes i afsnittet Individets rettigheder.

Tilsynsmyndigheder og det Europæiske Databeskyttelsesråd

Persondatabeskyttelseskontrolorganer kaldes tilsynsmyndigheder i Persondataforordningen.

En ledende tilsynsmyndighed, der er beliggende i den medlemsstat, hvor virksomheden har sin hovedvirksomhed, vil føre tilsyn med, at virksomheden overholder Persondataforordningen.

Det Europæiske Databeskyttelsesråd vil blive oprettet med henblik på at komme med skøn i særlige problemstillinger og dømme i tvister, der udspringer af tilsynsmyndigheders beslutninger.

Mere information om dette emne kan findes i afsnittet Tilsynsmyndigheder.

Hvor kan jeg læse mere?

Definitioner *Artikel 4* *Diverse (men hovedsageligt 51-62)*

Persondataprincipper

Resumé

- Persondataprincipperne er blevet revideret men er i stor udstrækning lig principperne i direktiv 95/46/EF ("Databeskyttelsesdirektivet"): Rimelighed, lovlighed, gennemsigtighed, formålsbegrænsning, dataminimering, rigtighed, opbevaringsbegrænsning, integritet og fortrolighed.
- Et nyt ansvarlighedsprincip gør dataansvarlige ansvarlige for at påvise overholdelse af persondataprincipperne.

To-do liste

☐	Gennemgå persondatapolitikkerne, adfærdskodeks og undervisningsmateriale for at sikre, at disse er i overensstemmelse med de reviderede principper.
☐	Identificer måder at påvise, "overholdelse af principperne" – f.eks. ved overholdelse af godkendte adfærdskodeks, skriftlig dokumentation af beslutninger, der vedrører databehandling og, hvor det er passende, foretag konsekvensanalyser.

Kommentar

Principperne i persondataforordningen er i høj grad de samme som principperne i databeskyttelsesdirektivet, men der er nogle nye elementer, som er fremhævet med kursiv nedenfor.

Lovlighed, rimelighed og gennemsigtighed

Persondata skal behandles lovligt, rimeligt og *på en gennemsigtig måde over for den registrerede*.

Formålsbegrænsning

Persondata kan indsamles til udtrykkeligt angivne og legitime formål og må ikke behandles på en måde, der er uforenelig med disse formål. Viderebehandling af persondata til *arkiveringsformål i samfundets interesse* eller til videnskabelig eller historisk forskning eller statistiske formål kan ikke anses for uforenelige med de oprindelige formål. Betingelserne i § 89, stk. 1 (som vedrører beskyttelse og begrænsninger i forbindelse med behandling til sådanne formål) skal dog overholdes.

Dataminimering

Persondata skal være tilstrækkelige, relevante og begrænset til det, der er nødvendigt i forhold til de formål, hvortil de behandles.

Rigtighed

Persondata skal være korrekte og om nødvendigt ajourførte. Der skal tages ethvert rimeligt skridt for at sikre, at persondata, der er urigtige i forhold til de formål, som de behandles til, straks slettes eller berigtiges.

Opbevaringsbegrænsning

Persondata skal opbevares *på en sådan måde, at det ikke er muligt at identificere de registrerede* i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de pågældende persondata behandles. Persondata kan opbevares i længere tidsrum for så vidt, at dataene alene behandles til arkiv*formål i samfundets interesse*, eller videnskabelig eller historisk forskning eller statistiske formål i overensstemmelse med § 89, stk. 1 og under forudsætning af, at der implementeres passende tekniske og organisatoriske foranstaltninger.

Integritet og fortrolighed

Personoplysninger skal behandles på en sådan måde, at der sikres en tilstrækkelig sikkerhed for de pågældende persondata, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse, under anvendelse af passende tekniske eller organisatoriske foranstaltninger.

Ansvarlighed

Den dataansvarlige er ansvarlig for og *skal kunne påvise overholdelse* af disse principper.

Hvor kan jeg læse mere?

Artikel 5 og præambel 39

Lovlig behandling og formålsbestemthed

Resumé

- Hjemlerne for behandling af persondata i henhold til Persondataforordningen er stort set den samme som i Databeskyttelsesdirektivet.
- Der er nye begrænsninger for brug af samtykke og for behandling af børns persondata.
- Der er specifikke begrænsninger for muligheden for at kunne anvende en "legitim interesse" som hjemmel for behandlingen, ligesom der indgår nogle beskrivelser af hvornår en sådan hjemmel kan benyttes.
- Der er en ikke-udtømmende liste med faktorer, som skal tages med i betragtning, når man afgør, om behandlingen af data til et nyt formål er foreneligt med de formål, hvortil dataene oprindeligt blev indsamlet.

To-do liste

☐	Du skal sikre dig, at du kender hjemlen til de behandlinger, som din virksomhed benytter, og undersøg, at hjemlen stadig er gyldig i medfør af Persondataforordningen.
☐	Når samtykke benyttes, skal du sikre, at samtykkes kvalitet er i overensstemmelse med de nye krav (se mere under afsnittet om samtykke).
☐	Overvej, om de nye regler vedrørende børns persondata vil vedrøre dig, og i givet fald hvilke nationale regler, som du skal følge (se mere under afsnittet om børn).
☐	Du skal sikre, at jeres interne styringsprocesser gør det muligt at dokumentere, hvordan beslutninger om at benytte data til viderebehandling er truffet, og at relevante faktorer er blevet overvejet.

Kommentar

Persondataforordningens artikel 6, stk. 1, fastsætter hjemlerne for lovlig behandling af personoplysninger (for bestemmelser vedrørende særlige kategorier af oplysninger, se afsnittet om Særlige kategorier af oplysninger og lovlig databehandling). Disse hjemler er stort set lig med hjemlerne i Databeskyttelsesdirektivet:

6, 1 a – Den registreredes samtykke

Persondataforordningen har en mere restriktiv tilgang til samtykke. Forordningen forsøger især at sikre, at samtykke er specifikt til bestemte formål for behandlingen (se afsnittet om Samtykke). Særlige bestemmelser gælder for børns persondata (se afsnittet om Børn).

6, 1 b – Nødvendigt for opfyldelsen af en kontrakt med den registrerede eller til gennemførelse af foranstaltninger forud for indgåelse af en kontrakt

Ingen ændringer i forhold til Databeskyttelsesdirektivet.

6, 1 c – Nødvendigt for overholdelse af retlige forpligtelser

Dette er en kopi af en tilsvarende hjemmel i Databeskyttelsesdirektivet. Artikel 6,3 og præambel 41 og 45 gør det klart, at den retlige forpligtelse skal være:

- En forpligtelse i henhold til EU- retten eller medlemsstaternes nationale ret, som den dataansvarlige er underlagt. Forpligtelser for koncernforbundne selskaber og forpligtelser, der har sin oprindelse uden for EU vil sandsynligvis ikke være gældende, og
- "*Klar og præcis*", og anvendelsen skal være forudsigelig for dem, som den gælder for.

Præamblerne gør det klart, at den relevante "retlige forpligtelse" ikke behøver at være lovbestemt (retspraksis vil være tilstrækkeligt, hvis det kan bestå testen om "*klar og præcis*"). En retlig forpligtelse kan gælde for flere behandlinger udført af den dataansvarlige, så det kan være, at det ikke er nødvendigt at identificere en bestemt retlig forpligtelse for hver enkelt behandling.

6, 1 d – Nødvendigt for at beskytte de registreredes eller andres vitale interesser

Præambel 46 skriver, at denne hjemmel kan finde anvendelse, når behandlingen er nødvendig af humanitære årsager (f.eks. overvågning af epidemier) eller i forbindelse med humanitære nødssituationer (f.eks. katastrofer). Præamblet angiver, at hvor persondata behandles i andres vitale interesser, kan man kun anvende denne hjemmel for behandlingen, hvis der ikke findes en anden hjemmel.

6, 1 e – Nødvendigt for udførelsen af en opgave af samfundets interesse eller til udøvelse af den dataansvarliges offentlige myndighedsudøvelse

Artikel 6, stk. 3 og præambel 45 gør det klart, at denne hjemmel kun gælder, hvor udførelse af opgaven eller den dataansvarliges autoritet, er foreskrevet i EU-retten eller i medlemsstaternes nationale ret, som den dataansvarlige er underlagt.

6, 1 f – Nødvendigt for at kunne forfølge en legitim interesse

Denne hjemmel kan ikke længere benyttes af offentlige myndigheder, der behandler persondata, som led i udførelsen af deres opgaver. Præamblerne 47-49 indeholder flere detaljer om, hvad der kan anses som en "*legitim interesse*". (Læs mere i afsnittet om Legitim interesse).

Medlemsstater kan introducere specifikke bestemmelser med henblik på overholdelse af artikel 6,1c og 6, 1e (behandling på grundlag af en retlig forpligtelse eller udførelsen af en opgave i samfundets interesse eller til udøvelse af den dataansvarliges offentlige myndighedsudøvelse), herunder i forhold til andre specifikke behandlingssituationer (f.eks. journalistik og forskning). Dette vil sandsynligvis resultere i flere variationer på tværs af EU. (Læs mere i afsnittet om Begrænsninger og specifikke behandlingssituationer).

Formålsbestemthed

Persondataforordningen fastsætter også reglerne (i artikel 6, 4) vedrørende de faktorer, som den dataansvarlige må tage i betragtning, når det skal vurderes, om et nyt behandlingsformål er foreneligt med det formål, hvortil dataene oprindeligt blev indsamlet. I det tilfælde, hvor denne behandling ikke er baseret på et samtykke eller EU-retten eller medlemsstaternes nationale ret vedrørende de tilfælde beskrevet i artikel 23, bør de følgende faktorer over-

vejes for at afgøre om et nyt behandlingsformål er foreneligt med det oprindelige formål:

- Enhver forbindelse mellem de oprindelige og de påtænkte formål;
- Den sammenhæng, hvori oplysningerne er indsamlet (navnlig med hensyn til forholdet mellem den registrerede og den dataansvarlige);
- Oplysningernes art (især om det er særlige kategorier af oplysninger eller oplysninger vedrørende kriminelle forhold);
- De mulige konsekvenser ved den påtænkte viderebehandling; og
- Fornødne garantier (inklusiv kryptering eller pseudonymisering).

Præambel nr. 50 indikerer, at viderebehandling til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål skal anses for at være forenelig med de formål, som persondataene oprindeligt blev indsamlet til (læs mere i afsnittet on Begrænsninger og specifikke behandlingssituationer).

Hvor kan jeg læse mere?

Artikel 6-11 præambel 40-57

Legitime interesser

» Resumé

- Med undtagelse af den bestemmelse, der retter sig mod offentlige myndigheder, er en "*legitim interesse*" som hjemmel for behandling ikke væsentligt forandret i Persondataforordningen.
- Offentlige myndigheder vil ikke kunne anvende en "*legitim interesse*" med henblik på at lovliggøre databehandling, der udføres som led i udførelsen af deres opgaver.
- Dataansvarlige, som anvender en "*legitim interesse*" som hjemmel, skal foretage registreringer af de vurderinger, de har foretaget, således at de kan dokumentere, at de nøje har overvejet de registreredes rettigheder og frihedsrettigheder.

√ To-do liste

☐	Du skal sikre dig, at du kender hjemlen til de behandlinger, som din virksomhed benytter, og undersøg, at hjemlen stadig er gyldig i medfør af Persondataforordningen (se mere i afsnittet om Lovlig behandling og formålsbestemthed).
☐	Hvis din virksomhed er en offentlig myndighed, som benytter en "*legitim interesse*" som hjemmel til behandling af persondata i forbindelse med udførelse af jeres opgaver, bør I finde et andet retsgrundlag for databehandlingen (f.eks. hvis behandlingen er nødvendig i samfundets interesse eller ved offentlig myndighedsudøvelse).
☐	I de tilfælde, hvor man anvender en "legitim interesse" som hjemmel for behandlingen, skal det sikres, at beslutninger, der tages i forhold til afvejningen af den dataansvarliges interesser (eller den relevante tredjepart) og de registreredes rettigheder, er dokumenteret. Dette gælder især, hvis det vedrører børn. Det skal også sikres, at de registrerede med rimelighed kan forvente, at deres data behandles på grundlag af den dataansvarliges eller den relevante tredjeparts legitime interesser.
☐	Hvis man benytter en "legitim interesse" som hjemmel for behandlingen, skal det sikres, at dette er beskrevet i den information, som den registrerede skal modtage i henhold til artikel 13 og 14 (læs mere i afsnittet om Oplysningspligt).

Kommentar

Artikel 6, stk. 1 i Persondataforordningen specificerer, at databehandling kun er lovlig, når mindst én af bestemmelserne i artikel 6, stk. 1 a-f er opfyldt.

Artikel 6, stk. 1 f er opfyldt, når:

"Behandling er nødvendig for, at den dataansvarlige eller en tredjemand kan forfølge en legitim interesse, medmindre den registreredes interesser eller grundlæggende rettigheder og frihedsrettigheder, der kræver beskyttelse af personoplysninger, går forud herfor, navnlig hvis den registrerede er et barn. Dette gælder ikke for behandling, som offentlige myndigheder foretager som led i udførelsen af deres opgaver."

Dette er hovedsageligt en gengivelse af den tilsvarende bestemmelse i Databeskyttelsesdirektivet, med undtagelse af, at:

- Behovet for specifikt at overveje børns interesser og rettigheder er nyt (se afsnittet om Børn). I praksis vil denne tilføjelse kræve, at den dataansvarlige sikrer, at enhver beslutning om at behandle oplysninger vedrørende børn ved anvendelse af en "*legitim interesse*" som hjemmel for behandlingen er nøje dokumenteret, og at en risikovurdering er udført; og

- En *"legitim interesse*" som hjemmel for behandlingen ikke længere kan benyttes af offentlige myndigheder i forbindelse med databehandling som led i udførelsen af deres opgaver.

Hvad er legitime interesser?

Præamblerne giver eksempler på databehandling, som kan udgøre legitime interesser. Disse inkluderer:

- Præambel 47: Behandling til direkte markedsføring eller til at forebygge svig;

- Præambel 48: Overførsel af personoplysninger inden for en koncern til interne administrative formål, herunder behandling af kunders og medarbejderes personoplysninger (bemærk, at internationale overførselskrav stadig gælder) (se afsnit om Overførsel af personoplysninger til tredjelande);

- Præambel 49: Behandling til at sikre net- og informationssikkerhed, herunder til at forhindre uautoriseret adgang til elektroniske kommunikationsnet samt til at stoppe beskadigelser på computersystemer og elektroniske kommunikationssystemer.

Præambel 47 angiver også, at dataansvarlige bør overveje de registreredes forventninger, når de vurderer, om de registreredes interesser vejer tungere end de dataansvarliges legitime interesser. De registreredes fundamentale interesser og rettigheder "*kan navnlig gå forud*" for den dataansvarliges interesser i de tilfælde, hvor de registrerede "*ikke med rimelighed forventer viderebehandling*".

Information skal nu beskrive legitime interesser

Hvor en "legitim interesse" benyttes som hjemmel til at behandle persondata, skal dette nu specificeres i den relevante information i henhold til artikel 13(1)(d) og 14(2)(b).

Adfærdskodeks

Ifølge artikel 40 skal medlemsstaterne, tilsynsmyndighederne, det Europæiske Databeskyttelsesråd og Kommissionen tilskynde til udarbejdelse af adfærdskodekser indenfor en lang række emner, herunder de legitime interesser, der forfølges af den dataansvarlige i specifikke sammenhænge. Medlemmer af fagforeninger eller lignende virksomheder skal passe på med at udarbejde disse kodekser, som kan medføre yderligere krav.

Dataoverførsel – nyt grundlag, som nok aldrig bliver benyttet i praksis

Artikel 49(1) angiver, at overførsel af data kan ske på baggrund af "vægtige legitime interesser", hvis overførslen ikke gentages. Dette gælder kun for et begrænset antal registrerede, og hvor den dataansvarlige har vurderet de konkrete omstændigheder og sikret et tilstrækkeligt beskyttelsesniveau. Denne hjemmel til overførsel af data kan kun anvendes, hvis den dataansvarlige ikke kan anvende andre hjemler, herunder Kommissionens Standardkontraktbestemmelser, Binding Corporate Rules

(BCRs), godkendte kontrakter og alle fra fravigelserne i artikel 49(1) (a)-(g). Den dataansvarlige vil så skulle informere tilsynsmyndigheden om, at man benytter dette grundlag for overførslen. Det forekommer usandsynligt, at en virksomhed vil kunne dokumentere, at den ikke kunne benytte andre grundlag for overførslen (se mere i afsnittet om Dataoverførsler).

Hvor kan jeg læse mere?

Artikel 6(1)(f), 13(1)(d), 14(2)(b) og 49(1) *Præambel 47-49*

Samtykke

Resumé

- Samtykke er reguleret flere steder i Persondataforordningen.

  Yderligere krav inkluderer et effektivt forbud mod et "*samlet*" samtykke og tilbud om serviceydelser, som er betinget af afgivelse af samtykke.

- Samtykke skal nu også klart kunne skelnes fra andre forhold, skal gives i en skriftlig erklæring i et klart og enkelt sprog og skal kunne tilbagekaldes lige så let som det afgives.

- Særlige regler gælder for børn, hvad angår informationssamfundstjenester.

To-do liste

- [ ] Du skal sikre dig, at du kender hjemlen til de behandlinger, som din virksomhed benytter, og undersøg, at hjemlen stadig er gyldig i medfør af Persondataforordningen (se mere i afsnittet om Lovlig behandling og formålsbestemthed).
- [ ] Overvej, om bestemmelserne vedrørende børn vil påvirke dig, og i så fald hvilke nationale regler, du skal overholde for at indhente samtykke (se mere i afsnittet om Børn).
- [ ] Hvis din virksomhed benytter samtykke til at behandle persondata til videnskabelige formål, kan du overveje at give de registrerede mulighed for kun at afgive samtykke til visse forskningsområder eller dele af forskningsprojekter.

- [ ] I det tilfælde, at samtykke benyttes som hjemmel for behandlingen, bør det sikres, at:

  - Samtykket er aktivt og ikke er afgivet ved tavshed, inaktivitet eller forudafkrydsede felter;
  - Samtykket til databehandling er i et klart og tydeligt sprog og er adskilt fra andre forhold;
  - Levering af en tjenesteydelse ikke er betinget af et samtykke til behandling af personoplysninger, som ikke er nødvendig for, at tjenesteydelsen kan leveres;
  - Registrerede er informeret om, at de har ret til at tilbagekalde deres samtykke til enhver tid, men at dette ikke vil berøre lovligheden af den behandling, der er sket baseret på samtykket inden tilbagekaldelsen;
    - Der er lette metoder til at tilbagekalde samtykket, herunder metoder, som benytter samme medie som i første omgang benyttes til at indhente samtykket;
    - Særskilt samtykke indhentes til særskilte behandlingsprocesser; og
    - Der ikke benyttes samtykke som hjemmel til behandling af persondata, hvor der er en tydelig skævhed mellem den registrerede og den dataansvarlige (især hvis den dataansvarlige er en offentlig myndighed).

Kommentar

Samtykke – en bredere definition

Artikel 4(11) i Persondataforordningen definerer "den registreredes samtykke" som "enhver *frivillig, specifik, informeret og utvetydig viljestilkendegivelse fra den registrerede, hvorved den registrerede ved erklæring eller klar bekræftelse indvilliger i, at personoplysninger, der vedrører den pågældende, gøres til genstand for behandling".*

Kravet om, at samtykke skal være "utvetydigt" er ikke en ændring, der har praktisk betydning. Artikel 7(A) i Databeskyttelsesdirektivet specificerer, at i de tilfælde, hvor man benytter samtykke som hjemmel for behandlingen, skal det angives "utvetydigt". Præambel 32 forslår, at dette kan gøres ved:

"*at sætte kryds i et felt ved besøg på et websted, ved valg af tekniske indstillinger til informationssamfundstjenester eller en anden erklæring eller handling, der tydeligt i denne forbindelse tilkendegiver den registreredes accept af den foreslåede behandling af vedkommendes personoplysninger. Tavshed, forudafkrydsede felter eller inaktivitet bør derfor ikke udgøre samtykke.*"

Udtrykkeligt samtykke kræves stadig som hjemmel til behandling af særlige kategorier af oplysninger (medmindre andre hjemler finder anvendelse – se afsnittet om Særlige kategorier af oplysninger og hjemmelskrav).

Gyldighed – tydelig, tilbagekaldelig og detaljeret

Artikel 7(1) i Persondataforordningen kræver, at hvor der benyttes samtykke som hjemmel for behandling, skal den dataansvarlige kunne påvise, at samtykket blev afgivet af den registrerede i forbindelse med behandlingen. Resten af artikel 7 beskriver betingelserne for et gyldigt samtykke:

- Artikel 7(2): Samtykke til behandling, der afgives i en skriftlig erklæring, der er udarbejdet af den dataansvarlige, skal forelægges på en måde, som klart kan skelnes fra de andre forhold i erklæringen, i en letforståelig og lettilgængelig form og i et klart og enkelt sprog. Præambel 42 citerer de urimelige vilkår i direktiv om forbrugeraftaler (Direktiv 93/13/EØF) som inspiration til disse forpligtelser. I praksis vil det kræve, at samtykke til behandling er tydeligt adskilt i almene kontrakter og aftaler.

- Præambel 42 skriver også, at samtykke kun anses for at være informeret, hvis den registrerede (som minimum) er bekendt med den dataansvarliges identitet og formålene med behandlingen;

- Artikel 7(3) Den registrerede har til enhver tid ret til at tilbagekalde sit samtykke, og det skal være lige så let at tilbagekalde samtykket som at give det. I praksis vil det som minimum kræve, at virksomheden tillader, at samtykket tilbagekaldes ved brug af det samme medie (f.eks. hjemmeside, e-mail, tekst), som det blev afgivet. Persondataforordningen anerkender, at en tilbagekaldelse af samtykke ikke berører lovligheden af den foregående behandling, men det kræver, at den dataansvarlige informerer den registrerede herom før samtykke afgives; og

- Artikel 7(4): Hvor opfyldelse af en kontrakt, herunder tjenesteydelser, er gjort betinget af samtykke til behandling af personoplysninger, som ikke er nødvendig for opfyldelse af kontrakten, vil der blive stillet spørgsmålstegn ved, om samtykke er givet frit.

Præambel 43 skriver, at samtykke ikke formodes at være givet frivilligt, hvis:

- Det ikke er muligt at give særskilt samtykke til forskellige behandlingsaktiviteter, selv om det er hensigtsmæssigt i det enkelte tilfælde; eller

- *"opfyldelsen af en kontrakt, herunder ydelsen af en tjeneste, gøres afhængig af samtykke, selv om et sådant samtykke ikke er nødvendigt for dennes opfyldelse".*

Som resultat heraf kan leveringen af en tjenesteydelse ikke gøres betinget af den registreredes samtykke til behandling af hans/hendes personoplysninger til formål, som ikke er nødvendige for at kunne levere tjenesteydelsen.

Børn og forskning

Særlige betingelser gælder for gyldigheden af samtykke afgivet af børn i forbindelse med informationssamfundstjenester, herunder indhentelse og verificering af forældres samtykke for børn under en bestemt aldersgrænse (se mere i afsnittet om Børn).

Præambel 33 i Persondataforordningen vedrører samtykke, som er indsamlet til videnskabelige forskningsformål. Det anerkendes, at "*det er ofte ikke muligt fuldt ud at fastlægge formålet med behandling af personoplysninger til videnskabelige forskningsformål, når oplysninger indsamles*", og skriver, at

- De registrerede bør derfor kunne give deres samtykke til bestemte videnskabelige forskningsområder i overensstemmelse med "*anerkendte etiske standarder*" for videnskabelig forskning; og
- Registrerede bør have mulighed for kun at give deres samtykke til "*bestemte forskningsområder eller dele af forskningsprojekter i det omfang, det tilsigtede formål tillader det*".

Hvor kan jeg læse mere?

Artikel 4(11), 6(1)(a), 7, 8 og 9(2(a)) *Præambel 32, 33, 42 og 43*

Børn

Resumé

- Der er en række bestemmelser i Persondataforordningen, der specifik vedrører børn, især hvad angår hjemmel for behandling og oplysningspligt.
- Børn identificeres som *"sårbare fysiske personer"*, som har brug for *"særlig beskyttelse"*.
- Behandling af børns persondata kan indebærer en særlig risiko, og yderligere restriktioner kan gælde som resultat af et adfærdskodeks.
- Persondataforordningen angiver ingen aldersgrænse for, hvornår en person anses for at være et barn.
- Når online-tjenester leveres til et barn, og samtykke benyttes som hjemmel for behandling af hans eller hendes data, skal samtykke afgives eller godkendes af en person, som er indehaver af forældremyndigheden over barnet. Dette krav gælder for børn under 16 år (medmindre medlemsstaten har bestemt en lavere aldersgrænse - som ikke kan være lavere end 13 år).

To-do liste

☐	Overvej, om bestemmelserne om børn vedrører dig.
☐	Hvis din virksomhed tilbyder informationssamfundstjenester direkte rettet mod børn, bør det overvejes, hvilke nationale regler der gælder, og det skal sikres, at de nødvendige forældresamtykkemekanismer er implementeret, herunder verificeringsprocesser.
☐	Vær fortsat opmærksom på national ret vedrørende offline behandling af børns data.
☐	Når serviceydelser tilbydes direkte til et barn, skal information udarbejdes så tydeligt, at et barn vil kunne forstå det.
☐	Det skal sikres, at hvis en *"legitim interesse"* benyttes som hjemmel for behandling af børns data, skal det understøttes af grundig og dokumenteret overvejelser omkring, hvorvidt barnets interesser går forud for virksomhedens interesser.
☐	Vær opmærksom på relevante adfærdskodekser, som kan påvirke foreninger eller grupper, som din virksomhed er medlem af.

Kommentar

Vigtigheden af at beskytte børn er nævnt flere steder i Persondataforordningen. I praksis er der meget lidt ny harmonisering i den endelige tekst, og de afgørende restriktioner vil højst sandsynligt komme fra enten eksisterende eller nye nationale love eller adfærdskodekser (se mere i afsnittet om Adfærdskodekser og certificeringer).

Samtykke fra indehaveren af forældremyndigheden

Direktiv 95/46/EF ("Databeskyttelsesdirektivet") indeholdt ingen specifikke restriktioner vedrørende behandling af børns data, og reglerne om børns evne til at afgive samtykke kommer fra de national ret love. Persondataforordningen tilbyder ikke meget harmonisering. Den vigtigste bestemmelse i relation til børn er artikel 8, som kræver, at samtykke fra indehaveren af forældremyndigheden indhentes i forbindelse med informationssamfundstjenester, der udbydes direkte til børn under 16 år – selvom loftet kan sænkes helt ned til 13 år af en medlemsstat, og gælder kun, hvis behandlingen skal foretages på baggrund af barnets samtykke.

I henhold til artikel 8(2) i Persondataforordningen skal den dataansvarlige under hensyntagen til den tilgængelige teknologi gøre "*rimelige bestræbelser*" på at kontrollere, at indehaveren af forældremyndigheden over barnet har givet eller godkendt samtykke.

Dette vedrører kun bestemte online data. Offline data vil fortsat være reguleret af medlemsstatens regler vedrørende evne til at afgive samtykke. Artikel 8(1) skal heller ikke anses for at påvirke den generelle aftalelov i de enkelte medlemsstater vedrørende gyldighed og indgåelse af en kontrakt med børn. Virksomheder skal stadig overveje de lokale regler på dette område.

Information rettet mod børn skal være børnevenlig

Artikel 12 beskriver, at forpligtelserne til at sikre, at information leveret til den registrerede er kortfattet, gennemsigtig, letforståelig, lettilgængelig og i et klart og enkelt sprog skal overholdes, "*navnlig når oplysninger specifikt er rettet mod et barn*". Præambel 58 uddyber dette:

"*Eftersom børn bør nyde særlig beskyttelse, bør alle oplysninger og meddelelser, hvis behandling er rettet mod et barn, være i et så klart og enkelt sprog, at et barn let kan forstå dem*".

Betegnelsen "barn" er ikke defineret i Persondataforordningen. Dataansvarlige skal derfor være forberedte på at kunne overholde disse krav til information til teenagers.

Diverse bestemmelser – hjælpelinje, adfærdskodekser og tilsynsmyndighedernes opgaver

Artikel 6(f) i Persondataforordningen indeholder en bestemmelse om, at den registreredes rettigheder og frihedsrettigheder "*navnlig*" kan gå forud for den dataansvarliges eller tredjeparts interesser, hvis den registrerede er et barn. Dataansvarlige skal sikre at gemme dokumentation, som kan påvise, at der er blevet taget hensyn til de konkurrerende interesser, når der benyttes legitime interesser som hjemmel for behandling af børns data.

Præambel 38 indeholder en bemærkning om, at brug af børns personoplysninger med henblik på markedsføring eller til at oprette personligheds- eller brugerprofiler og indsamling af oplysninger om børn, når de anvender tjenester, der tilbydes direkte til et barn, er et område, som kræver særlig beskyttelse i Persondataforordningen. Præambelen nævner også, at samtykke fra indehaveren af forældremyndigheden ikke er nødvendigt, når det drejer sig om forebyggende eller rådgivende tjenester, der tilbydes direkte til et barn, selvom dette ikke fremgår af selve teksten i Persondataforordningen.

Præambel 75 skriver, at børn er "*sårbare fysiske personer*", og at behandling af børns data kan forårsage risici af "*varierende sandsynlighed og alvor*".

Artikel 40 kræver, at medlemsstaterne, tilsynsmyndighederne, det Europæiske Databeskyttelsesråd og Kommissionen tilskynder til udarbejdelse af adfærdskodekser, herunder vedrørende børn og vedrørende måden hvorpå samtykke skal indhentes fra indehaveren af forældremyndigheden. Virksomheder, der behandler persondata om børn, skal være

opmærksomme på sådanne adfærdskodekser, som kan pålægge virksomheden yderligere forpligtelser.

Endelig skal tilsynsmyndighederne, når de skal fremme offentlighedens kendskab til og forståelse af risici, regler, garantier og rettigheder i forbindelse med behandling af personoplysninger i henhold til kravet i artikel 57(1) (b), have "*særlig fokus*" på aktiviteter, der er direkte rettet mod børn.

Hvor kan jeg læse mere?

Artikel 6(1)(f), 8, 12(1), 40(2)(g), 57 *Præambel 30, 58, 75*

Særlige kategorier af oplysninger og lovlig behandling

» Resumé

”*Særlige kategorier af personoplysninger*” vil nu inkludere ”*genetiske data*” og ”*biometriske data*”, når de behandles med henblik på at ”*identificere en person*”.

- Grundlaget for behandling af følsomme oplysninger i henhold til Persondataforordningen er stort set det samme som i Databeskyttelsesdirektivet, selvom der er et større grundlag i området for sundhed og forvaltning af sundhedsydelser.
- Der er også vide muligheder for medlemsstaterne til at fastsætte nye betingelser (og begrænsninger) vedrørende behandling af genetiske, biometriske og sundhedsdata.

√ To-do liste

☐	Du skal sikre dig, at du kender den hjemmel som din virksomhed anvender ved behandling af særlige kategorier af oplysninger, og du skal undersøge, om denne hjemmel stadig er gyldig i medfør af Persondataforordningen.
☐	Når samtykke benyttes som hjemmel, skal det sikres, at samtykkets kvalitet overholder de nye krav om indhentning af samtykke (se afsnittet om Samtykke).
☐	Overvej om bestemmelserne om børn vil påvirke din virksomhed, og i så fald hvilke nationale regler du skal overholde for at indhente gyldigt samtykke (se mere i afsnittet om Børn); og
☐	Hvis du behandler store mængder genetisk, biometrisk eller sundhedsdata, skal du være særligt opmærksom på den nationale udvikling, idet medlemsstaterne har vide muligheder for at indføre yderligere betingelser og restriktioner for den hjemmel, der er beskrevet i Persondataforordningen.

Kommentar

Artikel 9(2) angiver de situationer, hvor behandling af følsomme oplysninger, som ellers er forbudt, kan ske alligevel. De følgende kategorier af oplysninger anses for at være "følsomme" i henhold til artikel 9(1):

- Racemæssig eller etnisk oprindelse
- Politisk overbevisning
- Religiøs eller filosofisk overbevisning
- Fagforeningsmæssige tilhørsforhold
- Oplysninger vedrørende helbredsforhold, seksuelle forhold eller seksuel orientering
- Genetiske data (*ny*), og
- Biometriske data for entydigt at identificere en person (*ny*)

Bemærk, at Præambel 51 antyder, at behandling af fotografier ikke systematisk bør anses for at være en behandling af følsomme oplysninger (som det har været tilfældet i nogle medlemsstater indtil nu). Fotografier er kun omfattet af særlige kategorier af oplysninger, hvis de entydigt kan identificere en person biometrisk (når det fx benyttes som del af et elektronisk pas).

Hjemlen for behandling af persondata er stort set den samme som i Databeskyttelsesdirektivet:

Artikel 9(2)(a) - udtrykkeligt samtykke fra den registrerede, medmindre det ifølge EU-retten eller medlemsstaterne nationale ret ikke er tilladt at benytte denne hjemmel.

Her er ingen ændring, selvom nye betingelser for samtykke bør overvejes (se afsnittet om Samtykke).

9(2)(b) - Nødvendigt for at opfylde den dataansvarliges eller den registreredes forpligtelser og udøve vedkommendes specifikke rettigheder på området for arbejds-, sundheds- og socialret eller kollektiv overenskomst.

Bestemmelsen uddyber bestemmelsen i Databeskyttelsesdirektivet en smule ved at referere til overholdelse af kollektive overenskomster og forpligtelsen i henhold til sundheds- og socialret.

9(2)(c) - Nødvendigt for at beskytte den registreredes eller en anden persons vitale interesser i tilfælde, hvor den registrerede fysisk eller juridisk ikke er i stand til at give samtykke.

Dette gengiver den tilsvarende bestemmelse i Databeskyttelsesdirektivet.

9(2)(d) - Behandling foretages af et almennyttigt organ, hvis sigte er af politisk, filosofisk, religiøs eller fagforeningsmæssig art og på betingelse af, at behandlingen alene vedrører organets medlemmer, tidligere medlemmer eller personer (som på grund af organets formål er i regelmæssig kontakt hermed) og på betingelse af, at oplysningerne ikke videregives til tredjemand uden den registreredes samtykke.

Dette gengiver den tilsvarende bestemmelse i Databeskyttelsesdirektivet.

9(2)(e) - Personoplysninger, som tydeligvis er offentliggjort af den registrerede.

Dette gengiver den tilsvarende bestemmelse i Databeskyttelsesdirektivet.

9(2)(f) - Nødvendigt, for at retskrav kan fastlægges, gøres gældende eller forsvares, eller når domstole handler i deres egenskab af domstol.

Dette giver medlemsstaterne mulighed for ved lov at udvide rækken af situationer, hvor følsomme oplysninger kan behandles i samfundets interesse.

9(2)(h) - Nødvendigt med henblik på forebyggende medicin eller arbejdsmedicin til vurdering af arbejdstagerens erhvervsevne, medicinsk diagnose, ydelse af social- og sundhedsomsorg eller -behandling eller forvaltning af social- og sundhedsomsorg og -tjenester på grundlag af EU-retten eller medlemsstaternes nationale ret eller i henhold til en kontrakt med en sundhedsperson.

OG

9(2)(i) - Nødvendigt af hensyn til samfundsinteresser på folkesundhedsområdet, f.eks. beskyttelse mod alvorlige grænseoverskridende sundhedsrisici eller sikring af høje kvalitets- og sikkerhedsstandar-

der for sundhedspleje og lægemidler eller medicinsk udstyr.

Disse to bestemmelser udvider den tilsvarende bestemmelse i Databeskyttelsesdirektivet og berører kendte huller i Databeskyttelsesdirektivet ved f.eks. at give en formel juridisk begrundelse for regulatorisk brug af sundhedsoplysninger i sundheds- og medicinalsektoren og ved at give mulighed for at dele sundhedsoplysninger med dem, der udbetaler sociale ydelser.

Begge bestemmelser kræver, at man indfører yderligere sikkerhedsforanstaltninger i form af navnlig tavshedspligt (enten i forbindelse med opfyldelse af en kontrakt eller lov eller i forbindelse med forretningsadfærd eller regulering).

9(2)(j) - Nødvendigt med henblik på arkivformål i samfundets interesse eller til videnskabelige eller historiske forskningsformål eller statistiske formål i overensstemmelse med artikel 89, stk. 1.

Dette giver adgang til behandling af særlige kategorier af oplysninger til arkiverings-, forsknings- og statistiske formål, som skal ske i overensstemmelse med fornødne garantier, herunder foranstaltninger til at sikre overholdelse af princippet om dataminimering (se mere i afsnittet om Begrænsninger og specifikke behandlingssituationer).

Genetik, biometrik og sundhedsoplysninger

I henhold til artikel 9(4) i Persondataforordningen er medlemsstaterne berettigede til at opretholde eller indføre yderligere betingelser (herunder begrænsninger) for behandling af genetiske data, biometriske data eller helbredsoplysninger. De eksisterende forskelle i tilgangen til dette vil sandsynligvis blive opretholdt, og yderligere afvigelser vil blive tilladt. Virksomheder, som behandler disse kategorier af data, skal fortsætte med at være opmærksomme på udviklingen i national ret og overveje behovet for yderligere lobbyarbejde på dette område.

Straffedomme og lovovertrædelser

Data, der vedrører straffedomme og lovovertrædelser, er ikke kategoriserede som "følsomme oplysninger" i Persondataforordningen. Dette udgør dog ikke en ændring, idet (selvom den danske persondatalovgivning, Persondataloven, anser oplysninger vedrørende straffedomme og lovovertrædelser som semi-følsomme oplysninger) oplysninger af denne type ikke blev anset som følsomme oplysninger i henhold til Databeskyttelsesdirektivet.

Bestemmelserne i Persondataforordningen vedrørende straffedomme og lovovertrædelser afspejler bestemmelserne i Databeskyttelsesdirektivet. Artikel 10 angiver, at behandling af sådanne oplysninger foretages enten under kontrol af en offentlig myndighed, eller hvis behandling har hjemmel i EU-retten eller medlemsstaternes nationale ret, som giver passende garantier. Denne bestemmelse vil højst sandsynlig resultere i fortsat national afvigelse på dette område.

Hvor kan jeg læse mere?

Artikel 9 *Præambel 51-56*

Oplysningspligt

Resumé

- Dataansvarlige har orienteringspligt for at sikre, at der er gennemsigtighed i databehandlingen.
- Der skal gives specifik information, og der er også et generelt krav om gennemsigtighed.
- Det vil ofte være let at give den yderligere information – dog kan det være svært for virksomheder at anslå det tidsrum, hvor oplysningerne vil blive opbevaret.
- Der er lagt vægt på, at orienteringen sker på en klar og kortfattet måde.

To-do liste

☐	Gennemgå og opdatér eksisterende oplysningsmeddelelser.
☐	Det skal sikres, at der for de personoplysninger, der er indsamlet indirekte, er afgivet oplysning på det rette tidspunkt.
☐	Det skal aftales med relevante samarbejdspartnere, som indsamler personoplysninger på vegne af din virksomhed, hvem der har ansvaret for at gennemgå, opdatere og godkende oplysningsmeddelelser.

Kommentar

Princippet om "*rimelig og gennemsigtig"* databehandling betyder, at den dataansvarlige skal oplyse den registrerede om behandlingen af vedkommendes personoplysninger, medmindre den registrerede allerede er blevet informeret om dette. De oplysninger, som skal afgives, er anført i Persondataforordningen og på listen nedenfor. I forbindelse med særlige omstændigheder eller sammenhænge kan det være nødvendigt også at oplyse om andre ting for at behandlingen er retfærdig og gennemskuelig.

Oplysningerne skal afgives på en kortfattet, gennemsigtig, letforståelig og lettilgængelig måde, og der skal anvendes klar og almindelig sprogbrug (især hvis den registrerede er et barn).

Hvad skal den dataansvarlige oplyse den registrerede om?

I Persondataforordningen er der krav om, at der skal afgives mere information end i Databeskyttelsesdirektivet – men det er dog allerede obligatorisk i nogle medlemsstater.

De informationer, der ikke er nævnt i Databeskyttelsesdirektivet, er skrevet med kursiv.

- Den dataansvarliges identitet og kontaktoplysninger (eller deres repræsentant, hvis den dataansvarlige ikke er etableret indenfor EU); *databeskyttelsesrådgiverens kontaktoplysninger*.
- Formålet med behandlingen *og retsgrundlaget for databehandlingen – herunder den "legitime interesse", hvis dette lægges til grund for behandlingen af den dataansvarlige (eller tredjepart).*
- Modtagerne eller kategorier af modtagere.
- *Oplysninger om dataoverførsler udenfor EU:*
  - *Herunder hvordan oplysningerne vil blive beskyttet (fx at modtageren er bosiddende i et land med tilstrækkeligt beskyttelsesniveau; Binding Corporate Rules er på plads osv.); og*
  - *Hvordan den registrerede kan få en kopi af BCR eller andre beskyttelsesforanstaltninger, eller hvor sådanne beskyttelsesforanstaltninger er gjort tilgængelige.*
- *Det tidsrum, hvor personoplysningerne vil blive opbevaret – og hvis dette ikke er muligt, så de kriterier, der anvendes til at fastlægge dette tidsrum.*
- At den registrerede har ret til indsigt og *dataportabilitet,* berigtigelse, sletning *og til begrænsning af behandling af sine oplysninger og gøre indsigelse mod behandlingen og, hvis den er baseret på samtykke, til at tilbagetrække samtykke.*
- *At den registrerede kan klage til en tilsynsmyndighed.*
- *Hvorvidt oplysningerne afgives i forbindelse med en retlig forpligtelse eller opfyldelse af en kontrakt, og hvad konsekvenserne er, hvis oplysningerne ikke afgives.*
- Om der vil foregå automatisk databehandling – sammen med oplysninger om, hvilken logik der anvendes og betydningen og konsekvenserne af behandlingen for den registrerede.

Hvornår skal en dataansvarlig afgive oplysninger om dette?

Den dataansvarlige får oplysningerne direkte fra den registrerede

- Når oplysningerne afgives.

Den dataansvarlige skal også oplyse den registrerede om, hvilke oplysninger, der er obligatoriske og hvad konsekvenserne er, hvis oplysningerne ikke afgives.

Den dataansvarlige får ikke oplysningerne direkte

- Indenfor rimelig tid efter oplysningerne er afgivet (max en måned); eller
- Hvis oplysningerne anvendes til at kommunikere med den registrerede, så senest når den første kommunikation foregår; eller

- Hvis det påtænkes at videregive oplysningerne til en anden modtager, så senest før oplysningerne bliver videregivet.

Den dataansvarlige skal også oplyse den registrerede om oplysningernes kategorier og kilde(r), herunder om kilden er offentlig tilgængelig.

- Den dataansvarlige har ikke pligt til at informere den registrerede, hvis det er umuligt eller kræver en uforholdsmæssig stor indsats. I sådanne tilfælde skal der anvendes passende foranstaltninger til at beskytte de registreredes interesser og oplysningsmeddelelsen skal offentliggøres.

  Det er heller ikke nødvendigt at orientere:

  - hvis der i EU-lovgivningen eller en medlemsstats lovgivning er krav om, at den dataansvarlige indsamler/videregiver oplysningerne; eller

  - hvis oplysningerne skal forblive fortrolige pga. branche- eller lovbestemt tavshedspligt, der er foreskrevet af EU-lovgivning eller lovgivningen i en medlemsstat.

Hvis databehandleren senere foretager behandling af personoplysningerne med et nyt formål, der ikke dækkes af den oprindelige meddelelse, skal der sendes en ny meddelelse, der dækker den nye behandling.

At skulle oplyse alt dette er svært at forene med Persondataforordningens krav om kortfattethed og klarhed. For at afhjælpe dette er der mulighed for, at Kommissionen kan indføre standardiserede ikoner via delegerede retsakter. Hvis de bliver indført, skal disse også vises til de registrerede.

Hvor kan jeg læse mere?

Artikel 12 og 13 *Præambel 58,60,61 og 62*

Registreredes ret til indsigt, berigtigelse og dataportabilitet

» Resumé

- Grundlaget for behandling af følsomme oplysninger i henhold til Persondataforordningen er stort set det samme som i Databeskyttelsesdirektivet, selvom der er et større grundlag i området for sundhed og forvaltning af sundhedsydelser.
- Dataansvarlige skal på forespørgsel:
  - bekræfte, om de behandler den registreredes personoplysninger;
  - udlevere en kopi af oplysningerne (i et almindeligt anvendt elektronisk format i mange tilfælde); og
  - udlevere understøttende (og detaljeret) forklarende materiale.
- Registrerede kan også kræve, at deres personoplysninger overføres til dem selv eller en anden udbyder i maskinlæsbart format, hvis:

  1) de pågældende oplysninger blev afgivet af den registrerede til den dataansvarlige;
  2) der blev foretaget automatisk databehandling; og
  3) oplysningerne blev behandlet i henhold til samtykke eller opfyldelse af en kontrakt.
- Forespørgslen skal besvares indenfor en måned (forlængelse kan forekomme i nogle tilfælde), og hvis forespørgslen ikke imødekommes, skal der gives en forklaring til den registrerede.
- Hensigten med retten til indsigt er at give den registrerede mulighed for at tjekke, om behandlingen er lovlig, og retten til at få fremsendt en kopi må ikke påvirke andres rettigheder ugunstigt.

√ To-do liste

☐	Gennemgå processer og procedurer for og oplæring af medarbejdere, der har kontakt til kunder. Er de tilstrækkelige til at dække Persondataforordningens regler i forhold til indsigt og dataportabilitet?
☐	Udvikle skabeloner til svarbreve for at sikre, at alle understøttende oplysninger bliver medtaget.
☐	Vurdere din virksomheds evne til at stille oplysninger til rådighed i overensstemmelse med Persondataforordningens krav til format. Det kan være nødvenligt at udvikle nye formateringsmuligheder for at opfylde kravene om indsigt.
☐	Hvis kravet om dataportabilitet gælder for din virksomhed, så vurdér, om oplysninger let kan eksporteres i strukturerede, maskinlæsbare (og helst kompatible) formater. Vurdér om oplysningerne vedrører mere end en registreret og hvordan de vanskeligheder, der opstår herved, kan løses.
☐	Overvej, om der kan udvikles portaler, hvor de registrerede selv får direkte adgang til at udøve sine rettigheder til indsigt.

Ret til oplysninger og indsigt

Den registrerede har følgende rettigheder i forbindelse med den dataansvarlige:

- At få bekræftelse på, om hans/hendes personoplysninger bliver behandlet;
- At få indsigt i oplysninger (fx adgang til en kopi af oplysningerne); og
- At få fremsendt understøttende information om behandlingen.

Som det er tilfældet med alle registreredes rettigheder, skal den dataansvarlige svare "*uden unødig forsinkelse"* og *"senest indenfor en måned"*, der findes dog i nogle tilfælde mulighed for at forlænge dette.

Den dataansvarlige skal også træffe rimelige foranstaltninger til at identificere personen, der fremsætter ønsket – men må ikke indsamle oplysninger kun med det formål at kunne imødekomme forespørgsler vedrørende de registreredes ret til indsigt. Disse punkter er især relevante i forhold til onlinetjenester.

Retten til indsigt

Den dataansvarlige skal udlevere "*en kopi af de personoplysninger, der behandles*". Dette skal være gratis (en ændring i forhold til tidligere for dataansvarlige i Storbritannien), dog må den dataansvarlige opkræve et rimeligt administrationsgebyr, hvis der anmodes om yderligere kopier.

Hvis forespørgslen indgives i elektronisk form, skal oplysningerne fremsendes i et almindeligt anvendt elektronisk format (medmindre den registrerede ønsker noget andet). Dette kan medføre omkostninger for dataansvarlige, der anvender specielle formater eller har papirarkiv.

Præambel 63 foreslår, at den dataansvarlige, hvis det er muligt, kan stille et sikkert system til rådighed, så de registrerede kan få direkte adgang til sine oplysninger. Dette fremstår mere som et forslag end et krav.

Supplerende oplysninger

Den dataansvarlige skal også oplyse følgende (de punkter, der er skrevet med kursiv, er på nuværende tidspunkt ikke krævet af Databeskyttelsesdirektivet, dog er de krævet iht. lovgivningen i nogle medlemsstater):

- formålet med behandlingen;
- kategorier af de behandlede oplysninger;
- modtagerne eller kategorier af modtagere (*især oplysninger om overførsel til modtagere i tredjelande eller til internationale organisationer* (virksomheder, der reguleres af international ret, eller hvor der er aftaler mellem lande));
- *det påtænkte tidsrum, hvor oplysningerne vil blive opbevaret, eller hvis dette ikke er muligt, så ud fra hvilke kriterier dette bliver fastlagt;*
- *den registreredes rettighed til berigtigelse eller sletning, til at begrænse databehandlingen eller til at gøre indsigelse mod behandlingen og til at indgive en klage til tilsynsmyndigheden;*
- *information om kilden til oplysningerne (hvis de ikke er indsamlet fra den registrerede);* og
- alle lovregulerede automatiserede databehandlinger (fx beslutninger, der tages udelukkende på grundlag af automatiseret databehandling, som har retlig eller lignende betydning; dette gælder også for automatiseret databehandling, hvor følsomme personoplysninger er involveret) – herunder oplysninger om den anvendte logik og *den betydning og forventede konsekvenser, som behandlingen har for den registrerede.*

Hvis den dataansvarlige afviser henvendelsen, skal dette begrundes.

Undtagelser

Persondataforordningen anerkender, at den registreredes ret til indsigt kan stille andres rettigheder ugunstigt og foreskriver, at retten til at modtage en kopi af data ikke må påvirke andres rettigheder. Præambel 63 anfører, at dette kunne gælde for beskyttelse af IP-rettigheder og erhvervshemmeligheder (fx hvis offentliggørelse af den logik, der er anvendt til automatisk databehandling inkluderer offentliggørelse af sådanne oplysninger). Præamblen

anfører dog også, at den dataansvarlige ikke kan afvise at udlevere *al information* på det grundlag, at retten til indsigt krænker andres rettigheder.

Præambel 63 indeholder også 2 andre brugbare begrænsende bestemmelser:

- Hvis den dataansvarlige behandler mange oplysninger, kan den dataansvarlige anmode den registrerede om at præcisere, hvilke personoplysninger eller behandlinger denne ønsker adgang til. (Præamblen nævner dog ikke noget om, at der findes en undtagelse pga. store mængder af relevante oplysninger: den begrænsende bestemmelse har øjensynligt mere at gøre med at specificere ønsket end den dataansvarliges tidsforbrug og arbejdsindsats – selvom der selvfølgelig kan være en sammenhæng);

- Den registreredes rettighed er "*at kende til og at kontrollere, om databehandlingen er lovlig*". Dette bekræfter de bemærkninger, som EU-domstolen har i *YS v Minister voor Immigratie, Integratie en Asiel* (sagsnummer C-141/12), om at formålet med den registreredes ret til indsigt er at gøre det muligt at efterprøve, om oplysninger er korrekte og om behandlingen er lovlig og gøre det muligt at udøve retten til berigtigelse og indsigelse osv., hvis det er nødvendigt. Med andre ord er formålet relateret til rettighederne i loven om persondatabeskyttelse: henvendelser, der vedrører andre formål, der ikke er relateret til persondatabeskyttelse, kan muligvis blive afvist.

Berigtigelse

Personer kan anmode en dataansvarlig om at rette fejl i de personoplysninger, der vedrører dem. I tilfælde af at personoplysningerne er ufuldstændige, kan der anmodes om, at den dataansvarlige fuldstændiggør oplysningerne eller registrerer en supplerende erklæring.

Dataportabilitet

Den registreredes ret til indsigt, som findes i Persondataforordningen, giver allerede personer ret til at få adgang til deres oplysninger i et almindeligt anvendt elektronisk format.

Dataportabilitet tager skridtet videre og kræver, at den dataansvarlige giver adgang til oplysningerne i et struktureret, almindeligt anvendt og maskinlæsbart format. Endvidere kan den dataansvarlige blive pålagt at transmittere oplysningerne direkte til en anden dataansvarlig. Det er stadig uklart, om oplysningerne skal være i et indbyrdes kompatibelt format, eller om det er en praksis, som de dataansvarlige opfordres til at indføre.

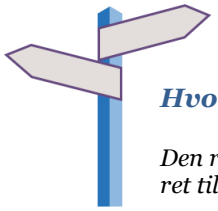
Retten til dataportabilitet er mere afgrænset end retten til indsigt. Den gælder:

- for personoplysninger, hvor behandlingen foretages automatisk (ikke papirkopi);

- for personoplysninger, som den registrerede har afgivet til den dataansvarlige; og

- kun, hvor retsgrundlaget for databehandlingen er baseret på samtykke, eller hvor databehandlingen sker af hensyn til opfyldelse af en kontrakt eller som forberedende foranstaltning til en kontrakt.

De oplysninger, som bliver overført, kan vedrøre mere end en person: dataportabilitetspligten må ikke krænke andre registreredes rettigheder. Den dataansvarlige skal formentlig ikke videregive oplysninger til en anden dataansvarlig (eller til den registrerede), hvis dette krænker andres rettigheder. Det er uklart, hvordan en dataansvarlig (fx udbydere af sociale medier) skulle kunne foretage denne vurdering.



Hvor kan jeg læse mere?

Den registreredes ret til indsigt	*Artikel 15*	*Præambel 59, 63 og 64*
Berigtigelse	*Artikel 16*	-
Dataportabilitet	*Artikel 20*	*Præambel 68*

Ret til indsigelse

Resumé

- Der findes en ret til indsigelse for specifikke typer behandlinger:
  - Direkte markedsføring;
  - Behandling, der har hjemmel i legitim interesse eller udførelse af en opgave, der er i samfundets interesse/pålagt af en offentlig myndighed; og
  - Behandling med henblik på forskningsformål eller statistiske formål.
- Det er kun retten til indsigelse mod direkte markedsføring, der er ufravigelig (dvs. at det ikke er nødvendigt at påvise grundlaget for indsigelsen, der er ingen undtagelser, som giver ret til fortsat behandling).
- Der er pligt til at orientere den registrerede om disse rettigheder på et tidligt tidspunkt – klart og uafhængigt af andre informationer.
- Online-tjenester skal have automatiserede midler til at gøre indsigelse.

To-do liste

☐	Gennemgå meddelelser og politikker vedrørende persondatabeskyttelse for at sikre, at de registrerede informeres klart og adskilt om deres ret til indsigelse på tidspunktet, hvor den 'første kommunikation' finder sted;
☐	Det skal sikres, at online-tjenester har automatiserede midler, hvor der kan gøres indsigelse; og
☐	Gennemgå markedsføringslister for at sikre, at der er processer på plads, der gør det muligt at overholde Persondataforordningen (herunder lister, der håndteres af samarbejdspartnere eller tjenesteudbydere på vegne af din virksomhed).

Ret til indsigelse

Ret til indsigelse gives i tre tilfælde i Persondataforordningen. Alle er i forbindelse med behandling, der udføres med specifikke formål, eller som har hjemmel i et bestemt grundlag. Den registrerede har ikke ret til indsigelse mod behandling generelt.

Der er ret til indsigelse i følgende tilfælde:

Behandling med henblik på direkte markedsføring

Dette er en ufravigelig ret; når den registrerede gør indsigelse, må oplysningerne ikke længere behandles med henblik på direkte markedsføring.

Behandling med henblik på videnskabelige/ historiske forskningsformål/ statistiske formål

Mindre "stærk" ret end retten til indsigelse mod direkte markedsføring – der skal være "*grunde, der vedrører [den registreredes] særlige situation*".

Kan fraviges, hvor behandlingen er nødvendig for at udføre en opgave af hensyn til samfundets interesse.

Der er ingen tilsvarende bestemmelse i Databeskyttelsesdirektivet.

Behandling med henblik på to specifikke formål:

1. legitim interesse lægges til grund (jf. Art. 6(1)(f)); eller
2. fordi behandling er nødvendig for udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse (jf. Art. 6(1)(e)).

Retten kan igen udøves af grunde, der vedrører den registreredes særlige situation.

Den dataansvarlige skal ophøre med behandlingen af personoplysningerne, medmindre:

- den dataansvarlige kan påvise vægtige legitime grunde, som går forud for den registreredes interesser; eller
- behandlingen er nødvendig for, at retskrav kan fastlægges, gøres gældende eller forsvares.

Så når den registrerede gør indsigelse på grundlag af hans eller hendes særlige situation, er det den dataansvarliges opgave at påvise, hvorfor de alligevel skal kunne behandle personoplysningerne på dette grundlag.

Dette er en stramning af reglerne i Databeskyttelsesdirektivet. I den tilsvarende bestemmelse er det den registrerede, der skal påvise 'vægtige legitime grunde' til indsigelsen, og behandlingen skal kun stoppes, hvis indsigelsen er berettiget.

Underretningspligt

Hvis der foretages behandling med direkte markedsføring som formål og behandling med grundlag i udførelse af en opgave i samfundets interesse/legitim interesse, skal den registrerede underrettes om indsigelsesretten senest ved den første henvendelse til den registrerede. Denne underretning skal være tydelig og adskilt fra anden information.

Underretningspligten gælder ikke i forbindelse med behandling, der har forskningsformål/statistiske formål.

I forbindelse med onlinetjenester skal den registrerede kunne udøve sin rettighed ved automatiserede midler.

Hvor kan jeg læse mere?

Ret til indsigelse Artikel 21 Præambel 56 & 57

Ret til sletning og retten til at begrænse behandling

Resumé

- Mere omfattende, og uklare, rettigheder indføres: retten til at blive glemt (som nu hedder retten til sletning) og retten til at begrænse behandling.
- Den registrerede kan kræve, at oplysninger bliver 'slettet', når der er problemer med behandlingens retsgrundlag, eller hvis den registrerede tilbagetrækker sit samtykke.
- Den registrerede kan kræve, at den dataansvarlige 'begrænser' behandlingen, mens klager (om fx berigtigelse) bliver afklaret, eller hvis behandlingen er ulovlig, men den registrerede modsætter sig sletning.
- Dataansvarlige, der har offentliggjort personoplysninger, som den dataansvarlige så anmodes om at slette, skal underrette andre, som behandler personoplysningerne, om anmodningen. Dette er en ny, vidtrækkende og udfordrende forpligtelse.

To-do liste

☐	Man skal sikre sig, at ansatte og leverandører, der kan tænkes at modtage anmodninger om sletning af personoplysninger, kan genkende dem og ved, hvordan de skal behandles.
☐	Fastlæg, om du arbejder i en branche, hvor overholdelse af rettighederne vedrørende sletning vil være så urimelige og uberettigede, at der skal forsøges at få indført yderligere undtagelser i den pågældende medlemsstat.
☐	Fastlæg, om systemer kan opfylde kravene mht. at markere oplysninger som spærret, mens klager bliver afklaret: påbegynd udvikling af systemet, hvis det er nødvendigt.

Retten til at blive glemt

Den registrerede har i visse situationer ret til at få deres personoplysninger 'slettet' – kort sagt i situationer, hvor behandlingen ikke lever op til kravene i Persondataforordningen. Retten kan udøves mod dataansvarlige, som skal reagere uden unødig forsinkelse (og altid indenfor en måned, dette kan dog forlænges i vanskelige tilfælde).

Hvornår kan retten anvendes?

- Når personoplysningerne ikke længere er nødvendige til det formål, hvortil de blev indsamlet eller behandlet.
- Hvis den registrerede trækker samtykket til behandling tilbage (og hvis der ikke er andre retsgrundlag for behandlingen).
    - Der er endnu en situation, der kan udløse retten til at blive glemt i forbindelse med tilbagetrækning af et samtykke, der tidligere er afgivet af et barn i forbindelse med onlinetjenester. Det skønnes dog ikke, at denne situation ændrer på det generelle princip om, at samtykke kan tilbagetrækkes, og når dette gøres, kan den registrerede kræve, at personoplysningerne bliver slettet.
- I forbindelse med behandling, hvor legitime interesser lægges til grund – hvis den registrerede gør indsigelse og den dataansvarlige ikke kan påvise, at der er legitime grunde til behandlingen, der går forud for dette.
- Hvis personoplysningerne på anden måde er behandlet ulovligt (dvs. på en anden måde, som er i strid med Persondataforordningen).
- Hvis oplysningerne skal slettes for at overholde en retlig forpligtelse i EU-retten eller medlemsstaternes nationale ret, som den dataansvarlige er underlagt.

Den sidste betingelse kunne fx finde anvendelse, hvis den registrerede mener, at den dataansvarlige opbevarer personoplysninger, hvor lovgivningen kræver, at sådanne oplysninger skal slettes efter en given periode (fx kontrol vedrørende ansættelse).

Den generelle 'rodekasse', der tillader, at der kan anmodes om sletning, hvor personoplysninger bliver behandlet *'ulovligt'*, er en potentiel stor byrde: der er mange grunde til, at personoplysninger kan være behandlet ulovligt i henhold til Persondataforordningen (de kan være utilstrækkelige; en del af underretningspligten er måske ikke opfyldt overfor den registrerede). Det er dog ikke oplagt, at dette skulle være grund til, at oplysningerne skal slettes. Den tilsvarende bestemmelse i Databeskyttelsesdirektivet lagde op til en mere skønsmæssig vurdering, der krævede, at personoplysninger skulle slettes, hvor det var relevant. Det er vigtigt at se, hvilke forslag til undtagelser, der kommer fra medlemsstaterne.

Offentliggjorte personoplysninger

Hvis den dataansvarlige har offentliggjort personoplysninger, og hvor de er forpligtet til at slette personoplysningerne, skal den dataansvarlige også underrette andre dataansvarlige, som behandler personoplysningerne, om at den registrerede har anmodet om, at personoplysningerne bliver slettet. Forpligtelsen skal styrke den registreredes rettigheder på online-området.

Den dataansvarlige er forpligtet til at tage *rimelige foranstaltninger,* og der skal tages hensyn til den teknologi, der er tilgængelig og omkostningerne i forbindelse med implementeringen. Forpligtelsen er potentielt temmeligt vidtrækkende og meget svær at gennemføre: fx da det nu drejer sig om offentliggjorte oplysninger, er spørgsmålet, hvordan den oprindelige dataansvarlige skal kunne identificere de dataansvarlige, som skal underrettes.

Andre tilfælde, hvor modtagere skal underrettes

Hvis den dataansvarlige skal slette personoplysninger, så skal den dataansvarlige underrette alle, som har fået kendskab til oplysningerne, med mindre dette er umuligt eller uforholdsmæssigt vanskeligt.

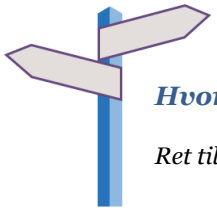
Undtagelser

Underretningspligten finder ikke anvendelse, hvis behandlingen er nødvendig:

- for at udøve retten til ytrings- eller informationsfrihed;

- for at overholde en retlig forpligtelse i henhold til EU-retten eller medlemsstaternes nationale ret;
- af hensyn til samfundets interesser eller offentlig myndighedsudøvelse;
- af hensyn til samfundsinteresser på folkesundhedsområdet;
- med henblik på arkivformål, forskningsformål eller statistiske formål (hvis nogen relevant betingelse for denne slags behandling opfyldes); eller
- for at retskrav kan fastlægges, gøres gældende eller forsvares ved en domstol.

Se også afsnittet om dispensation og særlige omstændigheder for andre tilfælde, hvor undtagelser kan være relevante, hvis det er anført i EU-lovgivning eller medlemsstatslovgivning.



Hvor kan jeg læse mere?

Ret til sletning	*Artikel 17 og 18b*	*Præambel 65, 66, 73*
Ret til begrænsning	*Artikel 18 og 19*	*Præambel 67, 73*

Retten til at begrænse behandlingen

Dette erstatter bestemmelserne om 'blokering' i Databeskyttelsesdirektivet. Denne ret giver den registrerede et alternativ til at kræve personoplysninger slettet i nogle situationer; i andre giver det den registrerede mulighed for at kræve behandling af personoplysninger midlertidigt stoppet, mens andre udfordringer løses.

Hvad er begrænsning?

Hvis personoplysninger 'begrænses', må den dataansvarlige kun lagre personoplysningerne. De må ikke behandles yderligere, medmindre:

- den registrerede samtykker; eller
- behandlingen er nødvendig med henblik på at fastslå et retskrav mm., for at beskytte en fysisk eller juridisk persons rettigheder; eller af hensyn til (Unionens eller en medlemsstats) vigtige samfundsinteresser.

Hvis der er tale om et automatisk behandlingssystem, skal der iværksættes tekniske tiltag, der kan stoppe behandlingen og gøre bemærkning herom i databehandlerens it-systemer. Dette kan være at flytte oplysningerne til et afgrænset system, midlertidigt blokere oplysningerne på hjemmesiden eller på anden måde gøre oplysningerne utilgængelige.

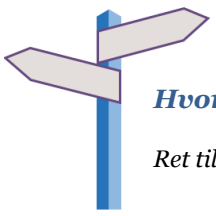
Hvis oplysningerne er videregivet til andre, skal den dataansvarlige underrette modtagerne om den begrænsede behandling (medmindre dette er umuligt eller uforholdsmæssigt vanskeligt).

Den dataansvarlige skal underrette den registrerede, inden begrænsningen af behandlingen ophæves.

Hvornår skal begrænsning foretages?

- Når rigtigheden af oplysninger bestrides af den registrerede, skal anvendelsen af personoplysningerne begrænses, indtil det fastslås, om de er korrekte;
- Når den registrerede har gjort indsigelse mod behandlingen (i medfør af legitime interesser), kan den registrerede kræve, at anvendelsen af personoplysningerne begrænses, indtil det fastslås, om grundlaget for behandlingen er lovligt;
- Når behandlingen er ulovlig, men den registrerede modsætter sig sletning og i stedet anmoder om, at anvendelsen begrænses; og
- Når den dataansvarlige ikke længere har brug for personoplysningerne, men de er nødvendige for, at den registrerede kan fastlægge retskrav, gøre dem gældende eller forsvare dem ved en domstol.

Den sidste betingelse kan fx betyde, at den dataansvarlige har pligt til at lagre oplysninger for tidligere kunder, hvis personoplysningerne er relevante for retssager, hvori den registrerede er impliceret.



Hvor kan jeg læse mere?

Ret til sletning	*Artikel 17 og 18b*	*Præambel 65, 66, 73*
Ret til begrænsning	*Artikel 18 og 19*	*Præambel 67, 73*

Profilering og automatiske afgørelser

» Resumé

- Reglerne om automatiske afgørelser ligner de tilsvarende regler i Databeskyttelsesdirektivet (forslag om at indføre begrænsning af 'profiling' blev i sidste ende ikke medtaget i den endelige udgave af Persondataforordningen).
- Reglerne vedrører beslutninger, der:
  - udelukkende tages baseret på automatisk behandling; og
  - som har retsvirkning eller på tilsvarende vis betydeligt påvirker den pågældende.
- Hvor beslutningen er:
  - nødvendig for indgåelse eller opfyldelse af en kontrakt; eller
  - har hjemmel i EU-ret eller medlemsstaternes nationale ret, som den dataansvarlige er underlagt; eller
  - baseret på den registreredes udtrykkelige samtykke

  er automatisk behandling lovlig. Der skal dog stadig være truffet passende foranstaltninger til at beskytte den registreredes interesser.
- Der er yderligere begrænsning på profilering, der er baseret på følsomme oplysninger – som kræver udtrykkeligt samtykke eller skal have hjemmel i EU-ret eller medlemsstaternes nationale ret, og er nødvendig af hensyn til vigtige offentlige interesser.

☑ To-do liste

☐	Undersøg hvilke væsentlige automatiske afgørelser, der anvendes. Find afgørelser, der beror på • samtykke; • har hjemmel i lovgivning; • eller som vedrører følsomme oplysninger eller børn.
☐	Hvis profilering har hjemmel i samtykke, skal det sikres, at samtykket er udtrykkeligt.
☐	Hvis profileringen har hjemmel i lovgivningen, så undersøg, om det er EU-ret eller medlemsstaternes nationale ret; hold et vågent øje med, om medlemsstaterne vil forsøge at lave ændringer i lovgivningen for at afspejle Persondataforordningen.
☐	Hvis profilering vedrører følsomme oplysninger: • Undersøg, om der kan opnås udtrykkeligt samtykke; • Hvis dette ikke er muligt, må der laves lobbyarbejde for, at medlemslandet eller EU juridisk vil understøtte sådan behandling.
☐	Hvis profilering vedrører børn, må der søges rådgivning: dette er underlagt begrænsninger.

Hvad betyder profiling

Profiling er "*enhver form for automatisk behandling af personoplysninger, der evalurer de personlige forhold vedrørende en fysisk person, navnlig for at analysere eller forudsige forhold vedrørende den registreredes arbejdsindsats, økonomiske situation, helbred, personlige præferencer eller interesser, pålidelighed eller adfærd eller geografiske position eller bevægelser*".

I løbet af lovgivningsprocessen var der forsøg på at indføre væsentlige begrænsninger på al profilering. Til sidst blev de dog ikke medtaget – selvom Præambel 72 nævner, at det Europæiske Databeskyttelsesråd kan udgive retningslinjer vedrørende profiling.

Begrænsninger på automatiske afgørelser med betydelige konsekvenser

Begrænsninger på afgørelser, der alene er baseret på automatisk databehandling (herunder profiling), gælder, hvis afgørelserne har retsvirkning eller på tilsvarende vis betydeligt påvirker den registrerede. Præambel 71 nævner eksempler som afslag på en onlineansøgning om kredit eller e-rekrutteringsprocedurer; den gør det også klart, at det der gøres indsigelse imod, er manglen på menneskelig indgriben.

Den registrerede har ret til ikke at blive underlagt sådanne afgørelser. (Dette kan enten læses som et forbud mod sådan behandling eller med betydningen, at behandlingen må foretages, men at den registrerede har ret til at gøre indsigelse. Denne tvetydighed findes også i Databeskyttelsesdirektivet og medlemsstaterne har forskellige holdninger til punktet).

Sådan betydelig automatiseret behandling må anvendes, hvis det er:

- nødvendigt for indgåelse eller opfyldelse af en kontrakt mellem den registrerede og en dataansvarlig;
- har hjemmel i EU-ret eller medlemsstaternes nationale ret; eller
- er baseret på den registreredes udtrykkelige samtykke.

Profiling baseret på udtrykkeligt samtykke eller opfyldelse af kontrakt

I det første og tredje tilfælde (opfyldelse af kontrakt og samtykke) skal den dataansvarlige gennemføre passende foranstaltninger til at beskytte den registrerede. Dette skal som minimum indebære den registreredes ret til menneskelig indgriben, til at fremkomme med sine synspunkter og til at bestride afgørelsen.

Den tilsvarende bestemmelse i Databeskyttelsesdirektivet angav, at dette ikke var nødvendigt, hvis formålet med afgørelsen tages efter anmodning fra den registrerede. Dette er ikke overført til Persondataforordningen, måske fordi det i sammenhæng med fx finance og forsikring vil kunne lade sig gøre for databehandleren at hævde, at det er på den registreredes anmodning, blot en kontrakt tilbydes (selvom den er på svære vilkår), og derved undgå bestemmelsens formål.

Præambel 71 lægger vægt på, at der skal anvendes passende statistiske procedurer, at der skal sikres gennemsigtighed, at der skal anvendes foranstaltninger, der kan sikre, at unøjagtigheder og fejl rettes, og at sikkerheden skal garanteres og diskriminerende faktorer forhindres. Præambel 71 nævner også, at sådanne foranstaltninger ikke angår børn.

Hjemmel i ret

I det andet tilfælde (hjemmel i ret) skal loven selv indeholde passende foranstaltninger, der beskytter den registreredes interesser. Præambel 71 nævner profiling for at garantere sikkerheden og pålideligheden af en tjeneste eller i forbindelse med overvågning af svig og skatteunddragelse som eksempler på automatiserede afgørelser, der kunne være tilladt på grundlag af EU-ret eller medlemsstaternes nationale ret.

Følsomme oplysninger

Automatiske afgørelser baseret på følsomme oplysninger er underlagt flere begrænsninger. Afgørelser, der er baseret på denne slags oplysninger, må kun finde sted:

- med udtrykkeligt samtykke; eller
- hvor behandlingen er nødvendig af hensyn til væsentlige offentlige interesser eller med hjemmel i EU-ret eller medlemsstaternes nationale ret – som skal indeholde foranstaltninger, der beskytter den registreredes interesser.

Hvor kan jeg læse mere?

Artikel 4 (4) & 22 Præambel 71 & 72

Forpligtelser, personoplysningssikkerhed og anmeldelsespligt ved brug på persondatasikkerheden

Resumé

- Persondataforordningen kræver, at alle virksomheder gennemfører en lang række foranstaltninger for at minimere risikoen for overtrædelse af Persondataforordningen og for at bevise, at virksomhederne tager datastyring alvorligt.
- Disse inkluderer ansvarlighedsforanstaltninger så som: Privatlivsbeskyttelsesvurdering, audit, gennemgang af politikker, aktivitetsrapport og (eventuel) udpegning af en databeskyttelsesrådgiver (DPO).
- For de virksomheder, som ikke tidligere har uddelt ansvaret for og haft et budget til databeskyttelse, vil disse krav være en stor byrde.

To-do liste

- ☐ Uddel ansvar for og et budget til databeskyttelse i din virksomhed. Uanset om du beslutter at udpege en databeskyttelsesrådgiver (DPO), vil Persondataforordningens lange liste om datastyring kræve, at én person har ansvaret for, at dette indføres i virksomheden.
- ☐ Vær tydeligt omkring, om den, du tildeler ansvar, er databeskyttelsesrådgiver (DPO) eller ikke (med hensyn til Persondataforordningen) på grund af den beskyttelse, databeskyttelsesrådgiveren (DPO) får gennem Persondataforordningen.
- ☐ Overvej rapporteringsproceduren. Tilsynsmyndighederne vil forvente en rapporteringslinje direkte til bestyrelsen og en jobbeskrivelse for de personer, der er udpeget til at have databeskyttelsesansvar.
- ☐ Overvej rapporteringsproceduren. Tilsynsmyndighederne vil forvente en rapporteringslinje direkte til bestyrelsen og en jobbeskrivelse for de personer, der er udpeget til at have databeskyttelsesansvar.
- ☐ Der skal designes et fuldstændigt program til din virksomhed, som sikrer, at Persondataforordningen overholdes, inklusiv en konsekvensanalyse (PIA), regelmæssige audit, HR politikgennemgang og opdateringer og uddannelse samt programmer for at øge opmærksomheden omkring datasikkerhed.
- ☐ Revidér de eksisterende leveringsaftaler og opdatér RFP og udbudsmateriale, således at de reflekterer Persondataforordningens behandlerforpligtelser.
- ☐ Overvåg tilsynsmyndighedernes/EU's publikationer og branchens leveringsbetingelser og praksiskodeks for at se, om de passer på din virksomhed. Hvis du er leverandør, bør du overveje, hvilken påvirkning Persondataforordningens bestemmelser vil få på din omkostningsstruktur og ansvar for at verificere lovligheden af dine kunders aktiviteter.
- ☐ Implementér foranstaltninger til at rapportere om din virksomheds behandlingsaktiviteter. Hvis du er leverandør, bør du udvikle en strategi til at kunne håndtere kunders anmodninger om assistance til udvikling af sådanne rapporter.

Persondataforordningen nedfælder en række "datastyrings-"koncepter, som lovgivere og tilsynsmyndigheder har lovprist i et stykke tid. Disse koncepter vil skabe store nye operationelle forpligtelser og omkostninger for mange virksomheder i den offentlige og den private sektor.

En generel forpligtelse indføres for dataansvarlige om at vedtage tekniske og organisatoriske foranstaltninger for at opfylde deres forpligtelser i forhold til Persondataforordningen (og for at være i stand til at påvise, at disse er opfyldt.) Det at gennemføre et audit-program samt andre foranstaltninger beskrevet nedenfor (især PIA), vil sandsynligvis blive set i et positivt lys af tilsynsmyndighederne i forbindelse med deres håndhævelse af Persondataforordningen.

Nøgleforpligtelserne inkluderer følgende:

Databeskyttelse gennem design (Privacy by design)

Virksomhederne skal indføre tekniske og organisatoriske foranstaltninger for at vise, at de har overvejet og integreret foranstaltninger til overholdelse af reglerne i deres databehandlingsaktiviteter.

En indførelse af passende medarbejderpolitikker nævnes især samt brugen af pseudonymisering (for at sikre overholdelse af dataminimeringsforpligtelsen).

Konsekvensanalyse (PIA)

En PIA er en analyse til at identificere og minimere risiciene for manglende overholdelse. Det er ikke et nyt koncept, og de gældende kontrolvejledninger anbefaler brugen af dem, og Bird & Bird har gennemført PIA for flere af deres klienter, men Persondataforordningen har nu formaliseret det som et krav, at der gennemføres PIAs.

Dataansvarlige skal især sikre, at en PIA er gennemført ved enhver behandling, der indebærer "*høj risiko*", før behandlingen foretages, hvilket måles ved risikoen for at krænke en persons rettigheder og friheder.

Behandling af "*store mængder*" følsomme oplysninger, eller profileringsaktiviteter nævnes som (ikke-udtømmende) eksempler på højrisiko behandling. Tilsynsmyndigheder skal offentliggøre information om yderligere eksempler og vejledning,

Persondataforordningen kræver, at en PIA som minimum indeholder:

- En beskrivelse: af behandlingsaktiviteterne og deres formål;
- En vurdering: af behovet for og proportionaliteten af behandlingen, de opståede risici og de foranstaltninger, der indføres for at minimere sådanne risici, dette gælder især sikkerhedsforanstaltninger til at beskytte personoplysninger og til overholdelse af Persondataforordningen.

Vi må forvente, at sektorkoder vil opstå i forbindelse med at PIA foretages.

Hvis en databeskyttelsesrådgiver er udpeget (se nedenfor), skal man få hans/hendes rådgivning ved gennemførsel af PIA.

Tilsynsmyndigheden skal konsulteres, før databehandlingen indledes, hvis en PIA viser, at behandlingen vil føre til et højt niveau af tydelig risiko i nogle situationer. Persondataforordningen indeholder særlige processuelle vejledninger for denne proces.

Dataansvarlige skal indhente de registreredes "*og deres repræsentanters*" synspunkter i forbindelse med gennemførsel af en PIA. I forbindelse med HR-databehandling vil dette sandsynligvis blive fortolket som en forpligtelse til at konsultere virksomhedens medarbejderudvalg.

Databeskyttelsesrådgiver (DPO – Data Protection Officer)

Dataansvarlige og databehandlere kan frivilligt udpege en databeskyttelsesrådgiver, men følgende skal udpege en databeskyttelsesrådgiver:

- Offentlige organer (med få undtagelser);
- Virksomheder, hvis kerneaktiviteter kræver:
    - *"regelmæssig og systematisk overvågning" af registrerede "i stort omfang"*, eller
    - Behandling i "stort omfang" af følsomme oplysninger eller oplysninger vedrørende straffedomme og lovovertrædelser; og
- De, som ifølge national lovgivning er forpligtede til det (lande som f.eks. Tyskland vil høre under denne kategori).

Hvor en databeskyttelsesrådgiver er udpeget, skal databeskyttelsesrådgiveren være valgt ud fra sine faglige kvalifikationer og ekspertise (som arbejdsgiveren er forpligtet til at hjælpe dem med at vedligeholde).

Deres opgaver bør som minimum inkludere: rådgivning af kollegaer og overvågning af virksomhedens overholdelse af Persondataforordningen/politikker om beskyttelse af personoplysninger, inklusiv undervisning og skabe opmærksomhed omkring emnet, gennemføre audits, rådgive i forbindelse med PIA og samarbejde med tilsynsmyndighederne.

Passende ressourcer skal benyttes til at give databeskyttelsesrådgiveren mulighed for at overholde forpligtelserne i henhold til Persondataforordningen, og databeskyttelsesrådgiveren rapporterer direkte til den øverste ledelse.

Koncernselskaber kan udpege en enkelt databeskyttelsesrådgiver. En databeskyttelsesrådgiver kan være en ansat eller en ansat konsulent.

Dataansvarlige og databehandlere skal sikre, at databeskyttelsesrådgiveren kan handle selvstændigt uden instruks og må ikke afskediges eller straffes for at udføre sine opgaver. Det bliver spændende at se, hvordan ansættelsesretten vil fortolke denne bestemmelse.

Databeskyttelsesrådgiverens kontaktoplysninger skal offentliggøres og også oplyses til virksomhedens tilsynsmyndighed, idet DPO'en skal være kontaktperson i forbindelse med persondatabeskyttelsesspørgsmål.

Brug af serviceleverandører (databehandlere)

Persondataforordningen pålægger dataansvarlige en stor forpligtelse, når de skal udvælge deres databehandlere af persondata, hvilket vil kræve udbudsprocesser og vil kræve, at udbudsmateriale vurderes regelmæssigt.

Kontrakter skal indgås med databehandlere, som omfatter en stor mængde oplysninger (f.eks. de data, der skal behandles, og varigheden af behandlingen) og forpligtelser (f.eks. assistance i tilfælde af sikkerhedsbrud, foranstaltninger i forhold til pseudonymisering og kryptering samt forpligtelser i forbindelse med bidrag til revisioner). Dette gælder ligeledes, hvis databehandleren ansætter en underdatabehandler.

Kommissionen og tilsynsmyndighederne vil forventeligt offentliggøre godkendte kontraktklausuler til databehandlere. Disse vil, fra databehandlerens synspunkt, sandsynligvis være byrdefulde. Databehandlernes syn på prisaftaler skal derfor efterses.

Databehandlere er udtrykkeligt forpligtet til straks at informere den berørte dataansvarlige, hvis en instruks, ifølge deres holdning, er i strid med Persondataforordningen eller anden EU-lovgivning om persondatabeskyttelse. Dette sætter databehandler-

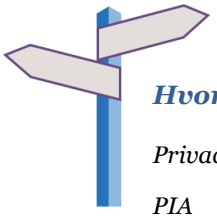
ne i en position, hvor de effektivt skal godkende lovligheden af de opgaver, de bliver bedt om at udføre.

Fortegnelse over databehandlingsaktiviteter

Virksomheder er forpligtede til at føre fortegnelser over deres databehandlingsaktiviteter (kategorier af de oplysninger, der behandles, formålene med behandlingen osv.), i lighed med de forpligtelser som dataansvarlige har til at registrere sig hos Datatilsynet i henhold til gældende lovgivning.

Databehandlere er ligeledes forpligtede til at føre fortegnelser over personoplysninger, som dataansvarlige beder dem om at behandle. Denne forpligtelse vil udfordre en del cloud- og kommunikationsserviceleverandører.

Hvor der ligger en undtagelse fra de ovennævnte forpligtelser for virksomheder, der har mindre end 250 ansatte, gælder denne undtagelse ikke, hvis der behandles følsomme data, hvilket sandsynligvis vil ophæve undtagelsens anvendelighed.



Hvor kan jeg læse mere?

Privacy by design	*Artikel 25*	*Præambel 74-78*
PIA	*Artikel 35-36*	*Præambel 84 / 89-94*
DPO	*Artikel 35-37*	*Præambel 97*
Brug af serviceleverandører	*Artikel 28*	*Præambel 80*
Fortegnelse over databehandlingsaktiviteter	*Artikel 30*	*Præambel 82*

Brud på datasikkerheden og anmeldelsespligt

» Resumé

- Dataansvarlige og databehandlere er nu underlagt et generelt anmeldelsessystem for brud på persondatasikkerheden.
- Databehandlere skal anmelde brud på persondatasikkerheden til dataansvarlige.
- Dataansvarlige skal anmelde brud på persondatasikkerheden til tilsynsmyndigheden og i nogle tilfælde underrette de berørte personer, og i begge tilfælde i overensstemmelse med særlige bestemmelser i Persondataforordningen.
- Dataansvarlige skal have en intern fortegnelse over brud.
- Overtrædelse af bestemmelserne kan resultere i en bødestraf på op til EUR 10.000.000, eller for selskaber op til 2 % af den totale globale omsætning i det foregående regnskabsår, hvad der end er højest.
- Det særlige system til anmeldelse om brud for kommunikationsserviceleverandører, jf. forordningen 611/2013, gælder dog stadig.

☑ To-do liste

☐	I tråd med ansvarlighedsprincippet i Persondataforordningen, skal dataansvarlige og databehandlere udvikle deres egne interne rapporteringsprocedurer til rapportering af brud, herunder et system, der kan identificere hændelser, og planer for, hvordan hændelser skal behandles.
☐	Disse procedurer skal testes og revideres regelmæssigt.
☐	Samarbejd med virksomhedens it-team for at sikre, at de indarbejder de nødvendige tekniske og organisatoriske beskyttelsesforanstaltninger, som gør dataene uforståelige i tilfælde af ulovlig adgang til dataene.
☐	Forsikringer skal gennemgås for at vurdere dækningen i tilfælde af brud.
☐	Skabeloner til databeskyttelsesbestemmelser og udbudsmateriale skal opdateres af kunderne, inklusiv (i) til at indeholde et krav til leverandører om at aktivt rapportere ethvert brud til kunden, og (ii) en understregning af parternes samarbejdspligt.

Brud, som skal anmeldes

I tilfælde af en hændelse, som defineres som "et brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet", gælder de nye regler for anmeldelse af brud i Persondataforordningen:

1. Forpligtelse for databehandlere til at underrette den dataansvarlige

Tidspunkt:

Uden unødig forsinkelse efter, at bruddet opdages.

Undtagelse:

Der er ingen undtagelser i Persondataforordningen (men det Europæiske Databeskyttelsesråd har fået til opgave at udarbejde retningslinjer vedrørende "*de særlige situationer, hvor en dataansvarlig eller en databehandler skal anmelde bruddet på persondatasikkerheden*").

Bemærkninger:

- Alle brud skal anmeldes.
- Det Europæiske Databeskyttelsesråd skal udarbejde retningslinjer, der specificerer betydningen af "uden unødig forsinkelse" og de særlige situationer, hvori en databehandler skal anmelde bruddet på persondatasikkerheden.

2. Forpligtelse for dataansvarlige til at anmelde til tilsynsmyndighederne

Tidspunkt:

Uden unødig forsinkelse og, hvis muligt, ikke senere end 72 timer efter, at man er blevet opmærksom på bruddet.

Undtagelse:

Der skal ikke anmeldes, hvis det er usandsynligt, at bruddet vil indebære en risiko for personers rettigheder og frihedsrettigheder.

Bemærkninger:

- Hvis forpligtelsen vedrørende tidspunkt ikke overholdes, skal dette begrundes over for tilsynsmyndigheden (f.eks. via anmodning fra en retshåndhævende myndighed)
- Det Europæiske Databeskyttelsesråd skal udarbejde retningslinjer, der specificerer betydningen af "uden unødig forsinkelse" og de særlige situationer, hvori en dataansvarlig skal anmelde bruddet på persondatasikkerheden.

3. Forpligtelse for dataansvarlige til at underrette de berørte personer

Hvis en dataansvarlig endnu ikke har gjort det, kan tilsynsmyndigheden kræve, at den dataansvarlige underretter de berørte personer, medmindre én af de tre undtagelser opfyldes.

Tidspunkt:

Uden unødig forsinkelse. Behovet for at mindske en umiddelbar risiko for skade kræver en hurtig underretning af de registrerede. Et behov for at indføre nødvendige foranstaltninger mod fortsatte eller lignende brud på databeskyttelsen, kan dog retfærdiggøre en længere forsinkelse.

Undtagelse:

Ingen rapportering, hvis:

- Bruddet ikke umiddelbart vil resultere i en høj risiko for personers rettigheder og frihedsrettigheder,
- Passende tekniske eller organisatoriske sikkerhedsforanstaltninger er gennemført på hændelsestidspunktet (f.eks. kryptering), eller
- Dette vil kræve en uforholdsmæssig indsats (hvor en offentlig meddelelse eller "tilsvarende foranstaltning" kan benyttes i stedet, således at de be-

rørte personer underrettes på en tilsvarende effektiv måde).

Kommentarer:

- Anmeldelsespligt er underlagt en skærpet tærskel.
- Det Europæiske Databeskyttelsesråd skal udarbejde retningslinjer vedrørende begrebet "høj risiko".

Dokumentationskrav

- Internt fortegnelse over brud på datasikkerheden: Den dataansvarlige forpligtes til at dokumentere enhver hændelse, "herunder de faktiske omstændigheder vedrørende bruddet, dets virkninger og de trufne afhjælpende foranstaltninger". Tilsynsmyndigheden kan anmodes om at vurdere, hvordan dataansvarlige overholder deres forpligtelse til at anmelde i forbindelse med brud på datasikkerheden.
- Der er ligeledes fastsat krav, der skal opfyldes ved kommunikation med tilsynsmyndigheden (f.eks. beskrivelse af karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede, og kategorier og omtrentlige antal berørte registreringer osv.) og kommunikation til berørte personer (f.eks. i klart og forståeligt sprog beskrive karakteren af bruddet på persondatasikkerheden samt følgende oplysninger: i) navn og kontaktoplysninger for databeskyttelsesrådgiveren eller et andet kontaktpunkt, hvor yderligere oplysninger kan indhentes; ii) sandsynlige konsekvenser af bruddet på persondatasikkerheden, og iii) de foranstaltninger, den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på datasikkerheden, herunder foranstaltninger for at begrænse dets mulige skadesvirkninger).

Sanktioner i tilfælde af manglende overholdelse

Hvis ovenstående krav ikke overholdes, vil virksomheden blive straffet med en administrative bøder på op til EUR 10.000.000, eller for virksomheder op til 2 % af den samlede årlige globale omsætning i det foregående regnskabsår, hvis dette beløb er højere.

Hvad med det andet EU-system for anmeldelse af brud, der gælder for leverandører af kommunikationstjenester?

Som tingene er nu, gælder lov nr. 611/2013, som beskriver en specifik procedure for anmeldelse af brud (i direktiv 2002/58/EF ("e-databeskyttelsesdirektivet") med ændringer) stadig for leverandører af offentligt tilgængelige telekommunikationstjenester (teleselskaber, internetudbydere og e-mailleverandører). Det er stadig uvist, om revideringen af e-databeskyttelsesdirektivet, som Kommissionen har annonceret i løbet af 2016, vil udløse en afstemning eller en opretholdelse af de to anmeldelsessystemer for brud.

Hvor kan jeg læse mere?

Artikel 24,33,34 70 og 83 *Præambel 85-88*

Adfærdskodekser og -certificeringer

Resumé

Persondataforordningen tillader godkendelse af adfærdskodeks ("Kodeks") og akkreditering af certificeringer, databeskyttelsesmærkninger og -mærker som hjælp for dataansvarlige og databehandlere til at bevise overholdelse af reglerne og best practice.

Adfærdskodeks:

- Sammenslutninger og andre repræsentative organer kan udarbejde adfærdskodeks, der skal godkendes, registreres og offentliggøres af en tilsynsmyndighed eller, hvor behandlingen foregår på tværs af medlemsstaterne, af det Europæiske Databeskyttelsesråd ("EDPB"). EU-Kommissionen kan erklære kodeks, som anbefales af EDPB, for at have generel gyldighed i EU.
- Kodeks kan være godkendt i relation til en lang række emner, og overholdelse af kodeks kan hjælpe dataansvarlige og databehandlere med at bevise deres overholdelse af forpligtelserne i Persondataforordningen.
- Overholdelse af kodeks vil være overvåget, hvilket kan udføres af passende kvalificerede og anerkendte organer. Dataansvarlige og databehandlere, som har krænket et relevant kodeks, kan blive suspenderet fra deltagelse i kodekset og vil blive rapporteret til tilsynsmyndigheden.

Certificeringer, databeskyttelsesmærkninger og -mærker:

- Der opfordres til etablering af certificeringsmekanismer for databeskyttelse, databeskyttelsesmærkninger og -mærker.
- Certifikater udstedes af certificeringsorganer (som endnu ikke er dannet).
- Certificering er frivilligt, men certificering vil gøre det muligt for dataansvarlige og databehandlere at påvise overholdelse af Persondataforordningen.
    - Certifikater vil være gyldige i tre år og skal fornyes.
    - Det Europæiske Databeskyttelsesråd vil opretholde et offentligt tilgængeligt register over alle certificeringsmekanismer, databeskyttelsesmærkninger og -mærker.

To-do liste

- ☐ *Adfærdskodeks*
  For at få et forspring før akkrediteringsprocedurerne indføres af tilsynsmyndighederne, bør databehandlere (så som cloud-leverandører) og dataansvarlige inden for særlige sektorer overveje at identificere eller etablere sammenslutninger eller repræsentative organer, som kan udvikle kodeks, der skal godkendes af tilsynsmyndigheden.
- ☐ *Certificeringer, mærkninger eller mærker*
  Databehandlere og dataansvarlige skal følge udviklingen i forhold til akkreditering af certificeringsvirksomheder og overveje, om de ønsker at ansøge om certificering, når tiden er inde.
- ☐ Så snart certificeringssystemerne er etablerede, skal dataansvarlige gøre sig bekendt med de relevante systemer og tage certificeringer, databeskyttelsesmærkninger og -mærker med i betragtning, når de udvælger deres databehandlere/serviceleverandører.

Adfærdskodeks

Kodekser er en vigtige for udbredelsen og tilpasningen af værktøjerne, som anvendes til at følge databeskyttelselovgivningen, som dataansvarlige og databehandlere kan trække på ved hjælp af en "semi-selvregulerende" mekanisme.

Det forventes, at kodeks kan give myndighedsvejledning på visse nøgleområder, herunder:

- Legitime interesser i specifikke sammenhænge;
- Pseudonymisering;
- Udøvelse af de registreredes rettigheder;
- Beskyttelse af mindreårige og forældresamtykke;
- Korrekt implementering af privacy by design og by default og sikkerhedsforanstaltninger;
- Anmeldelse af brud på datasikkerheden; og
- Tvistløsning mellem dataansvarlige og de registrerede.

Udviklingen og godkendelse af kodeks vil sandsynligvis resultere i en række fordele, herunder:

- Etablering og opdatering af best practice, som kan anvendes til overholde lovgivningen i specifikke former for databehandlingssammenhænge;

- At gøre det muligt for dataansvarlige og databehandlere at forpligte sig til at overholde de anerkendte standarder og praksis og blive anerkendt for at gøre det;

- Overholdelse af kodeks kan påvise, at dataimportører (både dataansvarlige og databehandlere) udenfor EU/EØS har indført passende sikkerhedsforanstaltninger til brug for Artikel 46. Overførsel, der foretages på baggrund af en godkendt adfærdskodeks sammen med bindende og retsgyldige forpligtelser for importøren til at benytte passende sikkerhedsforanstaltninger, kan ske uden særlig autorisation fra tilsynsmyndigheden, og adfærdskodeks kan derfor tilbyde en alternativ mekanisme til at håndtere internationale overførsler, på lige fod med kontraktbestemmelser og BCR.

Godkendelse af adfærdskodeks

Adfærdskodeks, som foreslås af sammenslutninger eller repræsentative organer i relation til databehandlingsaktiviteter, som kun vedrører en medlemsstat, skal indsendes til den relevante tilsynsmyndighed, som afgiver udtalelse om kodeksen og - efter eventuelle ændringer eller tilføjelser – godkender denne. Hvis en adfærdskodeks omfatter databehandling i flere medlemsstater, skal det indsendes til det Europæiske Databeskyttelsesråd (EDPB) til vurdering. Efter eventuelle ændringer og tilføjelser kan adfærdskodeksen og EDPBs vurdering indsendes til Kommissionen, som efter gennemgang heraf kan erklære det for gyldigt.

Kodeks skal samles i offentligt tilgængelige registre.

Kontrol af overholdelse

Kontrol af overholdelse af adfærdskodeks skal kun foretages af organer, der er akkrediteret af tilsynsmyndigheden.

For at bliver akkrediteret, skal sådanne organer påvise:

- Deres uafhængighed og ekspertise;
- At de har fastlagt procedurer til at vurdere databehandlers og dataansvarliges egnethed til at anvende kodeksen og til at overvåge overholdelse heraf samt til at foretage regelmæssig gennemgang af adfærdskodeksen;
- Evnen til at behandle klager over overtrædelser; og
- At de har indført processer til at undgå interessekonflikter

Akkrediteringer kan tilbagekaldes, hvis betingelserne for akkrediteringen ikke længere opfyldes.

Certificeringer, databeskyttelsesmærkninger og -mærker

Konceptet med at certificere databehandlingsaktiviteter er en væsentlig udvikling hen mod at opnå en pålidelig og reviderbar ramme for databehandlingsaktiviteter. Det vil sandsynligvis være særligt relevant i forbindelse med cloud-computing og andre former for multi-tenant tjenesteydelser, hvor selvstændig revision ofte ikke er mulig i praksis.

Medlemsstater, tilsynsmyndigheder, det Europæiske Databeskyttelsesråd og Kommissionen opfordres alle til at etablere certificeringsmekanismer for databeskyttelse, databeskyttelsesmærkninger og -mærker i forbindelse med særlige behandlingsaktiviteter.

Certificering er frivilligt og skal være tilgængelig i gennemsigtige processer. Tilsynsmyndigheden eller EDPB kan udvikle kriterier for en fælles certificering: Den Europæiske Databeskyttelsesmærkning.

Der er to hovedfordele ved certificeringer:

1. Dataansvarlige og databehandlere vil kunne påvise, at de overholder reglerne, især hvad angår implementering af tekniske og organisatoriske foranstaltninger.

2. Certifikater kan påvise, at dataimportører (dataansvarlige såvel som databehandlere) uden for EU/EØS har indført passende sikkerhedsforanstaltninger i henhold til Artikel 46. Overførsler, der foretages på baggrund af en godkendt certificeringsmekanisme sammen med bindende og retsgyldige forpligtelser for importøren til at anvende passende sikkerhedsforanstaltninger, kan foretages uden særlig tilladelse fra tilsynsmyndigheden, og certificeringer tilbyder derfor en alternativ mekanisme til at håndtere internationale overførsler på lige fod med kontraktbestemmelser og BCR.

Certificeringer til behandlingsaktiviteter udstedes for en periode på 3 år og kan forlænges eller tilbagetrækkes, hvis betingelserne for udstedelsen af certifikatet ikke længere er opfyldt.

EDPB skal samle alle certificeringsmekanismer, databeskyttelsesmærkninger og –mærker i et offentligt tilgængeligt register.

Certificeringer kan udstedes af – private eller offentlige – akkrediterede organer. De nationale akkrediteringsorganer og/eller tilsynsmyndigheden kan akkreditere organer (så de kan udstede certificeringer, mærker eller mærkninger), som (f.eks.):

- Har den krævede ekspertise og er uafhængige i forhold til certificeringens genstand;
- Har procedurer for revision og tilbagetrækning af certificeringer, databeskyttelsesmærkninger og -mærker;
- Kan behandle klager over overtrædelser af certificeringerne; og
- Har regler for håndtering af interessekonflikter.

Kriterier for akkreditering udvikles af tilsynsmyndighederne eller EDPB og skal være offentligt tilgængelige.

Akkreditering til certificeringsorganer udstedes for en maksimumperiode på fem år og kan forlænges eller tilbagetrækkes, hvis betingelserne for akkrediteringen ikke længere opfyldes.

Hvor kan jeg læse mere?

Adfærdskodeks	*Artikel 24, 32, 40, 41, 57, 58, 64, 70, 83*	*Præambel 71, 81, 98, 99, 148, 168*
Certificeringer, Databeskyttelsesmærkninger og mærker	*Artikel 24;25; 28; 32; 40; 42, 43, 46; 57; 58; 64; 70; 83*	*Præambel 77, 8 100, 166, 168*

Overførsel af personoplysninger

Resumé

- Overførsel af personoplysninger til modtagere i "tredjelande" (dvs. udenfor det Europæiske Økonomiske Samarbejdsområde ("EØS")) er fortsat lovreguleret og er under visse omstændigheder underlagt begrænsninger.
- Persondataforordningens forpligtelser er stort set magen til dem, som er pålagt af Databeskyttelsesdirektivet, med visse forbedringer i forhold til hvordan reglerne kan overholdes, især skal bemærkes, at reglen om, at tilsynsmyndighederne på forhånd skal underrettes om standardkontraktbestemmelser er fjernet, og at der tilskyndes til, at der udvikles godkendte adfærdskodeks og certificeringsmekanismer.
- Overførsel af personoplysninger vil stadig være en betydelig problemstilling for multinationale virksomheder og også for alle andre, der benytter sig af forsyningskæder, som behandler personoplysninger udenfor EØS.
- Overtrædelse af Persondataforordningens bestemmelser klassificeret i gruppen af overtrædelser, hvor det maksimale bødeniveau kan idømmes (på til 4 % af den årlige omsætning).
- Der kan lægges sag an for overtrædelser begået af dataansvarlige og databehandlere.

To-do liste

☐	Gennemgå og kortlæg de vigtigste internationale datastrømme.
☐	Find ud af hvilke mekanismer til overførsel af personoplysninger, der er på plads, og om de fortsat vil være tilstrækkelige.
☐	Gennemgå spørgsmålene, der findes på standard udbudsskabeloner og kontraktbestemmelser for at sikre, at du forstår oplysningerne om din leverandørs påtænkte overførsel af personoplysninger, som du er ansvarlig for og at overførsel foregår på lovlig måde.
☐	Hvis du eller din leverandør tidligere anvendte en safe harbor-certificering for at sikre tilstrækkelighed, er denne ikke længere gældende. Du må genoverveje dine forhold med serviceudbydere og/eller kunder for at fastlægge et nyt retsgrundlag for løbende transatlantiske dataoverførsler.
☐	For overførsel indenfor koncerner skal det overvejes, om bindende virksomhedsregler kunne være en brugbar løsning.
☐	Hvis du overfører personoplysninger udenfor EØS i forbindelse med, at du leverer varer eller tjenesteydelse, skal du være forberedt på at få spørgsmål fra kunder om, hvordan du (og dine leverandører) vil overholde reglerne om overførsel.
☐	Hold øje med udviklingen indenfor godkendte adfærdskodeks og certificeringsmekanismer, der gennemføres i forbindelse med en virksomheds aktiviteter.

Kommentar

Overførsel af personoplysninger til "tredjelande" (dvs. uden for EØS) er stadigvæk underlagt begrænsninger i Persondataforordningen. Det vil stadig være en betydelig problemstilling for alle multinationale virksomheder. De nuværende krav vil dog stort set opretholdes med visse forbedringer.

Den største forbedring er, at den nuværende proces, hvorved overførsler, der er baseret på standardkontrakter, skal indberettes til eller godkendes af databeskyttelsesmyndigheder, afskaffes.

Kommissionen har beføjelse til at afgøre, at visse lande, områder, specifikke sektorer eller internationale virksomheder yder tilstrækkelig beskyttelse i forbindelse med dataoverførsel. Den nuværende liste over lande, som tidligere er godkendt af Kommissionen, vil stadig være gældende, nemlig: Andorra, Argentina, Canada (hvor PIPEDA finder anvendelse), Schweiz, Færøerne, Guernsey, Israel, Isle of Man, Jersey, Den østlige republik Uruguay og New Zealand. Lande, der skal tilføjes til eller slettes fra denne liste, skal offentliggøres i EU-Tidende.

Den amerikanske safe habor-ordning, som tidligere har været godkendt af Kommissionen, er ikke længere gældende, men det omtaler Persondataforordningen ikke, denne problemstilling vil blive behandlet særskilt.

Persondataforordningen beskriver nøje de pågældende procedurer og kriterier, som Kommissionen skal tage i betragtning, når den fastlægger det tilstrækkelige beskyttelsesniveau, og påpeger, at det er nødvendigt at sikre, at tredjelande har et beskyttelsesniveau, der "*i al væsentlighed svarer til beskyttelsesniveauet i EU*", og som giver de registrerede effektive og eksigible rettigheder og retsmidler. Kommissionen skal rådføre sig med Det Europæiske Databeskyttelsesråd, når den vurderer beskyttelsesniveauer og skal sikre, at der foretages løbende overvågning og evaluering af de beslutninger om tilstrækkelighed, der er taget (mindst hvert fjerde år). Kommissionen har også beføjelse til at ophæve, ændre eller suspendere beslutninger om tilstrækkelighed.

Andre nuværende metoder til overførsel af personoplysninger vil stadig være accepteret: standardkontrakter (enten vedtaget af Kommissionen eller vedtaget af en tilsynsmyndighed og godkendt af Kommissionen) vil forsat være en løsning, og de nuværende godkendte standardkontrakter vil stadig være gældende.

Anvendelse af andre passende sikkerhedsforanstaltninger, som fx bindende virksomhedsregler og retligt bindende og eksigible instrumenter mellem offentlige myndigheder, accepteres også.

En markant ændring er, at overførsel vil være tilladt, hvis der anvendes en godkendt adfærdskodeks (baseret på den nye ordning i Artikel 40) eller en certificeringsmekanisme (baseret på den nye ordning i Artikel 42), forudsat at bindende og eksigible tilsagn er afgivet af den dataansvarlige og databehandleren i tredjelandet om at anvende de fornødne sikkerhedsforanstaltninger, herunder vedrørende den registreredes rettigheder. Der skal også træffes beslutninger om bestemmelser om ad hoc sikkerhedsforanstaltninger, der er underlagt godkendelse fra de pågældende tilsynsmyndigheder.

Med hensyn til bindende virksomhedsregler bliver de nuværende krav til dataansvarlige og databehandlere nu med Persondataforordningen skrevet ind i loven. De kræver stadig godkendelse fra den pågældende tilsynsmyndighed, men dette skal afgøres i overensstemmelse med sammenhængsmekanismen. Dette vil være nyttigt i de få medlemsstater, der stadig ikke accepterer bindende virksomhedsregler.

Der findes fortsat en række undtagelser, der tillader overførsel af personoplysninger under visse omstændigheder, som svarer til de nuværende undtagelser, herunder: udtrykkeligt samtykke, nødvendig af hensyn til opfyldelse af en kontrakt, vigtige samfundsinteresser, fastlægge retskrav, vitale interesser og oplysninger fra offentlige registre. Der er også en ny (begrænset) undtagelse, der kan anvendes, forudsat at overførsel ikke gentages, kun vedrører et begrænset antal registrerede, er nødvendig af hensyn til den dataansvarliges vægtige legitime interesser (som ikke tilsidesættes af den registreredes interesser eller rettigheder) og som den dataansvarlige har vurderet (og bevist) alle omstændigheder i forbindelse med overførslen og på grundlag heraf giver passende garantier. Den dataansvarlige skal underrette tilsynsmyndigheden og den registrerede, når denne undtagelse anvendes.

Afslutningsvist gør Persondataforordningen det som forventet klart, at det ikke er lovligt at overføre

personoplysninger udenfor EØS efter lovgivnings-
mæssigt krav fra tredjeland.

Hvor kan jeg læse mere?

Artikel 44-50 Præambel 101-116

Udnævnelse af tilsynsmyndigheder

Resumé

- Der vil fortsat være nationale databeskyttelsesmyndigheder.
- De skal samarbejde med EU-Kommissionen, og de skal overvåge anvendelsen af Persondataforordningen.
- De skal være uafhængige.
- Medlemmer af tilsynsmyndighederne skal være udpeget på en offentlig og gennemskuelig måde, og de skal have kendskab til databeskyttelse.

To-do liste

Intet (undtagen måske, hvis du er et medlem af eller ansat hos en eksisterende databeskyttelsesmyndighed!)

Kommentar

Der vil fortsat være nationale databeskyttelsesmyndigheder (tilsynsmyndigheder). De skal overvåge anvendelsen af Persondataforordningen for at beskytte de grundlæggende rettigheder i forbindelse med behandling af personoplysninger og lette fri udveksling af personoplysninger indenfor EU.

De skal samarbejde med hinanden og EU-Kommissionen for at bidrage til ensartet anvendelse af Persondataforordningen.

Stater, som fx Tyskland, kan have mere end en tilsynsmyndighed, men en af dem skal udpeges som repræsentant i Det Europæiske Databeskyttelsesråd ("EDPB").

Kommissionen skal informeres om de nationale love, som vedtages om oprettelse og udnævnelse af tilsynsmyndigheder.

Tilsynsmyndighederne skal være fuldt uafhængige (men være underlagt finansiel kontrol og retsligt tilsyn). Medlemmer af tilsynsmyndighederne skal være fri for udefrakommende indflydelse og må hverken søge eller modtage instrukser fra andre. De skal afholde sig fra enhver handling, der er uforenelig med deres hverv og må heller ikke, så længe deres embedsperiode varer, udøve uforenelig lønnet eller ulønnet virksomhed.

Hver medlemsstat skal sikre, at deres tilsynsmyndigheder råder over de nødvendige menneskelige, tekniske og finansielle ressourcer til effektivt at kunne udføre sine opgaver og udøve sine beføjelser.

Hver tilsynsmyndighed skal vælge, råde over og lede sit eget personale. Tilsynsmyndighedens budget skal være offentligt og skal føres særskilt, også selv om det er en del af det nationale budget.

Medlemsstaterne vedtager love om oprettelse af tilsynsmyndigheder, der fastsætter regler for deres medlemmer, deres kvalifikationer og udvælgelseskriterier. Deres embedsperiode skal være mindst 4 år og medlemsstaterne beslutter, om de kan genudnævnes. Medlemmernes forpligtelser vedrørende uafhængighed, som er beskrevet ovenfor, skal være inkorporeret i den nationale lovgivning. Medlemmer af tilsynsmyndighederne og deres personale har tavshedspligt både under og efter deres embedsperiode.

Bestemmelserne vedrørende oprettelse af tilsynsmyndigheder er en mere detaljeret præcisering af bestemmelserne i Artikel 28 i det gamle Databeskyttelsesdirektiv 95/46/EC. Der er ikke noget bemærkelsesværdigt i de nye regler. Nogle af punkterne er dog værd at bemærke: specificeringen af udnævnelsesperioden, fremhævelsen af uafhængigheden, fastholdelsen af bestemmelsen om tilstrækkelige ressourcer til hver tilsynsmyndighed og kravet om, at "*hvert medlem [af tilsynsmyndigheder] skal have de kvalifikationer, den erfaring og den kompetence, navnlig på området beskyttelse af personoplysninger, der er nødvenlige for at varetage dets hverv og udøve dets beføjelser*".

Der vil sandsynligvis blive diskussioner om, hvorvidt tilsynsmyndighederne får tilført tilstrækkelige midler, især i tilfælde, som fx Storbritannien, hvor den traditionelle kilde til finansiering fra registrerings- og anmeldelsesgebyrer ophører.

Hvor kan jeg læse mere?

Artikel 51-54 *Præambel 117-123, Kapitel VI Afdeling 1*

Kompetencer, opgaver og beføjelser

Resumé

- Tilsynsmyndigheder tildeles specifik kompetence til at udøve de beføjelser, der tillægges dem på deres egen medlemsstats område.
- En ledende tilsynsmyndighed har kompetence i grænseoverskridende sager (se afsnit om sammenhæng mellem tilsynsmyndigheder for flere oplysninger).
- Tilsynsmyndigheder tildeles en omfattende liste af beføjelser og opgaver.

To-do liste

☐	Sæt dig ind i de omfattende beføjelser og opgaver, som tilsynsmyndighederne har.
☐	Hvis du udfører grænseoverskridende behandling af personoplysninger, skal du sætte dig ind i systemet med ledende tilsynsmyndigheder (se afsnit om samarbejde og sammenhæng mellem tilsynsmyndigheder).
☐	Du ønsker måske også at overveje at arbejde hen mod at overholde en godkendt adfærdskodeks eller certificering, som kræver godkendelse fra en tilsynsmyndighed.

Kompetence

Tilsynsmyndigheder (også benævnt "Databeskyttelsesmyndigheder" eller "DPA") har kompetence "*til at udføre de opgaver og udøve de beføjelser",* som beskrives i Persondataforordningen på deres egen medlemsstats område. Præambel 122 fortæller os, at dette omfatter "*behandling, der påvirker registrerede på dens område, eller behandling, der udføres af en dataansvarlig eller en databehandler, som ikke er etableret i Unionen, når den er rettet mod registrerede, som har bopæl på dens område*".

I tilfælde hvor retsgrundlaget for behandling er, uanset om behandlingen foretages af private organer eller offentlige myndigheder, en retlig forpligtelse, eller hvor behandling er nødvendig for udførelse af en opgave i samfundets interesse eller i forbindelse med en offentlig myndighedsudøvelse, er det den pågældende myndighed, der alene har kompetence og systemet med grænseoverskridende, ledende tilsynsmyndighed er tilsidesat. Formuleringen er ret uklar, men i præambel 128 står der, at det kun er tilsynsmyndigheden i den medlemsstat, hvor den offentlige myndighed eller det private organ er etableret, der har kompetence, når behandlingen foretages i offentlighedens interesse. Det er uklart, om dette er i forhold til koncerner med flere afdelinger og er en måde at se bort fra one-stop shop mekanismen, eller om det alene er medlemsstatens tilsynsmyndighed, der har kompetence, også selv om behandlingen foregår et andet sted i EU. Dette kunne have mange anvendelsesmuligheder for private organer – fx finansielle institutioner, der udfører aktiviteter til bekæmpelse af hvidvaskning af penge i forhold til kunder andre steder i EU end i hjemlandet.

Tilsynsmyndigheder har ikke kompetence til at føre tilsyn med domstoles behandlingsaktiviteter, når disse handler i deres egenskab af domstol. 'Domstol' er ikke defineret, og det er ikke helt klart, hvor langt ned i retsvæsenets hierarki denne regel gælder.

Der oprettes et system med ledende tilsynsmyndigheder, der skal tage sig af grænseoverskridende behandlinger (se afsnit om Samarbejde og sammenhæng mellem tilsynsmyndigheder for mere information om denne komplicerede ordning).

Opgaver

Tilsynsmyndighederne får en meget opfattende liste med opgaver i Persondataforordningens Artikel 57. Der er ingen grund til at opremse dem alle sammen, for den sidste på listen er at *"udføre enhver anden opgave i forbindelse med beskyttelse af personoplysninger"*. Tilsynsmyndighederne skal derfor gøre alt, der med rimelighed kan siges at handle om "*beskyttelse af personoplysninger*".

Nogle opgaver er værd at bemærke. Tilsynsmyndigheder skal føre tilsyn med og håndhæve "*anvendelsen*" af Persondataforordningen og fremme offentlighedens, dataansvarliges og databehandleres kendskab til forordningen.

De skal rådgive deres regeringer og parlamenter om nye lovforslag.

At hjælpe registrerede, at behandle og undersøge klager, der indgives af en registreret eller repræsentative organer, at gennemføre undersøgelser og især at samarbejde med andre tilsynsmyndigheder er alle specifikt nævnt, ligesom at overvåge udvikling af teknisk praksis og handelspraksis inden for informationsteknologi er nævnt.

Tilsynsmyndigheder skal tilskynde til udarbejdelse af adfærdskodekser og certificeringsmekanismer, og de skal "*foretage akkreditering*" af certificeringsorganer og de organer, der overvåger adfærdskodekser.

Tilsynsmyndigheder kan ikke kræve betaling fra de registrerede eller databeskyttelsesrådgivere; der er dog ikke nævnt noget i Persondataforordningen om, hvorvidt der kan kræves betaling fra dataansvarlige og databehandlere for den ydelse, de modtager fra tilsynsmyndighederne.

Beføjelser

Persondataforordningens artikel 58 opremser de beføjelser, som medlemsstaterne kan give tilsynsmyndighederne, hvis de ønsker det. Mange af beføjelserne svarer til den specifikke liste over opgaver i artikel 57 og behøver ikke gentagelse.

Det er dog værd at nævne følgende: at give dataansvarlige eller databehandlere påbud om at afgive

oplysninger; at foretage undersøgelser i form af databeskyttelsesrevisioner; at få adgang til lokaler og oplysninger, udstede advarsler og udtale kritik og at pålægge bøder; at give dataansvarlige og databehandlere påbud om at overholde Persondataforordningen og de registreredes rettigheder; at forbyde behandling og overførsel af oplysninger til modtagere udenfor EU; godkende kontraktbestemmelser og bindende virksomhedsregler. Udøvelsen af tilsynsmyndighedens beføjelser er underlagt de fornødne garantier og retlig indsigelse.

Medlemsstater skal give tilsynsmyndigheder ret til at indbringe sager for judicielle myndigheder og "*om nødvendigt at indlede eller på anden måde deltage i retssager med henblik på at håndhæve bestemmelserne i denne forordning*". Der vil formentlig stadig være forskelle i beføjelserne i henhold til national lovgivning og bestemmelser.

Tilsynsmyndigheder skal udarbejde årlige rapporter.

Kort sagt er tilsynsmyndighedernes kompetencer, opgaver og beføjelser en omfattende liste over alt det, en tilsynsmyndighed skal og kan gøre. Dette er stort set en forudsigelig konsolidering af de nuværende praksisser med nogle nyskabelser i individuelle medlemsstater.

Hvor kan jeg læse mere?

Præambel 117-123, Kapitel VI Afdeling 2 Artikel 55- 59

Samarbejde og sammenhæng mellem tilsynsmyndigheder

Resumé

I tilfælde hvor der sker grænseoverskridende behandling indenfor EU, foreslog EU-Kommissionen en one-stop shop, hvorved tilsynsmyndigheden for den dataansvarliges hovedvirksomhed ville være den eneste tilsynsmyndighed, der skulle overvåge og sikre, at den dataansvarlige overholder forordningen i hele EU. Da dette blev mødt med megen modstand, er det blevet modereret. Der vil nu være en ledende tilsynsmyndighed, i tilfælde hvor der er tale om koncerner eller grænseoverskridende behandling indenfor EU, som vil være tilsynsmyndigheden for hovedvirksomheden, men tilsynsmyndigheder i andre lande, hvor den dataansvarlige er etableret eller hvor registrerede bliver betydeligt berørt eller myndigheder, som der er blevet klaget til, kan også blive involveret og den ledende tilsynsmyndighed skal samarbejde med dem. Tilsynsmyndigheder, der ikke er ledende tilsynsmyndigheder, kan også behandle sager, som alene er lokale, som involverer en grænseoverskridende dataansvarlig.

To-do liste

- ☐ Hvis du kun har aktiviteter i én medlemsstat – (som stadig er tilfældet for størstedelen af virksomheder), så er den ledende tilsynsmyndighed irrelevant og konfliktløsningsmekanismen berører dig sandsynligvis kun, hvis et relevant foreslået adfærdskodeks eller certificeringsmekanisme bliver forsinket, eller hvis Det Europiske Databeskyttelsesråd gør indsigelse imod det.
- ☐ Hvis du har aktiviteter i to eller flere medlemsstater, skal du finde ud af, hvem din ledende tilsynsmyndighed er og mødes med tilsynsmyndigheden i forløbet op til implementeringen ved fx at deltage i uddannelse og rådgivning, som den tilbyder.

Kommentar

Den ledende tilsynsmyndigheds kompetencer

Hvis en dataansvarlig eller databehandler udfører grænseoverskridende behandling, enten gennem flere virksomheder indenfor EU eller selv med kun en virksomhed, optræder tilsynsmyndigheden for hovedvirksomheden eller den eneste virksomhed som ledende tilsynsmyndighed i forhold til den grænseoverskridende behandling.

Den nationale tilsynsmyndighed har stadig kompetence til at udøve beføjelser, hvis en klage indgives, eller hvis en overtrædelse finder sted indenfor dens område, og hvis klagens eller overtrædelsens indhold kun relaterer sig til en virksomhed i det område eller i betydelig grad kun påvirker registrerede i den pågældende stat. Det Europæiske Databeskyttelsesråd ("EDPB") kan rådgive om, hvad der menes med at påvirke registrerede i mere end en medlemsstat *"i betydelig grad"*.

Sådanne lokale sager skal anmeldes til den ledende tilsynsmyndighed, som har tre uger til at beslutte, om de vil gribe ind (idet det tages i betragtning, om der er en virksomhed i en anden stat) og anvender så samarbejdsproceduren. Ikke-ledende tilsynsmyndigheder kan komme med forslag til afgørelse til den ledende tilsynsmyndighed.

Hvis den ledende tilsynsmyndighed ikke griber ind, behandler de lokale tilsynsmyndigheder sagen og anvender om nødvendigt beføjelserne til gensidig bistand og fælles undersøgelser.

Samarbejdsprocedure

Den ledende tilsynsmyndighed skal samarbejde med andre "*berørte*" tilsynsmyndigheder. De skal udveksle oplysninger og prøve at nå til enighed.

Den ledende tilsynsmyndighed skal underrette de andre tilsynsmyndigheder og kan anmode dem om at yde gensidig bistand og foretage fælles undersøgelser på deres områder. Den ledende tilsynsmyndighed skal straks forelægge et udkast til afgørelse til de berørte tilsynsmyndigheder, og de har fire uger til at gøre indsigelse. Derefter kan der forelægges et revideret udkast med en to-ugers indsigelsesperiode. Hvis den ledende tilsynsmyndighed ikke ønsker at følge de berørte myndigheders indsigelse, skal den forelægge sagen for den sammenhængsmekanisme, som Det Europæiske Databeskyttelsesråd fører tilsyn med.

Der er udførlige regler for, hvilken tilsynsmyndighed der skal træffe den formelle beslutning og informere den dataansvarlige, men den ledende tilsynsmyndighed har pligt til at sikre, at den dataansvarlige, i henhold til den formelle beslutning, træffer foranstaltninger til at overholde afgørelsen i alle dens virksomheder.

En ledende tilsynsmyndighed kan dog under ekstraordinære omstændigheder handle omgående uden at afvente sammenhængsmekanismens gennemførelse.

Systemet med en ledende tilsynsmyndighed har nogle åbenlyse svagheder og kunne blive underminеret på områder, hvor ikke-ledende tilsynsmyndigheder kan hævde, at de på grundlag af at registrerede i deres område bliver påvirket i betydelig grad af behandling, der udføres af en dataansvarlig, hvis hovedvirksomhed er et andet sted; systemets succes vil i stor udstrækning afhænge af, om der er enighed og forståelse mellem tilsynsmyndighederne.

Gensidig bistand, fælles aktiviteter og sammenhæng

Tilsynsmyndigheder skal yde bistand til hinanden i form af oplysninger eller gennemførelse af "*forudgående godkendelse og høringer, inspektioner og undersøgelser*". EU-Kommissionen kan fastsætte form og procedure for gensidig bistand.

Tilsynsmyndigheder kan foretage fælles undersøgelses- og håndhævelsesforanstaltninger. En tilsynsmyndighed har ret til at være en del af sådanne aktiviteter, hvis en dataansvarlig har en virksomhed i det område, eller hvis det er sandsynligt, at et betydeligt antal af de registrerede vil blive påvirket i betydelig grad. Hvis den nationale lovgivning tillader det, kan værtstilsynsmyndigheden delegere formelle undersøgelsesbeføjelser til udsendte medarbejdere. Tilsynsmyndigheder har udført fælles undersøgelser i henhold til den eksisterende lovgivning, så Persondataforordningen vil i praksis nok blot udvikle og styrke denne ordning.

Hvis tilsynsmyndigheder har taget visse formelle skridt eller er uenig eller ønsker bistand fra en anden tilsynsmyndighed, indeholder Persondataforordningen en sammenhængs- og tvistbilæggelsesmekanisme.

Det Europæiske Databeskyttelsesråd skal komme med udtalelser om diverse forslag fra tilsynsmyndigheder, herunder godkendelse af bindende virksomhedsregler, certificeringskriterier og adfærdskodekser. Hvis tilsynsmyndigheden ikke er enig i det Europæiske Databeskyttelsesråds udtalelse, overgår sagen til tvistbilæggelsesproceduren.

Denne procedure gælder også for tvister mellem ledende tilsynsmyndigheder og berørte tilsynsmyndigheder. I alle disse sager afgiver Det Europæiske Databeskyttelsesråd en bindende afgørelse med to tredjedeles flertal. Hvis der ikke er sådan et flertal, vil et simplet flertal være tilstrækkeligt efter en udsættelse. De involverede tilsynsmyndigheder skal rette sig efter afgørelsen og udstede afgørelser i overensstemmelse med Det Europæiske Databeskyttelsesråds afgørelse.

Hvor kan jeg læse mere?

Præambel 124-138 og Kapitel VII, Afdeling 1 & 2

Det Europæiske Databeskyttelsesråd

Resumé

- Den gamle Artikel 29-arbejdsgruppe, hvis medlemmer var EU's nationale tilsynsmyndigheder, Den Europæiske Tilsynsførende for Databeskyttelse og EU-Kommissionen, er blevet omdannet til Det Europæiske Databeskyttelsesråd, som har de samme medlemmer, men et uafhængigt sekretariat.
- Det Europæiske Databeskyttelsesråd har status som EU-organ og juridisk person og har omfattende beføjelser til at afgøre tvister mellem nationale tilsynsmyndigheder og til at rådgive og vejlede og til at godkende kodekser og certificeringer, der gælder i hele EU.

To-do liste

X	Umiddelbart er det ikke nødvendigt at gøre noget – undtagen måske hvis du er medlem at en national tilsynsmyndighed.
	Ikke desto mindre vil Det Europæiske Databeskyttelsesråd have en stor indflydelse på lovgivningen om beskyttelse af personoplysninger i EU og praksis, og det vil måske være nyttigt at finde ud af mere om, hvordan man kan have indflydelse på og anfægte dens afgørelser.

Kommentar

Artikel 29-arbejdsgruppen, som blev nedsat på grundlag af Direktiv 95/46/EC (Databeskyttelsesdirektivet) og består af repræsentanter fra EU-medlemsstaternes tilsynsmyndigheder sammen med EU-Kommissionen og Den Europæiske Tilsynsførende for Databeskyttelse, vil blive nedlagt i henhold til Persondataforordningen. Den bliver erstattet af Det Europæiske Databeskyttelsesråd, som på samme vis vil bestå af cheferne for de nationale tilsynsmyndigheder (eller deres stedfortrædere) og Den Europæiske Tilsynsførende for Databeskyttelse.

EU-Kommissionens repræsentant i Det Europæiske Databeskyttelsesråd har ikke stemmeret og i de stater (fx Tyskland), som har flere tilsynsmyndigheder, skal den nationale lovgivning sørge for, at en fælles repræsentant udpeges.

I tvistbilæggelsessager, hvor en bindende afgørelse skal træffes, har Den Europiske Tilsynsførende for Databeskyttelse kun stemmeret i tilfælde, hvor sagens principper vil være gældende i EU-institutionerne.

Det Europæiske Databeskyttelsesråd har en meget fremtrædende status. Det er ikke kun et rådgivende udvalg, men et uafhængigt organ i den Europæiske Union med status som juridisk person.

Rådet bliver formelt repræsenteret af sin formand, som har det øverste ansvar for at tilrettelægge Det Europæiske Databeskyttelsesråds arbejde og især i forbindelse med at administrere mæglingsprocedurerne for tvister mellem de nationale tilsynsmyndigheder. Formanden og to næstformænd bliver valgt blandt medlemmerne af Det Europæiske Databeskyttelsesråd for 5 år og kan genvælges en gang.

Det Europæiske Databeskyttelsesråd afgør normalt sager ved simpelt flertal, men forretningsordenen og bindende afgørelser (i første instans) skal afgøres med to tredjedeles flertal.

Det Europæiske Databeskyttelsesråd skal vedtage sin egen forretningsorden og tilrettelægge sin egen drift. Der bliver lagt vægt på, at Det Europæiske Databeskyttelsesråd er uafhængigt.

Det virker som om, at det er en underforstået hentydning til, at Kommissionen tidligere havde for stor indflydelse på Artikel 29-arbejdsgruppen og forsøgte at konsolidere denne beføjelse.

Den gamle Artikel 29-arbejdsgruppes sekretær var en embedsmand fra Kommissionen. Det nye Europæiske Databeskyttelsesråd vil få sit eget sekretariat, som stilles til rådighed af Den Europæiske Tilsynsførende for Databeskyttelse, men som kun er under instruks af formanden for Det Europæiske Databeskyttelsesråd.

Det Europæiske Databeskyttelsesråd har fået en lang og detaljeret opgaveliste, men Rådets primære rolle er at medvirke til, at Persondataforordningen anvendes på en ensartet måde i hele EU. Det skal rådgive Kommissionen, især i anliggender om den beskyttelse, der gives af tredjelande eller internationale organer, og støtte op om samarbejde mellem de nationale tilsynsmyndigheder.

Rådet skal udstede retningslinjer, henstillinger og erklæringer om bedste praksis: for eksempel om spørgsmål vedrørende hvornår et brud på persondatasikkerheden *"sandsynligvis vil indebære en høj risiko for rettigheder og frihedsrettigheder"* for personer eller om krav til bindende virksomhedsregler (BRC). Det skal fremme adfærdskodekser og certificeringer, som begge hjælper databehandlere og dataansvarlige med at påvise, at de overholder Persondataforordningen.

Meget af opgavelisten er en uddybning eller formalisering af den nuværende Artikel 29- gruppes aktiviteter, men det Europæiske Databeskyttelsesråds meninger og aktiviteter vil have større indvirkning og indflydelse.

Det Europæiske Databeskyttelsesråds mest markante nye rolle er at mægle i og afgøre tvister mellem nationale tilsynsmyndigheder. Læs mere om denne aktivitet i Kompetencer, opgaver og beføjelser. Den gamle Artikel 29-gruppe er ofte blevet kritiseret for ikke at rådføre sig nok, før beslutninger blev taget.

Det nye Europæiske Databeskyttelsesråd skal rådføre sig med berørte parter, *"når det er relevant"*. Til trods for "udvejs"-muligheden er dette en stor fordel for dem, som kan blive påvirket af udtalelser, retningslinjer, rådgivning og bedste praksis.

Det Europæiske Databeskyttelsesråds drøftelser skal holdes *"fortrolige, hvis Databeskyttelsesrådet vurderer, at det er nødvendigt, jf. dets forretningsordenen"*. Dette indikerer, at møder og drøftelser i

princippet skal være offentlige, med mindre det besluttes, at de ikke skal.

Det Europæiske Databeskyttelsesråd skal endvidere udarbejde et årsregnskab.

Hvor kan jeg læse mere?

Præambel 139-140 og Kapitel VII, Afdeling 3

Retsmidler og ansvar

Resumé

- Privatpersoner har de følgende rettigheder (overfor dataansvarlige og databehandlere):
  - Retten til at indgive en klage til tilsynsmyndighederne, hvis deres data er blevet behandlet i strid med Persondataforordningen;
  - Retten til effektive retsmidler, hvis den kompetente tilsynsmyndighed ikke kan håndtere klagen;
  - Retten til effektive retsmidler mod en relevant dataansvarlig eller databehandler; eller
  - Retten til kompensation fra en relevant dataansvarlig eller databehandler for materiel eller immateriel skade som følge af krænkelsen af Persondataforordningen.
- Både fysiske og juridiske personer har ret til at appellere en juridisk bindende afgørelser om dem afsagt af en tilsynsmyndighed til de nationale domstole.
- Privatpersoner kan anlægge krav for økonomisk tab og ikke kun kompensation. Der er ligeledes mulighed for at anlægge gruppesøgsmål.

To-do liste

☐	Dataansvarlige og deres databehandlere skal sikre, at databehandleraftaler og kontraktstyring tydeligt beskriver omfanget af databehandlerens ansvar og skal indeholde bestemmelser for tvistløsningsmekanismer i forbindelse med tvister om ansvar ved kompensationskrav.
☐	Dataansvarlige og databehandlere skal aftale at rapportere enhver relevant overtrædelse og andre klager eller krav modtaget fra registrerede til andre dataansvarlige eller databehandlere, som er involverede i samme databehandling.
☐	Forbundne dataansvarlige skal aftale deres individuelle forpligtelser til overholdelse af databeskyttelsesreglerne, deres ansvar for brud på databeskyttelsesreglerne og mekanismerne for tvistløsning i forbindelse med respektive ansvar for at afgøre kompensationskrav.

Klager til tilsynsmyndighederne

De registreredes ret til at indgive en klage til tilsynsmyndigheden er styrket en smule sammenlignet med Databeskyttelsesdirektivet. Direktivet giver tilsynsmyndighederne ret til at behandle klager, der er indgivet af registrerede, for at undersøge databehandlingens lovlighed og til at informere de registrerede om, at undersøgelsen foretages.

I henhold til persondataforordningen vil registrerede, hvis personlige oplysninger behandles i strid med Persondataforordningen, have en særlig ret til at indgive en klage til tilsynsmyndigheden, og tilsynsmyndigheden skal informere de registrerede om klagens status og udfaldet af klagen.

Retsmidler mod tilsynsmyndighedernes afgørelser

Både registrerede og andre påvirkede parter har ret til effektive retsmidler i forbindelse med særlige handlinger og afgørelser fra tilsynsmyndighederne.

- Alle personer har ret til effektive retsmidler mod tilsynsmyndighedens juridisk bindende afgørelser, der vedrører dem.
- De registrerede har ret til effektive retsmidler, hvis en tilsynsmyndighed ikke kan håndtere en klage eller ikke informerer de registrerede inden for 3 måneder vedrørende klagens status eller resultat.

Præambel 143 forklarer, at afgørelser og retssager, der afprøves ved en domstol, indeholder en undersøgelsesbeføjelse, korrigerende beføjelse og godkendelsesbeføjelse for tilsynsmyndigheden eller afslag eller afvisning af klager. Denne ret omfatter dog ikke andre foranstaltninger truffet af tilsynsmyndigheder, der ikke er juridisk bindende, som f.eks. udtalelser eller rådgivning fra tilsynsmyndigheden.

Retsmidler mod dataansvarlige & databehandlere

De registrerede, hvis rettigheder er blevet krænket, har ret til effektive retsmidler mod den dataansvarlige og databehandleren, som er ansvarlig for den hævdede misligholdelse. Databeskyttelsesdirektivet indeholder en tilsvarende bestemmelse for retsmidler mod dataansvarlige men ikke mod databehandlere.

Kompensationsansvar

Enhver, som har lidt skade som resultat af en krænkelse af Persondataforordningen, har ret til at modtage kompensation fra den dataansvarlige eller databehandleren. I henhold til Databeskyttelsesdirektivet, er kompensationsansvar begrænset til dataansvarlige.

Den følgende bestemmelse regulerer fordelingen af kompensationsansvar mellem dataansvarlige og databehandlere:

- Dataansvarlige er ansvarlige i tilfælde af skade, der er forvoldt af behandling, som ikke er i overensstemmelse med Persondataforordningen;
- Databehandlere er kun ansvarlige for skade, der er forvoldt af behandling i strid med de forpligtelser, der specifikt er pålagt databehandlere i Persondataforordningen, eller som er forvoldt af databehandling, som fortages udenfor eller i strid med lovlige instrukser fra den dataansvarlige; og
- For at sikre effektiv kompensation til registrerede er de dataansvarlige og databehandlere, som er involveret i samme databehandling og er ansvarlige for enhver skade, der forvoldes, ansvarlige for den fulde skade. En dataansvarlig eller databehandler, som er kompensationsansvarlig, er dog på denne baggrund berettiget til at inddrive den andel af kompensationen, som svarer til deres andel af ansvaret for skaden, fra andre relevante parter.

Hvor Databeskyttelsesdirektivet udelukkende refererer til retten til kompensation som *'skade'*, understreger Persondataforordningen, at kompensation

kan inddrives vedrørende både økonomiske og ikke-økonomiske tab. Denne afklaring er dog i overensstemmelse med den gældende juridiske fortolkning af betydningen af skade i forbindelse med kompensationskrav i henhold til Databeskyttelsesdirektivet (se Google Inc. mod Vidal-Hall & Others [2015] EWCA civ 311).

Persondataforordningen foreskriver, at dataansvarlige og databehandlere er fritaget fra erstatningsansvar, hvis den pågældende beviser "*ikke at være ansvarlig for den forvoldte skade*".

Repræsentative organer

Persondataforordningen berettiger registrerede til at udpege repræsentative organer til at indgive klager til tilsynsmyndigheden på deres vegne og udøve adgangen til retsmidler på deres vegne mod tilsynsmyndighedens afgørelse eller mod dataansvarlige eller databehandlere. Bestemmelsen gælder for repræsentative organer, som:

- Er etableret i overensstemmelse med medlemsstatens nationale ret;
- Ikke arbejder med gevinst for øje;
- Hvis vedtægtsmæssige formål er i samfundets interesse; og
- Som er aktive på området for beskyttelse af personoplysninger.

Registrerede kan ligeledes udpege sådanne organer til på deres vegne at udøve deres rettigheder til inddrivelse af kompensation fra dataansvarlige eller databehandlere, hvis dette er i overensstemmelse med medlemsstatens nationale ret.

Hvor medlemsstaten har bemyndiget repræsentative organer hertil, kan de repræsentative organer, uafhængigt af den registreredes bemyndigelse hertil, indgive en klage til tilsynsmyndigheden og have adgang til effektive retsmidler mod tilsynsmyndighedens afgørelse eller mod dataansvarlige eller databehandlere.

Der findes ingen tilsvarende bestemmelse i Databeskyttelsesdirektivet.

Hvor kan jeg læse mere?

Artikel 77-82 Præambel 141-146

Administrative bøder

Resumé

- Tilsynsmyndigheder bemyndiges til at pålægge væsentlige administrative bøder for både dataansvarlige og databehandlere.
- Der kan pålægges bøder i stedet for eller sammen med foranstaltninger, som kan pålægges af tilsynsmyndighederne. Bøder kan pålægges for en lang række overtrædelser, inklusiv rene proceduremæssige krænkelser.
- Administrative bøder er mere skønsmæssige end obligatoriske. De skal pålægges fra sag til sag og skal være "effektive, stå i rimeligt forhold til overtrædelsen og have afskrækkende virkning".
- Der er to niveauer af administrative bøder:
  - Nogle overtrædelser straffes med administrative bøder på op til EUR 10.000.000, eller for virksomheder 2 % af den globale omsætning, afhængigt af hvilket beløb, der er højest.
  - Andre straffes med administrative bøder på op til EUR 20.000.000, eller for virksomheder på 4 % af den globale omsætning, afhængigt af hvilket beløb, der er højest.
- Medlemsstaterne kan afgøre om og i hvilken udstrækning, offentlige myndigheder kan straffes med administrative bøder.

To-do liste

☐	Kør en compliance-analyse i forhold til Persondataforordningen for at identificere de områder, hvor der er mindst compliance og for at prioritere lempende foranstaltninger, især i forhold til højrisiko databehandlingsaktiviteter.
☐	Opdatér risiko-register.
☐	Vurdér eksponering af forpligtelser i henhold til eksisterende kunde-, leverandør- og/eller partneraftaler, inklusiv en vurdering af begrænsning af kontraktuelle forpligtelser og udelukkelsesklausuler.
☐	Gennemgå forsikringsaftaler.

Generelle overvejelser

Administrative bøder gælder ikke automatisk og skal pålægges fra sag til sag. Præambel 148 beskriver, at i tilfælde af et en mindre overtrædelse, eller i de tilfælde hvor en bøde vil pålægge en fysisk person en uforholdsmæssig stor byrde, kan man udstede en irettesættelse i stedet for en bøde.

Der varieres i høj grad i medlemsstaterne i forhold til pålæggelse af bødestraffe af tilsynsmyndighederne. Selvom bestemmelserne i Persondataforordningen giver mulighed for pålæggelse af maksimum bøder og giver tilsynsmyndighederne en grad af valg i forhold til pålæggelse af bøder, indikerer præambel 150, at en sammenhængsmekanisme kan benyttes til at fremme en konsekvent anvendelse af administrative bøder.

Hver medlemsstat kan dog udstede regler, der beskriver, om og i hvilken grad administrative bøder kan pålægges de offentlige myndigheder og organer i den enkelte medlemsstat.

Maksimumstørrelse af administrative bøder

Persondataforordningen indeholder to maksimumsgrænser for administrative bøder for relevante overtrædelser.

I begge tilfælde angives maksimumgrænsen i euro eller, for virksomheder, som en procentdel af den årlige omsætning i det forgående år, såfremt dette beløb er højere. Præambel 150 bekræfter, at en "virksomhed" i denne forbindelse er defineret i Artikel 101 og 102 i traktaten om Den Europæiske Unions funktionsmåde ("TFEU") (dvs. selskaber med økonomiske aktiviteter generelt set).

For overtrædelser af følgende bestemmelser i Persondataforordningen kan der pålægges administrative bøder på op til EUR 20.000.000, eller hvis det drejer sig om en virksomhed, med op til 4 % af virksomhedens samlende globale årlige omsætning i det forgående regnskabsår, såfremt dette beløb er højere:

- de grundlæggende principper for behandling, herunder betingelserne for samtykke (artikel 5, 6, 7 og 9);
- de registreredes rettigheder (artikel 12-22);
- internationale overførsler (artikel 44-49);
- forpligtelser i medfør af medlemsstatens nationale ret vedtaget i henhold til kapitel IX; og
- manglende overholdelse af et påbud udstedt af tilsynsmyndigheden (som refereret til i artikel 58, stk. 2).

- Andre overtrædelser straffes med administrative bøder på op til EUR 10.000.000 eller, hvis det drejer sig om en virksomhed, med op til 2 % af dens samlede globale årlige omsætning i det foregående regnskabsår, såfremt dette beløb er højere. Overtrædelser, der straffes med maksimumbøderne inkluderer overtrædelser af følgende forpligtelser:
- Forpligtelser til at indhente samtykke til behandlingen af børns personlige oplysninger (artikel 8);
- Forpligtelser til at implementere tekniske or organisatoriske foranstaltninger til at sikre beskyttelse af data by design og default (artikel 25);
- Forpligtelse for fælles dataansvarlige til at aftale fælles forpligtelse til overholdelse (artikel 26);
- Forpligtelse for dataansvarlige og databehandlere, som ikke er etableret i EU, til at udpege repræsentanter (artikel 27);
- Forpligtelse for dataansvarlige i forbindelse med engagering af databehandlere (artikel 28);
- Forpligtelse for databehandlere til udelukkende at udlicitere med forudgående samtykke fra databehandlere og til udelukkende at behandle data ud fra den dataansvarliges instruktioner (artikel 28-29);
- Forpligtelser til at føre skriftlig dokumentation (artikel 30);
- Forpligtelse for dataansvarlige og databehandlere til at samarbejde med tilsynsmyndighederne (artikel 31);
- Forpligtelse til at træffe passende tekniske og organisatoriske foranstaltninger (artikel 32);

- Forpligtelse til at anmelde brud på persondatasikkerheden, når dette kræves af Persondataforordningen (artikel 33 og 34);
- Forpligtelse i forbindelse med konsekvensanalyse vedrørende databeskyttelse (artikel 35 og 36);
- Forpligtelser i forbindelse med udpegningen af en databeskyttelsesrådgiver (artikel 37-39);
- Forpligtelser for visse certificeringsmekanismer (artikel 42);
- Forpligtelser for tilsynsmyndighederne om at handle i tilfælde af overtrædelser af adfærdskodekser (artikel 40-41).

I tilfælde hvor den samme eller relateret databehandling indeholder overtrædelser af flere bestemmelser i Persondataforordningen, vil bøderne muligvis ikke overstige det beløb, der er angivet for the mest alvorlige overtrædelse.

Faktorer til overvejelse

Artikel 83, 2 a nævner en række faktorer, som skal overvejes, når det besluttes, om der skal pålægges en administrativ bøde, og når beløbet på den bøde, der pålægges, skal besluttes. Dette inkluderer bl.a.:

- overtrædelsens karakter, alvor og varighed med hensyn til pågældende behandlings karakter, omfang eller formål samt antal registrerede, der er berørt, og omfanget af den skade, som de har lidt
- hvorvidt overtrædelsen blev begået forsætligt eller uagtsomt
- foranstaltninger, der er truffet af den dataansvarlige eller databehandleren for at begrænse den skade, som den registrerede har lidt
- den dataansvarliges eller databehandlerens grad af ansvar
- eventuelle relevante tidligere overtrædelser
- graden af samarbejde med tilsynsmyndigheden
- de kategorier af personoplysninger, der er berørt af overtrædelsen
- om den dataansvarlige eller databehandleren har underrettet om overtrædelsen
- tidligere foranstaltninger truffet over for den pågældende dataansvarlige eller databehandler
- overholdelse af godkendte adfærdskodekser i henhold til artikel 40-41 eller godkendte certificeringsmekanismer i henhold til artikel 42
- om der er andre skærpende eller formildende faktorer ved sagens omstændigheder, såsom opnåede økonomiske fordele eller undgåede tab som direkte eller indirekte følge af overtrædelsen.

I de tilfælde, hvor bøder pålægges personer, som ikke er en virksomhed, skal tilsynsmyndigheden også have det generelle lønniveau i medlemsstaten med i deres overvejelser sammen med personens økonomiske situation, når de fastsætter en passende bødestørrelse.

Hvor kan jeg læse mere?

Artikel 83 Præambel 147-151

Begrænsninger og specifikke behandlings-situationer

» Resumé

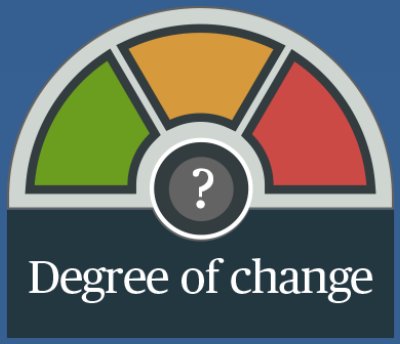
Medlemslandene har stadig mulighed for at indføre begrænsninger, hvor det er påkrævet af hensyn til statens sikkerhed, forebyggelse eller efterforskning af strafbare handlinger og i visse andre situationer. I overensstemmelse med retspraksis ved den Europæiske Unions Domstol skal sådanne begrænsninger respektere det væsentligste indhold i retten til persondatabeskyttelse og være en nødvendig og forholdsmæssig foranstaltning. I disse særlige tilfælde enten kræver eller tillader Forordningen, at Medlemslandene indfører supplerende love. Behandling med henblik på historiske eller videnskabelige forskningsformål, statistiske formål eller arkivering kan det endda danne lovgrundlag for behandling af særlige kategorier af oplysninger.

Det forventes, at Medlemsstater vil indføre særlige love på visse områder, herunder behandling af medarbejderoplysninger, behandling i forbindelse med ytringsfrihed og tavshedspligt (hvor det forventes, at tilsynsmyndigheders ret til auditere begrænses).

Dataansvarlige (og i visse tilfælde databehandlere) skal undersøge og tilpasse sig Medlemsstaternes forskellige tilgange på disse områder.

☑ To-do liste

☐	Vurder, om du udfører behandling, der kan være underlagt begrænsninger eller specifikke behandlingssituationer i forbindelse med Persondataforordningen.
☐	Hvis en begrænsning eller specifik behandlingssituation gælder for en behandling, du foretager, skal det undersøges, i hvilken jurisdiktion behandlingen foretages.
☐	Overvej at udføre lobby-arbejde i lande, hvor lokale begrænsninger kan få indflydelse for dig.
☐	Hvis der gælder regler om tavshedspligt for personlige oplysninger, som en dataansvarlig eller databehandler har modtaget eller fået adgang til, skal det sikres, at de er markeret, så de kan beskyttes mod at blive overført til tilsynsmyndigheder.



Ukendt – Der er mange af den samme slags begrænsninger og specifikke behandlingssituationer under Direktiv 95/46 EC ("Databeskyttelsesdirektivet"), men det er vanskeligt at forberede sig på at skulle overholde sådanne regler, da eventuelle ændringer afhænger af, hvordan Medlemsstaterne indfører eller bibeholder love og regler på dette område.

Kommentar

Særlige tilfælde

Persondataforordningen indeholder brede begrænsninger og undtagelser på to hovedområder: (1) i Kapitel III, afdeling 5, vedrørende *"begrænsning"* af forpligtelser og rettigheder i forbindelse med databeskyttelse; og (2) i Kapitel IX, vedrørende *"specifikke databehandlingssituationer"*.

Artikel 23 – Begrænsninger

Persondataforordningens artikel 23 giver Medlemsstater ret til at indføre begrænsninger i databeskyttelseslovgivningen i visse situationer: det er også tilfældet i Databeskyttelsesdirektivet. Medlemsstater kan indføre begrænsninger i gennemsigtighedsforpligtelserne og den registreredes rettigheder, men kun hvis foranstaltningen "*respekterer det væsentligste indhold af ... grundlæggende rettigheder og frihedsrettigheder og er ... nødvendig og forholdsmæssig ... i et demokratisk samfund.*"

Foranstaltningen skal garantere et af de følgende:

- statens sikkerhed;
- forsvaret;
- den offentlige sikkerhed;
- forebyggelse, efterforskning, afsløring eller retsforfølgning eller fuldbyrdelse af strafferetlige sanktioner;
- andre vigtige samfundsinteresser, særligt økonomiske eller finansielle interesser (fx budget- og skatteanliggender);
- beskyttelse af retsvæsenets uafhængighed og retssager;
- kontrol-, tilsyns- eller reguleringsfunktioner vedrørende sikkerhed, forsvar, andre vigtige offentlige interesser eller forebyggelse af strafbare handlinger eller brud på de etiske regler;
- beskyttelse af de registreredes eller andres rettigheder og frihedsrettigheder; eller
- håndhævelse af civilretlige krav.

For at foranstaltningen er acceptabel, skal den (i overensstemmelse med artikel 23(2)) indeholde specifikke bestemmelser vedrørende:

- formålene med behandlingen;
- kategorierne af personoplysninger;
- rækkeviden af begrænsningerne af Persondataforordningen, som foranstaltningen indfører;
- garantierne for at undgå misbrug eller ulovlig adgang eller overførsel;
- specifikation af de dataansvarlige, som kan anvende begrænsningerne;
- gældende opbevaringsperioder og garantier;
- risiciene for de registreredes rettigheder og frihedsrettigheder; og
- de registreredes ret til at blive underrettet om begrænsningen, medmindre dette kan skade formålet med begrænsningen.

Artikel 85-91: "Specifikke behandlingssituationer"

Bestemmelserne i kapitel IX i Persondataforordningen giver et blandet sæt regler for fravigelser, undtagelser og beføjelser til at indføre yderligere krav, med hensyn til Persondataforordningens pligter og rettigheder, for visse typer af behandling. Disse forskellige bestemmelser bygger på specifikke behandlingssituationer, som allerede blev håndteret af Databeskyttelsesdirektivet.

Artikel 85: Ytrings- og informationsfriheden

Denne bestemmelse gentager en forpligtelse, som Medlemslandene også havde under Databeskyttelsesdirektivet, til at indføre undtagelser til Persondataforordningen, hvor det er nødvendigt for at forene *"retten til beskyttelse af personoplysninger...med retten til ytrings- og informationsfrihed"*. Dette gælder særligt for behandling i journalistisk øjemed eller med henblik på akademisk, kunstnerisk eller litterær virksomhed. Medlemsstaterne skal meddele Kommissionen, hvordan de har implementeret dette krav og eventuelle ændringer til sådanne love.

Artikel 86: Aktindsigt i officielle dokumenter

Denne bestemmelse udvider præampel 72 i Databeskyttelsesdirektivet og tillader, at personoplysninger i officielle dokumenter må videregives i overensstemmelse med medlemsstatens nationale ret, som tillader aktindsigt i officielle dokumenter. Dette er ikke tilladt uden begrænsninger – sådanne love bør, ifølge præampel 154 i Persondataforordningen, *"forene aktindsigt i officielle dokumenter…med retten til beskyttelse af personoplysninger"*. Direktiv 2003/98/EC ("PSI-direktivet") om *"overførsel af den offentlige sektors informationer"* ændrer ikke myndighedernes forpligtelser, eller fysiske personers rettigheder, der er fastsat i Persondataforordningen.

Artikel 87: Nationale identifikationsnumre

Denne bestemmelse gentager medlemsstaters ret til at fastsætte deres egne betingelser for behandling af nationale identifikationsnumre, som findes i Databeskyttelsesdirektivet. Den eneste udvidelse er lavet for at præcisere, at dette kræver, at der er fornødne garantier på plads.

Artikel 88: Medarbejderoplysninger

Det er tilladt for medlemslandene at fastsætte (enten ved lov eller i medfør af kollektive overenskomster) mere specifikke bestemmelser med hensyn til behandling af medarbejderes personoplysninger, herunder alle betydelige forhold i ansættelsescyklussen fra ansættelse til opsigelse. Dette omfatter muligheden for at implementere bestemmelser, der fastlægger, hvornår samtykke kan anses som gyldigt i et ansættelsesforhold. Sådanne bestemmelser skal omfatte specifikke foranstaltninger til beskyttelse af den registreredes *"menneskelige værdighed, legitime interesser og grundlæggende rettigheder"* og Persondataforordningen anfører gennemsigtighed i behandlingen, overførsler inden for en koncern som områder, hvor der skal tages særligt hensyn til disse anliggender. Medlemsstaterne skal meddele Kommissionen de bestemmelser, som de vedtager i henhold til denne artikel, når Persondataforordningen træder i kraft, og de skal også underrette om eventuelle ændringer.

Artikel 89(1) og (2): Videnskabelige eller historiske forskningsformål eller statistiske formål

Artikel 89(1) anerkender, at dataansvarlige må behandle oplysninger til disse formål, hvis der er oprettet fornødne garantier (se også afsnittet om lovlig behandling og viderebehandling (Kapitel 2) og særlige kategorier af oplysninger og lovlig behandling (Kapitel 2)). Hvor det er muligt, skal databehandlere opfylde disse formål med oplysninger, der ikke gør det muligt eller ikke længere gør det muligt at identificere de registrerede; hvis anonymisering ikke er muligt, skal pseudonymisering anvendes, med mindre dette også vil skade formålet med forskningen eller den statistiske proces.

Artikel 89(2) gør det lovligt for Medlemsstater at fastsætte undtagelser fra de registreredes ret til indsigt, berigtigelse, sletning, begrænsning og indsigelse (med forbehold for de garantier, der er fastsat i Artikel 89(1)), såfremt sådanne rettigheder "*vil gøre det umuligt eller i alvorlig grad hindre"* opfyldelse af de specifikke formål, og undtagelserne er nødvendige for at opfylde formålene.

Præamplerne tilføjer flere detaljer om, hvordan "*videnskabelige forskningsformål*", "*historiske forskningsformål*" and "*statistiske formål*" skal fortolkes. Præampel 159 anfører, at videnskabelige forskningsformål skal "*fortolkes bredt*" og omfatte privat finansieret forskning så vel som forskning, der er udført i offentlighedens interesse. Hvis behandling skal betragtes som statistisk, anfører præampel 162, at resultatet af behandlingen ikke er "*personoplysninger, men aggregerede data*" og at resultatet ikke må anvendes til støtte for foranstaltninger eller afgørelser, der vedrører bestemte fysiske personer.

Artikel 89(1) og (3): Arkivformål i samfundets interesse

De samme undtagelser og fornødne garantier eksisterer i forbindelse med "*arkivering i samfundets interesse",* som er nævnt ovenfor i forhold til behandling med henblik på videnskabelige forskningsformål og statistiske formål, bortset fra at undtagelser også kan fastsættes for retten til dataportabilitet. Præampel 158 indeholder flere detaljer, som lægger op til, at dette kun skal anvendes af organer eller myndigheder, som har en forpligtelse til at håndtere fortegnelser, der har "*blivende værdi i samfundets interesse"* i henhold til EU-ret eller medlemsstaternes nationale ret.

Artikel 90: Tavshedspligt

Denne artikel giver Medlemsstater lov til at vedtage specifikke regler for at sikre *"faglig"* eller "*tilsvarende tavshedspligt"*, hvor tilsynsmyndigheder har beføjelser til at få adgang til personoplysninger eller lokaler. Disse regler skal *"forene retten til beskyttel-*

se af personoplysninger med tavshedspligt" og gælder kun for personoplysninger, der er modtaget eller indhentet under en aktivitet, der er underlagt denne tavshedspligt. Igen skal Medlemsstaterne oplyse Kommissionen om de eventuelle love, der indføres i henhold til denne artikel og senest den dato, hvor Persondataforordningen træder i kraft, og Kommissionen skal også underrettes om eventuelle senere ændringer.

Artikel 91: Kirker og religiøse sammenslutninger

Denne artikel beskytter eksisterende og "*omfattende"* regler for kirker, religiøse sammenslutninger og samfund, forudsat at de bringes i overensstemmelse med Forordningens bestemmelser. Sådanne enheder skal stadig være underlagt tilsyn af en uafhængig tilsynsmyndighed i henhold til betingelserne i kapitel VI (se afsnit om Samarbejde og sammenhæng mellem tilsynsmyndigheder (Kapitel 6)).

Hvor kan jeg læse mere?

Begrænsninger	*Artikel 23*	*Præambel 73*
Specifikke behand-lingssituationer	*Artikel 6(2), 6(3), 9(2)(j), 85-91*	*Præambel 50, 53, 153 165*

Delegerede retsakter, gennemførelses-foranstaltninger og afsluttende bestemmelser

Resumé

De sidste kapitler i Persondataforordningen bekræfter, hvornår Persondataforordningen træder i kraft (25. maj 2018) sammen med dens påtænkte forhold til andre EU-databeskyttelsesinstrumenter, herunder Direktiv 2002/58/EF ("e-Privacy-direktivet"). Kommissionen vil aflægge rapporter om Forordningen regelmæssigt, når den er trådt i kraft. De afsluttende bestemmelser giver også Kommissionen beføjelse til at vedtage visse delegerede retsakter i forbindelse med Persondataforordningen (fx i forbindelse med brugen af ikoner og certificeringsmekanismer).

To-do liste

☐	Bemærk datoen, hvor Persondataforordningen vil træde i kraft.
☐	Begynd at planlægge de ændringer, der skal foretages for at imødegå de nye krav. Se to-do-listerne i de andre kapitler.
☐	Hvis det er relevant for din virksomhed, så hold øje med den videre udvikling i forbindelse med e-Privacy-direktivet. Rådgivning vil være nært forstående.

Kommentar

Persondataforordningens kapitel 10 giver Kommissionen beføjelse til at vedtage delegerede retsakter (som nævnt i artikel 12(8) med hensyn til standardiserede ikoner og i artikel 48 (8) med hensyn til certificeringsmekanismer) Disse beføjelser kan tilbagetrækkes af Europa-Parlamentet eller Rådet til enhver tid. De vedtagne retsakter træder i kraft indenfor 3 måneder, hvis hverken Europa-Parlamentet eller Rådet gør indsigelse. Denne periode kan forlænges. Kommissionen bistås af et udvalg i overensstemmelse med forordning nr. 182/2011. Det er navnlig vigtigt, at Kommissionen gennemfører relevante høringer under sit forberedende arbejde, herunder på ekspertniveau (præambel 166).

Kommissionen tildeles også beføjelser, der skal sikre ensartede betingelser for implementering af Persondataforordningen, som også skal udøves i overensstemmelse med forordning nr. 182/2011.

Persondataforordningens kapitel 11 bekræfter, at Databeskyttelsesdirektivet bliver ophævet, når Persondataforordningen træder i kraft, som vil ske to år og tyve dage efter offentliggørelse i Den Europæiske Unions Tidende (25. maj 2018) og at referencer til det ophævede Databeskyttelsesdirektiv skal fortolkes som referencer til Persondataforordningen.

Persondataforordningen gælder umiddelbart i alle Medlemsstater.

Kommissionen skal regelmæssigt aflægge rapport om Persondataforordningen til Europa-Parlamentet og Rådet med særligt fokus på bestemmelserne om overførsel af personoplysninger og bestemmelserne om samarbejde og sammenhæng. Den første rapport skal forelægges senest fire år efter Forordningens ikrafttræden og derefter hvert fjerde år. Rapporterne offentliggøres.

Persondataforordningen indfører ikke yderligere forpligtelser for personer for så vidt angår behandling af personoplysninger i forbindelse med levering af offentlige tilgængelige elektroniske kommunikationstjenester i offentlige kommunikationsnet i EU for så vidt angår spørgsmål, hvor de er underlagt specifikke forpligtelser med samme formål som det, der er fastsat i e-Privacy-direktivet (artikel 89). Kommissionen er dog forpligtet til at revidere andre EU-databeskyttelsesinstrumenter og navnlig e-Privacy-direktivet (præambel 173) for at sikre forenelighed med Persondataforordningen.

Præampel 171 præciserer, at hvis behandling er baseret på samtykke i henhold til det nuværende Databeskyttelsesdirektiv, er det ikke nødvendigt, at den registrerede på ny giver sit samtykke, såfremt den måde, som samtykket er givet på, er i overensstemmelse med Persondataforordningen.

Hvor kan jeg læse mere?

Artikel 94-99 Præambel 166-173

Ordliste

Dataansvarlig

En person eller et organ, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler personoplysninger behandles.

Databehandler

En person eller et organ, der behandler oplysninger på den dataansvarliges vegne.

Databeskyttelsesdirektivet

EU direktiv 95/46/EC, som tidligere regulerede behandling af personoplysninger i EU, og som nu erstattes af Persondataforordningen.

Databeskyttelsesrådgiver (Data Protection Officer)

Hvis (i) behandling foretages af en offentlig myndighed; eller (ii) behandlingen består af "systematisk overvågning af registrerede i stort omfang" eller; (iii) den dataansvarliges eller databehandlerens "hovedaktiviteter" består i behandling af oplysninger "i stort omfang af særlige kategorier af data", er der en forpligtelse til at ansætte en databeskyttelsesrådgiver (DPO), som orienterer og rådgiver om anliggender om persondatabeskyttelse, fører tilsyn med overholdelse af reglerne og samarbejder med, og er kontaktperson for, tilsynsmyndighederne.

Det Europæiske Databeskyttelsesråd (EDPB)

Det Europæiske Databeskyttelsesråd erstatter Artikel 29-gruppen, og dens funktioner vil bl.a. være at sikre ensartethed i indførelsen af Persondataforordningen, rådgive EU-kommissionen, udstede retningslinjer, adfærdskodekser og anbefalinger, akkreditere certifice-

EØS

Det Europæiske Økonomiske Samarbejdsområde omfatter alle 28 EU-medlemsstater plus Island, Lichtenstein og Norge. Schweiz er ikke omfattet.

Personoplysninger

Dette omfatter alle oplysninger, som vedrører en identificeret eller identificerbar fysisk person, en registreret. En registreret er en identificeret eller identificerbar fysisk person, som direkte eller indirekte kan identificeres eller er identificerbar.

PIA (Privacy Impact Assess-ment) - Konsekvensanalyse

Persondataforordningen indfører en ny forpligtelse for dataansvarlige og databehandlere til at udføre en konsekvensanalyse vedrørende databeskyttelse (også kaldet 'privacy impact assessment') før udførelse af behandling, der vil medføre en specifik risiko i forbindelse med databeskyttelse i medfør af sin karakter, omfang eller formål. Kapitel IV, Afdeling 3, indeholder en ikke-udtømmende liste over kategorier af behandlinger, som falder under denne bestemmelse.

Behandling

Dette bliver stadig bredt defineret som værende enhver aktivitet eller række af aktiviteter, som personoplysninger gøres til genstand for, både med og uden automatisk databehandling. Eksempler på behandling er bl.a. indsamling, registrering, organisering, opbevaring, brug og tilintetgørelse af personoplysninger.

Pseudonymisering

Teknik til behandling af personoplysninger, så det ikke længere kan henføres til den enkelte person, uden brug af supplerende oplysninger, som skal opbevares separat og under sådanne tekniske og organisatoriske foranstaltninger, så enkelte personer ikke længere kan identificeres.

Retten til sletning / retten til at blive glemt

De registreredes nuværende ret til sletning af deres personoplysninger i visse situationer er blevet udvidet til nu at bestå i den nye "retten til at blive glemt" i de situationer, der angives i Kapitel III, Afdeling 3, i Persondataforordningen.

Særlige kategorier af oplysninger

Dette blev tidligere kaldt 'følsomme oplysninger'. Persondataforordningen har udvidet definitionen til at omfatte både biometriske og genetiske data.

De registreredes ret til indsigt

Dette er den registreredes ret til altid, efter forespørgsel, at få visse informationer udleveret fra den dataansvarlige vedrørende behandlingen af egne personoplysninger, som beskrevet i kapitel III, Afdeling 2, i Persondataforordningen.

Tilsynsmyndighed/ledende tilsynsmyndighed

Tilsynsmyndigheder er nationale databeskyttelsesmyndigheder, som har beføjelse til at indføre Persondataforordningen i deres egne medlemsstat.

'One-stop-shop'-princippet: hvis en virksomhed er etableret i mere end en medlemsstat, vil den have en 'ledende tilsynsmyndighed', der afgøres af, hvor dens 'hovedvirksomhed' i EU er (fx stedet, hvor hoveddelen af behandlingsaktiviteterne finder sted). En tilsynsmyndighed, som ikke er en ledende tilsynsmyndighed i forhold til en bestemt virksomhed, kan også have regulerende rolle i forhold til den virksomhed, for eksempel hvis behandlingen kan påvirke de registrerede i lande, hvor tilsynsmyndigheden er den nationale myndighed.

Overførsel

Overførsel af personoplysninger til lande uden for EØS eller til internationale virksomheder, som er underlagt begrænsninger, som fremgår af Kapitel V i Persondataforordningen. Som i Databeskyttelsesdirektivet er det ikke nødvendigt, at oplysninger bliver flyttet fysisk for at blive overført.

Virksomhed

Denne betegnelse anvendes i flere forskellige betydninger i Persondataforordningen, oftest i betydningen en juridisk enhed, der beskæftiger sig med "økonomisk aktivitet". Betegnelsen har en speciel betydning i forbindelse med Persondatalovens bestemmelser om bødestraffe. Virksomheder er underlagt bøder, der udregnes som en procentdel af deres årsomsætning på verdensplan. I denne sammenhæng overfører betegnelsen principperne, som er udviklet i sammenhæng med EU's konkurrencelovgivning.

Lederne af Bird & Bird's persondataretsteam

Jesper Langemark
Partner

T: 7424 1212
M: 2226 2002
E: jesper.langemark@twobirds.com

Nis Peter Dall
Partner

T: 7424 1212
M: 2075 2747
E: nis.dall@twobirds.com