GDPR PERSONDATA FORORDNINGEN

PERSONDATA FORORDNINGEN – I KORT FORM

Persondataforordningen får virkning fra den 25. maj 2018. Fra denne dato skal alle virksomheder kunne dokumentere, at de overholder forordningen og dens mange nye krav.

Denne vejledning giver et samlet overblik i over de vigtigste regler i Persondataforordningen. Mange af reglerne og en del af forpligtelserne findes allerede i den nuværende persondatalov, men på grund af en række skærpelser og risikoen for bødestraf er der behov for øget fokus på området.

Kort sagt regulerer Persondataforordningen hvornår og hvordan personoplysninger om medarbejdere, kunder, samarbejdspartnere og andre interessenter må behandles. Alle virksomheder, B2B som B2C, har derfor behov for at kende reglerne. For virksomheder, hvor der i dag gælder særregulering, må det forventes, at dette i vid udstrækning også vil være tilfældet fremover.

Dansk Industri

1

ORD OG BEGREBER

For at forstå Persondataforordningen er en række begreber centrale:

PERSONOPLYSNING. Persondataforordningen beskytter oplysninger om en fysisk person, der er identificeret eller identificerbar. Når en oplysning kan knyttes til en fysisk person, er det en "personoplysning". Det gælder også selvom koblingen kun kan ske ved hjælp af oplysninger fra andre kilder og selv om disse kilder er utilgængelige for jeres virksomhed, f.eks. navnet på indehaveren af en pc med en bestemt IP-adresse (som i udgangspunktet kun er tilgængeligt for teleselskabet).

Personoplysninger er f.eks. navn, e-mail adresse, CPR-nr., kundenummer, helbredsoplysninger, fingeraftryk, fagforeningsmedlemsskab, portrætfoto, civilstatus, ip-adresse, lokationsdata, medarbejderevalueringer, forbrugshistorik og produktkøb.

Alle fysiske personer er beskyttet af reglerne i Persondataforordningen. Fysiske personer kan f.eks. være medarbejdere, privatkunder, passagerer, patienter, forsøgspersoner, journalister, politiske forbindelser, bestyrelsesmedlemmer, en leverandørs medarbejdere og besøgende på hjemmesiden.

DEN DATAANSVARLIGE. Den dataansvarlige er den virksomhed, der overordnet bestemmer, hvilke personoplysninger der skal behandles, hvorfor de behandles og hvordan. Virksomhedens forpligtelser efter Persondataforordningen afhænger af, om den er dataansvarlig eller databehandler.

DATABEHANDLER. Den dataansvarlige kan antage en databehandler til at indsamle eller behandle personoplysninger på sine vegne. F.eks. vil en hosting-leverandør, en cloudleverandør og en ekstern lønadministration ofte være databehandlere.

BEHANDLING. Begrebet omfatter groft sagt enhver håndtering af en personoplysning, f.eks. indsamling af oplysninger, samkøring, videregivelse, opbevaring, ændring og sletning. Persondataforordningen omfatter en hver automatisk (digital) behandling, men også manuel behandling er omfattet af Persondataforordningen, hvis personoplysningerne er eller vil blive indeholdt i et register.

2

PRINCIPPER FOR BEHANDLING AF PERSONOPLYSNINGER

Når I behandler personoplysninger, skal I overholde en række grundlæggende principper. Overordnet set handler principperne om, at man skal behandle personoplysninger ansvarligt og med omhu:

LOVLIGHED, RIMELIGHED OG GENNEMSIGTIGHED. For det første gælder der et princip om, at oplysninger skal behandles lovligt, rimeligt og på en gennemsigtig måde. Det betyder f.eks. at personoplysninger ikke må behandles, hvis det strider mod anden lovgivning eller en tidligere kommunikeret privatlivspolitik.

FORMÅLSBESTEMTHED. For det andet indebærer princippet om formålsbestemthed, at der skal være et eller flere udtrykkelige saglige og legitime formål med behandlingen, og at senere behandling ikke må stride mod disse oprindelige formål.

DATAMINIMERING OG PROPORTIONALITET. For det tredje skal de personoplysninger, der behandles, være tilstrækkelige, relevante og begrænsede til det, der er nødvendigt i forhold til at varetage formålene. En god tommelfingerregel er at behandle de oplysninger, som er "need to know" og ikke "nice to know".

DATAKVALITET. For det fjerde medfører princippet om datakvalitet, at personoplysningerne skal være korrekte, ajourførte, og at urigtige personoplysninger skal slettes eller berigtiges. Personoplysninger skal kunne opdateres eller slettes i IT-systemer.

OPBEVARINGSBEGRÆNSNING. Det femte princip om opbevaringsbegrænsning betyder, at personoplysninger skal slettes eller anonymiseres, når virksomheden ikke længere har behov for at behandle dem (herunder som følge af en lovmæssig forpligtelse).

For at opfylde slette-forpligtelsen skal I afgøre, hvor lang tid forskellige typer af personoplysninger skal og må behandles. I bør udarbejde slettepolitikker og –procedurer og rydde op i nuværende lagre af personoplysninger. Vi anbefaler, at I sætter god tid af til den proces.

INTEGRITET OG FORTROLIGHED. Endelig skaber det sjette princip om integritet og fortrolighed en forpligtelse til at sørge for de nødvendige sikkerhedsforanstaltninger, så oplysninger ikke kommer i de forkerte hænder, behandles ulovligt, går tabt, tilintetgøres eller beskadiges.

3

JURIDISK GRUNDLAG FOR BEHANDLINGEN

3.1 Generelt om behandlingsgrundlag

Ud over at overholde alle de grundlæggende principper, må personoplysninger kun behandles, når der er et såkaldt "behandlingsgrundlag". Hvilket behandlingsgrundlag, der kan være tale om, afhænger af typen af personoplysningerne og formålet med behandlingen.

ALMINDELIGE PERSONOPLYSNINGER. Langt de fleste personoplysninger er "almindelige personoplysninger". Det gælder f.eks. identifikationsoplysninger, men også mere personlige oplysninger som civilstatus, løn- og skatteforhold, eksamensresultater og antal sygedage.

De almindelige personoplysninger kan eksempelvis behandles, hvis den registrerede har givet sit samtykke til behandlingen, der er indgået en kontrakt med den registrerede, virksomheden skal overholde en retlig forpligtelse eller hvis en afvejning af parternes interesser falder ud til virksomhedens fordel.

FØLSOMME PERSONOPLYSNINGER. Når personoplysninger er "følsomme" omtales de i Persondataforordningen som "særlige kategorier af personoplysninger". For disse kategorier af oplysninger gælder der andre og mere restriktive regler for, hvornår oplysningerne må behandles. Følsomme personoplysninger er:

Oplysninger om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssigt tilhørsforhold, genetiske data, biometriske data til identificering af den registrerede person, helbredsoplysninger og seksuelle forhold eller oplysninger om seksuel orientering.

CPR-numre og oplysninger om straffedomme og lovovertrædelser vil forventeligt bliver underlagt særregler.

VIDEREGIVELSE. Hvis personoplysninger skal videregives til en tredjepart, f.eks. et andet koncernselskab, en offentlig myndighed, en faglig organisation eller øvrige virksomheder, der selv bliver dataansvarlige for de modtagne oplysninger, skal der også være et behandlingsgrundlag for at foretage denne videregivelse. Der gælder særlige krav, hvis oplysningerne videregives til lande uden for EU og EØS.

3.2 Særligt om samtykke

Når det juridiske behandlingsgrundlag er samtykke, skal hvert samtykke være frivilligt, specifikt, informeret og utvetydigt. Hvis der er tale om behandling af følsomme oplysninger skal samtykket være udtrykkeligt.

FRIVILLIGT. At samtykket skal være frivilligt betyder, at den registrerede skal have et reelt og frit valg. Hvis det skader den registrerede ikke at give samtykket eller at trække samtykket tilbage senere, er samtykket ikke umiddelbart frivilligt.

SPECIFIKT. At samtykket skal være specifikt betyder, at det skal være klart og afgrænset for den registrerede, hvilke personoplysninger der skal behandles af hvem.

INFORMERET. At samtykket skal være informeret betyder, at den registrerede skal have tilstrækkeligt information om behandlingen til at vurdere, om personen ønsker at samtykke.

UTVETYDIGT. At samtykket skal være utvetydigt betyder, at den registrerede kan give sit samtykke f.eks. ved en handling eller en erklæring.

UDTRYKKELIGT. Ved samtykke til f.eks. følsomme oplysninger skal samtykket som nævnt være udtrykkeligt. Det skærper kravene til klarheden hvormed samtykket er givet.

For at samtykket er gyldigt, skal den registrerede oplyses om, at samtykket kan trækkes tilbage. I skal have procedurer for tilbagekaldelser og eventuel følgende sletning af oplysninger.

DOKUMENTATION. Den nødvendige dokumentation for et samtykke kan f.eks. sikres ved at gemme samtykkeerklæringer eller ved teknisk at indrette IT-systemer, så personoplysninger først kan indsamles efter, at den registrerede person har givet sit samtykke.

Hvis et eksisterende samtykke ikke opfylder betingelserne, skal de registrerede personer give samtykke på ny inden den 25. maj 2018. Vi anbefaler at sætte god tid af til den proces.

4

REGISTREREDES RETTIGHEDER

4.1 Procedurer ved registreredes anmodninger

Registrerede personer har nogle personlige rettigheder i forhold til den dataansvarlige:

- Retten til information om behandlingen af de registrerede persons oplysninger.
- Retten til indsigt i, hvilke oplysninger, der behandles om den registrerede person og få udleveret en kopi af de personoplysninger, der behandles.
- Retten til berigtigelse af urigtige oplysninger.
- Retten til at blive glemt (herunder sletning af oplysninger).
- Retten til dataportabilitet, dvs. at få oplysninger overført til en ny leverandør
- Retten til begrænsning (”blokering”) af personoplysninger, f.eks. ved indsigelse mod behandlingen.
- Retten til at gøre indsigelse mod selve behandlingen.
- Retten til at gøre indsigelse mod automatiske individuelle afgørelser og profilering.
- Retten til at trække et afgivet samtykke tilbage.
- Retten til at indgive en klage over behandlingen til Datatilsynet.

Virksomheder skal fastsætte og indføre procedurer for, hvordan det praktisk håndteres, når en registreret person retter henvendelse og ønsker at gøre brug af en af rettighederne. IT-systemerne skal også tilpasses, så de understøtter rettigheder og procedurer.

4.2 Oplysningspligten over for den registrerede

Virksomheder skal oplyse den registrerede om behandlingen af personoplysninger, f.eks. i en privatlivspolitik. Der skal blandt andet gives disse oplysninger:

- Hvem er dataansvarlig?
- Hvilke kategorier af personoplysninger indsamles?
- Hvad er formålet med behandlingen?
- Hvor lang tid opbevares oplysningerne?
- Hvilke rettigheder har den registrerede person?
- På hvilket juridisk grundlag behandles oplysninger?
- Hvem videregives oplysningerne til?
- På hvilket grundlag overføres oplysninger til lande uden for EU/EØS?
- Konsekvenserne og betydningen af automatiske, individuelle afgørelser (se nedenfor).

Virksomheden skal kunne dokumentere, at informationen er givet.

4.3 Særligt om indsigelsesret

Den registrerede har ret til at gøre indsigelse mod behandlingen af personoplysninger, hvis det juridiske grundlag for eksempel er interesseafvejning eller hvis personoplysningerne behandles til direkte markedsføring. Der skal gives særskilt oplysning om retten til at gøre indsigelse i første kommunikation med den registrerede.

4.4 Særligt om automatiske individuelle afgørelser og profilering

Profilering kan anvendes i mange situationer, og de fleste er nok blevet profileret enten som jobansøger (personlighedstest9 eller som låntager (kreditvurdering). Profilering er en automatiseret analyse, evaluering og forudsigelse af den registreredes personlige karaktertræk og adfærd. Vurderinger kan f.eks. omfatte personens indsats på arbejdspladsen, økonomisk situation, helbred, personlige præferencer, interesser eller geografisk position.

Automatiske individuelle afgørelser er beslutninger, der kan træffes på baggrund af profilering. Det kan være, når en potentiel kunde via et forsikringsselskabs ansøger om en forsikring, og systemet automatisk og alene på baggrund af de indtastede oplysninger afgør, om kunden kan tegne forsikring.

Den registrerede person har altid ret til at gøre indsigelse mod, at der træffes automatiserede afgørelser og har – afhængig af behandlingsgrundlag – som minimum ret til, at der træffes en afgørelse baseret på personens synspunkter frem for en ren maskinel afgørelse. Hvis profileringen anvender følsomme personoplysninger f.eks. om helbred, skal den registrerede givet udtrykkeligt samtykke, eller særlovgivning skal tillade profileringen.

4.5 Særligt om underretning af tredjeparter

I de tilfælde, hvor personoplysninger berigtiges, blokeres eller slettes, fordi en registreret person har gjort indsigelse og anmodet herom, skal virksomheden give besked til de tredjeparter, som har modtaget de pågældende personoplysninger. Disse modtagere skal have besked om at foretage samme berigtigelse, blokering eller sletning.

Det vil være nødvendigt at fastlægge særlige procedurer så de relevante tredjeparter underrettes om, at en registreret person har gjort brug af sine rettigheder.

5

DATABESKYTTELSESRÅDGIVER

Virksomheder, der som led i deres kerneaktivitet behandler følsomme oplysninger (og oplysninger om straffedomme) i stort omfang eller systematisk overvåger personer i stort omfang, bliver forpligtede til at udpege en databeskyttelsesrådgiver.

Databeskyttelsesrådgiveren skal fungere som den interne vagthund og skal holde øje med, at virksomheden overholder reglerne om persondatabeskyttelse. Databeskyttelsesrådgiveren skal rapportere til virksomhedens øverste ledelse. Databeskyttelsesrådgiveren skal også rådgive virksomheden om behandlingen af personoplysninger og skal være den person, som både Datatilsynet og de registrerede kan kontakte.

EKSPERTISE. Det er et krav, at databeskyttelsesrådgiveren har ekspertise og erfaring inden for persondataret og -praksis. Det er underordnet, om databeskyttelsesrådgiveren er en medarbejder i virksomheden eller en ekstern konsulent, så længe personen har de nødvendige kvalifikationer.

UAFHÆNGIGHED. Det er også et krav, at databeskyttelsesrådgiveren er uafhængig. Det betyder, at virksomheden ikke må instruere databeskyttelsesrådgiveren i, hvordan opgaverne skal udføres. Databeskyttelsesrådgiveren må gerne varetage andre arbejdsopgaver, men de stillingerne må ikke skabe interessekonflikter, f.eks. at databeskyttelsesrådgiveren kontrollerer sit eget arbejde.

6

DATABESKYTTELSESPOLITIK OG SIKKERHED

6.1 Databeskyttelsespolitik og konsekvensanalyser

Virksomheden kan udarbejde en databeskyttelsespolitik og procedurer for, hvordan behandlingen af personoplysninger håndteres.

Efter 25. maj 2018 skal virksomheder gennemføre konsekvensanalyser, hvis en behandling indebærer en særlig høj risiko for den registrerede person. En konsekvensanalyse er mere intensiv og dybdegående end en risikoanalyse, og virksomheden skal forsøge at reducere risiciene med behandlingen mest muligt.

6.2 Sikkerhedsforanstaltninger

Persondataforordningen stiller mange krav til, hvilke sikkerhedsforanstaltninger virksomheder skal implementere. Virksomheden skal sikre den organisatoriske sikkerhed ved at begrænse adgangen til personoplysninger til de medarbejdere, som har et arbejdsbetinget behov for at have adgang. Herudover skal virksomheden sikre den tekniske sikkerhed f.eks. ved at kryptere personoplysninger, når de transporteres via et åbent netværk.

Det påkrævede sikkerhedsniveau afhænger af hvor risikofyldt den konkrete behandling er for den registrerede. Det afklares i en forudgående risikoanalyse.

6.3 Sikkerhedsbrud

Hvis der sker et brud på persondatasikkerheden, kan virksomheden være forpligtet til at orientere Datatilsynet inden for 72 timer. Afhængig af særlovgivning skal også andre myndigheder informeres. De berørte registrerede skal også orienteres, hvis sikkerhedsbruddet indebærer en høj risiko for de registrerede.

Vi anbefaler, at I forbereder jer på, at sikkerhedsbrud kan indtræffe alle steder og i alle virksomheder. En god forberedelse og handlingsplan giver jeres ledelse og organisation en bedre mulighed for at navigere mellem egne afdelinger, de registrerede, pressen og myndighederne. Alle sikkerhedsbrud skal dokumenteres i en log.

7

BRUG AF DATABEHANDLERE

7.1 Pre-audits og løbende audits

Før virksomheder, der er dataansvarlige, indgår aftaler med databehandlere, skal virksomheden undersøge, at databehandleren er i stand til at overholde Persondataforordningen og de instrukser, som den dataansvarlige virksomheder giver. Den dataansvarlige skal løbende kontrollere, at databehandleren efterlever reglerne og instrukserne. Databehandlerens sikkerhed, databeskyttelsespolitikker og procedurer for behandlingen af personoplysninger bør gennemgås. Kontrollerne skal ske med passende mellemrum, som tommelfingerregel en gang årligt. Kontrol kan f.eks. udføres ved hjælp af et spørgeskema eller ved, at databehandleren får udarbejdet en uafhængig tredjepartserklæring f.eks. en revisorerklæring.

Når aftalen om behandling af personoplysninger er ophørt, skal den dataansvarlige sikre, at alle personoplysningerne slettes hos databehandleren.

Virksomheden bør udarbejde procedurer for, hvordan databehandlere undersøges og kontrolleres før, under og efter aftaleforholdet.

7.2 Databehandleraftaler

Det er et krav, at den dataansvarlige og databehandleren indgår en skriftlig databehandleraftale. Persondataforordningen indeholder desuden en lang række krav til indholdet af aftalen. Kravene er langt mere omfattende end de gældende krav. Det betyder, at alle databehandleraftaler skal genforhandles. Også dette krav gør det nødvendigt at danne sig et overblik over, hvilke databehandlere I anvender, og hvilke underdatabehandlere databehandleren anvender.

Ved standardiseret databehandling kan I anvende DI's standarddatabehandleraftale. Hvis aftaleforholdet er mere komplekst, anbefaler vi at I søger individuel rådgivning. DI's tjekliste til gennemgang af databehandleraftaler kan anvendes, når I modtager et aftaleudkast fra jeres samarbejdspartnere. Både aftalen og tjeklisten beskriver, hvilke forhold der som minimum skal være reguleret i databehandleraftalen.

8

FORTEGNELSEN OVER BEHANDLINGER

Alle virksomheder skal udarbejde og løbende opdatere fortegnelser over behandlinger af personoplysninger, som foretages af selve virksomheden selv eller på virksomhedens vegne. Persondataforordningen beskriver, hvilken information der som minimum skal indgå i fortegnelserne. I kan anvende DI's format til dokumentation for behandlingen af personoplysninger til at udarbejde fortegnelserne.

9

INTERNE PROCEDURER, TRÆNING OG AWARENESS

Virksomheder bør udarbejde procedurer og retningslinjer for, hvordan medarbejdere må og skal indsamle, behandle og videregive personoplysninger. Procedurerne kan med fordel målrettes medarbejdernes forskellige funktioner. For eksempel bør medarbejdere i HR-afdelingen modtage en procedure, der er skræddersyet til arbejdsopgaverne i denne afdeling, mens medarbejdere i IT-afdelingen bør modtage en anden. HR-afdelingen vil have behov for at vide, hvordan fratrådte medarbejderes personalemapper må håndteres, mens IT-afdelingen skal vide i hvilke tilfælde, de må give en leder adgang til medarbejderens e-mail-konto. I kan også igangsætte awareness-kampagner eller lignende med fokus på privatlivsbeskyttelse.

10

HVAD GØR I NU?

Vi har erfaret, at mange virksomheder ikke har overblik over, hvilke personoplysninger, de egentligt behandler, hvorfor de behandles, hvem de deles med og om de slettes. Det vil derfor typisk være nødvendigt at få skabt dette overblik for at kunne tilpasse organisationen og processerne til de fremtidige Persondataforordningen.

Overblikket kan bl.a. skabes ved at gennemføre en datastrømsanalyse. Den har til formål at afdække virksomhedens behandling af personoplysninger og identificere, hvor reglerne overholdes og hvor virksomheden skal rettes til.

Datastrømsanalysen kan gennemføres ved at anvende DI's standardspørgeskema med tilhørende vejledning til procesafdækning.

I bør sigte efter at få afdækket processer, gennemført spørgeskemaundersøgelse/interviews og have færdiggjort analysen om de nødvendige tiltag og derefter forberede og implementere tiltagene inden den 25. maj 2018. For større virksomheder kan det vise sig vanskeligt og prioriteringer kan blive nødvendige, men det er vigtigt at I kommer i gang hurtigst muligt - og holder tempoet oppe, når projektet er sat i søen.

Dansk Industri ønsker vores medlemmer god arbejdslyst!

GDPR PERSONDATA FORORDNINGEN

Dansk Industri