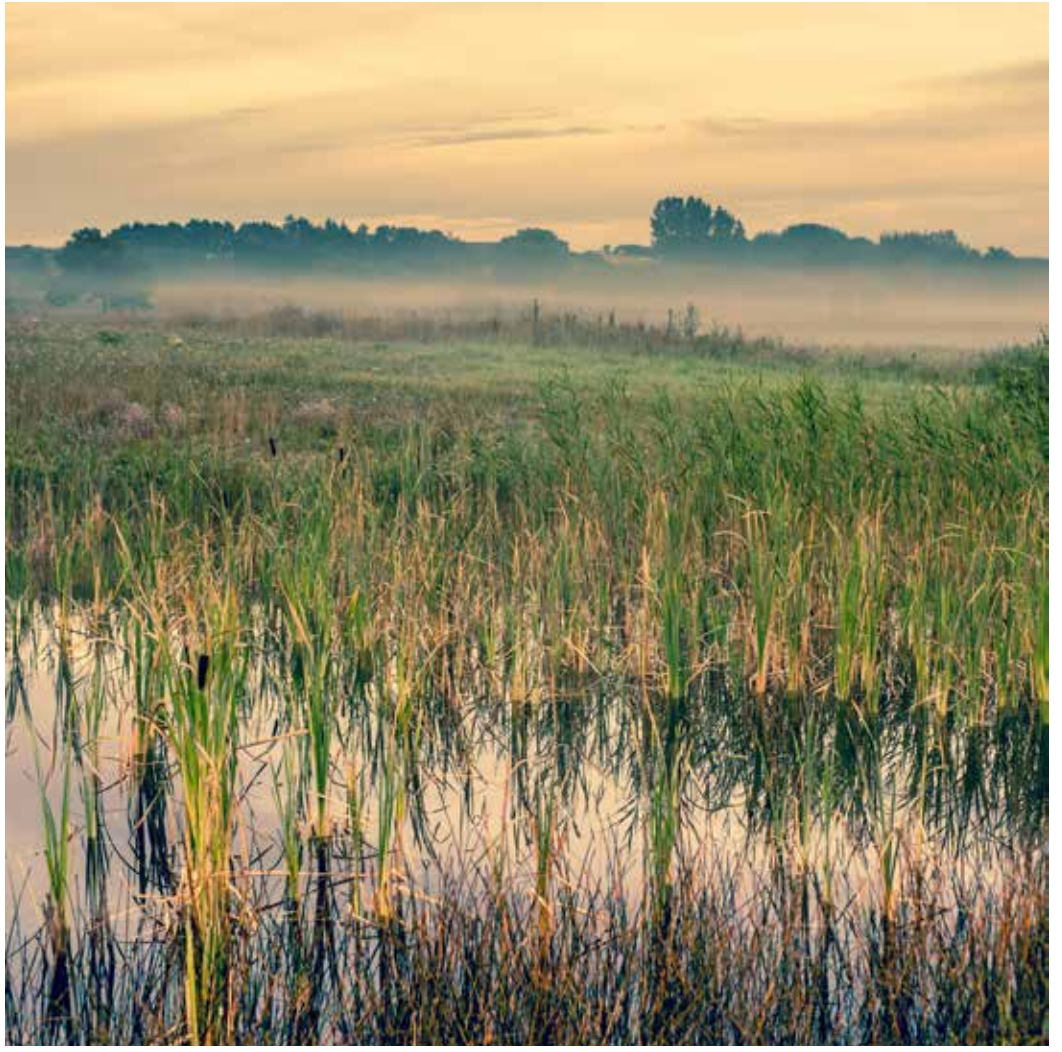
DEN NYE PERSONDATAFORORDNING

– er din virksomhed klar?



DEN NYE PERSONDATAFORORDNING – ER DIN VIRKSOMHED KLAR?

Den nye europæiske persondataforordning, General Data Protection Regulation, træder i kraft den 25. maj 2018. De nye regler er blevet tilpasset informationssamfundet og er en harmonisering af reglerne indenfor EU.

Mange virksomheder behandler, opbevarer og videregiver store mængder persondata uden at have taget stilling til, hvordan man opbevarer og behandler persondata sikkert.

Med de nye regler bliver det endnu vigtigere at have styr på processerne, da mange regler i den nye forordning er blevet skærpet væsentligt. Det gælder blandt andet de nye krav til datasikkerhed og dokumentation samt til sanktioner, da det fremadrettet kan blive meget dyrt ikke at overholde de nye persondataregler.

Hvis virksomheder fra den 25. maj 2018 bryder forordningen, vil bødeniveauet kunne komme helt op på 20 mio. euro eller 4% af den samlede globale koncernomsætning, hvis det beløb er højere.

De nye regler kan endvidere få andre konsekvenser for virksomheden, bl.a. erstatningskrav fra de registrerede personer, skade på virksomhedens renommé samt brud på tilliden til virksomheden.

Persondataforordningen kan derfor ses som en anledning til at få styr på sikkerheden og til at få gennemgået virksomhedernes nuværende persondata, opbevaring og behandling af personoplysninger.

Virksomheder bør hurtigst muligt forberede sig på, hvordan de ny regler kan efterleves, så overgangen bliver så let som mulig.

Formålet med denne vejledning er at introducere til forordningen. Vejledningen er ikke fyldestgørende og kan ikke erstatte konkrete vurderinger.

HVAD ER PERSONDATA?

Persondata er alle oplysninger, der kan være om en fysisk person, eller som kan henføres til en fysisk person. Det kan for eksempel være navn, adresse, cpr-nummer, telefonnummer, e-mail adresse, pasnummer, fotos, kreditkortnummer, IP- adresse, testresultater, straffeattest, helbredsoplysninger, medlemskaber, etnisk oprindelse mv. Persondata er dermed både fortrolige og følsomme oplysninger og almindelige ikke-følsomme oplysninger.

Virksomhederne skal sørge for at behandle personoplysninger i overensstemmelse med lovgivningen.

Til og med den 24. maj 2018 er den gældende persondatalov, lov nr. 429 af 31/05/2000, en gennemførelse af Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger.

OVERHOLDELSE AF GÆLDENDE OG KOMMENDE LOVGIVNING

Det er vigtigt, at virksomhedens eksisterende retningslinjer overholder gældende lovgivning og inden den 25. maj 2018 er tilpasset den nye persondataforordning.

Det er ligeledes vigtigt, at virksomhedens ledelse og andre personer med ledelsesansvar kender til betydningen af at overholde persondataforordningen, samt hvilke konsekvenser de nye regler kan få for virksomheden, hvis reglerne ikke overholdes.

Hvorledes en virksomhed overholder den kommende persondataforordning, er der desværre ikke nogle entydige løsninger på, men for at komme godt i gang kan de fleste virksomheder følge følgende trin.

1. OVERHOLDELSE AF DE GÆLDENDE OG NYE REGLER

Det er vigtigt, at virksomhedens behandling af data er lovlig i forhold til de nuværende regler. Derefter er det vigtigt, at der bliver set på, hvad der skal til, for at overholde de nye persondataregler, og om de informationer som virksomhederne har om de registrerede er nødvendige, samt hvor længe de er nødvendige.

2. FORBEREDELSESFASEN

I forberedelsesfasen er det vigtigt, at virksomhederne undersøger, om de informationer, de ønsker at behandle, er omfattet af forordningen, og i givet fald hvilken kategori (personfølsomme, ikke-personfølsomme) de tilhører. Ud fra kategorien af personoplysninger, er det vigtigt, at virksomheden undersøger, om de må behandle disse oplysninger.

Det er også vigtigt at undersøge, om virksomheden er dataansvarlig eller databehandler i forhold til den konkrete behandling af de enkelte personoplysninger.

Definitioner i persondataforordningen:

Dataansvarlige: Den, der har ansvaret for behandling af data, dvs. den der afgør, til hvilket formål og med hvilke hjælpemidler, der må foretages behandling af personoplysninger.

Databehandler: Den, der behandler personoplysningerne på vegne af den dataansvarlige. Databehandleren har egne forpligtelser og kan ifl. de nye regler idømmes bøde, hvis de ikke overholdes.

De registrerede: De fysiske personer, som personoplysningerne vedrører.

Personoplysninger: Information der kan identificere en fysisk person. Ikke-personfølsomme eller følsomme personoplysninger.

3. DATASTRØMME

Det er vigtigt, at få afdækket virksomhedens datastrømme– både indsamlede og behandlede data samt behandling af data hos tredjepart, fx cloud- og outsourcingpartnere.

Dette kræver et overblik over de interne processer og at man følger selve data. Resultatet heraf kan være en oversigt over systemanvendelse og indhold af systemerne - både hvad angår de registrerede personer og typer af oplysninger, der behandles mv.

Der kan være tale om oplysninger om kunder, der er indsamlet, fordi de bruger virksomhedens produkt(er). Oplysninger som først vil blive slettet efter personen ikke længere bruger virksomhedens produkt(er).

Der kan også være tale om oplysninger om medarbejdere, der er indsamlet i jobansøgninger. Nogle oplysninger vil først blive slettet efter ansættelsesforholdets ophør.

Som ovenfor anført, er det vigtigt at dele oplysningerne op i følsomme personoplysninger og ikke-følsomme personoplysninger.

4. OPBEVARING AF PERSONDATA

Det er vigtigt, at få et overblik over, hvorledes virksomheden opbevarer persondata.

Interne oplysninger opbevares gerne i forskellige systemer fx personalemapper, mail- og arkiveringssystemer, lønsystemer, virksomhedens intranet og eksterne servere mv.

Oplysninger om kunder findes som oftest i kundedatabaser, mail- og arkiveringssystemer, CRM-systemer, mailinglister mv.

Det er vigtigt, at være opmærksom på sikkerheden ved at tage højde for tredjepartssystemer og opbevaringsløsninger herunder cloud-baserede løsninger. Det er ligeledes vigtigt, at tage højde for, hvordan oplysninger gemmes på ansattes computere, om der er en intern kundeliste eller lignende, og hvordan oplysninger deles eller ikke deles internt i virksomheden.

Den dataansvarlige har også en række pligter, som skal opfyldes for at kunne behandle personoplysninger. Blandt andet skal de beskytte personoplysningerne i deres IT-systemer, kunne dokumentere deres behandling og sikkerhedstiltag samt kunne reagere på sikkerhedshændelser og meddele dette til myndighederne og eventuelle berørte registrerede.

Den dataansvarlige skal have kontrol med databehandleren, og databehandleren skal selv opfylde en række krav i persondataforordningen.

5. DE REGISTREREDES RETTIGHEDER

Virksomhederne skal Ifølge den nye persondataforordning informere de registrerede om virksomhedernes retlige grundlag til at indsamle informationer om personerne. Det er vigtigt, at personerne også bliver oplyst om deres ret til at få slettet deres personoplysninger igen, og at de har ret til at få deres oplysninger udleveret.

Det er derfor vigtigt at undersøge, hvilke personoplysninger der er tale om, og på hvilket retligt grundlag de skal behandles.

De registreredes rettigheder kan efter forordningen være forskellige, afhængig af det retlige grundlag for behandlingen af oplysningerne.

Den nye persondataforordning indeholder endvidere et krav om dokumentationspligt for virksomheder. Det skal kunne bevises, at der er iværksat de nødvendige foranstaltninger for at sikre, at forordningens regler overholdes. Der skal gives flere oplysninger om databehandlingen, end virksomhederne gør i dag. Oplysningerne skal bl.a. indeholde dataansvarliges kontaktinformationer, formålet med databehandlingen, perioden for behandlingen, retten til indsigelse og retten til begrænsning af behandlingen, muligheden for at trække samtykke tilbage og muligheden for at klage til tilsynsmyndigheden (i Danmark er klageinstansen Datatilsynet).

Virksomhederne er også forpligtet til at berigtige informationer om en person, også i de tilfælde hvor der er blevet delt forkerte informationer om en person. Det er derfor vigtigt, at vide hvilke personoplysninger der behandles, hvor oplysningerne kommer fra, og hvem de deles med, for at være i stand til at efterleve denne forpligtelse.

Følgende er som i den nuværende lovgivning og skal overholdes:

- *God databehandlingsskik, dvs. databehandlingen skal være lovlig og rimelig.*
- *Behandling af persondata må kun foretages på baggrund af et sagligt og legitimt formål, som er udtrykkeligt angivet.*
- *Der må kun indhentes relevante, nødvendige og tilstrækkelige oplysninger.*
- *Proportionalitetsprincippet skal overholdes, dvs. behandlingen af data kun må finde sted, hvis den er nødvendig ift. formålet og samme resultat ikke kan opnås uden.*
- *Den dataansvarlige har en slette- og berigtigelsespligt, da personoplysninger, som ikke længere tjener til deres formål, skal slettes og ukorrekte oplysninger skal korrigeres.*

I den nye persondataforordning sker der følgende udvidelse:

- *Krav om dokumentation; det skal kunne bevises, at kravet til behandling af personoplysninger overholdes.*
- *Udvidet oplysningspligt, dvs. de registrerede personer har ret til at vide, hvordan deres oplysninger behandles på en klar og forståelig måde, hvor længe oplysningerne behandles og om muligheden for at klage til tilsynsmyndigheden (i Danmark er klageinstansen Datatilsynet). Alt i et klart og letforståeligt sprog.*
- *Ret til dataportabilitet, dvs. den registrerede person under visse omstændigheder har ret til at få udleveret oplysninger om sig selv.*
- *Ret til begrænsning af databehandling, retten til at få slettet data mv.*

For at overholde den nye persondataforordning bør virksomheden derfor løbende sikre, at virksomhedens politikker eller retningslinjer for håndtering af personoplysninger, sletning heraf, indsamling, løbende behandling mv. revideres i henhold til gældende lovgivning. Herunder er det vigtigt at se på formålene med databehandlingen, om data er nødvendige i forhold til formålet med at have og indsamle dem, om de er forældede, ikke nødvendige af have og rydde ud heri samt se på dokumentationspligten.

6. SAMTYKKE TIL BEHANDLING AF PERSONDATA

Selv om der i den nye persondataforordning er sket en skærpelse af kravene til samtykke, er der kun i et forhold sket en skærpelse af reglerne i Danmark, da Danmark allerede har regler om samtykke.

Samtykket skal være frivilligt, specifikt, informeret og utvetydigt. Det nye er, at samtykket skal være utvetydigt, hvilket er tilfældet, når de registrerede foretager en bekræftende handling, hvor de tilkendegiver, at de accepterer den konkrete behandling af deres personoplysninger til et bestemt formål. Dette kunne fx ske ved, at den registrerede klikkede af i en boks eller på anden måde tilkendegiver samtykket.

Samtykke kan dermed ikke være stiltiende, og virksomhederne skal som dataansvarlige kunne dokumentere, at samtykket er givet.

Samtykketeksten skal desuden være forståelig, klar og lettilgængelig i formen, samtidig med at et samtykke skal adskilles fra den øvrige tekst i en kontrakt, betingelser mv.

Det er vigtigt, at virksomhederne allerede nu har fokus på det nye aspekt i samtykkereglerne. Indhentning af samtykker bør derfor være fremadrettet og tilpasset den nye forordning med opdaterede samtykketekster, så de også er gældende efter den 25. maj 2018.

Er der tidligere indhentet samtykker, der ikke er gyldige efter den nye persondataforordning, skal virksomhederne indhente et nyt samtykke, for at sikre at virksomheden overholder lovgivningen.

7. BEHANDLING AF PERSONOPLYSNINGER OM BØRN

Virksomhederne bør overveje, hvordan det fremgår, hvor gamle de registrerede personer er, og hvordan der indhentes samtykke fra forældremyndighedsindehavere, når der behandles oplysninger om børn.

Der indføres i den nye persondataforordning en særlig beskyttelse af personoplysninger om børn. Den er som hovedregel gældende for børn under 16 år, men de enkelte EU-lande har mulighed for at fastsætte en lavere aldersgrænse til børn, dog ikke under 13 år.

8. SIKKERHEDSFORANSTALTNINGER FOR AT BESKYTTE PERSONDATA

Det er vigtigt, at have sikkerhedsforanstaltninger for at beskytte personoplysninger. Det kan være begrænset adgang, passwords, firewalls, kryptering mv.

Persondataforordningen indeholder nye bestemmelser om, hvad virksomhederne skal gøre for at beskytte persondata, og hvis der sker et brud på persondatasikkerheden.

Alle brud på persondatasikkerheden som indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder, skal kunne dokumenteres. Bruddet skal anmeldes til den relevante tilsynsmyndighed inden for 72 timer.

Hvis det drejer sig om højrisikobrud på sikkerheden fx identitetstyveri, bedrageri mv., skal virksomhederne endvidere uden unødig forsinkelse underrette de registrerede om bruddet.

Der er i forordningen nye begreber på dette område, som databeskyttelse gennem design (data protection by design) og databeskyttelse gennem standardindstillinger (data protection by default), som skal bidrage til beskyttelse af personoplysninger.

Databeskyttelse gennem design kræver, at design af systemer, der skal håndtere persondata fremadrettet, er særligt indrettet til at tage højde for databeskyttelse.

Databeskyttelse gennem standardindstillinger indeholder et princip om, at de mest begrænsende standardindstillinger skal anvendes som udgangspunkt for håndtering af persondata.

Der er en række krav til offentlige myndigheder i sikkerhedsbekendtgørelsen (nr. 528 af 15. juni 2000 med senere ændringer), som ikke er gældende for private virksomheder, hvor der kan hentes inspiration fra.

Det er dermed vigtigt, at virksomhederne har procedurer på plads til at opdage, rapportere og undersøge brud på sikkerheden og at alvorligheden af et brud på persondatasikkerheden kan vurderes, så fristen for underretningen kan overholdes.

9. OVERBLIK OVER TREDJEPARTER/DATABEHANDLERE

Virksomheder må kun gøre brug af databehandlere, hvis der indgås en skriftlig databehandleraftale mellem parterne med et nærmere bestemt indhold. Det er et krav at typen af oplysninger, kategorier af registrerede mv. skal fremgå af aftalen. Endvidere bør det overvejes at indsætte en bestemmelse om ansvar i aftalen, da der er sket en væsentlig ændring ift. de nuværende regler.

I de nye regler hæfter virksomheden, der er dataansvarlig, og aftaleparten, der er databehandler, solidarisk for ulovlig behandling, der foretages af databehandleren, i modsætning til de nuværende regler hvor den dataansvarlige ifalder alt ansvar, herunder for handlinger databehandleren foretager sig på dataansvarliges vegne. Derfor bør der også tages højde for tredjeparts adgang til data, og hvis der skal foretages back-up af IT-systemerne.

Ift. den udvidede oplysningspligt i persondataforordningen er det derfor vigtigt, at virksomhederne skaber et overblik over hvilke tiltag, der er nødvendige for at overholde forordningens regler, og gennemgå deres databehandleraftaler, så de er i overensstemmelse med den ny persondataforordning.

10. OVERFØRELSE AF DATA TIL UDLANDET

Det kræver ikke særlige forholdsregler, at overfører persondata til andre EU-lande, men hvis der er tale om lande uden for EU, skal data beskyttes. EU-Kommissionen har flere standardkontrakter, som ikke kræver Datatilsynets tilladelse, hvis ordlyden anvendes uændret, ved overførsel af data til lande uden for EU.

Ved overførsel af data til USA kan det være relevant at anvende den nye Privacy Shield-aftale, som er godkendt af EU-Kommissionen, og som de amerikanske virksomheder, som ønsker denne certificering, har kunne tilslutte sig siden 1. august 2016. Det er også muligt, at benytte Binding Corporate Rules inden for en koncern eller ved at indhente samtykke fra de registrerede personer.

Det er vigtigt at være opmærksom på, at Safe Harbour-aftalen er ugyldig. Virksomheder er i sommeren 2016 blevet idømt bøder, for at have brugt den nu ugyldige aftale for overførsel af data mellem EU og USA. Bødenivauet var på 8.000-11.000 euro, men forventes at stige, hvis virksomheder stadig ikke har fået rettet op på overførsler, som sker på baggrund af Safe Harbour-aftalen, da dette skulle være sket inden udgangen af januar 2016.

Det er vigtigt at holde sig opdateret omkring reglerne for at overføre personoplysninger til lande udenfor EU, da det retslige grundlag herfor løbende forandres.

11. HANDLINGSPLAN, IMPLEMENTERING OG VEDLIGEHOLDELSE

Det er vigtigt, at beslutte hvor ansvaret for databeskyttelsesspørgsmål skal være placeret og eventuelt udpege en Data Protection Officer (DPO). Persondataforordningen stiller krav om, at visse organisationer skal udpege en DPO. Dette gælder for eksempel alle offentlige myndigheder og virksomheder, som foretager en omfattende behandling af særlige (følsomme) persondata, eksempelvis medico/ pharma-virksomheder, jf. afsnit 12.

Hvis en virksomhed har selskaber i flere EU-lande, er den kompetente tilsynsmyndighed placeret i det EU-land, hvor hovedkontoret er beliggende eller i det land, hvor der træffes beslutninger om behandling af personoplysninger.

I organisationer med spredte ansvarsområder, hvor beslutninger om behandling af personoplysninger ofte tages forskellige steder, kan det være forskellige behandlinger, der falder under forskellige tilsynsmyndigheder.

Derfor er det vigtigt, at der foretages en kortlægning af hvor i organisationerne, de mest betydningsfulde beslutninger om behandling af personoplysninger træffes.

Som hovedregel får virksomheder ét lands datatilsyn som myndighed i stedet for alle EU-landenes datatilsyn. Den dataansvarlige skal derfor som hovedregel alene interagere med datatilsynet i det EU-land, hvor virksomheden foretager beslutninger vedrørende behandlingen af persondata. Tvister, der opstår i et andet EU-land, end der hvor virksomheden har sit datatilsyn, skal afgøres af datatilsynene i de to lande samstemmigt. Hvis der ikke kan træffes en afgørelse af de to tilsynsmyndigheder, skal afgørelsen træffes i et samarbejde mellem alle EU-datatilsyn.

12. DATA PROTECTION OFFICER, DPO, OG KURSER I PERSONDATAREGLER

Med vedtagelsen af den nye persondataforordning indføres et krav om udpegning af en Data Protection Officer (DPO). De virksomheder, der som kerneaktivitet behandler helbredsoplysninger i stort omfang, herunder oplysninger om eksempelvis bivirksomheder og forskningsdata, vil være omfattet. Det har ikke betydning, om en virksomhed har kliniske miljøer eller ej.

En DPO er ekspert i vurdering af virksomhedens behandling af persondataoplysninger. Det er ikke et juridisk krav for alle virksomheder at udpege en DPO, og det er også muligt at have en ekstern rådgiver.

Virksomhederne bør udpege en intern/ekstern DPO inden en eventuel inspektion fra Datatilsynet. Det er her vigtigt at påpege, at den samme person ikke bør både rådgive og sikre, at virksomheden overholder lovgivningen og at der ikke i øvrigt er en interessekonflikt.

Medicoindustrien udbyder kurser i persondataret. Desuden udbyder vi i samarbejde med advokatfirmaet DELACOUR en DPO uddannelse rettet særligt mod varetagelse af opgaver indenfor medicobranchen. Uddannelsen er tilrettelagt således, at deltagerne opnår det kompetenceniveau, der er nødvendigt, for at kunne bestride posten som DPO i henhold til persondataforordningen.

Se mere på
www.medicoindustrien.dk

MEDICO
INDUSTRIEN

Medicoindustrien
Agern Allé 13
2970 Hørsholm

Tlf.: 4918 4700
E-mail: medico@medicoindustrien.dk
www.medicoindustrien.dk