

PROVA



# Persondataloven - en vejledning for it-folk



**Forbundet af It-professionelle**

**prosa.dk**

Telefon: 3336 4141

Fax: 3391 9044

prosa@prosa.dk

formand@prosa.dk

faglig@prosa.dk

akasse-kbh@prosa.dk

**København - hovedkontor**

Ahlefeldtsgade 16,

1359 København K.

Åbningstid: 9 - 15, mandag dog 10 - 15

**Århus**

Møllegade 9 - 13,

8000 Århus C.

Åbningstid: alle hverdage kl. 10 - 15

**Odense**

Overgade 54,

5000 Odense C.

Åbningstid: alle hverdage kl. 10 - 15

**Ålborg**

Steen Blichersgade 10,

9000 Aalborg.

**Teknisk produktion:**

PROSA

Marts 2006

**Tryk:**

Paritas Digital Service ApS

**Persondataloven - en vejledning for it-folk**

**Tekst: Steffen Stripp**

**Denne pjece suppleres af en Internetdel på  
PROSAs netsted: [www.prosa.dk](http://www.prosa.dk)**

# Indhold

---

<b>Indledning</b> .....	<b>5</b>
<b>Databeskyttelse</b> .....	<b>7</b>
Persondatalovens område .....	7
Retlige standarder .....	10
God databehandlingsskik .....	10
It-folks arbejde med persondata .....	11
<b>Behandlingsregler</b> .....	<b>12</b>
Formål .....	12
Datakvalitet .....	13
Oplysningstyper .....	14
Behandling af almindelige oplysninger .....	15
Behandling af følsomme oplysninger .....	16
Behandling af andre følsomme oplysninger .....	17
Videregivelse .....	17
Samtykke .....	18
<b>Anmeldelse</b> .....	<b>19</b>
<b>Anvendelser - specifikke bestemmelser</b> .....	<b>21</b>
Dataansvarlige .....	21
Oplysninger .....	23
<b>Den registreredes rettigheder</b> .....	<b>23</b>
Oplysningspligt .....	24
Indsigt .....	27
Indsigelse mod behandling .....	28
Korrektion .....	29
Tilbagekalde samtykke .....	29
Indsigelse med it-behandlede individuelle afgørelser .....	29
Klage .....	30
<b>Behandlingssikkerhed</b> .....	<b>30</b>
It sikkerhed .....	31

# **Persondataloven - en vejledning for it-folk**

I denne pjece findes en vejledning for it- professionelle om persondataloven. Vejledningen består dels af nærværende trykte vejledning og dels af supplerende information på PROSAs hjemmeside: [www.prosa.dk](http://www.prosa.dk). På hjemmesiden findes en FAQ-sektion, som opdateres med svar på spørgsmål fra medlemmerne og information om nye afgørelser og vejledninger fra Datatilsynet.

It-professionelle, som udvikler eller er driftsansvarlige for it-systemer, der behandler personoplysninger, har en forpligtelse til at kende persondataloven og medvirke til, at behandlingen sker i overensstemmelse med gældende retsregler.

## **Vejledningen er skrevet af Steffen Stripp.**

Steffen er datanom og har beskæftiget sig med databeskyttelse siden begyndelsen af 1980'erne. Han har skrevet PROSAs vejledning om lovregulering af persondata siden den første vejledning blev udsendt i 1992.

Steffen var fra 1985 - 1990 formand for PROSA. Han var fra 1995 - 2001 medlem af Statens It-sikkerhedsråd og har i 2005 været medlem af Teknologirådets arbejdsgruppe om Sikkerhed og Databeskyttelse i den digitale forvaltning.

Denne pjece fra PROSA er en vejledning for it-folk om lov om behandling af personoplysninger, lov nr. 429 af 31. maj 2000. Loven har fået kaldenavnet persondataloven.

Persondataloven er en databeskyttelseslov, idet formålet er at beskytte den person, hvis data behandles, mod misbrug eller afsløring. Det hedder i det EU-direktiv, som ligger til grund for loven:

*„databehandlingssystemer er til for menneskenes skyld; de skal være i overensstemmelse med de grundlæggende rettigheder og frihedsrettigheder, der gælder for fysiske personer, uanset statsborgerskab og bopæl, herunder retten til privatlivets fred, og bidrage til at sikre økonomiske og sociale fremskridt og til at fremme samhandelen og det enkelte menneskes velfærd“*

Citatet er taget fra "Europa-Parlamentets og Rådets direktiv 94/46/EF om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger, betragtning (2)".

## **Lovens historie**

Siden 1979 har behandling af personoplysninger været reguleret af to registerlove for henholdsvis private virksomheders og offentlige myndigheders registre. Samtidig med den nye persondatalov bortfaldt de to registerlove. I midten af 80'erne blev der fremsat en del kritik af specielt loven om de offentlige registre, og der blev fra politisk hold tilkendegivet et ønske om en mere omfattende revision. Men revisionsplanerne blev sat i stå, da EU-Kommissionen i 1990

fremstillede forslag om et EU-direktiv, der ville regulere samme område som registerlovene. Det skulle vise sig overordentlig vanskeligt at få vedtaget EU-direktivet - og først i 1995 kunne et væsentligt ændret direktiv „om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger“ vedtages.

Direktivet skulle være implementeret i dansk ret senest 1. oktober 1998 - men også denne opgave viste sig at være ganske vanskelig. Et udvalg nedsat af Justitsministeren kom i december 1997 i en murstenstyk betænkning (nr. 1345), med et forslag til en hel ny lovgivning. Justitsministeren fremsatte i april 1998 et lovforslag. Det var en stor opgave for Folketingets retsudvalg at gennemarbejde dette omfattende lovforslag, og forslaget blev ikke behandlet færdigt før Folketingsårets udløb. Forslaget blev gennemført i oktober 1998, men kunne heller ikke færdigbehandles i folketingsåret 1998/99. Et nyt - noget ændret - lovforslag blev fremsat oktober 1999 og det lykkedes, med en række yderligere ændringer, at få vedtaget den nye persondatalov i juni 2000.

Med den nye lov skiftede Registertilsynet navn til Datatilsynet. Datatilsynet spiller en central rolle ved at træffe afgørelser, som fortolker loven og ved at udsende cirkulærer og vejledninger, som nærmere fastlægger lovens regler. Datatilsynet har en meget informativ hjemmeside: [www.datatilsynet.dk](http://www.datatilsynet.dk), hvor du kan finde yderligere oplysninger.

## **It-folk og databeskyttelsen**

It-folk, som udvikler it-systemer eller er ansvarlige for drift af it-systemer, der behandler personoplysninger, har en forpligtigelse til at kende persondataloven

og medvirke til, at behandlingen sker i overensstemmelse med gældende retsregler. De centrale begreber for at arbejde med it-systemer professionelt er kvalitet og ansvar. En del af denne holdning må være, at man tager ansvar for behandlingen af personoplysninger. Persondataloven indeholder, som støtte hertil, en overordnet bestemmelse om, at „oplysninger skal behandles i overensstemmelse med god databehandlingskik”.

Hvis du bliver sat til at arbejde med en opgave, som er i strid med persondataloven, er din ansættelsesretlige stilling klar: Man er ikke forpligtet til at udføre en handling eller undladelse, som vil stride mod lovgivningen. Tværtimod er man forpligtet til ikke at udføre opgaven. Inden du nægter at udføre en opgave, bør du kontakte PROSA, der vil yde praktisk og juridisk bistand. Det er vigtigt at inddrage foreningen, så sagen behandles rigtigt og ikke eskaleres unødigt, f.eks. ved at arbejdsgiveren overreagerer med en bortvisning.

### **Vejledningens indhold**

Personoplysninger behandles overalt i samfundet, og den samlede databeskyttelsesret er blevet meget omfattende. Vi kan derfor ikke gennemgå denne - eller blot i detaljer behandle alle bestemmelser i persondataloven. PROSA ønsker med denne vejledning at give it-folk et grundlag for at arbejde med personoplysninger. Det er helt nødvendigt for alle it-folk at kende de generelle behandlingsregler, og i den konkrete situation at medvirke til afklaring af de specifikke regler for den konkrete anvendelse.

Vejledningen består dels af nærværende

pjece og dels af information på PROSAs hjemmeside: [www.prosa.dk](http://www.prosa.dk). På hjemmesiden findes en FAQ-sektion, som vil blive opdateret med svar på spørgsmål fra medlemmerne og information om Datatilsynets afgørelser og vejledninger. Vejledningens form som pjece/Internet er også valgt, fordi reglerne i den ny persondatalov hele tiden bliver nærmere klarlagt gennem Datatilsynets afgørelser og vejledninger, og der er derfor behov for en løbende opdatering, som ikke praktisk kan foregå i en trykt version.

Den trykte del af vejledningen indeholder i kapitel 2 en introduktion til databeskyttelsen, en afklaring af persondatalovens område og et bidrag til forståelse af lovens centrale bestemmelse om god databehandlingskik.

I kapitel 3 beskrives lovens behandlingsregler med de generelle betingelser for, hvornår personoplysninger kan behandles og en introduktion til opdelingen af personoplysninger i almindelige og følsomme oplysninger samt til lovens krav til et samtykke. Kapitel 4 beskriver reglerne om anmeldelse af behandlinger til Datatilsynet.

Kapitel 5 giver en kort oversigt over persondatalovens specifikke behandlingsregler for henholdsvis dataansvarlige og særlige oplysninger, herunder personnummer.

Den registreredes rettigheder beskrives i kapitel 6. Disse rettigheder omfatter bl.a. den dataansvarliges oplysningspligt og retten til indsigt i behandlede oplysninger.

Vi har ikke optrykt loven i pjecen, men den kan hentes fra Internetdelen af vejledningen. På Internetdelen kan du også finde henvisninger til litteratur og links.

Databeskyttelsen skal sikre personer mod, at deres oplysninger indsamles og anvendes på en måde, de ikke er interesseret i. Databeskyttelsen handler alene om oplysninger om fysiske personer. Begrebet databeskyttelse har ikke et klart velafgrænset indhold, men man nævner sædvanligvis elementer som det at kunne leve uden indblanding og dermed selv bestemme om andre - for slet ikke at tale om offentlighed via massemedier - skal have kendskab til ens personlige forhold. Videre nævnes, at andre ikke skal have viden om en, som kan krænke den personlige integritet og i den forbindelse, at den enkelte har en urørligheds zone som er så personlig og følsom, at den bør kunne holdes helt privat. Nu lever vi i et moderne samfund med en udbygget velfærdsstat - og ikke på en øde ø - og der er derfor mange situationer, hvor andre personer, virksomheder og offentlige myndigheder skal have adgang til personoplysninger som led i den almindelige tilværelse. Her fastsætter databeskyttelsen en række spilleregler for indsamling og behandling af personoplysninger uden for den private sfære. Det er et vigtigt element i databeskyttelsen, at den sætter grænser for statsmagtens indsamling af oplysninger om borgerne. Men der er ikke tale om klare regler eller grænser. F.eks. er det også en del af databeskyttelsen, at man skal kunne leve uden overvågning, men det er lovligt at foretage videoovervågning på offentlige steder. Det er op til en stadig politisk debat, hvordan databeskyttelsen skal udmøntes i praksis.

Det er i Europarådets særlige databeskyttelseskonvention fra 1981 slået fast, at databeskyttelsen er en del af retten til privatlivets fred. Konventionen har til formål „...at sikre det enkelte menneske respekt for dets grundlæggende rettigheder og andre

rettigheder, især retten til privatlivets fred, i forbindelse med elektronisk databehandling af personoplysninger om den enkelte.” Retten til privatlivets fred er en del af de grundlæggende menneskerettigheder og fastslået i Den Europæiske Menneskerettigheds Konvention §8: „Enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin korrespondance.”

Databeskyttelseskonventionen fastlægger en række grundprincipper for databeskyttelsen, som EU-direktivet og Persondataloven præciserer og udvider. To helt afgørende principper er for det første *formålsbestemthed* - det vil sige, at personoplysninger kun må indsamles og behandles til rimelige, legitime og udtrykkelig angivne formål. For det andet at behandling af personoplysninger skal ske *åbent* og være *transparent* - det vil sige, det skal være kendt for personen, at der indsamles oplysninger, og at vedkommende skal kunne få indsigt i behandlingen af sine data.

## Persondatalovens område

Persondataloven er hovedloven for, hvornår og hvordan personoplysninger kan behandles. Men behandling af personoplysninger er også reguleret i en række andre love. Straffeloven indeholder bestemmelser, som skal beskytte privatlivets fred bl.a. om brevhemmeligheden, om aflytning og med et forbud mod at fotografere personer på offentlige steder. I en række love er indarbejdet regler om behandling af persondata, f.eks. markedsføringsloven, lov om visse betalingsmidler, forvaltningsloven. Gennem de sidste år er behandlingen af personoplysninger blevet reguleret i stadig flere love. Denne lovpraksis betyder, at fastlæggelse af databeskyttelsen sker i en konkret sammenhæng, hvor brugen af

personoplysninger kan foretages detaljeret. Med den nye persondatalov må det forventes, at denne praksis vil blive anvendt i højere grad. Det fastslås i loven, at kun regler i anden lovgivning, som giver en bedre beskyttelse, går forud for reglerne i persondataloven. Men ifølge lovforslagets bemærkninger til §2, stk. 1 gælder dette dog ikke hvis en dårligere retsstilling har været tilsigtet af Folketinget ved vedtagelse af særloven. Der vedtages (beklægeligvis!) love som giver en dårligere retsstilling og i praksis må man som udgangspunkt anvende reglerne i gældende særlove.

§2, stk. 1 Regler om behandling af personoplysninger i anden lovgivning, som giver den registrerede en bedre retsstilling, går forud for reglerne i denne lov.

Persondataloven gælder som hovedregel for al behandling af personoplysninger med anvendelse af it-systemer. Desuden gælder loven for manuel behandling af personoplysninger, som er indeholdt i et register. Loven gælder for både den private sektor i virksomheder, foreninger og organisationer og i alle offentlige myndigheder.

§1, stk. 1 Loven gælder for behandling af personoplysninger, som helt eller delvist foretages ved hjælp af elektronisk databehandling, og for ikke-elektronisk behandling af personoplysninger, der er eller vil blive indeholdt i et register.

Ved personoplysninger forstås enhver form for information, som kan knyttes til en identificerbar person. Der er således ikke kun tale om oplysninger, der direkte fortæller om personen, men om alle oplysninger der har relation til vedkommende. Det kan være om økonomiske forhold, den dataansvarliges bemærkninger om personsens forhold og alle andre oplysninger som er registreret i forbindelse med en person.

Ved udtrykket identificerbar person forstås en person, der direkte eller indirekte kan identificeres, f.eks. ved identifikationsnummer eller et eller flere elementer, der er særlige for en given persons fysiske, fysiologiske, psykiske, økonomiske, kulturelle eller sociale identitet. Oplysninger der er gjort anonyme, således at de ikke på nogen måde kan henføres til bestemte personer, er ikke omfattet af loven. I denne definition indføres begrebet „den registrerede”, og det er i og for sig besynderligt, fordi loven ikke omhandler oplysninger i registre. Baggrunden er, at man ikke har kunne finde på et udtryk for det engelske begreb „data subjekt”, og derfor bruger persondataloven begrebet den registrerede om de personer, hvis data behandles. Man kan sige, at man indsamler oplysninger om personer og i øvrigt behandler oplysninger om den registrerede. Det er her uden betydning, hvordan oplysningerne opbevares.

§3 I denne lov forstås ved  
1) Personoplysninger: Enhver form for information om en identificeret eller identificerbar fysisk person (den registrerede).

Selvom databeskyttelsen sigter på personer, så gælder persondataloven også delvist for behandling af oplysninger som vedrører virksomheder mv.

Mange steder er persondataloven opbygget på den måde, at der er en hovedregel og derefter en række undtagelser. Dette er også tilfældet for det område, loven gælder for.

### Loven omfatter således ikke:

- Behandling af personoplysninger som foretages af privatpersoner er omfattet af loven, men undtaget herfra er behandlinger af rent privat karakter. Loven gælder ikke for behandling af personoplysninger som del af en personlig eller familiemæssig aktivitet, f.eks. ved udarbejdelse af private breve på pc'en, en

- adressebog eller en elektronisk dagbog.
- Behandling af personoplysninger som er beskyttet af informations- og ytringsfriheden. Loven er f.eks. ikke til hinder for behandling af personoplysninger i forbindelse med udarbejdelse af læserbreve, debatindlæg og lignende og loven forhindrer heller ikke, at man deltager i en offentlig debat på Internettet.
  - Visse af lovens regler om den registreredes rettigheder mv. gælder ikke inden for det strafferetlige område for domstolene, eller politi og anklagemyndighed. Her er det reglerne i retsplejeloven, der gælder.
  - Behandlinger der foretages af Folketinget og institutioner med tilknytning hertil.
  - Massemediernes interne redaktionsdatabaser og offentligt tilgængelige informationsdatabaser. Disse behandlinger er omfattet af medieansvarsloven og lov om massemediernes informationsdatabaser.
  - Behandlinger der udføres for politiets og forsvarrets efterretningstjenester. Disse behandlinger følges af et særligt kontroludvalg bestående af fem medlemmer af Folketinget.

Lovens paragraffer er inddelt i afsnit, som dernæst er opdelt i kapitler, med henblik på at give et overblik over lovens indhold. I skemaet nedenfor er denne oversigt vist.

<b>Persondataloven</b>		
Afsnit	Kapitel	§§
I Indledende bestemmelser	1 Lovens område 2 Definitioner 3 Lovens geografiske område	1 - 2 3 4
II Behandlingsregler	4 Behandling af oplysninger 5 Videregivelse til kreditoplysningsbureauer af oplysninger om gæld til det offentlige 6 Kreditoplysningsbureauer 7 Overførsel af oplysninger til tredjelande	5 - 14  15 - 18 19 - 26 27
III Den registreredes rettigheder	8 Oplysningspligt over for den registrerede 9 Den registreredes indsigtsret 10 Øvrige rettigheder	28 - 30 31 - 34 35 - 40
IV Sikkerhed	11 Behandlingssikkerhed	41 - 42
V Anmeldelse	12 Anmeldelse af behandlinger, der foretages for den offentlige forvaltning 13 Anmeldelse af behandlinger, der foretages for en privat dataansvarlig 14 Anmeldelse af behandlinger der foretages for domstolene 15 Øvrige bestemmelser [om databehandlere]	43 - 47 48 - 51 52 53 - 54
VI Tilsyn og afsluttende bestemmelser	16 Datatilsynet 17 Tilsyn med domstolene 18 Erstatnings- og strafansvar 19 Afsluttende bestemmelser, herunder ikrafttrædelsesbestemmelser mv.	55 - 66 67 - 68 69 - 71 72 - 83

## Retlige standarder

Persondatalovens paragraffer er i vid udstrækning udformet som såkaldte retlige standarder. Der er ikke tale om en præcis regel, men om mere generelle rammer, som giver en rettesnor for behandlingen af personoplysninger. Sådanne retlige standarder udgør et udgangspunkt, som efterfølgende må „fyldes ud” eller gives et præcist indhold gennem Datatilsynets - og domstolens - afgørelser.

Denne fremgangsmåde i loven anvendes, fordi behandling af persondata finder sted i utrolig mange sammenhænge og bestandigt på nye måder, så det er ikke muligt at give detaljerede regler. I de tilfælde hvor behandlingen giver anledning til tvivl, debat eller klager, kan Datatilsynet gå ind og træffe afgørelse om, hvordan persondataloven skal tolkes i denne konkrete situation. Datatilsynet bidrager også til denne afklaring ved udsendelse af vejledninger og gennem udtalelser og information om særlige spørgsmål. Datatilsynets afgørelser kan prøves ved domstolene, men det vil sandsynligvis kun ske yderst sjældent.

Anvendelse af retlige standarder betyder, at man ikke umiddelbart ud af lovteksten kan læse klare regler, som kan anvendes i den konkrete situation. Lovens paragraffer giver et overordnet billede, som ofte vil være tilstrækkelig. Men i den konkrete situation må man undersøge, om Datatilsynet har behandlet en tilsvarende situation for at få et klart retsgrundlag. Det er den dataansvarlige, som må foretage vurderingen. Der er dog mulighed for at rette en forespørgsel til Datatilsynet.

## God databehandlingsskik

Persondataloven indeholder en helt ny bestemmelse, der udgør en overordnet ramme for behandling af personoplysninger. Med bestemmelsen indføres begrebet „god databehandlingsskik”.

§5, stk. 1 Oplysninger skal behandles i overensstemmelse med god databehandlingsskik.

Der findes ikke i bemærkninger til lovforlaget en nærmere præcisering af, hvad der menes med god databehandlingsskik. Det anføres, at behandlingen skal være rimelig og lovlig, og at det i øvrigt må overlades til Datatilsynet at udfylde den retlige standard for god databehandlingsskik. Datatilsynet skriver i sin generelle informationspjece, at god databehandlingsskik „indebærer at den dataansvarlige nøje skal overholde reglerne i loven, såvel i ånd som bogstav, og ikke må forsøge at omgå reglerne.” Brancheorganisationer og andre organisationer, som repræsenterer en kategori af dataansvarlige, kan i samarbejde med Datatilsynet udarbejde en adfærdskodeks, der skal bidrage til korrekt anvendelse af reglerne i persondataloven. Rigtigt udformet vil en adfærdskodeks kunne bidrage til udvikling af god databehandlingsskik.

Kravet om god databehandlingsskik synes at kunne anvendes i to sammenhænge. For det første som en generalklausul for hvornår en indsamling og behandling af personoplysninger overhovedet kan finde sted i overensstemmelse med loven. God databehandlingsskik kan i denne sammenhæng ses i sammenhæng med den ovenfor citerede præambel fra EU-direktivet, som overordnet fastslår, at databehandlingssystemer er til for menneskenes skyld. God databehandlingsskik åbner således op for en etisk og faglig vurdering af, om behandlingen er rimelig. Man kan her f.eks. henvise til Kants etiske princip, hvorefter man skal stile efter, at man altid benytter andre mennesker som mål og aldrig blot som middel. Behandling af andres personoplysninger kan næppe siges at være i overensstemmelse med god databehandlingsskik, hvis den ikke tjener et formål, som de kan acceptere og i et eller andet omfang har egen fordel af.

For det andet kan kravet om god databehandlingsskik anvendes som et overordnet krav til den dataansvarliges organisation, når man behandler personoplysninger. Det er en forudsætning for behandling af personoplysninger, at der er en dataansvarlig. Man må kræve, at der er etableret en klar organisation, hvor forskellige ansvarsforhold er placeret og at disse ansvarsforhold er kommunikeret ud i organisationen. Videre skal der være etableret fornøden it-sikkerhed. Man må dog ikke forveksle it-sikkerhed med databeskyttelse. It-sikkerhed beskytter systemer og andre aktiver, og ikke de personer, hvis data behandles. Men it-sikkerhed er et middel til at opnå dele af databeskyttelsen ved at beskytte de registrerede data mod forskellige trusler for misbrug. Endvidere må det kræves, at der foreligger fastlagte procedurer for behandlingen af personoplysningerne, som sikrer, at formålet med behandlingen og de forskellige opgaver ved behandlingen er beskrevet og kendt. Procedurerne skal være kendt af alle medarbejdere, og det skal kontrolleres, at de følges. En følge af bestemmelsen om god databehandlingsskik er således, at det forudsætter en velorganiseret it organisation, hvis man ønsker at behandle personoplysninger.

### **It-folks arbejde med persondata**

Det må forventes at it-folk, som led i en professionel holdning, spiller en særlig rolle ved behandling af personoplysninger. De centrale begreber for en it professionel etik er ansvar og kvalitet. Ansvar for at den databehandling som gennemføres er etisk forsvarlig, i overensstemmelse med faglige standarder og med lovgivningen - og dermed også med god databehandlingsskik. Kvalitet fordi det må være en professionel målsætning at levere høj kvalitet, men kvalitet er ikke en absolut størrelse og spørgsmålet er: hvor godt er godt nok? En del af denne holdning er, at it-folk tager ansvar for

behandlingen af personoplysninger. Dette ansvar udfoldes inden for de organisatoriske rammer, som den enkelte arbejder i. Som medarbejder i en organisation kan man have forskellige arbejdsopgaver og ansvarsområder, men uanset hvor man arbejder, har man et selvstændigt ansvar for at vurdere den behandling af personoplysninger, man medvirker til. I kapitel 3 vil de generelle regler for behandling af personoplysninger, som it-folk altid bør forholde sig til, blive gennemgået og i kapitel 7 behandles behandlingssikkerhed, som det må antages, at it-folk har et særligt ansvar for.

Persondata behandles overalt i samfundet, og der findes særlige regler i persondataloven og i anden lovgivning, som nærmere fastlægger retsregler for behandlingen. I kapitel 5 findes en oversigt over disse regler i persondataloven. Det kan ikke forventes, at it-folk har kendskab til alle disse regler eller kan være ansvarlige for, at sådanne retsregler overholdes. it-folk må formodes at indgå i en organisation eller i et team med andre fagfolk, som klarlægger retsgrundlaget. Men det er en del af it-folks professionelle ansvar at sikre, at grundlaget er afklaret og dokumenteret, således at persondatalovens principper om formålsbestemthed og åbenhed, samt øvrige generelle behandlingsregler er overholdt.

Det er i persondataloven fastsat, at det er den dataansvarlige, som har beføjelsen til at fastsætte, hvorledes en behandling skal finde sted. Den dataansvarlige skal give instrukser for, hvordan behandlingen skal gennemføres.

§41, stk.1 Personer, virksomheder mv., der udfører arbejde under den dataansvarlige eller databehandleren, og som får adgang til oplysninger, må kun behandle disse efter instruks fra den dataansvarlige, med mindre andet følger af lov eller bestemmelser fastsat i henhold til lov.

It-folk skal således have en instruks om deres arbejde - ligesom der i øvrigt skal foreligge en instruks og dermed klarlagte procedurer for andre medarbejders behandling af personoplysninger. Der er ikke i loven stillet krav til instruksens udformning, og det er ikke et krav, at den skal være skriftlig. Instruksen kan fremgå af almindelige

arbejdsbeskrivelser eller være en del af medarbejderens stillingsbeskrivelse. Hvis der opstår tvivl om en behandling, f.eks. fordi allerede registrerede data behandles på en ny måde eller skal videregives til andre, bør man sikre, at der foreligger en instruks som efterfølgende kan dokumenteres, og det sikres bedst når instruksen er skriftlig.

## Behandlingsregler

## 3

I dette kapitel gennemgås lovens bestemmelser for, hvornår behandling af personoplysninger må finde sted. Bestemmelser gælder for alle behandlinger af personoplysninger, og omfatter:

- For enhver behandling af personoplysninger skal der fastsættes et udtrykkeligt formål.
- Ved behandling af personoplysninger skal den dataansvarlige sikre oplysningernes datakvalitet.
- En behandling kan finde sted, når en nærmere fastsat betingelse er opfyldt. Der er fastsat forskellige betingelser for følsomme og almindelige oplysninger.
- Behandling kan som hovedregel finde sted med personens samtykke.

Begrebet behandling omfatter enhver form for anvendelse af personoplysninger, bl.a. indsamling, registrering, systematisering, opbevaring, tilpasning eller ændring, selektion, søgning, brug, videregivelse ved transmission, formidling eller enhver anden overladelse, sammenstilling eller sammenkøring samt blokering, sletning eller tilintetgørelse. Loven gælder således for persondatas samlede livscyklus og både for strukturerede data, som behandles i it-systemer og for persondata i ustruktureret

form f.eks. i tekstbehandling, journalsystem og e-mails og andre it-systemer.

§3. I denne lov forstås ved:

- 2) **Behandling:** Enhver operation eller række af operationer med eller uden brug af elektronisk databehandling, som oplysninger gøres til genstand for.

Det er vigtigt at være opmærksom på, at hver type af behandling skal vurderes for sig. Fordi en dataansvarlig kan foretage en bestemt type behandling, er det ikke givet, at han kan foretage en anden. Den særskilte vurdering af hver type behandling for sig har særlig betydning, hvis den dataansvarlige ønsker at videregive eller sammenkøre personoplysninger.

### Formål

Lovens bestemmelse om at indsamling af personoplysninger kun må ske til udtrykkeligt angivne og saglige formål, er det mest centrale krav i databeskyttelsen. Når en dataansvarlig ønsker at påbegynde indsamling af personoplysninger, skal formålet været klarlagt på forhånd. Det angivne formål er helt afgørende for hvilke behandlinger, der efterfølgende kan gennemføres, og formålet skal samtidig bidrage til den ønskede åben-

hed, idet det skal oplyses til de personer, hvis data indsamles.

§5, stk. 2 Indsamling af oplysninger skal ske til udtrykkeligt angivne og saglige formål, og senere behandling må ikke være uforenelig med disse formål. Senere behandling af oplysninger, der alene sker i historisk, statistisk eller videnskabeligt øjemed, anses ikke for uforenelig med de formål, hvortil oplysningerne er indsamlet.

Formålet skal være formuleret udtrykkeligt. Det betyder, at formuleringen af formålet skal være så præcis og velafgrænset, at formålet kan skabe klarhed og åbenhed om behandlingen. Det er således ikke godt nok at formulere formålet i generelle vendinger, som f.eks. „til administrative formål” eller „til kommercielle formål”. Formålet skal defineres i tilknytning til de enkelte funktioner ved myndigheden eller virksomheden.

Endvidere skal formålet være sagligt. Om et formål er sagligt beror på de konkrete omstændigheder. Generelt kan man sige, at det kræver, at personoplysningerne skal anvendes til at løse opgaver, som er naturlige for myndigheder eller virksomheder af den pågældende type. Det er ikke tilladt at indsamle oplysninger, hvis man ikke aktuelt har behov for dem men blot forventer, at der senere viser sig et formål.

Senere behandling - typisk registrering og brug - må ikke være uforenelig med det oprindelige formål. Det må forventes, at de relevante senere behandlinger fremgår af formålet, som ikke blot fastlægger indsamling, men den samlede behandling. I modsat fald skabes der ikke megen klarhed og åbenhed over behandlingen. Som udgangspunkt kan indsamlede personoplysninger kun benyttes til det oprindelige formål. Men der kan opstå situationer, hvor en dataansvarlig ønsker at anvende registrerede personoplysninger på en anden måde end det oprindelige formål

fra indsamlingstidspunktet uden at indhente samtykke fra samtlige registrerede. Dette er efter loven muligt, men den ny behandling må ikke være uforenelig med det oprindelige formål. Bestemmelsen indebærer, at de oplysninger en dataansvarlig har indsamlet til et formål ikke frit vil kunne genbruges, videregives mv. Der vil således heller ikke frit kunne videregives oplysninger inden for den offentlige forvaltning. Der er formentligt meget snævre muligheder for at ændre på behandlingen i forhold til det oprindelige formål.

Senere behandling, der alene sker i historisk, statistisk eller videnskabeligt øjemed er altid forenelig med de formål, hvortil oplysningerne er indsamlet.

### **Datakvalitet**

Den dataansvarlige skal sikre datakvaliteten af de persondata som behandles. Det indebærer

- at oplysningerne skal være relevante og tilstrækkelige.
- at oplysningerne løbende skal ajourføres og kontrolleres.
- at uaktuelle oplysninger skal slettes.

§ 5, stk. 3 Oplysninger, som behandles, skal være relevante og tilstrækkelige og ikke omfatte mere, end hvad der kræves til opfyldelse af de formål, hvortil oplysningerne er indsamlet, og de formål, hvortil oplysningerne senere behandles.

§5, stk. 4 Behandling af oplysninger skal tilrettelægges således, at der foretages fornøden ajourføring af oplysningerne. Der skal endvidere foretages den fornødne kontrol for at sikre, at der ikke behandles urigtige eller vildledende oplysninger. Oplysninger, der viser sig urigtige eller vildledende, skal snarest muligt slettes eller berigtiges.

§5, stk. 5 Indsamlede oplysninger må ikke opbevares på en måde, der giver mulighed for at identificere den registrerede i et længere tidsrum end det, der er nødvendigt af hensyn til de formål, hvortil oplysningerne behandles.

Et af målene med krav om datakvalitet er, at der ikke sker en dataophobning. Der må derfor kun indsamles oplysninger som er nødvendige (relevante og tilstrækkelige) i forhold til formålet. Man må ikke indsamle og registrere „ekstra oplysninger“, når man nu alligevel er i gang. Endvidere skal oplysningerne slettes - eller anonymiseres - når de ikke længere er aktuelle. Den dataansvarlige skal ved forberedelsen af behandlingen - sammen med fastsættelse af formål mv. - fastlægge en slettefrist. Offentlige myndigheder kan dog i stedet overføre oplysningerne til Statens Arkiver, hvor der gælder særlige regler for, hvem der har adgang til oplysningerne.

Behandlingen af oplysninger må endvidere ikke gå videre end, hvad der kræves for at opfylde de fastsatte formål.

Den dataansvarlige skal tilrettelægge passende procedurer for ajourføring og kontrol af oplysninger. Det beror på oplysningernes karakter og konsekvenser ved fejl, hvor hurtigt og grundigt denne kontrol og ajourføring skal tilrettelægges. Opdages ukorrekte oplysninger skal disse slettes eller blokeres, og der skal eventuelt gives besked (berigtigelse) til andre, som har fået adgang til oplysningerne. Blokering kan f.eks. anvendes af offentlige myndigheder og andre som har en journalpligt og derfor ikke kan slette fejl og tidligere anvendte oplysninger. Ved blokering skal oplysningerne markeres som ukorrekte og ikke længere anvendes, herunder specielt ikke videregives til tredjemand.

## Oplysningstyper

Loven opdeler personoplysninger i tre typer.

- Følsomme oplysninger om menneskers rent private forhold. Det drejer sig om oplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold og oplysninger om helbredsmæssige eller seksuelle forhold.
- Andre typer oplysninger om rent private forhold anses også for være følsomme. Det drejer sig om oplysninger om strafbare forhold, væsentlige sociale problemer der ikke omfatter helbredsoplysninger og andre oplysninger om rent private forhold, f.eks. om interne familieforhold (familiestridigheder, separation- og skilsmissebegæringer og adoptionsforhold) og oplysninger om foreningsmæssige tilhørsforhold.
- De oplysninger, der ikke vedrører rent private forhold, kaldes for almindelige personoplysninger. Almindelige personoplysninger kan være identifikationsoplysninger, oplysninger om økonomiske forhold, kundeforhold eller andre lignende ikke følsomme oplysninger.

Opdelingen i almindelige og følsomme oplysninger tilsigter at indføre en graduering af betingelser og procedurer for behandlingen af henholdsvis de almindelige oplysninger, hvor beskyttelsesbehovet er mindre, og de følsomme oplysninger, hvor beskyttelsesbehovet er massivt. Opdelingen af de rent private forhold i følsomme oplysninger og andre følsomme oplysninger beror på juridiske finurligheder ved implementeringen af EU-direktivet, som desværre har ført til, at persondataloven er blevet yderligere kompliceret.

Det er hovedprincippet, at personoplysninger kan indsamles, når personen giver sit samtykke hertil. Og det er uafhængigt af om oplysninger indhentes hos vedkommende selv eller fra andre kilder. Selvom der indhentes samtykke, er det fortsat en

betingelse, at de grundlæggende betingelser for behandling af personoplysninger er opfyldt - bl.a. at indsamlingen sker til et sagligt formål, og at oplysningerne er relevante og tilstrækkelige.

Nedenfor behandles lovens bestemmelser om, hvornår de forskellige typer oplysninger kan behandles. Private dataansvarlige skal have tilladelse af Datatilsynet før følsomme oplysninger kan behandles.

## Behandling af almindelige oplysninger

Almindelige oplysninger kan behandles, når den registrerede har givet sit udtrykkelige samtykke. Dernæst kan almindelige oplysninger behandles, når behandlingen er nødvendig af en række forskellige grunde. Kravet om nødvendighed indebærer, at der skal være en betydelig sikkerhed for, at behandlingen er velbegrundet. Det er i første omgang den dataansvarlige, som må skønne om behandlingen er nødvendig. Dette skøn vil altid kunne efterprøves af Datatilsynet - ligesom man kan rette forespørgsel til tilsynet forud for behandlingen. Det må forventes, at der ad åre, gennem Datatilsynets praksis, vil danne sig et rimeligt klart billede af, hvilke behandlinger der kan gennemføres med henvisning til disse bestemmelser. Det skal fremhæves, at denne nødvendighed skal vurderes for hver enkelt behandlingsform for sig.

§6, stk. 1 Behandling af oplysninger må kun finde sted, hvis

- 1) den registrerede har givet sit udtrykkelige samtykke hertil,
- 2) behandlingen er nødvendig af hensyn til opfyldelsen af en aftale, som den registrerede er part i, eller af hensyn til gennemførelse af foranstaltninger, der træffes på den registreredes anmodning forud for indgåelsen af en sådan aftale,

- 3) behandlingen er nødvendig for at overholde en retlig forpligtelse, som påhviler den dataansvarlige
- 4) behandlingen er nødvendig for at beskytte den registreredes vitale interesser,
- 5) behandlingen er nødvendig af hensyn til udførelsen af en opgave i samfundets interesse
- 6) behandlingen er nødvendig af hensyn til udførelsen af en opgave, der henhører under offentlig myndighedsudøvelse, som den dataansvarlige eller en tredjemand, til hvem oplysningerne videregives, har fået pålagt, eller
- 7) behandlingen er nødvendig for, at den dataansvarlige eller den tredjemand, til hvem oplysningerne videregives, kan forfølge en berettiget interesse, og hensynet til den registrerede ikke overstiger denne interesse.

Almindelige oplysninger kan behandles (nr. 2), når der foreligger et aftaleforhold mellem den dataansvarlige og den registrerede. Det er en betingelse, at den registrerede er aftalepart. En aftale mellem den dataansvarlige og den registreredes arbejdsgiver eller faglige organisation kan ikke begrunde behandling af oplysninger om den registrerede. Af bestemmelsen følger, at der i forbindelse med opfyldelse af en aftale kan foretages den nødvendige behandling af bl.a. ordrer, fakturaer og lignende.

Almindelige oplysninger kan behandles (nr. 3), når det er nødvendigt for, at den dataansvarlige kan overholde en retlig forpligtelse. En retlig forpligtelse kan være fastsat i en lov, en bekendtgørelse eller en domsafgørelse, men ikke i en privat aftale. Som et eksempel kan nævnes, at arbejdsgivere gennem regler i skattelovgivningen er forpligtede til at indsamle forskellige indkomstoplysninger om de ansatte og videregive dem til skattemyndighederne.

Almindelige oplysninger kan behandles (nr. 6), når det er nødvendigt for offentlig

myndighedsudøvelse. Bestemmelsen retter sig mod offentlige myndigheders forvaltning, f.eks. afgørelser om sociale ydelser eller skatteansættelse.

Almindelige oplysninger kan behandles (nr. 7), når det er nødvendigt for at forfølge en berettiget interesse, og hensynet til den registrerede ikke overstiger denne interesse. Der er tale om en afvejningsregel, hvor man skal vurdere om den dataansvarliges interesse er mere tungtvejende end hensynet til den registrerede. Denne bestemmelse er meget bredt formuleret, og vil sandsynligvis være grundlag for en betydelig del af persondatabehandlingerne i den private sektor og i den offentlige sektor uden for myndighedsudøvelse (nr. 6). Det skal understreges, at behandlingen skal være nødvendig, og det må antageligt forudsættes, at den enkeltes samtykke i realiteten ville være en formalitet.

De øvrige bestemmelser (nr. 4 og 5) vil kun kunne anvendes i meget særlige situationer.

## Behandling af følsomme oplysninger

Der må som udgangspunkt ikke behandles følsomme oplysninger. Denne hovedregel suppleres dog af en række undtagelser, hvorefter følsomme oplysninger kan behandles.

§7, stk. 1 Der må ikke behandles oplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssig tilhørsforhold og oplysninger om helbredsmæssige og seksuelle forhold.

§7, stk. 2 Bestemmelsen i stk. 1 finder ikke anvendelse, hvis

- 1) den registrerede har givet sit udtrykkelige samtykke til en sådan behandling,
- 2) behandlingen er nødvendig for at beskytte den registrerede eller en anden persons

vitale interesse i tilfælde, hvor den pågældende ikke fysisk eller juridisk er i stand til at give sit samtykke

- 3) behandlingen vedrører oplysninger, som er blevet offentliggjort af den registrerede, eller
- 4) behandlingen er nødvendig for, at et retskrav kan fastlægges, gøres gældende eller forsvares.

Selvom hovedreglen modificeres af en række undtagelser er den udtryk for, at der skal vises stor tilbageholdenhed med at behandle følsomme oplysninger, og at behandling af følsomme oplysninger kræver et meget velbegrunder sagligt formål. Dette skal især holdes for øje i relation til muligheden for at behandle følsomme oplysninger med den registreredes samtykke.

Følsomme oplysninger kan behandles (nr. 3), hvis de er offentliggjorte. Oplysninger er offentliggjorte, når de er meddelt til en bredere kreds f.eks. i TV, aviser eller andre landsdækkende medier. Det er en betingelse, at oplysningerne er offentliggjorte på den registreredes eget initiativ.

Følsomme oplysninger kan behandles (nr. 4), hvis det er nødvendigt for, at et retskrav kan fastlægges. Omfattet er behandlinger som foretages i den dataansvarliges, den registreredes eller tredjemands interesse. Som eksempler nævnes, at en arbejdsgiver eller forsikringsselskab behandler helbredsoplysninger for at vurdere et erstatningskrav. Eller en social myndighed som pga. mistanke om incest eller andre seksuelle overgreb mod børn behandler oplysninger om disse forhold med henblik på politianmeldelse.

Herudover findes en række yderligere undtagelser

- Behandling af medlemskab af en fagforening kan ske, hvis det er nødvendigt for, at den dataansvarlige kan overholde en arbejdsretlig forpligtelse.

- Almennyttige foreninger kan under visse betingelser behandle følsomme oplysninger om medlemmer og andre personer, som er i regelmæssig kontakt med foreningen.
- Behandling af helbredsoplysninger mv. kan foretages af personer, som er undergivet tavshedspligt indenfor sundhedssektoren (skal i øvrigt ses i sammenhæng med lov om patienters retsstilling).
- Politi, anklagemyndighed og domstole kan behandle følsomme oplysninger i forbindelse med straffesager.

Endelig fastsættes det udtrykkeligt, at en offentlig myndighed ikke må føre it-registre med oplysninger om politiske forhold, som ikke er offentligt tilgængelige. Private må kun behandle sådanne oplysninger med samtykke.

### Behandling af andre følsomme oplysninger

Andre følsomme oplysninger, herunder strafbare forhold og væsentlige sociale problemer, er særskilt reguleret i persondataloven. Reguleringen er her opdelt med bestemmelser for den offentlige forvaltning og bestemmelser for private.

Den offentlige forvaltning må kun behandle disse følsomme oplysninger, når det er nødvendigt for myndighedens opgaver.

§8, stk. 1 For den offentlige forvaltning må der ikke behandles oplysninger om strafbare forhold, væsentlige sociale problemer og andre rent private forhold end de i §7, stk. 1 nævnte, med mindre det er nødvendigt for varetagelsen af myndighedens opgaver.

Andre følsomme oplysninger vil desuden kunne behandles, hvis en af betingelserne for de følsomme oplysninger er opfyldt. Det betyder bl.a., at de i overensstemmelse med hovedreglen kan behandles med personens samtykke.

Private må ligeledes behandle andre følsomme oplysninger, hvis personen giver sit udtrykkelige samtykke hertil. Uden samtykke kan de andre følsomme oplysninger kun undtagelsesvis behandles. Det kan ske, hvis det er nødvendigt for at varetage en berettiget interesse som klart overstiger hensynet til den registrerede. Bemærk, at kravet er skærpet i forhold til den tilsvarende bestemmelse i §6, stk. 1 nr. 7 med tilføjelse af ordet „klart”. Andre følsomme oplysninger vil desuden kunne behandles, hvis en af betingelserne for de følsomme oplysninger er opfyldt.

§8, stk. 4 Private må behandle oplysninger om strafbare forhold, væsentlige sociale problemer og andre rent private forhold end de i §7, stk. 1 nævnte, hvis den registrerede har givet sit udtrykkelige samtykke hertil. Herudover kan behandling ske, hvis det er nødvendigt til varetagelse af en berettiget interesse, og denne interesse klart overstiger hensynet til den registrerede.

Private må ikke - hverken manuelt eller elektronisk - føre et fuldstændigt register over straffedømme.

Som eksempel på en privat behandling af disse andre følsomme oplysninger nævner Datatilsynet en virksomheds registrering af oplysninger om butikstyveri (strafbare forhold) med henblik på indgivelse af politianmeldelse.

### Videregivelse

Videregivelse af registrerede personoplysninger til andre (tredjemand) er en selvstændig behandling, som kun kan finde sted, når en af de nævnte betingelser er opfyldt, herunder med den registreredes samtykke. Det er en vigtig del af databeskyttelsen at hindre spredning af personoplysninger uden personens viden, og uden at det er sagligt begrundet.

For andre følsomme oplysninger er offentlige myndigheders adgang til at videregive

oplysninger begrænset. Reguleringen omfatter såvel videregivelse til andre offentlige myndigheder og videregivelse til private. Videregivelsen kan ikke ske blot fordi den er nødvendig, men der skal enten indhentes et samtykke eller en af flere nærmere betingelser skal være opfyldt. Endvidere findes en særlig regulering af videregivelse inden for det sociale område af følsomme oplysninger.

Private må ikke videregive de nævnte andre følsomme oplysninger uden den registreredes udtrykkelige samtykke. Dog kan videregivelse ske, hvis den dataansvarlige varetager en interesse som klart overstiger hensynet til den registrerede.

## Samtykke

Behandling af en persons oplysninger vil kunne finde sted, når vedkommende giver samtykke hertil. Kravene til et samtykke er derfor et meget afgørende led i databeskyttelsen. Det er en forudsætning, at der ikke må herske tvivl om, at den registrerede har givet sit samtykke.

§3. I denne lov forstås ved:

- 8) Den registreredes samtykke: Enhver frivillig, specifik og informeret viljestilkendegivelse, hvorved den registrerede indvilliger i, at oplysninger, der vedrører den pågældende selv, gøres til genstand for behandling.

I definitionen fastlægges hvornår et samtykke er gyldigt, og de opstillede betingelser skal sikre, at samtykket er reelt ment.

Der er ikke formkrav til et samtykke - det skal blot være en viljestilkendegivelse. Det vil sige, at samtykket ikke skal være udformet på en bestemt måde, og at det kan afgives mundtligt eller skriftligt, ligesom samtykket kan afgives digitalt. Da det er den dataansvarlige, som har bevisbyrden for, at

den registrerede har afgivet sit samtykke må det dog anbefales, at samtykke i videst muligt omfang afgives skriftligt. Dette gælder navnlig, hvis der gives samtykke til behandling af følsomme oplysninger eller samtykket har stor betydning for en eller flere af parterne. I lovens forskellige bestemmelser, som kræver samtykke, hedder det, at samtykket skal være udtrykkeligt. Det er derfor ikke tilstrækkeligt med et indirekte eller stilltiende samtykke.

Samtykket skal være afgivet frivilligt. Det må derfor ikke være afgivet under tvang eller pression fra den dataansvarlige eller andre. Et samtykke kan dog godt være afgivet under „frivillig tvang”, f.eks. fordi det er en forudsætning for at komme i betragtning til en ansøgning eller leje af en video.

Samtykket skal være specifikt. Det skal således af et meddelt samtykke fremgå, hvilke typer af oplysninger der må behandles, hvem der kan foretage behandling af oplysningerne om „den samtykkende” og til hvilke formål behandlingen kan ske.

Personen skal være fuldt ud klar over, hvad det er, der gives samtykke til. Samtykket skal være informeret og personen skal have tilstrækkelig information til at kunne vurdere, om han vil give sit samtykke. Den dataansvarlige skal give besked i et letforståeligt sprog, og informationen må ikke pakkes ind i rosende og tvetydige formuleringer. Der stilles ikke krav til denne information, men den bør være skriftlig på papir eller digitalt.

Samtykket skal normalt afgives af personen selv, men han kan give en anden fuldmagt til at gøre det.

En registreret kan på ethvert tidspunkt tilbagekalde sit samtykke. Virkningen heraf vil være, at behandlingen af oplysningerne ikke længere må finde sted. Den registrerede kan ikke tilbagekalde sit samtykke med tilbagevirkende kraft.

Det er persondatalovens hovedregel, at behandling af personoplysninger skal anmeldes til Datatilsynet. Men loven indeholder betydelige undtagelser, og i praksis er det kun en mindre del af behandlingerne, som skal anmeldes.

For it-folk tilvejebringer anmeldelsesproceduren et grundlag for den behandling af personoplysninger, de skal medvirke til. Det er ikke op til it-folk at iværksætte en databehandling og heller ikke at sikre, at den er i overensstemmelse med specifikke retsregler. Men kravene til anmeldelse udgør en sikkerhed for, at den dataansvarlige har foretaget de nødvendige overvejelser og beslutninger, og at disse er dokumenteret som grundlag for systemudvikling og drift.

Anmeldelsen skal foretages inden behandlingen iværksættes. Bortset fra særlige behandlinger - hvor der skal indhentes udtalelse eller tilladelse - kan behandlingen iværksættes, når anmeldelsen er foretaget.

Det er ganske præcist beskrevet i loven, hvad anmeldelsen skal indeholde:

§43, stk. 2 Anmeldelsen skal indeholde oplysninger om følgende:

- 1) Navn og adresse på den dataansvarlige, dennes eventuelle repræsentant og på en eventuel databehandler.
- 2) Behandlingens betegnelse og formål.
- 3) En generel beskrivelse af behandlingen.
- 4) En beskrivelse af kategorierne af registrerede og de typer af oplysninger, der vedrører dem.
- 5) Modtagere eller kategorier af modtagere, som oplysningerne kan overføres til.
- 6) På tænkte overførsler af oplysninger til tredjelande.
- 7) En generel beskrivelse af de foranstaltninger, der iværksættes af hensyn til

behandlingssikkerheden

- 8) Tidspunktet for påbegyndelse af behandlingen.
- 9) Tidspunktet for sletning af oplysningerne.

Anmeldelsen skal indeholde formålsangivelsen (punkt 2). Formålet bliver her dokumenteret og er til rådighed ved information ved indsamling af oplysninger og senere vurdering af, om brugen af personoplysninger er i overensstemmelse med behandlingens formål.

Behandlingens betegnelse (punkt 2) skal gøre det muligt at identificere behandlingen.

Anmeldelsen skal (punkt 3) indeholde en beskrivelse af de behandlingstyper, som vil blive anvendt. I punkt 9 skal der være taget stilling til, hvornår oplysninger om den enkelte person slettes.

Den dataansvarlige skal altid udarbejde en dokumentation for en behandling af persondata, som mindst indeholder de oplysninger, som skal fremgå af en anmeldelse. Dokumentationen må forudsættes at være alle ansatte hos den dataansvarlige, som skal udføre arbejdsopgaver i forbindelse med behandlingen, bekendt. Endvidere skal den dataansvarlige stille oplysningerne (dog bortset fra punkt 3) til rådighed for enhver, som anmoder om dem.

Anmeldelse af behandlinger kan ske fra Datatilsynets hjemmeside. Tilsynet har udsendt en vejledning om anmeldelse til den offentlige forvaltning. For behandlinger som skal anmeldes, men hvor den dataansvarlige ikke skal afvente en udtalelse/tilladelse, henstiller Datatilsynet, at den dataansvarlige foretager anmeldelse mindst fire uger før behandlingen påbegyndes, således at Datatilsynet har mulighed

for at reagere, hvis anmeldelsen giver anledning til det.

Ændringer i behandlingen skal for de anmeldelsespligtige behandlinger anmeldes til Datatilsynet. For mindre vigtige ændringer er det ikke nødvendigt at indhente en forudgående udtalelse/tilladelse.

### **Udtalelse og tilladelse**

Nogle behandlinger anses for at have så alvorlig risiko for den personlige databeskyttelse, at Datatilsynet skal foretage en vurdering af behandlingen før, den kan iværksættes. Når en behandling omfatter følsomme oplysninger kan behandlinger først påbegyndes, når den dataansvarlige har modtaget en udtalelse/tilladelse fra Datatilsynet.

Det er fastsat, at der for følgende behandlinger for en offentlig forvaltning skal indhentes udtalelse fra Datatilsynet inden, behandlingen iværksættes:

- behandlingen omfatter følsomme oplysninger.
- retsinformationssystemer og behandlinger i videnskabelig og statistisk øjemed.
- behandlingen omfatter sammenstilling eller sammenkøring i kontroløjemed.

Det er fastsat, at der for følgende behandlinger, som foretages af en privat dataansvarlig, skal indhentes en tilladelse fra Datatilsynet inden, behandlingen iværksættes:

- behandlingen omfatter følsomme oplysninger.
- behandlingen sker med henblik på at advare andre mod forretningsforbindelser eller ansættelsesforhold til en registreret (advvarselsregistre).
- behandlingen sker med henblik på erhvervsmæssig videregivelse af oplysninger om økonomisk soliditet og kreditværdighed.
- behandlingen sker med henblik på er-

hvervsmæssig bistand ved stillingsbesættelse (headhuntervirksomhed)

- retsinformationssystemer.
- overførsel af oplysninger til tredje-lande.

Datatilsynet kan i forbindelse med sin tilladelse meddele særlige vilkår for udførelsen af behandlingen.

### **Undtaget fra anmeldelse**

Som nævnt undtager persondataloven behandlinger, som anses for at indebære mindre risiko for den personlige databeskyttelse, fra anmeldelse til Datatilsynet.

For den offentlige forvaltning skal behandlinger, som ikke omfatter oplysninger af fortrolig karakter, ikke anmeldes. Behandlingen kan endvidere omfatte identifikationsoplysninger, herunder personnummer, og oplysninger om betaling til og fra en offentlig myndighed. Med fortrolig karakter henvises til oplysninger, som er omfattet tavshedspligt. I en bekendtgørelse fra Justitsministeriet er yderligere undtaget en række nærmere definerede behandlinger inden for: miljø- og energisystemer, fødevarer-, landbrugs- og fiskerisystemer, søfartssystemer, bevillingssystemer, personaleadministrative systemer, undervisningssystemer, bibliotekssystemer, beredskabssystemer og offentlige service-systemer - under forudsætning af at der ikke behandles følsomme oplysninger.

Private dataansvarlige skal ikke foretage anmeldelse når

- behandlingen omfatter oplysninger om ansatte. Behandlingen må dog ikke omfatte følsomme oplysninger - bortset fra helbredsoplysninger som behandles i henhold til lovgivning, samt oplysninger som er nødvendige som følge af kollektiv overenskomst eller kollektiv aftale på arbejdsmarkedet. Behandlingen kan omfatte fagforeningsmæssig

tilhørsforhold i forbindelse med aftaler om kontingentindeholdelse.

- behandlingen omfatter oplysninger om kunder, leverandører eller andre forretningsforbindelser. Behandlingen må dog ikke omfatte følsomme oplysninger.
- behandlingen foretages med henblik på udførelse af markedsundersøgelser. Behandlingen må dog ikke omfatte følsomme oplysninger.
- behandlingen foretages af en forening eller lignende, og der alene behandles oplysninger om foreningens medlemmer.
- behandlingen foretages af advokater eller

revisorer som led i deres virksomhed, og der alene behandles oplysninger om klientforhold.

- behandlingen foretages af læger, sygeplejesker, tandlæger, kliniske tandteknikere, apotekere, terapiassistenter, kiropraktorer og lignende personer med autorisation til at udøve virksomhed inden for sundheds- og sygeplejen. Behandlingen må dog ikke ske for et privat sygehus.
- Behandlingen foretages til brug ved en bedriftssundhedstjeneste.

## Anvendelser - specifikke bestemmelser

## 5

Ved behandling af personoplysninger er det nødvendigt at undersøge om, der findes en specifik regulering for denne type behandling. Sådanne regler får også betydning for it-folk, når de optræder i hverdagslivets forskellige roller som borgere, forbrugere, objekter for videnskabelige undersøgelser osv.

Specifikke bestemmelser om behandling af personoplysninger findes i stigende grad i andre love, og it-folk må i deres professionelle virke i samarbejde med andre fagfolk afklare retsgrundlaget for behandling af persondata. I dette kapitel findes en oversigt over de specifikke regler, som findes i persondataloven. Det falder uden for vejledningen at gennemgå disse regler i detaljer, og der er alene tale om en orientering. Nogle af reglerne vil være nærmere gennemgået i vejledningens Internetdel.

De specifikke regler i persondataloven kan opdeles i bestemmelser, som vedrører en type dataansvarlige og bestemmelser vedrørende særlige oplysningstyper.

### Dataansvarlige

Persondataloven har i §§19-26 en detaljeret regulering af kreditoplysningsbureauers virksomhed. Der tænkes her på virksomheder, som registrerer oplysninger om personer og virksomheders økonomiske soliditet og kreditværdighed med henblik på videregivelse til andre. I denne sammenhæng findes i §§15-18 særlige regler for offentlige myndigheders videregivelse af oplysninger om gæld til det offentlige til disse kreditoplysningsbureauer.

I persondatalovens §12 reguleres *adresse- og kuverteringsbureauers* virksomhed. Der tænkes her på virksomheder, som sælger fortegnelser over grupper af personer, samt foretager adressering og udsendelse af meddelelser til sådanne grupper.

Retsinformationssystemer, som indeholder information om lovgivning og retsregler, samt om domme og administrative afgørelser, der kan indeholde personop-

lysninger, er særligt reguleret i lovens §9. Der kan behandles personoplysninger, når det er nødvendigt for, at systemets formidlingsfunktion kan opfyldes.

Der er i §10 fastsat særlige bestemmelser for *statistiske og videnskabelige undersøgelser*. Undersøgelser og statistik, som udføres af en offentlig dataansvarlig, skal anmeldes til Datatilsynet, mens dette kun er krævet for en privat dataansvarlig, når der indgår følsomme oplysninger i undersøgelsen. Datatilsynet skal fremkomme med en udtalelse til offentlige dataansvarlige og give en tilladelse til private dataansvarlige. Datatilsynet kan overfor de private dataansvarlige fastsætte nærmere vilkår for udførelsen af behandlingen til beskyttelse af de registreredes privatliv. Der er ikke registerindsigt for den enkelte til egne personoplysninger i statistiske og videnskabelige undersøgelser.

*Massemedier og journalistisk arbejde* har en særlig regulering i persondataloven. Massemediernes informationsbaser, som dels omfatter informationsbaser med offentliggjorte artikler o.l. og dels omfatter interne redaktionelle informationsbaser, er undtaget fra loven og reguleres i en særlov. Desuden er det i §2, stk. 2 bestemt, at loven ikke finder anvendelse, hvis det vil være i strid med informations- og ytringsfriheden. Endelig må den dataansvarliges instrukser om hvordan personoplysninger skal behandles ifølge §41, stk. 2 ikke begrænse den journalistiske frihed.

Virksomheder der yder bistand til erhversmæssig bistand ved *stillingsbesættelse* skal efter §50, stk. 1 nr. 4 anmeldes til Datatilsynet, og skal inden behandlingen iværksættes have tilladelse fra Datatilsynet.

*En stiftelse, en forening eller en anden almennyttig organisation* hvis sigte er politisk, filosofisk, religiøs eller faglig art kan efter §7, stk. 4 inden for rammerne af sin virksomhed behandle følsomme oplysninger om organisationens medlemmer eller

personer, der på grund af organisationens formål er i regelmæssig kontakt med denne. Bestemmelsen omfatter ikke-kommercielle organisationer, der må anses for at have samfundsmæssig betydning.

Endelig findes der i persondataloven en lang række bestemmelser om særlige vilkår for den *offentlige forvaltning*. Selv om persondataloven, som udgangspunkt har fælles regler for alle dataansvarlige såvel offentlige som private, er der alligevel på en række områder forskellige vilkår, som afspejles i persondataloven. I den offentlige forvaltning skal persondataloven samvirke med forvaltningsloven og offentlighedsloven, som hidtil har reguleret behandlingen af personoplysninger, der ikke indgik i et it-register. Der er særlige regler vedrørende behandling af de omtalte andre følsomme oplysninger, og det er udtrykkeligt bestemt, at den offentlige forvaltning ikke må føre it-registre med oplysninger om politiske forhold, som ikke er offentligt tilgængelige. Inden for det sociale område er der i §8, stk. 3 en særlig bestemmelse om videregivelse af andre følsomme oplysninger, herunder specielt væsentlige sociale problemer, til andre myndigheder. Desuden findes en særlig regulering i §7, stk. 5 af sundhedssektorens behandling af følsomme oplysninger, hvor helbredsoplysninger er umiddelbart relevante. Politi og anklagemyndighed har særlige regler, idet de er undtaget fra lovens regler om oplysningspligt og den registreredes ret til indsigelse mod behandling, ret til korrektion og ret til indsigelse mod afgørelser, der alene er baseret på elektronisk databehandling. Den registrerede har således ret til indsigt - medmindre den i øvrigt er undtaget, som det er tilfældet med Kriminalregisterets efterforskningsdel. Endvidere er der i §7, stk. 6 givet politi og anklagemyndighed tilladelse til behandling af følsomme oplysninger til varetagelse af opgaver på det strafferetlige område. Domstolene har en særstatus i persondataloven.

Anmeldelse efter de almindelige regler skal ske til Domstolsstyrelsen (§52), der også fører tilsyn med domstolenes behandling af personoplysninger (§§67-68). Domstolene er ligeledes undtaget fra lovens regler om oplysningspligt og den registreredes ret til indsigelse mod behandling, korrektion og ret til indsigelse med afgørelser, der alene er baseret på elektronisk databehandling. Der er endvidere ikke ret til indsigt for den registrerede til domstolenes behandling af persondata.

## Oplysninger

Persondataloven indeholder en opdeling af personoplysninger i almindelige og følsomme samt andre følsomme oplysninger, idet reguleringen i mange sammenhænge er forskellig alt efter om der behandles almindelige eller følsomme oplysninger.

Et fuldstændigt register over strafedømme må efter §8, stk. 7 kun føres for en offentlig myndighed - det eneste eksisterende register er Det Centrale Kriminalregister.

I den offentlige forvaltning kan behandles *identifikationsoplysninger*, herunder personnummer, og *oplysninger om betaling* til og fra en offentlig myndighed uden behandlingen af den grund skal anmeldes.

I persondataloven findes en regulering af *oplysninger om forbrugere* som i samspil med markedsføringsloven regulerer virksomheders *markedsføring* ved direkte henvendelser og virksomhedernes videregivelse af personoplysninger til en anden

virksomhed med henblik på markedsføring (§6, stk. 2-4 og §36).

Persondataloven regulerer i §11 anvendelsen af *personnummer*. Offentlige myndigheder kan behandle oplysninger om personnummer med henblik på en entydig identifikation eller som journalnummer. Personnummer må ikke anvendes som adgangskode. Private virksomheder må behandle oplysninger om personnummer, når det følger af lov eller bestemmelse i lov, som det f.eks. er tilfældet med skattekontrolloven, der er grundlag for de fleste registreringer af personnummer i private virksomheder. Endvidere kan personnummer behandles, når den registrerede har givet sit udtrykkelige samtykke hertil, og behandlingen i øvrigt har et sagligt formål. Dernæst kan personnummer behandles til videnskabelige og statistiske formål. Personnummer kan videregives, når det er et naturligt led i den normale drift af virksomheder af den pågældende art og videregivelsen er af afgørende betydning for at sikre en entydig identifikation af den registrerede. Videre kan personnummer videregives af private virksomheder, når det kræves af en offentlig myndighed. Uanset disse muligheder for videregivelse må der ikke ske en offentliggørelse af personnummeret uden udtrykkeligt samtykke.

Offentlige myndigheder og private virksomheder må ikke foretage automatisk registrering af, hvilke *telefonnumre* der er foretaget opkald til fra deres telefoner.

# Den registreredes rettigheder 6

---

Persondataloven giver den enkelte en række rettigheder, som bidrager til åbenhed, og kan gøre den registrerede i stand til at varetage sine interesser. Personens rettigheder omfatter

- ret til at få information fra den dataansvarlige om, at der indsamles oplysninger om en selv
- ret til at gøre indsigelse mod, at behandlingen finder sted

- ret til indsigt i de oplysninger, der behandles om en selv
- ret til at få korrigeret oplysninger, der er urigtige eller vildledende
- ret til at tilbagekalde et samtykke
- ret til at gøre indsigelse mod at blive underkastet afgørelser, der har retsvirkninger, og som alene er truffet på grundlag af elektronisk databehandling
- ret til at klage til Datatilsynet

Datatilsynet har udsendt en omfattende vejledning om den registreredes rettigheder, og nedenfor gennemgås hovedreglerne.

### Legitimationskrav

Ved henvendelser fra en registreret person skal den dataansvarlige sikre, at det er den rette person, man udleverer oplysninger til. Der må kun udleveres oplysninger, når vedkommende har legitimeret sig behørigt eller der på anden måde er skabt sikkerhed for at den, der f.eks. fremsætter en indsigtsbegæring, er identisk med den person, som oplysningerne vedrører.

Der er ikke specifikke regler for, hvorledes dette skal sikres. Datatilsynet nævner følgende eksempler på situationer, hvor udlevering kan ske:

- Man kender personen og er sikker på, det er ham/hende.
- Legitimation med billede er forevist. F.eks. pas, kørekort eller lignende.
- Oplysningerne sendes med post til den adresse, som personen er angivet med i myndighedens sag. Vær på vagt over for c/o adresser.
- Telefonisk udlevering efter tilbage-ringning kan ske i nogle tilfælde, men pas på! Man bør også være sikker på, at det telefonnummer man ringer til er til den registrerede person, og at andre ikke har adgang til dette.

De nærmere procedurer er selvsagt af-

hængige af, om der udleveres fortrolige eller følsomme oplysninger eller blot ordinære oplysninger. I det hele taget beror det på en konkret vurdering i den enkelte situation, hvilke procedurer der er nødvendige for at sikre, at oplysninger ikke udleveres til uvedkommende.

Datatilsynet understreger, at oplysninger ikke må udleveres til en person, blot fordi denne kan oplyse personnummeret. I fremtiden, hvor det bliver almindeligt, at der gives adgang til egne personoplysninger fra en hjemmeside på Internettet, kan personnummer ikke kan anvendes som adgangskode - men godt som brugernavn.

### Oplysningspligt

Den dataansvarlige har en oplysningspligt, når han vil indsamle personoplysninger. Oplysningspligten gælder både ved indsamling af oplysninger fra personen selv og ved indsamling af oplysninger fra andre kilder. Den dataansvarlige skal på eget initiativ give meddelelse til de personer, hvis data skal indsamles. Der er altså ikke tale om, at den dataansvarlige skal besvare en henvendelse fra personen, men at den dataansvarlige selv skal sikre, at personen får informationer om den planlagte behandling.

Når oplysningerne indhentes hos personen selv, skal vedkommende have meddelelse om de påtænkte behandlinger samtidig med, at oplysningerne indsamles. I de tilfælde hvor oplysningerne indsamles i forbindelse med, at den registrerede f.eks. skal indlevere en ansøgning, blanket eller lignende til den dataansvarlige, kan oplysningspligten opfyldes ved, at de fornødne informationer er trykt på ansøgningen, blanketten mv. Det gælder også, hvis oplysningerne indsamles elektronisk gennem en hjemmeside på Internettet. Henvender personen sig på eget initiativ til den dataansvarlige, skal meddelelse gives snarest muligt og i almindelighed inden for 10 dage.

Også når personoplysninger indsamles fra

andre kilder end personen selv, skal vedkommende informeres om behandlingen. Meddelelse skal gives ved registreringen og i almindelighed inden for 10 dage. Den dataansvarlige kan dog udnytte praktiske hensyn og benytte en anden snarlig henvendelse til den registrerede til samtidig at give information om indsamlingen. Hvis indsamlingen alene sker med henblik på videregivelse til tredjemand, kan meddelelse gives ved den første videregivelse, dog under forudsætning af at videregivelse sker forholdsvist hurtigt efter registreringen.

Den dataansvarlige er alene forpligtet til at give meddelelse til den registrerede én gang. Dette gælder såvel for enkeltstående indsamlinger som ved løbende indsamling af oplysninger hos personen. De efterfølgende indsamlinger af oplysninger må dog ikke gå ud over rammerne for den informationen person fik ved første indsamling.

Der er ingen formkrav til meddelelsen - det vil sige, der er ikke i loven en beskrivelse af, hvordan informationen skal udformes. Det er således heller ikke et krav, at den skal være skriftlig. Da det imidlertid er den dataansvarlige, som - i tilfælde af uenighed om hvorvidt der er givet den fornødne information - skal kunne dokumentere, at oplysningspligten er opfyldt, bør meddelelsen være skriftlig. Meddelelsen skal være klar og tydelig og i det hele taget udformet på en måde, så den er let forståelig for de personer, som skal læse den.

§28, stk. 1 Ved indsamling af oplysninger hos den registrerede skal den dataansvarlige eller dennes repræsentant give den registrerede meddelelse om følgende:

- 1) Den dataansvarliges og dennes repræsentants identitet.
- 2) Formålene med den behandling, hvortil oplysningerne er bestemt.
- 3) Alle yderligere oplysninger, der under hensyn til de særlige omstændigheder,

hvorunder oplysningerne er indsamlet, er nødvendige for, at den registrerede kan varetage sine interesser, som f.eks.

- a) Kategorier af modtagere.
- b) Om det er obligatorisk eller frivilligt at besvare stillede spørgsmål samt mulige følger af ikke at svare.
- c) Om reglerne om indsigt i og om berigtigelse af de oplysninger, der vedrører den registrerede.

§29, stk. 1 Hvor oplysningerne ikke er indsamlet hos den registrerede, påhviler det den dataansvarlige eller dennes repræsentant ved registreringen, eller hvor de indsamlede oplysninger er bestemt til videregivelse til tredjemand, senest når videregivelsen af oplysningerne finder sted, at give den registrerede meddelelse om følgende:

- 1) Den dataansvarliges og dennes repræsentants identitet.
- 2) Formålene med den behandling, hvortil oplysningerne er bestemt.
- 3) Alle yderligere oplysninger, der under hensyn til de særlige omstændigheder, hvorunder oplysningerne er indsamlet, er nødvendige for, at den registrerede kan varetage sine interesser, som f.eks.
  - a) Hvilken type oplysninger det drejer sig om.
  - b) Kategorier af modtagere.
  - c) Om reglerne om indsigt i og om berigtigelse af de oplysninger, der vedrører den registrerede.

I persondataloven er reguleringen teknisk opdelt alt efter om der indsamles oplysninger hos personen (den registrerede) eller oplysninger indsamles hos andre, da der er nogle forskelle for de to situationer.

Den dataansvarlige skal for at opfylde sin oplysningspligt mindst give den information, som er beskrevet i loven.

Information skal oplyse navn og adresse på den dataansvarlige og dennes repræsentant. Hvis det er en anden end den dataansvarlige, f.eks. en medarbejder

eller en anden virksomhed, som forestår indsamlingen, skal navn og adresse på den dataansvarlige også oplyses.

Dernæst skal formålene med indsamlingen altid oplyses. I kravet om formålsangivelse ligger, at der skal gives tilstrækkelig information til, at personen kan blive klar over, hvorfor der indsamles oplysninger om pågældende, og hvad oplysningerne vil blive brugt til.

Endelig skal der gives meddelelse om alle yderligere oplysninger, der er nødvendige for, at personen kan varetage sine interesser. Det må ud fra den konkrete situation vurderes hvilke oplysninger, der er nødvendige. I loven angives nogle eksempler på oplysninger, der normalt vil være relevante, men der kan udmærket være behov for yderligere oplysninger.

Det vil være relevant at oplyse kategorier af modtagere, hvis oplysningerne skal videregives. Med kategorier menes ikke de konkrete modtagere med navn, men hvis der er tale om færre kendte modtagere, vil det være rimeligt at nævne disse.

Videre vil det altid være relevant at oplyse om den registreredes ret til indsigt og ret til korrektion, se nedenfor.

Når oplysningerne indsamles hos den registrerede, vil det ofte være en naturlig del af oplysningspligten at oplyse om, der er pligt til at besvare de stillede spørgsmål, herunder om eventuelt strafansvar og andre konsekvenser ved ikke at afgive oplysningerne.

I de situationer, hvor oplysninger indsamles fra andre, vil det normalt være relevant at oplyse typen af oplysninger, som indsamles. Det påhviler ikke den dataansvarlige at informere om de konkrete personoplysninger, der er indsamlet om pågældende, men alene en beskrivelse af hvilke typer oplysninger, der er indsamlet.

### **Undtagelser fra oplysningspligten**

Oplysningspligten er et væsentlig led i den åbenhed som persondataloven skal sikre,

men samtidig har det været opfattelsen, at det kan være ganske byrdefuldt og vanskeligt for den dataansvarlige at opfylde denne oplysningspligt. Persondataloven har derfor en række undtagelser, hvorefter den dataansvarlige er fritaget for at informere de berørte personer.

Hvis personen allerede er bekendt med de oplysninger, som skulle have været meddelt, kan den dataansvarlige undlade at meddele dem igen. Det beror på en konkret vurdering om dette er tilfældet. Men hvis oplysninger indsamles på en blanket, hvor der er trykt information om behandlingen, eller personen selv henvender sig til den dataansvarlige kan det antages, at vedkommende er bekendt med de nævnte oplysninger. Hvis den dataansvarlige er i tvivl, bør han opfylde oplysningspligten ved en selvstændig information.

Dernæst kan oplysningspligten undlades i nogle sjældne tilfælde, hvor den registreredes interesser i at få kendskab til oplysningerne findes at burde vige for afgørende hensyn til private interesser, herunder hensynet til pågældende selv. Oplysningspligten kan endvidere i sjældne tilfælde vige for afgørende hensyn til offentlige interesser, f.eks. til statens sikkerhed.

Når oplysningerne indsamles fra andre kan oplysningspligten undlades når registreringen eller videregivelsen er udtrykkelig fastsat i lov eller bestemmelser fastsat i henhold til en lov. I kravet om „udtrykkeligt“ ligger, at der ikke må være tvivl om, at det er fastsat i lovgivningen, at den dataansvarlige skal foretage registrering eller videregivelse af de indsamlede oplysninger. Pligten eller retten til at registrere eller videregive oplysninger kan indgå i en lov, f.eks. skattekontrolloven eller lov om Danmarks Statistik eller følge af administrative forskrifter. Det må forudsættes, at behandlingen som følge af lovgivningen er kendt.

Videre kan oplysningspligten undlades, når oplysningerne indsamles fra andre, hvis

underretningen af den registrerede viser sig umulig eller uforholdsmæssig vanskelig. Med udtrykket „uforholdsmæssig vanskelig” menes, at der skal foretages en afvejning af på den ene side betydningen af en sådan underretning for den registrerede og på den anden side omfanget af den dataansvarliges arbejdsindsats for at gennemføre informationen. I Datatilsynets vejledning peges på, at der i stedet kan gennemføres generelle offentlige informationskampagner.

## Indsigt

Retten til at få oplyst hvilke data en dataansvarlig har registreret og behandler om en selv anses for en helt fundamental rettighed i databeskyttelsen. Denne indsigtret - eller egenaces - kan endvidere bidrage til datakvaliteten, idet personen selv kontrollerer de registrerede data. Persondatalovens ret til indsigt supplerer den ret til aktindsigt, som borgerne har i den offentlige forvaltning efter Forvaltningsloven og Offentlighedsloven.

Enhver har ret til at rette henvendelse til en virksomhed, offentlig myndighed eller anden dataansvarlig og anmode om indsigt i de behandlede oplysninger. Der er ingen formkrav til henvendelsen og den kan ske telefonisk, med brev eller e-mail. Den dataansvarlige kan ikke forlange en begrundelse for ønsket om indsigt.

Der kan efter persondataloven ikke stilles krav om, at den person som fremsætter begæringen om indsigt skal kunne identificere de behandlinger, der ønskes indsigt i. En begæring om indsigt kan derfor principielt vedrøre alle de behandlinger, en dataansvarlig foretager. I praksis kan der foretages en dialog mellem den dataansvarlige og personen om hvilke behandlinger, der ønskes indsigt i. F.eks. kan den dataansvarlige udlevere en liste over behandlinger, og anmode ansøgeren om at krydse af hvilke behandlinger, der ønskes indsigt til. Såfremt der ønskes ind-

sigt til en behandling, som vedkommende ikke indgår i, skal den dataansvarlige give meddelelse herom.

Datatilsynets fortegnelse over anmeldte behandlinger er tilgængelig fra tilsynets hjemmeside. Denne praksis vil kunne bidrage til, at man kan finde relevante behandlinger og giver mulighed for at kontrollere behandlingens formål.

Når en person har fået meddelelse med indsigt i en behandling, har vedkommende ikke krav på fornyet indsigt før seks måneder efter seneste meddelelse, medmindre der kan godtgøres en særlig interesse heri.

§31, stk. 1 Fremsætter en person begæring herom, skal den dataansvarlige give den pågældende meddelelse om, hvorvidt der behandles oplysninger om vedkommende. Behandles sådanne oplysninger, skal der på en let forståelig måde gives den registrerede meddelelse om

- 1) hvilke oplysninger der behandles,
- 2) behandlingens formål
- 3) kategorier af modtagere af oplysningerne, og
- 4) tilgængelig information om, hvorfra disse oplysninger stammer.

Den dataansvarlige skal snarest besvare modtagne begæringer om indsigt. Den tid der vil gå med at ekspedere en henvendelse kan variere efter de konkrete omstændigheder. Ukomplicerede indsigtbegæringer skal besvares hurtigst muligt. Ved behandlinger hvor oplysningerne ajourføres løbende, kan den dataansvarlige afvente førstkommande periodiske kørsel, såfremt dette sker månedligt eller oftere. Såfremt begæringen ikke er besvaret inden for fire uger, skal den dataansvarlige give underretning om årsagen, og orientere om hvornår svar kan forventes.

I besvarelsen af begæring om indsigt skal den dataansvarlige give den pågældende meddelelse om en række forhold. Først

og fremmest skal svaret indeholde alle de oplysninger, som den dataansvarlige behandler. De oplysninger der skal meddeles, er de oplysninger, som behandles på tidspunktet for begæringen, samt oplysninger der er kommet til indtil begæringen eskpederes.

Herudover skal den dataansvarlige give en række supplerende oplysninger. Meddelelsen skal indeholde information om behandlingens formål, således at pågældende kan blive klar over, hvad oplysningerne bruges til. Dernæst skal det oplyses, om nogle oplysninger videregives til andre og i så fald kategorier af modtagere. Endelig skal det oplyses, hvorfra oplysningerne stammer. Denne pligt gælder kun, hvis oplysningerne om, hvorfra de registrerede oplysninger stammer, rent faktisk foreligger. Det påhviler således ikke den dataansvarlige at tilvejebringe eller opbevare sådanne oplysninger.

Svaret på begæring om indsigt skal som udgangspunkt gives skriftligt, hvis personen anmoder herom. I tilfælde, hvor vedkommende møder personligt op hos den dataansvarlige, bør det søges klarlagt, om personen ønsker skriftlig svar eller en mundtlig underretning om oplysningerne.

Oplysninger skal gives i en let forståelig form, og de skal umiddelbart kunne læses uden brug af hjælpemidler. Skriftlige meddelelser bør normalt foreligge som en maskinel udskrift af behandlingerne. Meddelelsen må ikke indeholde koder mv., som ikke er umiddelbart forståelige. Mundtlige meddelelser bør kun anvendes af hensyn til den registreredes interesser, f.eks. sker meddelelse om alvorlige helbredsoplysninger bedst ved en samtale.

Private dataansvarlige kan opkræve en betaling for skriftlige besvarelser. Gebyret kan udgøre 10 kr. pr. side, dog maksimalt 200. Hvis der ikke er krævet skriftligt svar fra virksomheden, kan den ikke opkræve betaling. Indsigt hos offentlige myndigheder er gratis.

## **Undtagelser fra retten til indsigt**

Retten til indsigt gælder i de fleste tilfælde, men der findes undtagelser, som gælder for særlige situationer.

Hensyn til private interesser kan begrundes, at der ikke kan gives indsigt. Det kan være muligt at nægte indsigt, hvis man derved giver indsigt i forretningshemmeligheder, kontraktforhold og lignende. Retten til indsigt kan endvidere vige for hensyn til offentlige interesser, herunder statens sikkerhed.

Endvidere er indsigtsretten bragt i overensstemmelse med retten til aktindsigt efter Forvaltnings- og Offentlighedsloven, således at der ikke er indsigt i offentlige myndigheders interne arbejdspapirer.

Der er desuden ikke indsigt, når oplysningerne udelukkende behandles i videnskabelig øjemed og til udarbejdelse af statistikker.

## **Indsigelse mod behandling**

Den registrerede kan til enhver tid gøre indsigelse mod, at oplysninger om den pågældende behandles af den dataansvarlige.

§35, stk. 1 Den registrerede kan til enhver tid over for den dataansvarlige gøre indsigelse mod, at oplysninger om vedkommende gøres til genstand for behandling

Stk. 2 Hvis indsigelsen efter stk. 1 er berettiget, må behandlingen ikke længere omfatte de pågældende oplysninger.

I de tilfælde, hvor den dataansvarlige finder, at indsigelsen er berettiget, skal den iværksatte behandling ophøre. Hvis den dataansvarlige træffer afgørelse om, at behandlingen ikke er uberettiget, kan den fortsættes. Inden for den offentlige forvaltning er der tale om en afgørelse i Forvaltningslovens forstand, og der skal derfor gives en begrundelse. Er personen uenig kan vedkommende klage til Datatilsynet.

En indsigelse mod en behandling af personoplysninger vil naturligvis være berettiget, hvis behandlingen ikke er lovlig, dvs. finder sted i strid med persondataloven eller anden lovgivning.

En indsigelse kan være berettiget, selvom behandlingen i øvrigt er lovlig. Dette vil være tilfældet, hvis den registrerede har tungtvejende grunde til støtte for, at behandlingen pga. den registreredes særlige, individuelle situation ikke bør finde sted.

## Korrektion

Den dataansvarlige har pligt til at foretage korrektion af ukorrekte oplysninger, når der fremsættes begæring herom fra den registrerede.

§ 37, stk. 1 Den dataansvarlige skal berigtige, slette eller blokere oplysninger, der viser sig urigtige eller vildledende eller på lignende måde er behandlet i strid med lov eller bestemmelser udstedt i medfør af lov, hvis en registreret person fremsætter anmodning herom.

Stk. 2 Den dataansvarlige skal underrette den tredjemand, hvortil oplysningerne er videregivet, om, at de videregivne oplysninger er berigtiget, slettet eller blokeret i henhold til stk. 1, hvis en registreret person fremsætter anmodning herom. Dette gælder dog ikke, hvis underretningen viser sig umulig eller er uforholdsmæssig vanskelig.

En anmodning om korrektion skal vedrøre oplysninger om den registrerede selv. Den dataansvarlige er ikke efter persondataloven forpligtet til at korrigere oplysninger om andre personer, men det vil normalt påhvile den dataansvarlige at kontrollere og korrigere andre oplysninger, når der er anledning hertil.

Der er ikke formkrav til anmodningen om korrektion, der således kan fremsættes såvel skriftligt som mundtligt.

Den registrerede kan stille krav om, at tredjemand, som har fået udleveret oplysninger, skal underrettes om korrektionen. Formålet med underretningen er, at denne tredjemand kan foretage en tilsvarende korrektion. Det må antages, at den nævnte undtagelse kun kan bruges i sjældne situationer. Det kan f.eks. indgå i overvejslen, at der er gået lang tid siden videregivelsen, og at underretningen ikke vil have konsekvenser.

## Tilbagekalde samtykke

Den registrerede kan på et hvert tidspunkt tilbagekalde sit samtykke til en behandling. (Om samtykke, se side 18). Bestemmelsen finder anvendelse, når grundlaget for en behandling er samtykke og ikke en af de øvrige betingelser for behandling.

§ 38 Den registrerede kan tilbagekalde et samtykke.

Efter tilbagekaldelsen kan samtykket ikke længere være grundlag for behandlingen - og det må i den konkrete situation vurderes, om de registrerede oplysninger skal slettes eller blokeres.

## Indsigelse mod it-behandlede individuelle afgørelser

Hvis en person gør indsigelse kan den dataansvarlige ikke foranstalte, at personen undergives afgørelser, som alene er truffet på grundlag af elektronisk databehandling. Udgangspunktet er, at et menneske ikke skal være forpligtet til at acceptere afgørelser af væsentlig karakter, som kun har været behandlet af et it-system.

Når afgørelser er truffet af it-systemer, har den afgørelsen vedrører ret til at få at vide hvilke beslutningsregler, der er anvendt i systemet.

§39, stk. 1 Fremsætter en registreret person indsigelse herimod, kan den dataansvarlige

ikke foranstalte, at den registrerede undergives afgørelser, der har retsvirkninger for eller i øvrigt berører den pågældende i væsentlig grad, og som alene er truffet på grundlag af elektronisk databehandling af oplysninger, der er bestemt til at vurdere bestemte personlige forhold.

Stk. 2 Bestemmelsen i stk. 1 gælder ikke, hvis

- 1) den pågældende afgørelse træffes som led i indgåelsen eller opfyldelsen af en aftale, såfremt den registreredes anmodning om indgåelse eller opfyldelse af aftalen er blevet efterkommet, eller der findes passende sikkerhedsforanstaltninger til at beskytte den registreredes berettigede interesser, eller
- 2) den pågældende afgørelse er hjulmet i en lov, der indeholder bestemmelser til beskyttelse af den registreredes berettigede interesser.

Stk. 3 Den registrerede har ret til hos den dataansvarlige snarest muligt og uden ugrundet ophold at få at vide, hvilke beslutningsregler der ligger bag en afgørelse som nævnt i stk. 1. § 30 finder tilsvarende anvendelse

Det er ikke ganske klart i hvilke tilfælde, denne ret kan anvendes. Der skal være tale om personlige forhold, f.eks. en person erhvervsvevne, kreditværdighed, pålidelighed, adfærd og lignende. Man kan forestille sig bestemmelsen vil kunne anvendes ved be-

handling af et ekspertsystem eller ved selvbetjening på Internettet - man kan sige, at bestemmelsen nærmest er en vejledning for, hvornår it-systemer ikke kan stå alene.

Endvidere giver bestemmelsen en person ret til at få oplyst, hvordan it-systemet „beregner” sin afgørelse. Denne ret fører dog ikke til, at den dataansvarlige skal udlevere forretningshemmeligheder eller oplysninger, der er beskyttet af anden lovgivning, f.eks. opretshavsloven.

## Klage

Loven giver enhver mulighed for at klage til Datatilsynet, hvis man mener, at ens personoplysninger behandles i strid med persondataloven.

§ 40 Den registrerede kan klage til vedkommende tilsynsmyndighed over behandling af personoplysninger vedrørende den pågældende.

Datatilsynet træffer i spørgsmål om den private sektor bindende afgørelser om, hvorvidt virksomheder mv. har givet en person de rettigheder, som tilkommer vedkommende.

Også for den offentlige forvaltning er lovens ordning den, at Datatilsynet træffer bindende afgørelse om overholdelse af reglerne om den registreredes rettigheder. Dette gælder dog ikke i spørgsmål om tilbagekaldelse af samtykke, hvor tilsynets udtalelse alene er vejledende.

# Behandlingssikkerhed

7

Persondatalovens bestemmelser om sikkerhed må siges at have en særlig relevans for it-folk, som med deres vidensbaggrund har et særligt ansvar for, at sikkerheden etableres. I større organisationer vil der

findes en arbejdsdeling mellem de ansatte it-medarbejdere, således at nogle it-folk har fået tildelt sikkerheden som et særligt arbejdsområde. Men i takt med at personoplysninger behandles overalt og it-udvikling

sker decentralt, vil mange it-folk stå med den opgave at indføre sikkerhed - eller i det mindste sikre, at denne opgave blive behandlet ansvarligt.

Persondatalovens regulering af sikkerhed omfatter dels bestemmelser om den overordnede organisering ved behandling af personoplysninger; dels bestemmelser om god databehandlingsskik og datakvalitet og dels bestemmelser som omhandler it-sikkerhed.

Udgangspunktet for den overordnede organisering er, at der altid er en entydig dataansvarlig for behandlingen. En behandling af persondata kan ikke iværksættes uden, der er en dataansvarlig.

§3. I denne lov forstås ved

- 4) Den dataansvarlige: Den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der alene eller sammen med andre afgør, til hvilket formål og med hvilke hjælpemidler, der må foretages behandling af oplysninger
- 5) Databehandleren: Den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der behandler oplysninger på den dataansvarliges vegne

Den dataansvarlige er på alle måder ansvarlig for behandlingen af personoplysninger og skal sikre, at den sker i overensstemmelse med persondataloven og anden lovgivning. Såfremt den dataansvarlige overlader en behandling til en anden uden for sin egen organisation - en databehandler - skal der foreligge en skriftlig aftale. Det skal fremgå af den skriftlige aftale, at databehandleren skal opfylde kravene til it-sikkerhed, og den dataansvarlige skal aktivt kontrollere at dette sker. Der tænkes her især på de situationer, hvor databehandlingen er overladt til et it-servicebureau.

I den dataansvarliges organisation skal de medarbejdere, som har arbejdsopgaver med behandling af personoplysninger, udføre ar-

bejdet ud fra en instruks. Og medarbejderne må kun behandle persondata i overensstemmelse med denne instruks, dvs. de må ikke behandle oplysninger på eget initiativ eller til egne formål.

Når behandlingen overlades til en databehandler, skal den dataansvarlige sikre sig, at databehandleren træffer de krævede sikkerhedsforanstaltninger. Databehandlere, der er etableret i Danmark og som udøver edb-servicevirksomhed, skal anmeldes til Datatilsynet.

Persondataloven indeholder i de generelle behandlingsregler en bestemmelse om, at behandling af persondata skal ske i overensstemmelse med god databehandlingsskik, som bl.a. indebærer, at der skal etableres en velordnet organisation med klare ansvarsforhold for alle medarbejdere, som medvirker ved behandlingen. Videre skal den dataansvarlige sikre datakvaliteten, således, at de behandlede persondata er korrekte og opdaterede.

Endelig skal den dataansvarlige tilvejebringe en fornøden it-sikkerhed, som i det hele taget kan sikre persondata integritet, tilgængelighed og hemmeligholdelse.

## It-sikkerhed

Den dataansvarlige skal formulere en sikkerhedspolitik og træffe fornødne sikkerhedsforanstaltninger. Persondatalovens krav til it-sikkerhed må ses som et led i den dataansvarliges samlede it-sikkerhed, og forudsætter at der er etableret en formel og dokumenteret sikkerhed.

§ 41, stk. 3 Den dataansvarlige skal træffe 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. Tilsvarende gælder for databehandlere.

Datatilsynet har udsendt en vejledning om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles i den offentlige forvaltning. Persondatalovens bestemmelser om behandlingssikkerhed gælder naturligvis både for den offentlige forvaltning og for private dataansvarlige, og det må antages, at kravene tilsvarende skal opfyldes af private virksomheder.

Den dataansvarlige skal udarbejde interne bestemmelser om sikkerhedsforanstaltninger, som uddyber de krav som udtrykkelig fremgår af vejledningen og det i det hele taget beskriver, hvorledes sikkerhedsarbejdet er tilrettelagt. De interne bestemmelserne skal foreligge skriftligt således, at it-sikkerheden er dokumenteret. Den dataansvarlige skal ved uddannelse, instruktion mv. sikre, at medarbejderne har den nødvendige viden om disse interne bestemmelser og sikkerhedspolitikken generelt.

Endelig skal den dataansvarlige mindst en gang årligt gennemgå dokumentationen og de interne bestemmelser for at sikre, at de afspejler de faktiske forhold og i øvrigt er aktuelle.

Ved behandling af personoplysninger må det forudsættes, at der er etableret en it-sikkerhed, som er i overensstemmelse med Dansk Standard DS 484, Norm for edb-sikkerhed, eller en tilsvarende standard f.eks. ISO/IEC 17799, Code of practice for information security management. Normen indeholder en række „basale krav“, som stort set altid bør opfyldes, og dernæst „skærpede krav“, som kan indføres på baggrund af en risikoanalyse og bør overvejes, når der behandles fortrolige og følsomme oplysninger.

I forbindelse med administration af sikkerhedsforanstaltninger og driftsafvikling kan det være nødvendigt at registrere personoplysninger om medarbejderne, f.eks. forskellige logninger og sikkerhedskopier for at kunne finde årsager til fejl, driftsfor-

styrrelser samt andre sikkerhedsmæssige formål. Datatilsynet har udtalt, at behandling af persondata til sådanne tekniske og sikkerhedsmæssige formål har et sagligt formål. Tilsynet har vurderet, at behandlingen forfølger en berettiget interesse, der overstiger hensynet til den registrerede, således at indsamlingen kan ske uden, der indhentes samtykke. Behandlingen skal overholde persondatalovens forskellige bestemmelser, herunder oplysningspligten, således at medarbejderne er informeret om logningen, og bestemmelsen om at oplysninger skal slettes, når der ikke længere er behov for dem til det fastsatte formål.

De sikkerhedsforanstaltninger der er fastsat i Datatilsynets vejledning retter sig navnlig mod hemmeligholdelse, således at personoplysningerne ikke kommer til uvedkommendes kendskab eller bliver misbrugt. I det følgende findes en oversigt over disse krav.

### **Fysisk sikkerhed**

Der skal træffes foranstaltninger således, at uvedkommende ikke får adgang til oplysningerne. Forholdsreglerne er et led i den dataansvarliges gængse regler om fysisk sikkerhed, såsom aflåsning af lokaler og bygningsafsnit, alarmsystem, begrænset adgang til serverrum samt placering af skærme og printere (specielt i ekspeditiøns- og publikumsområder).

### **Inddata og uddata**

Inddatamateriale må kun behandles af medarbejdere, som er beskæftiget med inddateringen og skal opbevares aflåst, når det ikke anvendes.

Inddatamateriale med personoplysninger skal tilintetgøres, når der ikke længere er behov for det, og den dataansvarlige skal fastsætte en tidsfrist herfor. Der skal tilrettelægges en procedure således, at personoplysningerne ikke kommer til uvedkommendes kendskab som led heri. Der kan

i denne forbindelse f.eks. være tale om at opsamle materiale i aflåste containere med efterfølgende anvendelse af en pålidelig makuleringsservice for fortroligt materiale.

Inddatamateriale som journaliseres og opbevares i en sag eller opbevares som dokumentation i ringbind eller lignende falder uden for kravet om tilintetgørelse - men skal selvsagt her opbevares, så det ikke kan komme til uvedkommendes kendskab.

Uddatamateriale må kun anvendes af medarbejdere, der er beskæftiget med de formål, til hvilke behandlingen af personoplysningerne foretages. Det gælder både for uddatamateriale på papir og i elektronisk form.

Uddatamateriale skal opbevares på betryggende vis og skal tilintetgøres, når der ikke længere er behov for det. Ved tilintetgørelse af uddatamateriale på papir skal der i lighed med inddata materiale tilrettelægges en procedure, så det ikke kommer til uvedkommendes kendskab.

### **Adgangskontrol**

Kun de medarbejdere, som skal benytte personoplysningerne i deres arbejde, må have adgang til disse. Der skal derfor fastlægges en formel autorisationsordning og -arbejdsgang. Medarbejdere som skal have adgang til personoplysningerne, skal først autoriseres hertil. Det forudsættes, at der i den formelle autorisationsprocedure vil indgå en forudgående vurdering af, hvad den enkelte bruger har behov for at være autoriseret til. Den enkelte bruger må ikke autoriseres til anvendelser, vedkommende ikke har behov for. Hvis en medarbejder skifter arbejdsområde skal autorisationen inddrages.

Der skal etableres en teknisk adgangskontrol i systemerne således, at autoriserede brugere skal identificere sig overfor systemet for at få adgang til at behandle personoplysninger. Den mest almindelige form for adgangskontrol er brugeridentifi-

kation med tilhørende password, men andre former er ikke udelukket. Såfremt password anvendes, skal der fastsættes nærmere retningslinier for behandling og udformning af password.

Når behandlingen er anmeldelsespligtig - dvs. den omfatter fortrolige og følsomme oplysninger - suppleres bestemmelserne om adgangskontrol med nogle yderligere krav. Disse krav skal kun opfyldes for de fortrolige og følsomme oplysninger.

Den dataansvarlige skal tage stilling til, om den enkelte bruger skal kunne foretage forespørgsler eller om brugeren også skal kunne inddatere, ændre eller slette oplysninger. Såfremt det er brugeren, som kun skal autoriseres til enkelte af disse funktioner, skal systemerne være teknisk indrettet således, at brugerne kun får adgang til oplysninger i overensstemmelse med de givne autorisationer.

Brugeridentifikation og password skal være personlig. Der må således ikke anvendes fælles koder, som kan anvendes af flere brugere.

Der skal være tilrettelagt arbejdsgange, som sikrer, at der tilgår funktionen, som administrerer autorisationen, oplysninger om ændringer af brugernes behov for autorisationen. Mindst hvert halve år skal der foretages en kontrol af, at autorisationerne ajourføres.

Der skal foretages registrering af alle afviste adgangsforsøg. Systemet skal udvise en reaktion således, at yderligere forsøg på adgang forhindres, f.eks. efter et vist antal forsøg på at gætte password.

Endvidere skal der foretages en logning af alle anvendelser af de fortrolige og følsomme personoplysninger. Dog skal aktiviteter i forbindelse med driftsafvikling og driftsovervågning foretaget af systemmedarbejdere ikke logges. Loggen skal bl.a. omfatte brugernavn, identifikation af den person oplysningerne vedrørte, tidspunkt og type af anvendelse. Det er ikke et krav,

at loggen udskrives og gennemgås - medmindre der er anledning til det. Normalt skal loggen slettes efter seks måneder.

## **Eksterne**

### **kommunikationsforbindelser**

Der må kun etableres eksterne kommunikationsforbindelser, hvis der træffes særlige foranstaltninger for at sikre, at uvedkommende ikke kan få adgang til personoplysninger. De særlige sikkerhedsforanstaltninger skal træffes efter den dataansvarliges risikovurdering af alle elementer i kommunikationsforbindelsen.

Ved tilslutning til Internettet skal der træffes foranstaltninger, som sikrer imod, at en indtrænger får adgang fra det åbne net til den dataansvarliges interne net. Ved transmission af personoplysninger over Internettet skal hemmeligholdelse sikres med kryptering. Sikkerhed for autenticitet (brugerens identitet) og integritet (at oplysningerne ikke er ændrede) skal sikres ved passende sikkerhedsforanstaltninger, f.eks. elektronisk signatur eller individuelle, fortrolige adgangskoder.

Ved transmission af personoplysninger over opkaldsforbindelser (analog telefonforbindelse, ISDN, mobiltelefon og lignende) skal der træffes foranstaltninger mod, at en indtrænger kan foretage opkald. Det kan bl.a. være relevant at anvende faciliteter som tilbagekald eller lukkede brugergrupper.

### **Hjemmearbejdsplads**

Mens der i forbindelse med arbejde på den almindelige arbejdsplads gennem lang tids praksis er indarbejdet rutiner og adfærd, som sikrer en forsvarlig behandling af persondata, eksisterer der ikke på forhånd en tilsvarende praksis, som sikrer, at behandlingen af persondata fra en hjemmearbejdsplads sker med tilsvarende sikkerhed. Ved arbejde på en pc fra en hjemmearbejdsplads - eller en

anden arbejdsplads uden for den dataansvarliges lokaliteter, f.eks. en bærbar pc - er der en række sikkerhedsmæssige forhold, som skal overvejes.

- Lokal lagring af oplysninger. Hvis det er nødvendigt at opbevare oplysninger på hjemme pc'en bør oplysningerne krypteres.
- Lokal udskrivning af oplysninger. Hvis det er nødvendigt at udskrive oplysninger, skal der fastsættes klare regler for opbevaring og tilintetgørelse.
- Anden anvendelse af hjemme-pc'en. Hvis den dataansvarlige tillader privat anvendelse af hjemme-pc'en, skal der etableres nødvendige sikkerhedsforanstaltninger, som bl.a. sikrer, at andre ikke får adgang til personoplysningerne.
- Fysisk sikkerhed. Den fysiske sikkerhed må antages at være mindre end hos den dataansvarlige, og der skal - specielt hvis der lokalt lagres personoplysninger - være opmærksomhed på den fysiske sikkerhed.
- Anvendelse af opkaldslinier. Der skal træffes foranstaltninger mod, at uvedkommende kan foretage opkald til det centrale system. Som eksempler på sådanne foranstaltninger kan nævnes tilbagekald, lukkede brugergrupper og passwordbeskyttelse.

Det bør overvejes om, der skal etableres en særlig logning af anvendelsen af hjemmearbejdspladsen. Der bør løbende ske en kontrol af de særlige retningslinier vedrørende hjemmearbejdspladser for at sikre, at bestemmelserne om sikkerhedsforanstaltningerne iagttages.

### **Reparation og salg af udstyr**

På baggrund af en konkret sag om personoplysninger, som kunne læses på harddiske fra udfasede pc'er, der var solgt i udlandet, har Datatilsynet taget reparation og salg af

udstyr op i vejledningen.

Ved reparation og service af udstyr - f.eks. en pc med harddisk - hvor der er lagret personoplysninger, skal det ved aftale sikres, at personalet hos pågældende virksomhed vil behandle oplysninger, de måtte blive bekendt med, fortroligt.

Ved kassation af lagringsmedier og udstyr, som indeholder personoplysninger, bør lagringsmedier destrueres eller afmagnetiseres, så der ikke er mulighed for at læse indholdet. Hvis den dataansvarlige frem for at destruere lagringsmedier afhænder disse med henblik på genbrug, skal de lagrede oplysninger slettes effektivt ved overskrivning. Datatilsynet anbefaler, at der anvendes et specialprogram, som overskriver data i flere omgange.

