

# **Retningslinjer for behandling af personoplysninger og informationssikkerhed**

## Indholdsfortegnelse

1	Indledning.....	1
2	Opdatering og kontrol med retningslinjerne og dokumentation .....	1
3	Indsamling af og adgang til oplysninger.....	1
4	Videregivelse af personoplysninger .....	1
5	Databehandleraftaler.....	1
6	Den ansvarliges opgaver .....	2
7	Adgangskoder .....	2
8	Sikkerhedsbrud .....	2

## **1 Indledning**

- 1.1 Dette dokument udgør de grundlæggende regler, Virksomheden har vedtaget for at overholde persondataforordningen.
- 1.2 Retningslinjerne er delt op i ansvarsområder: Generelt for administration samt it.

## **DEL I – Generelt**

### **2 Opdatering og kontrol med retningslinjerne og dokumentation**

- 2.1 Ledelsen vil mindst én gang om året revurdere disse retningslinjer og alt dokumentation i forhold til persondataforordningen. Særligt skal ledelsen se på, om virksomhedens har udvidet sit forretningsområde i forhold til før, om der er ny og relevant retspraksis for persondata, samt om den teknologiske udvikling gør, at virksomheden bør ændre på sikkerhedsniveauet.
- 2.2 Ledelsen vil mindst én gang om året foretage en stikprøvekontrol og se, om retningslinjerne bliver overholdt.

### **3 Indsamling af og adgang til oplysninger**

- 3.1 Ved kontakt med personer, må der kun indsamles personoplysninger, der er nødvendige for udførelsen af opgaven. Hvis man ved, en oplysning ikke er nødvendig i en relation til en opgave, må oplysningen ikke indsamles.
- 3.2 Man må ikke skaffe sig unødvendig adgang til oplysninger, der falder uden for ens arbejdsopgaver.

### **4 Videregivelse af personoplysninger**

- 4.1 Der må ikke videregives personoplysninger til personer, der ikke har en saglig grund til at tilgå personoplysningerne.

### **5 Databehandleraftaler**

- 5.1 Der skal indgås databehandleraftaler med samtlige databehandlere. En liste over databehandlere fremgår af fortegnelsen.
- 5.2 Udskiftes en leverandør fra listen, eller antages der en ny leverandør, skal der indgås en ny databehandleraftale med vedkommende leverandør.

## DEL II – Administration samt IT

### 6 Den ansvarliges opgaver

6.1 Ledelsen er ansvarlig for administration og for, at retningslinjerne i DEL II overholdes.

### 7 Adgangskoder

7.1 Der skal være adgangskontrol til alt it-udstyr med tilgang til personoplysninger via brug af adgangskoder.

7.2 Adgangskoden må ikke deles med andre, og må ikke fremgå af papirlapper eller lignende ved computeren.

7.3 Adgangskoden skal fornyes mindst én gang hver tredje måned.

7.4 Det anbefales, at adgangskoden indeholder både bogstaver (både store og små), tal og specialtegn. Det anbefales ligeledes, at adgangskoden er på mindst 8 tegn og ikke indeholder personoplysninger om en selv, familie, venner eller lignende.

### 8 Sikkerhedsbrud

8.1 Ved et sikkerhedsbrud (fx datalæk, hackerangreb), skal skaden for det første forsøges stoppet/minimeret. Dette kan kræve ekstern it-bistand.

8.2 Efter angrebet er standset, skal det vurderes, om det har haft nogle nævneværdige konsekvenser for den registrerede (er der fx skaffet adgang til krypterede oplysninger, der alligevel ikke kan læses, har det ikke konsekvenser for de registrerede).

8.3 Senest 72 timer efter bruddet er konstateret, skal der ske underretning af episoden til Datatilsynet, se kontaktinformation på Datatilsynet.dk. Dette gælder også, selvom sikkerhedsbruddet er sket hos en databehandler. Går der mere end 72 timer, skal der desuden medfølge en begrundelse for forsinkelsen.

8.4 Underretningen af Datatilsynet skal beskrive karakteren af sikkerhedsbruddet. Hvis det er muligt, skal kategorierne af de berørte oplysninger og registrerede samt antallet af berørte registrerede meddeles. Desuden skal man angive navn og kontaktoplysninger på en kontaktperson i Virksomheden. De sandsynlige konsekvenser af sikkerhedsbruddet skal beskrives, og man skal yderligere beskrive de foranstaltninger, der er foretaget for at begrænse sikkerhedsbruddet.