Sådan får du styr på persondataforordningen

Er du i tvivl om, hvad den nye persondataforordningen betyder for din virksomhed? Vi har samlet en nem oversigt over de væsentligste regler, som skal overholdes.

I 2018 træder EU's ny persondataforordning i kraft. Den ny persondataforordning introducerer en række nye forpligtelser i forbindelse med indsamling og behandling af personoplysninger.

Mange af disse forpligtelser kræver, at virksomheden indfører nye interne procedurer for løbende at sikre, at virksomheden overholder de persondataretlige regler.

Det er derfor en god ide, for din virksomhed at benytte perioden ind til forordningen træder i kraft på at forberede din virksomhed på de nye regler.

Det skal du have styr på inden 2018

Nedenfor kan du få et overblik over, hvad din virksomhed skal have styr på inden den ny persondataforordning træder i kraft.

Dataansvarlig eller databehandler

I persondatalovens § 3, nr. 4, defineres "den dataansvarlige" som den der afgør, til hvilket formål og hvordan der må foretages behandling af oplysninger.

Det kan f.eks. være en myndighed, der er blevet pålagt at behandle personoplysninger eller en arbejdsgiver, der behandler personoplysninger om sine ansatte og sine kunder.

I persondatalovens § 3, nr. 5, defineres en "databehandler", som den der behandler oplysninger på den dataansvarliges vegne. Databehandleren behandler aldrig personoplysninger til egne formål og må kun bruge de oplysninger som aftalt med den dataansvarlige.

I praksis kan en databehandler f.eks. være en virksomhed, som varetager en anden virksomhed IT-systemer. Det kan også være en udbyder af et webhotel eller et inkassobureau.

Forordningen fastsætter at databehandlere kan blive ansvarlige for flere områder end tidligere. Databehandlere er nu også ansvarlige for, at:

- Man ikke behandler data på andre måder, end man har aftalt med den dataansvarlige
- Udarbejde reporter over behandlingsaktiviteterne
- Implementere passende tekniske og organisatoriske sikkerhedsforanstaltninger
- Informere den dataansvarlige ved databrud - og uden unødigt ophold
- Udpege en DPO hvis det er påkrævet
- Overholde reglerne for overførsel af data til lande uden for EU

Det har den konsekvens at også databehandlere kan ifalde bøde ansvar efter de nye bøde regler.

Placering af data

Der må overføres da til lande uden for EU og EØS (tredjelande) når modtagerlandet sikrer et tilstrækkeligt beskyttelsesniveau. Forordningen åbner op for muligheder for at også sektorer og internationale organisationer kan sikre et tilstrækkeligt beskyttelsesniveau, og man derfor også kan overfører dertil.

Derudover kan der overføres til tredjelande når virksomheder anvender kommissionens standardklausuler, Binding Corporate Rules godkendt af Datatilsynet, eller at en af de specifikke situationer, der er nævnt i forordningen, herunder samtykke, finder anvendelse.

Forordninger har i forhold til tidligere lovgivning tilføjet et hjemmelsgrundlag, hvorefter der kan overføres data til tredjelande, når overførslen er nødvendigt for den dataansvarliges legitime formål, og dennes interesse ikke overstiger den registrerede persons interesse.

Data Protection Officer (DPO)
Fra 2018 bliver det et krav for dataansvarlige og databehandlere at udpege en Data Protection Officer (DPO), hvis virksomhedens hovedaktivitet beror på databehandlingsprocesser, hvor det er nødvendigt med omfattende og systematisk overvågning af personer.

Du skal også have en DPO, hvis virksomhedens hovedaktivitet beror på en omfattende behandling af følsomme personoplysninger, som fastsat under forordningens artikel 9, eller oplysninger om strafferetlige forhold, som fastsat under forordningens artikel 9a.

Du overholder kravene til en DPO, hvis:

- Du har ansat en DPO, som enten er fast medarbejder eller er en ekstern konsulent. Er DPO'en en fast medarbejder, må denne gerne udføre andre opgaver i virksomheden - så længe disse andre opgaver ikke resulterer i interessekonflikter i forhold til stillingen som DPO
- Din DPO sikrer, at virksomheden lever op til reglerne og procedurerne for den nye persondataforordning. Derfor skal virksomheden sikre, at DPO'en er involveret i alle situationer vedrørende beskyttelse af persondata. Virksomheden skal også sikre, at DPO'en har de nødvendige ressourcer og adgange til persondataoplysninger, for at kunne udføre sine opgaver
- Virksomheden sikrer at DPO'en ikke modtager instruktioner om, hvordan opgaverne skal udføres. DPO'en kan ikke blive fyret eller straffet for at uføre sine opgaver og skal rapportere til virksomhedens øverste ledelse
- DPO'en kan udføre sine opgaver fortroligt
- DPO'en informerer og rådgiver virksomheden om forpligtelserne i henhold til forordningen. Dette inkluderer også rådgivning om konsekvensanalyser, fastsat i forordningens artikel 33
- DPO'en samarbejder med den lokale databeskyttelsesmyndighed (i Danmark Datatilsynet) og fungere som kontaktperson for Datatilsynet vedrørende behandling af persondata.

DPO'en skal desuden fungere som kontaktperson for personer, som har behov for at udøver deres rettigheder under forordningen eksempelvis at indsigt eller rette data.

Samtykkekrav
På nuværende tidpunkt skal et samtykke til behandling af ens personoplysninger være frivilligt, specifikt og informeret. Det betyder, at et samtykke skal være udtrykkeligt og dermed ikke kan være stiltiende eller underforstået.

Det betyder, at den virksomhed, der indsamler persondata, skal oplyse om, hvilke typer af persondata, der indsamles, hvem der kan foretage behandling af disse data og til hvilket formål.

Hvis eksempelvis et HR- eller lønprogram indsamler og systematisere følsomme personoplysninger, skal der inden denne indsamling erhverves et frivilligt, specifikt og informeret samtykke fra de personer hvis persondata, der indsamles.

Det betyder, at du som virksomhed tydelige skal informere om, hvilke informationer I indsamler

(f.eks. personens navn, adresse, etc.), hvem der bruger disse data (kun virksomheden selv) og hvad de skal bruges til (udbetaling af løn).

Hvis et af de forhold som samtykket bygger på, eksempelvis formålet eller typen af behandling, ændres, skal der indhentes et nyt samtykke. Det betyder, at du sørger for, at brugerne giver nyt samtykke, hver gang der opdateres noget på hjemmesiden eller i et bestemt software, som gør, at databrugen ændres og at din hjemmeside eller software, der opsamler persondata, ikke kan bruges, før der er tilknyttet et opdateret samtykke fra den enkelte bruger.

Forordningen fastsætter yderligere krav til, hvad der udgør et samtykke i forbindelse med behandling af persondata.

Den dataansvarlige skal kunne dokumentere, at et samtykke er givet specifikt til at behandle personoplysninger. Samtykket skal derudover kunne adskilles fra andre vilkår. Det er f.eks. ikke længere gyldigt, at skrive samtykket ind under generelle brugervilkår.

Forespørgslen på et samtykke skal desuden være forståelig, være i en nemt tilgængelig form og anvende klart og tydeligt sprog. Det kunne eksempelvis foregå ved, at en bruger af at program krydser af i et felt, der er ledsaget af en beskrivelse af behandlingen og de persondata, der indsamles. Desuden skal det stå specifikt informeret, hvis man behandler følsomme oplysninger.

Børn under 16 år kan fremover ikke give samtykke til behandling af persondata. Er du f.eks. en virksomhed, som laver app's til børn, skal du derfor være opmærksom på, at det skal stå tydeligt i samtykket, at det skal være en forælder eller værge, som giver samtykket.

Som virksomhed betyder det for dig, at:

- Et samtykke skal indhentes forud for enhver type behandling (herunder indsamling) ligesom det skal være frivilligt, specifikt og informeret samtykke
- Der skal indhentes et nyt samtykke hvis behandlingen eller formålet ændres
- En forespørgsel på samtykke skal være adskilt fra andre typer af vilkår – og det skal være klart og tydeligt beskrevet og i let tilgængelig form
- Hvis du behandler børns persondata, skal du indhente samtykke fra forældre eller værge

Oplysningsforpligtelse
Ved indsamling af persondata er der en forpligtelse til at oplyse den registrerede person om indsamlingen, herunder om:

- Formålet med indsamlingen,
- Kontaktoplysninger på den dataansvarlige
- Modtagere eller kategorier af modtagere af oplysningerne
- Den registreredes rettigheder til at rette og slette data
- Hjemmelsgrundlaget for behandlingen
- Rettigheder til at trække samtykke tilbage og
- Muligheder for at klage til den nationale datebeskyttelsesmyndighed (Datatilsynet)

Husk at forordningen indfører et krav om, at virksomheder skal oplyse om det specifikke hjemmelsgrundlag som virksomheden har baseret indsamlingen og behandlingen af persondata på.

Dataportabilitet
Forordningen fastsætter en række rettigheder for den registrerede person, herunder en ret til dataportabilitet.

Dataportabilitet betyder, at personer fremover har ret til at kræve de persondata, som en virksomhed behandler, udleveret eller overført til en anden dataansvarlig, såfremt behandlingen af persondata beror på samtykke eller nødvendigheden for gennemførelse af en kontrakt, og at behandlingen foregår med automatiske midler f.eks. hvis man gerne vil have overført sin data fra Facebook til Google+.

Den registrerede kan anmode om at persondata overføres direkte fra den ene dataansvarlige til den anden dataansvarlige, hvor det er teknisk muligt.

Et tænkt eksempel herpå kunne være at en virksomhed, der sælger kontaktlinser, har indsamlet oplysninger om en kundes navn, adresse, styrke på kontaktlinser og hvor ofte der skal sendes nye kontaktlinser til vedkommende. En kunde, som ønsker at skifte leverandør af kontaktlinser, kan så anmode om at disse oplysninger overføres til den nye leverandør af kontaktlinser.

I praksis vil denne bestemmelse dog have størst betydning i forhold til sociale medier, hvis formål er at behandle personoplysninger.

Som virksomhed skal du være forberedt på:

- At personer har krav på at få udleveret eller flyttet al sin persondata, som din virksomhed besidder
- At såfremt formålet med din virksomhed er at behandle persondata, såsom at drive et socialt medie, skal dine systemer kunne håndtere udlevering af personoplysninger
- At du skal kunne udlevere personoplysninger i et struktureret og almindelig anvendt maskinlæsbart format

Right to be forgotten

Forordningen fastsætter en ret for de registrerede til at blive ”glemt”. Registrerede personer har en ret til at blive glemt hvis:

- Det ikke er nødvendigt at behandle persondata for at kunne forfølge formålet
- Den registrerede trækker sit samtykke tilbage, og der ikke er et andet hjemmelsgrundlag at basere behandlingen på
- Databehandlingen er ulovlig
- Sletningen er nødvendig for at opfylde et lovkrav
- Registreret person er under 16 år gammel

Virksomheder må gerne forsætte med at behandle persondata, efter den registrerede har anmodet om at blive glemt, hvis hjemmelsgrundlaget har været samtykke og et andet hjemmelsgrundlag finder anvendelse - eller hvis behandlingen er nødvendig for et af de specifikke formål beskrevet i artikel 17(3), herunder ytringsfrihed eller af hensyn til offentlig sundhed

Hvis en person har trukket sit samtykke tilbage, kan det I overveje om I i stedet kan argumentere for, at behandlingen er nødvendig for at gennemføre en kontrakt med den pågældende eller at behandlingen er nødvendig for at forfølge den dataansvarliges legitime interesser, og at disse interesser ikke overstiger den registreredes interesse i ikke at blive behandlet.

Din virksomhed skal derfor være klar over, at:

- Registrerede kan anmode om at få slettet eller rettet oplysninger. De ha ret til at få slettet oplysninger, hvis ovenstående betingelser er opfyldt. De har ret til at få rettet oplysninger, hvis oplysningerne er irrelevante eller forkerte
- Når en person kræver data slettet, gælder det fremover også parter, som den dataansvarlige evt. har videregivet personoplysningerne til – dermed er det din

virksomheds ansvar også at sørge for, at alle samarbejdspartnere informeres om anmodningen om at få persondata slettet

Privacy-by-design/ Privacy-by-default/
Privacy-by-design eller Privacy-by-default betyder, at persondatabeskyttelse skal medtænkes når du udvikler ny teknologi, produkter eller ydelser. Persondata skal medtænkes i hele forløbet så passende organisatoriske og tekniske sikkerhedsforanstaltninger indarbejdes i produktet eller ydelsen.

Du skal være opmærksom på, at:

- Hvis din virksomhed udvikler en ydelse eller et produkt, skal I overveje om ydelsen eller produktet indebærer en behandling af persondata. Hvis produktet eller ydelsen indebærer en behandling af persondata skal passende sikkerhedsforanstaltninger indarbejdes fra start
- Hvis du f.eks. udvikler en app, skal du f.eks. være opmærksom på, om der er behov for at kryptere dele af informationerne og kun dele af virksomhedens ansatte, skal kunne tilgå dataen, etc.
- De sikkerhedsforanstaltninger, der vil være tilstrækkelige, afhænger af den specifikke situation. Du skal derfor vurdere, hvor følsomme oplysningerne er, omfanget af dataen der behandles, og hvilken teknologi der anvendes ved databehandling

Impact Assessment
Forordning fastsætter en pligt til at gennemføre en impact assessment (konsekvensanalyse) af de risici, en behandling kan have. En dataansvarlig har derfor pligt til at udarbejde en impact assessment når der anvendes nye teknologier, produkter eller processer, der indeholder en behandling af persondata.

En impact assessment kan indeholde:

- En generel beskrivelse af de planlagte behandlings metoder
- En evaluering af hvilke risici der er for de registrerede
- Hvilke metoder der er planlagt for at imødekomme risici, herunder sikkerhedsforanstaltninger og mekanismer til beskyttelse af persondata og dokumentation af overensstemmelse med forordningen

Underretningspligt ved databrud
Virksomheder har pligt til at underrette den nationale persondatamyndighed (i Danmark Datatilsynet), hvis der forekommer et brud på datasikkerheden. Det kan f.eks. være, hvis persondata bliver tilgængelig for andre end de medarbejdere, virksomheden har givet lov til at bearbejde de pågældende persondata.

Sker der et brud har den dataansvarlige pligt til at underrette Datatilsynet inden 72 timer efter bruddet på sikkerheden. En databehandler har pligt til at underrette den dataansvarlige om databrud, uden ugrundet ophold.

En underretning skal som minimum indeholde:

- En beskrivelse af databruddet, samt hvor mange personer er berørte, og hvor meget data er omfattet
- Kontaktinformationer på en DPO eller anden kontaktperson i virksomheden
- En beskrivelse af mulige konsekvenser ved databruddet
- En beskrivelse af de handlinger virksomheden planlægger at foretage for at imødegå bruddet

I tilfælde hvor et brud resulterer i en risiko for indgreb i den registreredes rettigheder og frihed, skal den dataansvarlige underrette den registrerede person herom, uden unødigt ophold. Denne underretning skal have samme indhold som den ovenfor, med undtagelse af antallet af berørte personer og hvor meget data er omfattet.

Compliance programmer
Forordningen fastsætter, at den dataansvarlige skal implementere passende foranstaltninger for at sikre, at forordningen overholdes og at den dataansvarlige kan demonstrere dette.

Desuden skal den dataansvarlige føre en fortegnelse over, hvilke kategorier af behandlingsaktiviteter, der foretages.

Virksomheder skal derfor:

- Bedømme deres nuværende compliance programmer for at sikre, at de er i overensstemmelse med forordningen
- Sikre at der føres en oversigt over, hvilke kategorier af behandlingsaktiviteter der foretages.

Husk det med bøderne
Datatilsynet kan pålægge bøder for overtrædelse af forordningen. Der er i forordningen fastsat to bødeniveauer.

Bøder på det laveste bødeniveau fastsættes til det højeste af enten 2 % af virksomhedens globale omsætning eller 10 millioner euro. Dette bødeniveau bruges i situationer, hvor virksomheden ikke har underrettet Datatilsynet om et databrud, hvor der ikke er udarbejdet en impact assessment eller hvor oplysningspligten over for de registrerede personer ikke er overholdt.

Bøder på det højeste bødeniveau fastsættes til det højeste af enten 4 % af virksomhedens globale omsætning eller 20 millioner euro. Dette bødeniveau bruges i situationer, hvor virksomheden foretager behandling uden hjemmelsgrundlag, undlade at slette, give indsigt i eller rette data samt ved ulovlig overførsel af data til tredjelande.

Og One Stop Shop princippet
Forordningen fastsætter et administrativt behandlingsprincip om, at en virksomhed kan nøjes med at henvende sig til én persondatamyndighed i et enkelt EU-land.

Det har betydning for virksomheder, der behandler og/eller indsamler, persondata i flere medlemslande.

Er du f.eks. etableret i Danmark, men er aktiv i flere EU-lande, kan du nøjes med at anvende Datatilsynet. Det er så Datatilsynets ansvar at informere og rådføre sig med andre myndigheder i de relevante lande for at sikre en ensartet håndhævelse af forordningen.

Fakta om persondata
De persondataretlige regler finder i praksis anvendelse for næsten al indsamling og behandling af persondata.

Persondata er alle former for oplysninger, der kan knytte sig til en bestemt person, eller en oplysning, der kan bruges til at identificere en bestemt person direkte eller indirekte.

Persondata omfatter f.eks. navne, adresser, telefonnumre, ip-adresser, e-mailadresser, CPR-numre, og omfatter eksempelvis også geografiske oplysninger indhentet via geotagging eller social

medier. Den ny persondataforordning omfatter, som i dag, næsten alle tænkelige kategorier af persondata inkl. biometriske data som f.eks. gen data.

Derfor er såvel de gældende regler som de nye regler under forordningen relevante for langt de fleste danske virksomheder.

Generelle principper om persondata
Virksomheder må alene behandle persondata, hvis der er et hjemmelsgrundlag hertil. Med hjemmelsgrundlag forstås der en række specifikke situationer fastsat i lovgivningen, der giver en virksomhed lov til at behandle personoplysninger.

Der gælder forskellige hjemmelsgrundlag afhængigt af, om der er tale om almindelige personoplysninger eller følsomme personoplysninger.

Følsomme personoplysninger er oplysninger om race, etnisk oprindelse, politisk holdning, religiøs eller filosofisk overbevisning, medlemskab af fagforening, gen data, biometrisk data der kan identificere en person, helbred og seksualitet. Der gælder desuden særlige regler for strafbare forhold.

Såfremt oplysningerne ikke er følsomme eller semi-følsomme, er det tale om almindelige personoplysninger.

Eksempler på hjemmelsgrundlag for almindelig personoplysninger, kunne være at:

- Den registrerede har givet samtykke
- Behandlingen er nødvendig for gennemførelse af en kontrakt med den registrerede person
- Behandlingen er nødvendig for at forfølge den dataansvarliges legitime interesser, og at disse interesser ikke overstiger den registrerede persons interesse i ikke at blive behandlet

På nuværende tidspunkt er der særregler for en kategori af semi-følsomme personoplysninger. Denne kategori ophæves ved forordningen, og disse oplysninger skal nu anses for at være almindelige.

Samtykke kan også anvendes til at behandle følsomme personoplysninger.

Der er desuden et krav om at behandling af persondata alene må gennemføres i henhold til fast definerede formål og ikke i videre udstrækning end nødvendigt.

Hvis du vil vide mere?
Allerede i dag kan det være en udfordring at få styr på, om virksomheden lever op til de gældende regler i persondataloven.

Derfor har Erhvervsstyrelsen udarbejdet PrivacyKompasset, der kan hjælpe dig med at vurdere, i hvilken grad din virksomhed opfylder reglerne på området. Du skal blot svare på 17 spørgsmål for at finde ud af, om din virksomhed lever op til de gældende regler.

PrivacyKompasset vil blive opdateret inden for kort tid, så det fremover kan guide din virksomhed, om de regler, der skal efterleves under den ny forordning fra 2018.

Derudover er du altid velkommen til at kontakte IT-Branchen på 72 25 55 02/itb@itb.dk eller at kontakte advokatfirmaet Gorrissen Federspiel, der har været med til at udarbejde den guide.