



Augustenborg Fjernvarme

Medarbejder information
Persondataloven.



Augustenborg Fjernvarme

Persondata

Information og retningslinjer til ansatte omkring håndtering af persondata. Dækker både persondata på forbrugere og ansatte.

Generelt – hvorfor?

I forbindelse med opdatering af loven om persondata beskyttelse er kravene blevet skærpet. Datatilsynet vil følge op på om virksomhederne efterlever kravene til beskyttelse af persondata.

- Kun relevant persondata må opbevares i virksomheden
- Persondata skal som udgangspunkt slettes, med mindre de er nødvendige for drift af virksomheden.
- Hvis en person henvender sig og ønsker aktindsigt i egne oplysninger skal virksomheden kunne oplyse hvilke persondata man opbevarer på pågældende.
- Man har krav på at blive glemt, dvs. få slettet persondata i virksomheden på forlangende, med mindre virksomheden lovgivningsmæssigt er forpligtet til at opbevare disse.
- Rettigheder for alle :
 - Ret til at se oplysninger - Ret til berigtigelse - Ret til sletning –
Ret til begrænsning af behandling - Ret til indsigelse



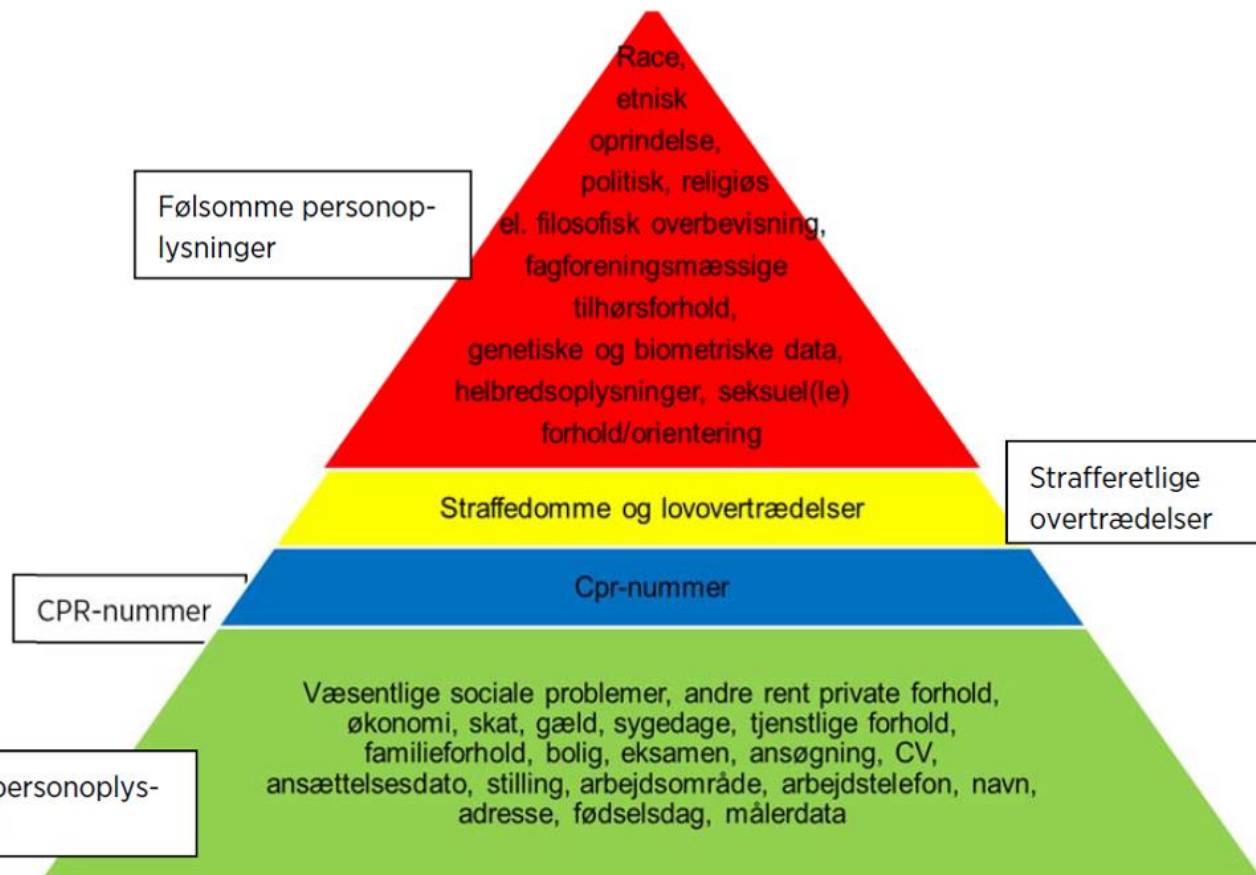
Dokumenter angående persondatasikkerhed

- Brug af portrætfoto
- Forbrugerinformation
- Medarbejderinformation (dette dokument)
- Personleadministration
- Privatlivspolitik for ansatte
- Privatlivspolitik for Augustenborg Fjernvarme
- Privatlivspolitik for jobansøgere



Hvad er persondata?

- Data der giver information en person som fx:
 - Navn, adresse, telefonnummer, e-mail adresse.
 - Familieforhold, antal sygedage, fødselsdag.
 - Målerdata som forbrug, flow og temperatur.
- Personfølsomme
 - Race, politisk overbevisning, seksuel orientering.



Hvad må og må vi ikke?

Hvad må vi?

- Bruge og notere nødvendig information (need-to-have)
 - Navn, adresse, telefonnummer, e-mail adresse.
 - For ansatte: Familieforhold, antal sygedage, fødselsdag og anden relevant ansættelsesmæssige forhold
 - For forbrugere: Målerdata som forbrug, flow og temperatur.

Hvad må vi ikke?

- Bruge og notere unødvendig information (nice-to-have)
 - Race, politisk overbevisning, seksuel orientering.
 - Organisatoriske forhold (fagforening)



Hvordan beskytter vi persondata?

- Beskyt data:
 - Gemmer så vidt muligt persondata digitalt.
 - Sikre mod uautoriseret dataadgang via oplåste PC'er
 - Fx lås pc når den efterlades (uovervåget)
 - Undgå at læse uopfordret på andres skærme
 - Efterlad ikke papir med persondata så det kan læses af forbigående
 - Undgå at opbevare data fysisk
 - Forbrugerdata skal gemmes i FOF, på netværket eller i mail systemet.
 - Papir med persondata skal generelt destrueres efter anvendelse, og må ikke gemmes.
 - Papir med persondata som **skal** opbevares aflåst.
 - Lad være med at notere følsomme persondata
- Ansøgninger
 - Ansøgninger som modtages på papirform scannes ind og gemmes elektronisk. Papir udgaven makuleres
 - Ansøgninger som modtages på e-mail, gemmes på en USB-pen, som opbevares i pengeskab og slettes fra e-mail systemet.
- På den måde kan vi sikre at ansøgninger slettes efter endt rekruteringsproces.

Politiker og persondata

Hvad skal jeg vide?

- Der er udarbejdet 3 privatlivs-politikker i AUGFJV:
 - Generelt for alle
 - Ansøgere
 - Ansatte

Persondata - personale

- Der er oprettet mapper til personale data, som er begrænset i adgang, således vi opretholder fortrolighed mellem leder og ansatte, men samtidig kan overholde persondata forordningen.
- Ved fratrædelse.
 - Mapperne flyttes til en mappe med fratrådte medarbejdere.
 - Ikke relevant data bliver slettet.
 - Relevant data bliver opbevaret i henhold til privatlivspolitikken.
 - Indeværende år + 5 år.

Hvad skal jeg vide og gøre - IT?

- Udvis forsigtighed og overhold vores IT politik
 - Modtager du mails med links så tryk ikke på dem før mailen er tjekket.
 - Vær kritisk i forhold til memorystiks / USB harddiske. Undlad gratis udleveret eller reklame USB diske.
 - Udvis sund fornuft på nettet.
 - Mails er som udgangspunkt firmaets ejendom. Det er derfor en god idé at undgå at bruge firmaets email system til privat e-mail, og omvendt.
- Opdager I, at der er adgang til data, som I ikke mener at være berettigede til, så sig det til it-ansvarlige.
- Blot fordi man har adgang, betyder det ikke man skal læse / se.
- Data skal gemmes på et netværksdrev så det sikres der bliver taget backup
- Vores it sikkerhedssystemer må ikke omgås.
- Husk at skifte kodeord med jævne mellemrum, på de systemer som ikke selv beder om det.
- Kodeord er personlige og må ikke noteres ned.