

Skanderborg, den 20. april 2016
Initialer

Persondatalovgivning; kort introduktion til loven samt personoplysninger med relation til forsyningernes personaleadministration

Af Susanne Vangsgård

”Rolig, ingen grund til at piske dig selv over, at du ikke har overblikket og forstår alle facetter i persondatalovgivningen”: Grundloven for håndtering af persondata indeholder nemlig et hav af emner og udfordringer, når man gerne vil forstå og efterleve den i hverdagen.

En tilgang synes at være, at man tager den i små bidder, og i nærværende artikel vil fokuset således være på:

- Udvalgte centrale principper og definitioner
- Personoplysninger med relation til vandselskabernes personale

Der vil således være en synliggøre, at dels Datatilsynets sikkerhedsmæssige krav i forbindelse med anmeldelse af behandling af personaledata dels inspiration fra multiforsyningen Provas i forhold til at løfte sin informationsforpligtigelse overfor personalet, når de ansatte bliver de registrerede efter persondataloven.

Generelt om persondataloven

Den danske persondatalov, lov nr. 429/2000, der er baseret på et EU direktiv måtte igennem tre lovforslag, før den blev vedtaget af Folketinget. Loven er en general regulering, der omfatter myndigheder, virksomheder, foreninger m.m., og den gælder, medmindre der er gjort konkrete undtagelser i selve persondataloven eller i sektorlovgivning. Loven er med andre ord grundloven for indsamling, registrering, videregivelse og beskyttelse af alle typer personoplysninger.

Anvendelse

Persondataloven gælder som hovedregel for al elektronisk behandling af personoplysninger. Desuden gælder loven for manuel behandling af personoplysninger, som er indeholdt i et register.

I den private sektor gælder persondataloven endvidere for systematisk behandling af personoplysninger, selvom den ikke foregår elektronisk. F.eks. sagsmapper, ringbind m.v. Offentligt ejede selskaber er ikke eksplicit omtalt i loven eller i lovbemærkningerne – men bl.a. Datatilsynet har tilkendegivet, at den privatretlige organisationsform er baggrund for, at de kommunalt ejede forsyninger anses som værende private efter denne lov.

Personoplysninger

Persondataloven opdeler personoplysninger i tre typer: Følsomme oplysninger, oplysninger om andre rent private forhold (semi-følsomme oplysninger) og almindelige ikke-følsomme oplysninger, §§ 6-8.

Opdelingen findes, fordi der gælder forskellige betingelser og procedurer for behandling af personoplysninger afhængig af oplysningernes følsomhed. Reglerne er udtryk for, at jo mere følsomme oplysningerne er, jo mindre manøvrerum for indsamling, registrering, opbevaring, videregivelse mv.

Begrebet personoplysninger er kort omtalt i den generelle definitionsbestemmelse, § 3, og heraf fremgår, at der er tale om enhver form for information om en identificeret eller identificerbar fysisk person (den registrerede). Dette inkluderer:

- personhenførbare informationer (ex.vis BBR-oplysninger)
- objektive og subjektive oplysninger (ex.vis ID-oplysninger, økonomi, helbred, familieforhold, uddannelse, erhverv, billede, disciplinære forhold, bedømmelse)
- bipersoner (ex.vis pårørende, professionelle aktører som lærer, læge, sagsbehandler)
- afdøde
- enkeltmandsejede virksomheder incl. små interessentselskaber

Samtykke og rettigheder for den registrerede

Et andet centralt begreb er samtykke, der er beskrevet som: "Enhver frivillig, specifik og informeret viljestilkendegivelse, hvorved den registrerede indvilliger i, at oplysninger, der vedrører den pågældende selv gøres til genstand for behandling". I den forbindelse er det værd at bemærket, at der ikke er krav om skriftlighed – selvom det må være anbefalingen ud fra et dokumentationsbehov ved tvister. Der er således et krav om et udtrykkeligt samtykke, og dertil kommer at et sådant faktisk kan tilbagekaldes, se § 38.

Den registrerede har en række andre rettigheder herunder:

- Ret til indsigt i de oplysninger, der behandles om den registrerede,
- Ret til at få information om, at der indsamles oplysninger om den registrerede
- Ret til at få slettet eller rettet urigtige oplysninger
- Ret til at tilbagekalde samtykke.

Privates anmeldelse til Datatilsynet af anmeldelsespligtige personoplysninger – er omtalt i lovens kapitel 13. Udgangspunktet er faktisk, at der skal anmeldelse, men der er en række undtagelse, og den korte, forsimplede udlægning er, at der ved behandling af følsomme og semi-følsomme oplysninger (§§ 7 og 8) skal ske anmeldelse – og det samme gør sig gældende for flere almindelige oplysninger omfattet af § 6, når de har fortrolig karakter.

Data om forsyningernes personale

Når en virksomhed indsamler og opbevarer oplysninger om personer, der er ansat i virksomheden, eller som har været ansat, eller som søger job i virksomheden, gælder persondataloven.

Konkrete oplysningstyper

I forbindelse med personaleadministration opbevarer virksomhederne forskellige typer af oplysninger om de ansatte: Almindelige oplysninger er f.eks. identifikationsoplysninger, såsom medarbejderens navn, adresse og telefonnummer, fødselsdato, nær familie, oplysninger om uddannelse, udtalelser, tidligere beskæftigelse, nuværende stilling, arbejdsopgaver, arbejdstider og andre tjenstlige forhold, oplysninger om løn, skat, sygefravær og sygdomsperioder, oplysninger om andet fravær fra arbejdet, oplysninger om pensionsforhold, kildeoplysninger og oplysninger om kontonummer, hvortil løn skal anvises.

Sådanne almindelige oplysninger vil normalt kunne registreres, i det omfang virksomheden skal bruge oplysningerne. Virksomheden må endvidere normalt registrere de oplysninger om en ansøger, som personen selv afgiver i sin ansøgning. Reglerne om behandling af almindelige personoplysninger findes i lovens § 6. Følsomme oplysninger er f.eks. oplysninger om helbredsforhold, herunder misbrug af nydelsesmidler, alkohol m.v., oplysninger om medlemskab af en fagforening, oplysninger om strafbare forhold samt andre tilsvarende rent private forhold, f.eks. om at en medarbejder er bortvist fra jobbet på grund af en grov tilsidesættelse af ansættelsesforholdet. En personlighedstest vil som regel også skulle betragtes som en følsom oplysning.

Følsomme oplysninger er også oplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, seksuelle forhold og væsentlige sociale problemer, se §§ 7 og 8.

Som hovedregel må en virksomhed kun registrere følsomme oplysninger om en medarbejder, hvis medarbejderen har givet udtrykkeligt samtykke til dette. Opbevarer forsyningen anmeldelsespligtige oplysninger – hvilket den højst sandsynlig gør, så kræver loven anmeldelse til Datatilsynet. Se Datatilsynets hjemmeside og vær opmærksom på de særlige krav, der er, <https://www.datatilsynet.dk/forside/>

Krav om datasikkerhed

I forbindelse med personaleadministration skal persondatalovens regler i det hele iagttages. Det indebærer blandt andet, at den dataansvarlige virksomhed skal leve op til lovens krav om datasikkerhed. Der skal således træffes de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven, se § 41, stk. 3.

Datatilsynet har udformet nedenstående specifikke minimumskrav for sikkerhed i forbindelse med personaleadministration, og de indgår som standardkrav i forbindelse med tilladelserne.

- 1) Beskriv hvordan forsyningen beskytter personaleoplysninger i personaleadministration og hvordan sel-skabet i praksis har implementeret pkt. 2-12 i den nærværende oplystning. Beskrivelsen kan være særlige retningslinjer, der indgår i virksomhedens uddybende sikkerhedsregler, i en it-sikkerhedspolitik eller som en del af virksomhedens information til medarbejderne.
- 2) Adgang til oplysningerne skal begrænses til personer, der har et sagligt behov for adgang til oplysningerne. Det skal være så få personer som muligt.

- 3) Medarbejdere, der håndterer personaleoplysninger, skal have instruktion og oplæring i, hvad de må gøre med oplysningerne, og hvordan de skal beskytte oplysningerne.
- 4) Personaleoplysninger på papir – f.eks. i kartoteker og ringbind – skal opbevares aflåst, når de ikke er i brug. Et aflåst rum, hvor andre end de medarbejdere, der håndterer personaleoplysningerne har adgang er ikke tilstrækkeligt. Så skal de selve de reoler eller skuffer, hvori der opbevares personaleoplysninger være aflåst. Når dokumenter (papirer, kartotekskort mv.) med personaleoplysninger skal smides ud, skal der anvendes makulering eller anden foranstaltning, der forhindrer, at uvedkommende kan få adgang til oplysningerne.
- 5) Der skal anvendes adgangskode for at få adgang til pc'er og andet elektronisk udstyr med personoplysninger. Kun de personer, der skal have adgang, må få en kode. De personer, der har adgangskode, må ikke overlade koden til andre eller lade den ligge, så andre kan se den. Kontrol af tildelte koder skal foretages mindst en gang hvert halve år.
- 6) Det skal registreres, hvis der er forgæves forsøg på at få adgang til it-systemer med følsomme personaleoplysninger. Hvis der registreres et nærmere fastsat antal på hinanden følgende afviste adgangsforsøg, skal der blokeres for yderligere forsøg.
- 7) Hvis personaleoplysninger lagres på en USB-nøgle, skal oplysningerne beskyttes. Der kan f.eks. bruges en USB-nøgle med adgangskode og kryptering. Ellers skal USB-nøglen opbevares i aflåst skuffe eller skab. Tilsvarende gælder ved opbevaring af personaleoplysninger på andre bærbare datamedier.
- 8) PC'er koblet til internettet skal have en opdateret firewall og viruskontrol installeret.
- 9) Hvis der benyttes hjemmesideformularer, hvor følsomme personaleoplysninger og personnummer kan indtastes og fremsendes, skal der anvendes kryptering.
- 10) Hvis følsomme personaleoplysninger og personnummer sendes med e-mail via internettet, anbefaler Datatilsynet kryptering.
- 11) I forbindelse med reparation og service af dataudstyr, der indeholder personoplysninger, og når datamedier skal sælges eller kasseres, skal der træffes de fornødne foranstaltninger, så oplysninger ikke kan komme til uvedkommendes kendskab.
- 12) Ved brug af en ekstern databehandler til håndtering af oplysninger, skal persondatalovens § 42 om skriftlig databehandleraftale mv. følges. Det gælder eksempelvis, når der anvendes et eksternt dokumentarkiv eller rekrutteringssystem på internettet.

Oplysningspligt

Den registreredes/personalets rettigheder er kort berørt tidligere i artiklen – og i tilknytning hertil skal understreges, at der er en pligt for den dataansvarlige i forsyningen til at give oplysninger ved indsamling af data

Den nævnte informationsforpligtigelsen har hjemmel i lovens § 28 eller § 29, og DANVA kan oplyse, at multiforsyningen Provas har stillet sit informationsnotat til medarbejderne fra 2015 til rådighed som inspiration, se DANVAs hjemmeside.

Afslutningsvis

Der ligger mange opgaver i dels en sikker håndteringen af personoplysninger i forbindelse med personaleadministrationen i forsyningerne dels i virkeliggørelsen af informationspligten.

Anmeldelsespligten, som vi formoder relativt få forsyninger har løftet på nuværende tidspunkt, er forbundet med betaling af et gebyr på 2.000 kroner. I forhold til dette punkt er det værd at bemærket, at kravet om anmeldelse i de nævnte tilfælde sandsynligvis forsvinder ved ikrafttrædelse af den kommende EU forordning om beskyttelse af persondata. Der er ingen tvivl om, at gældende lovgivning skal overholdes. Om datatilsynet på trods af dette, vil se med milde øjne på manglende anmeldelse indtil da er uvist – men det er DANVAs håb, at der i løbet af 2016 kommer afklaring der på. Det er i hvert fald sikkert, at hvis alle selskaber m.fl., der i øjeblikket ikke har lavet det fornøden anmeldelse fremsender sådanne, vil Datatilsynet få rigeligt at lave.

DANVA sekretariatet har ikke ekspertviden om persondataretlige område, og vi vil gerne opfordre til, at forsyningerne deltager i kurser m.m. – og følger med i samarbejdet mellem DANVA og Dansk Fjernvarmeforening samt resultaterne heraf, som vil blive omtalt på bl.a. vores hjemmeside efterhånden, som de foreligger.