Generelt om persondata og EU's persondataforordning

Persondata er i Danmark allerede beskyttet af Persondataloven. Her stilles strenge krav til omgangen med persondata, og disse krav ændres der i princippet ikke ved. Men der ændres i fordelingen af ansvar og straffene for overtrædelse. Dertil kommer at den enkelte borgere får langt flere rettigheder og kontrol over egne data, og oplysningspligt og krav til samtykke ved registrering skærpes.

Hvad er persondata og hvem berører det?

Persondata er alt der kan henføres til en konkret og identificerbar person, og alle oplysninger om vedkommende. Kort fortalt er det alle data om personer – lige fra simple oplysninger om navn og adresse, til oplysninger om adfærd, løn, helbred, køb, CPR-numre etc.

Derfor berører reglerne alle virksomheder og organisationer. For alle opbevarer oplysninger om personer – som minimum egne medarbejdere, men ofte også kunder/medlemmer, tidligere ansatte, samarbejdspartnere etc.

Der er ikke noget galt i at have disse oplysninger, men de skal opbevares forsvarligt, bruges med omtanke, dem de omhandler skal informeres og give samtykke og de skal slettes, når de ikke længere er nødvendige at gemme.

Opbevaring af persondata

Generelt bør persondata kun opbevares så længe der er behov for dem, hverken mere eller mindre. De skal beskyttes, og opbevares sikkert mod alle andre end dem der skal bruge dem.

De vigtigste regler om opbevaring af persondata

- Persondata må kun opbevares når de tjener et formål.
- Kun de oplysninger der er strengt nødvendige må gemmes.
- Kun dem der har behov for det skal have adgang tid dem, og kun så længe det er nødvendigt.
- De skal opbevares sikkert og beskyttet for alle andre.
- Når data ikke længe skal bruges, skal de slettes.

Når persondata opbevares på en computer, skal den være beskyttet med et sikkert password, og når computeren forlades skal adgangen til den være låst (eller adgang til lokalet være låst). Computere forbundet med internettet skal være sikret med opdateret virusbeskyttelse.

Persondata der opbevares fysisk, er underlagt samme krav om beskyttelse. Dvs. hvis de findes i f.eks. en mappe, skal den være låst inde, når ikke den bruges. Der må ikke ligge papir med

persondata frit tilgængeligt på bordet, når et rum efterlades ulåst, og når data ikke længe bruges, skal de makuleres.

Om sikre password

- Et password bør være personligt, og ikke skrives ned steder hvor det er frit tilgængeligt.
- Et password bør bestå af både tal og bogstaver, der er ulogiske for andre og som ikke referere til personlige oplysninger der er nemme at regne ud (f.eks. fødselsdato eller navne på ens børn).
- Et password bør bestå af mindst 8 tegn, gerne flere (for hvert tegn udvides beskyttelsen gevaldigt), samt både små og store bogstaver og tal.
- Det er godt at bruge en remse eller sætning, der kun giver mening for en selv, da det er nemt at huske og svært for en computer eller hacker at regne sig frem til.
- Passwords bør ikke genbruges.

Samtykke og oplysningspligt

Når du gemmer personoplysninger, har du pligt til at informere dem der registreres. Denne oplysningspligt gælder altid, og den registrerede skal give samtykke til ikke bare at oplysningerne gemmes, men også til de måder oplysningerne anvendes på, eller hvis de videregives til andre.

Reglerne her er blevet skærpet, og samtidig er der også skærpet dokumentationskrav. Dvs. at når man gemmer persondata, skal man til enhver tid, hvis f.eks. Datatilsynet kommer på besøg, kunne dokumentere at man eksplicit samtykke til alt det persondata man har, og til præcis den måde det anvendes på.

Det skal oplyses

- Præcis hvilke oplysninger der gemmes (f.eks. navn, adresse, CPR-nummer etc.), og hvor længe (det behøver ikke at være en konkret slutdato, men kan f.eks. være så længe du er medlem).
- Formålet med registreringen (f.eks. at kunne udbetale løn eller kunne udbetale feriepenge).
- Hvem der bruger data (hvis de anvendes uden for virksomheden, f.eks. af et lønservicebureau).
- Hvis data kan overdrages til andre, og formålet med det (f.eks. hvis SSV kan få adgang til data i forbindelse med support).
- Kontaktoplysninger til dataansvarlig, rettighed til at få slettet data, mulighed for at klage.

Den registrerede skal herefter give sit samtykke. For samtykket gælder følgende:

Samtykke

- Samtykket skal være frivilligt og oplyst.
- Forespørgsel om samtykke skal være tydeligt beskrevet og være adskilt fra andre vilkår.
- Samtykket skal være eksplicit og må ikke være indirekte eller underforstået (f.eks. ved ansættelse).
- For hver gang der ændres i anvendelse, vilkår, formål eller hvis data videregives til andre (end oprindeligt oplyst), skal der indhentes et nyt samtykke.

For brugere af SSV's programmer, vil det være fordel hvis der fra start, når data registreres, indhentes samtykke til at data kan overdrages til SSV i forbindelse med support. Det kan være en formulering i stil med *"De registrerede data kan kortvarigt eller midlertidigt overdrages til vores systemleverandør, SSV, i forbindelse med support, test eller systemopgradering. Data opbevares sikkert og beskyttet, vores systemleverandør er underlagt fortrolighed og alle data slettes igen, når sagen er afsluttet."*

Ellers skal der indhentes et nyt samtykke hver gang.

Ret til at blive glemt/slettet

Helt afgørende i Persondataforordningen, er at enhver person har den fulde ret over sine egne data. Det er en selv der ejer sine data, og når andre opbevarer dem, så må det kun ske frivilligt, på et oplyst grundlag og med samtykke.

Samtidig har enhver ret til, til en hver tid, at få indsigt i de data der er gemt om vedkommende, ændre data eller få data slettet eller blive glemt, dvs. få slettet alt data og historik. Det er samtidig et lovkrav at det skal være lige så let at trække et samtykke tilbage, som det er at afgive et samtykke.

Denne ret til, til en hver tid, at blive glemt, står som en helt afgørende borgerrettighed.

Men der er forbehold, og det er væsentligt at være opmærksom på.

Man har lov til fortsat at gemme persondata, hvis der er givet samtykke (der opfylder kravene) og hvis dataene er afgørende nødvendige for at kunne opretholde den aftale der er med den registrerede om formålet med registreringen. Eller sagt på en anden måde, du kan godt bede din arbejdsgiver om at han sletter alle dine persondata, men så kan du ikke få nogen løn.

Du har altså lov til at afvise at slette data, hvis der er en god grund til det, og dataene er nødvendige for at du kan udføre dit arbejde (og formålet i øvrigt er fornuftigt og inden for rimelighedens grænser).

Men vigtigt er det at være opmærksom på at de oplysninger, man ikke kan dokumentere er strengt nødvendige for at opretholde formålet, har man pligt til at slette, hvis man anmodes om det. Og man er forpligtet til at sikre at det også sker hos alle man har overdraget data til eller som behandler data på vegne af en.

Ansvarlig for data

Allerede i dag skelner man i persondataloven mellem dataansvarlig og databehandler.

- Dataansvarlig er den der er ansvarlig for at data skal indsamles og til hvilket formål de skal gemmes.
- Databehandler er den der i praksis behandler data på vegne af den dataansvarlige. Det kan være samme virksomhed, men det kan også være en anden virksomhed der behandler data på vegne af den dataansvarlige, f.eks. et lønservicebureau eller en systemleverandør.

Det er den dataansvarlige der udstikker rammerne for hvordan data skal og må behandles, og en databehandler må kun opbevare og behandle data efter aftale og forskrifter fra den dataansvarlige.

Det nye i persondataforordningen er at databehandleren pålægges langt mere ansvar, og også kan idømmes markant højere bøder.

Det er nu databehandlerens ansvar at man overholder de aftaler der er med dataansvarlig om anvendelsen af data, at data opbevares sikkerhedsmæssigt forsvarligt og at sikre øvrige regler overholdes for de data de har i deres varetægt.

Selvom man kun opbevarer data for andre, skal man altså være langt mere opmærksom på at reglerne overholdes – og bøderne man kan pålægges, er hævet ret markant.

Underretningspligt ved databrud

Et punkt hvor der også er strammet markant, er underretningspligten ved databrud – det gælder både for datasnaverlig og databehandler.

Databrud kan være hvis uvedkommende får adgang til data via hacking eller et læk af data, men det kan også være hvis andre medarbejdere end de betroede medarbejdere der har fået lov til at arbejde med data, får adgang til dem.

Den dataansvarlige skal underrette Datatilsynet senest 72 timer efter bruddet, og databehandler skal underrette dataansvarlig, så hurtigt som det er muligt.

En underretnings skal indeholde:

- En beskrivelse af databruddet, antal berørte personer og mængde og type af data
- Beskrivelse af mulige konsekvenser
- Beskrivelse af handlinger man planlægger at foretage for at imødegå bruddet
- Kontaktperson i virksomheden.

Registrerede personer der er direkte berørt, hvis data er blevet tilgængelige for andre, skal ligeledes underrettes, hvis det skønnes at data kan misbruges til skade for de registrerede. Underretningen skal indeholde ovenstående informationer, men ikke information om antallet af berørte personer og mængden af data.