Håndbogsreol 2
ex 2

Bilag

til betænkning nr. 1345 om behandling af personoplysninger

Afgivet af
udvalget om registerlovgivningen

Betænkning nr. 1345

1997

Betænkning nr. 1345 + bilagsdel

Købes hos boghandleren
eller hos Statens Information,
Publikationsafdelingen
Postboks 1103, 1009 København K
Tlf. 33 37 92 28
Fax. 33 37 92 80
E-post: sp@si.dk

170,- kr. inkl. moms

Tryk: Herrmann & Fischer A/S

ISBN 87-601-3133-0

INDHOLDSFORTEGNELSE

Bilag

1. Sammenskrivning af lov om private registre (hentet fra Registertilsynets årsberetning 1996) 5

2. Sammenskrivning af lov om offentlige myndigheders registre (hentet fra Registertilsynets årsberetning 1996) 13

3. Lov om massemediers informationsdatabaser 21

4. Relevante bestemmelser i tinglysningsloven 25

5. Relevante bestemmelser i forvaltningsloven 29

6. Lov om offentlighed i forvaltningen 37

7. Den officielle danske oversættelse af Europa-Parlamentet og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger 43

8. Den officielle engelske udgave af direktiv 95/46/EF 63

9. Den officielle franske udgave af direktiv 95/46/EF 83

10. Europarådets konvention nr. 108 af 28. januar 1981 om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger 103

11. Den danske oversættelse af henstilling 1/97 om databeskyttelseslovgivningen og medierne fra den arbejdsgruppe, som er nedsat i henhold til artikel 29 i direktiv 95/46/EF 119

12. Det norske personregisterlovutvalgs lovudkast således som dette fremgår af betænkning NOU 1997:19, "Et bedre personvern" 129

13. Den svenske datalagskomités lovudkast, således som dette fremgår af betænkning SOU 1997:39, "Integritet - offentlighet - informationsteknik" 137

14. Opinionsundersøgelse foretaget i august 1996 af AIM Nielsen A/S vedrørende danskernes holdning til brugen af personnummer 155

15. Spørgeskemaundersøgelse foretaget i september-oktober 1995 af Instituttet for Fremtidsforskning for Post Danmark og Datacentralen A/S (forkortet udgave) 161

16. Justitsministeriets notits af 10. september 1996 om udformningen af lovbestemmelser i tilknytning til gennemførelse af direktiver i danske ret 189

17. Justitsministeriets notat af 9. juni 1997 om direktiv 95/46/EF og kreditoplysningsbureauers behandling af personoplysninger 195

18. Registertilsynets notits af 29. september 1997 om anmeldelsesordningen 205

19. Registertilsynets notits af 28. oktober 1997 om visse spørgsmål i forbindelse med behandlingen af personoplysninger på Internettet 209

Lov om private registre m.v.

Kapitel 1

Lovens anvendelsesområde

§ 1. Registrering, der omfatter personoplysninger, og hvor der gøres brug af elektronisk databehandling, og systematisk registrering, der omfatter oplysninger om personers, institutioners, foreningers eller virksomheders private eller økonomiske forhold eller i øvrigt oplysninger om personlige forhold, som med rimelighed kan forlanges unddraget offentligheden, må kun finde sted efter reglerne i kapitel 2, 2 a, 2 b, 2 c og 3.

Stk. 2. **Ved personoplysninger forstås oplysninger, som kan henføres til bestemte personer, selv om det forudsætter kendskab til personnummer, registreringsnummer eller lignende særlige identifikationer.**

§ 2. Loven omfatter ikke registrering, der foretages for en offentlig myndighed, eller som i øvrigt omfattes af lov om offentlige myndigheders registre, jf. dog kapitel 5.

Stk. 2. **Loven omfatter ikke registrering, der alene finder sted til brug for personalhistoriske undersøgelser eller udgivelse af almindelige opslagsværker.**

Stk. 3. **Loven omfatter ikke registrering, der alene finder sted til videnskabelige eller statistiske formål. Registrering til disse formål af oplysninger som nævnt i § 3, stk. 2, må dog kun ske efter forudgående anmeldelse til registertilsynet Registertilsynet kan fastsætte nærmere vilkår for registeret til beskyttelse af de registreredes privatliv, herunder om samtykke fra den registrerede, om sletning og ajourføring af oplysninger samt om sikkerhedsforanstaltninger mod, at registeret misbruges eller kommer til uvedkommendes kendskab.**

Stk. 4. **Loven finder ikke anvendelse på edb-registre, der er omfattet af lov om massemediers informationsdatabaser.**

Stk. 5. **Loven finder ikke anvendelse på edb-registre, hvori der udelukkende er indlagt allerede offentliggjorte periodiske skrifter eller lyd- og billedprogrammer, der er omfattet af medieansvarslovens § 1, nr. 1 eller 2, eller dele heraf, når indlæggelsen i informationsdatabasen er sket uændret i forhold til offentliggørelsen.**

Stk. 6. **Loven gælder endvidere ikke for informationsdatabaser, hvori der udelukkende er indlagt allerede offentliggjorte tekster, billeder og lydprogrammer, der omfattes af medieansvarslovens § 1, nr. 3, eller dele heraf, når indlæggelsen i informationsdatabasen er sket uændret i forhold til offentliggørelsen.**

Stk. 7. **Loven finder ikke anvendelse på manuelle arkiver over udklip fra offentliggjorte, trykte publikationer.**

Stk. 8. **Loven omfatter endvidere ikke edb-registre, der alene indeholder retskildemateriale (retsinformationssystemer), som indgår i det statslige retsinformationssystem, og som er offentligt tilgængelige.**

Stk. 9. **Registertilsynet kan tillade, at andre retsinformationssystemer helt eller delvis undtages fra lovens bestemmelser, når dette skønnes ubetænkeligt. Registertilsynet kan fastsætte betingelser for tilladelsen til beskyttelse af de registreredes privatliv.**

Kapitel 2

Erhvervsvirksomheder **m.v.**

§ 3. Erhvervsvirksomheder, erhvervsdrivende, institutioner, foreninger og lignende må kun foretage registrering som nævnt i § 1 i det omfang, registreringen er et naturligt led i den normale drift af virksomheder m.v. af den pågældende art.

Stk. 2. **Oplysninger om enkeltpersoners rent private forhold, herunder oplysninger om race, religion og hudfarve, om politiske, seksuelle og strafbare forhold samt oplysninger om helbredsforhold, væsentlige sociale**

problemer og misbrug af nydelsesmidler og lign., må ikke registreres, medmindre dette følger af anden lovgivning. Registrering må dog ske, såfremt oplysningen er afgivet af den pågældende selv eller indhentet med hans samtykke og der foreligger omstændigheder, hvor han må vide, at oplysningen vil blive registreret. Det er endvidere en betingelse, at det er nødvendigt for virksomheden m.v. at være i besiddelse af den pågældende oplysning for at muliggøre en berettiget varetagelse af virksomhedens eller andres tarv.

Stk. 3. Registertilsynet kan tillade, at oplysninger registreres, uanset at betingelserne i stk. 2 ikke er opfyldt, når det er nødvendigt for virksomheden m.v. at være i besiddelse af den pågældende oplysning for at muliggøre en berettiget varetagelse af offentlige eller private interesser, herunder hensynet til den pågældende selv, der klart overstiger hensynet til de interesser, der taler imod registrering.

Stk. 4. Registre, hvor der gøres brug af elektronisk databehandling, og som indeholder oplysninger som nævnt i stk. 2, må kun oprettes efter forudgående anmeldelse til registertilsyn et. Dette gælder dog ikke for så vidt angår registre, der føres af foreninger og lign., i det omfang registeret alene omfatter oplysninger om foreningens medlemmer.

Stk. 5. Justitsministeren kan efter indhentet udtalelse fra registertilsynet undtage bestemte typer registre som nævnt i stk. 4 fra anmeldelsespligten.

Stk. 6. Oprettelse af registre med henblik på at advare andre mod forretningsforbindelser med eller ansættelsesforhold til en registreret må kun finde sted efter forudgående tilladelse fra registertilsynet.

Stk. 7. Tilladelse efter stk. 6 kan betinges bl.a. af, at bestemte typer oplysninger ikke registreres, samt af, at registeret helt eller delvis undergives reglerne i kapitel 3.

Stk. 8. Justitsministeren kan efter indhentet udtalelse fra registertilsynet fastsætte, at nærmere angivne registre helt eller delvis undergives reglerne i kapitel 3, og at bestemte typer oplysninger ikke må indgå i de pågældende registre.

§ 4. Registrerede oplysninger om enkeltpersoners rent private forhold, herunder oplysninger om race, religion og hudfarve, om politiske, seksuelle og strafbare forhold samt oplysninger om helbredsforhold, væsentlige sociale problemer og misbrug af nydelsesmidler og lign., må ikke videregives uden samtykke fra den registrerede eller den, der handler på dennes vegne, medmindre dette følger af anden lovgivning. Registertilsynet kan dog tillade, at oplysninger som nævnt i 1. pkt. videregives, når videregivelse sker lil varetagelse af offentlige eller private interesser, herunder hensynet til den pågældende selv, der klart overstiger hensynet til de interesser, der begrunder hemmeligholdelse.

Stk. 2. Andre registrerede oplysninger må kun videregives uden den registreredes samtykke i det omfang, videregivelse uden sådant samtykke er et naturligt led i den normale drift af virksomheder m.v. af den pågældende art. Oplysninger om forhold, der ligger mere end 5 år tilbage, må dog ikke videregives uden samtykke, medmindre det er åbenbart, at det er af afgørende betydning for bedømmelsen af det forhold, som søges belyst, at oplysningen videregives, eller adgangen til videregivelse følger af anden lovgivning.

Stk. 3. Bestemmelsen i stk. 2 gælder ikke for videregivelse, der alene finder sted til brug i videnskabeligt eller statistisk øjemed. I samme øjemed må der uanset bestemmelsen i stk. 1 ske videregivelse af oplysninger om helbredsforhold.

Stk. 4. Samkøring af forskellige virksomheders registre, hvor der gøres brug af elektronisk databehandling, må ikke finde sted. Det samme gælder dog ikke samkøring, der foretages med henblik på ajourføring af oplysninger om navne, adresser og lignende.

Stk. 5. Registertilsynet kan give tilladelse til samkøring som nævnt i stk. 4, 1. pkt., når betingelserne i § 4, stk. 1-3, for videregivelse af oplysningerne er opfyldt og hensynet til de interesser, som samkøringen skal varetage, klart overstiger hensynet til de registrerede personer og der er givet disse meddelelse om, at samkøring kan finde sted. Registertilsynet kan fastsætte nærmere vilkår for tilladelsen, herunder vilkår for anvendelsen af de oplysninger, der fremkommer ved samkøringen.

§ 4 a. Oplysninger om personnummer må kun registreres, når betingelserne i § 3, stk. 2, er opfyldt

Stk. 2. Registrerede oplysninger om personnummer må kun videregives, når betin-

gelbierne i § 4, stk. 2, er opfyldt, og når videregivelse er af afgørende betydning for at sikre en entydig identifikation af den registrerede eller videregivelsen kræves af en offentlig myndighed.

§ 4 b. Virksomheder må ikke videregive registrerede oplysninger om forbrugere til andre virksomheder til brug ved markedsføring.

Stk. 2. Videregivelse som nævnt i stk. 1 kan dog ske, når betingelserne i § 4 er opfyldt og den virksomhed, som ønsker at videregive oplysningerne, ved kundeforholdets begyndelse eller på et senere tidspunkt har givet den registrerede tydelig skriftlig meddelelse om, at videregivelse kan finde sted, og den registrerede har givet sit udtrykkelige samtykke til videregivelsen.

Stk. 3. Meddelelse som nævnt i stk. 2 skal indeholde oplysning om, til hvilken type virksomhed oplysningerne agtes givet.

§ 5. Nægter virksomheden m.v. efter anmodning fra en registreret at slette eller berigtige oplysninger, der angives at være urigtige eller vildledende, eller at slette oplysninger, der ikke må registreres, eller har virksomheden ikke inden 4 uger besvaret en henvendelse herom fra den registrerede, kan den registrerede indbringe spørgsmålet for registertilsynet, der træffer afgørelse om, hvorvidt der skal foretages slettelse eller berigtigelse.

Stk. 2. Registertilsynet kan pålægge virksomheden at give skriftlig underretning om berigtigelsen til alle, der har modtaget oplysningen inden for de sidste 6 måneder, før den registrerede fremsatte sin anmodning over for virksomheden. Virksomheden skal samtidig give den registrerede meddelelse om, hvem der har modtaget underretning efter 1. pkt.

§ 6. I registre, hvor der gøres brug af elektronisk databehandling (cdb-rcgistre), skal en oplysning slettes, når den på grund af alder eller af andre grunde har mistet sin betydning for varetagelsen af registerets opgaver.

Stk. 2. Edb-registre, der anvendes løbende, skal indrettes således, at der kan foretages fornøden ajourføring af oplysningerne.

Stk. 3. Virksomheder m.v. skal foretage den fornødne kontrol til sikring af, at der ikke indføres urigtige eller vildledende oplysninger i et edb-register. Oplysninger, der viser sig urigtige eller vildledende, skal snarest muligt slettes eller berigtiges.

Stk. 4. Der skal træffes de fornødne sikkerhedsforanstaltninger mod, at oplysninger i et edb-register misbruges eller kommer til uvedkommendes kendskab.

§ 7. Bestemmelserne i § 6 gælder, uanset om registeret underkastes elektronisk databehandling i udlandet.

Kapitel 2 a

Registrerede personers adgang til oplysninger om sig selv

§ 7 a. Hvor der ved registerets førelse gøres brug af elektronisk databehandling, skal virksomheden m.v. på begæring fra en person give denne meddelelse om, hvad der er registreret om den pågældende.

Stk. 2. Bestemmelsen i stk. 1 gælder ikke, hvis den registreredes interesse i at få kendskab til oplysningerne findes at burde vige for afgørende hensyn til offentlige eller private interesser, herunder hensynet til den pågældende selv. Gor sådanne hensyn sig kun gældende for en del af oplysningerne, skal den registrerede gøres bekendt med de øvrige oplysninger.

Stk. 3. En person, der har fået meddelelse efter stk. 1, har ikke krav på ny meddelelse før 12 måneder efter sidste meddelelse, medmindre den pågældende kan godtgøre en særlig interesse heri.

§ 7 b. Virksomheder m.v. skal på begæring give meddelelse som nævnt i § 7 a, stk. 1, skriftligt.

Stk. 2. Ved registre, der indeholder oplysninger om helbredsforhold, kan meddelelse gives i form af en mundtlig underretning, når væsentlige hensyn til den registrerede taler herfor.

Stk. 3. Justitsministeren fastsætter regler om betaling for skriftlige meddelelser.

§ 7 c. Virksomheder m.v. skal snarest besvare begæringer som nævnt i § 7 a, stk. 1. Er begæringen ikke besvaret inden 4 uger efter modtagelsen, skal virksomheden skriftligt underrette den pågældende om grunden hertil.

Stk. 2. Afslår virksomheden m.v. den registreredes begæring efter § 7 a, stk. 1, jf. stk. 2, skal virksomheden samtidig oplyse, den registrerede om adgangen til at indbringe spørgsmålet for registertilsynet.

§ 7 d. Afgørelser om retten til at få meddelt oplysninger efter bestemmelserne i §§ 7 a, 7 b og 7 c kan indbringes for registertilsynet.

§ 7 e. Bestemmelserne i §§ 7 a-d gælder, uanset om registeret underkastes elektronisk databehandling i udlandet.

Kapitel 2 b

Registrering af telefonnumre

§ 7 f. 1 virksomheder m.v. må der ikke foretages automatisk registrering af, hvilke telefonnumre der er foretaget opkald til fra virksomhedens telefoner. Registrering må dog ske efter forudgående tilladelse fra registertilsynet i tilfælde, hvor afgørende hensyn til private eller offentlige interesser taler herfor. Registertilsynet kan fastsætte nærmere vilkår for tilladelse.

Stk. 2. Bestemmelserne i stk. 1 gælder ikke, hvis andet følger af lov eller for så vidt angår de koncessionerede telefonselskabers registrering af, til hvilke telefonnumre der er foretaget opkald, enten til eget brug med henblik på opkrævning af betaling eller til brug ved teknisk kontrol.

Kapitel 2 c

Pressens informationsregistre

Kapitlet er ophævet

Kapitel 3

Kreditoplysningsbureauer

§ 8. Den, som ønsker at drive virksomhed med registrering af oplysninger til bedømmelse af økonomisk soliditet og kreditværdighed med henblik på videregivelse (kreditoplysningsbureau), skal, inden virksomheden begyndes, foretage anmeldelse til registertilsynet.

§ 9. Kreditoplysningsbureauer må kun registrere og videregive oplysninger, som efter deres art er af betydning for bedømmelse af økonomisk soliditet og kreditværdighed.

Stk. 2. Oplysninger som nævnt i § 3, stk. 2, må ikke registreres eller videregives.

Stk. 3. Oplysninger om forhold, der taler imod kreditværdighed, og som er mere end 5 år gamle, må ikke registreres eller videregives, medmindre det i det enkelte tilfælde er åbenbart, at forholdet er af afgørende betydning for bedømmelsen af den pågældendes økonomiske soliditet og kreditværdighed.

§ 10. Kreditoplysningsbureauer skal inden 4 uger efter registreringen give meddelelse til den, der første gang optages i registeret med oplysninger om andet end navn, adresse, stilling, erhverv eller oplysninger, der fremgår af Statstidende eller frit kan indhentes fra erhvervsregisteret. Meddelelsen skal indeholde oplysning om den registreredes adgang til at få oplysninger fra registeret efter bestemmelserne i § 11.

Stk. 2. Justitsministeren kan efter indhentet udtalelse fra registertilsynet fastsætte, at andre typer af oplysninger kan registreres, uden at der skal gives meddelelse efter stk. 1.

§ 11. Kreditoplysningsbureauet skal til enhver tid på begæring af den registrerede inden 4 uger meddele denne indholdet af de oplysninger og bedømmelser, bureauet har videregivet om den pågældende inden for de sidste 6 måneder, samt af de øvrige oplysninger, som bureauet på tidspunktet for begæringens fremsættelse har på kartotekskort, hulkort, magnetbånd eller på anden måde i bearbejdet form, herunder af foreliggende bedømmelser af den pågældende.

Stk, 2. Er bureauet i besiddelse af yderligere materiale om den registrerede, skal dette samtidig meddeles den pågældende med oplysning om materialets art samt om, at den registrerede kan få adgang til at gennemgå det ved personlig henvendelse til bureauet.

Stk. 3. Den registrerede kan ikke forlange at blive gjort bekendt med, hvorfra oplysningerne stammer, jf. dog § 14.

Stk. 4. Den registrerede kan forlange, at bureauet giver meddelelse som nævnt i stk. 1 skriftligt. Justitsministeren fastsætter regler om betaling for skriftlige meddelelser.

§ 12. Oplysninger om økonomisk soliditet og kreditværdighed må kun meddeles skriftligt, jf. dog § 11, stk. 1 og 2. Bureauet kan dog til abonnenter meddele summariske oplysninger mundtligt eller på lignende måde, såfremt spørgerens navn og adresse noteres og opbevares i mindst 6 måneder.

Stk. 2. **Kreditoplysningsbureauers publikationer må kun indeholde oplysninger i summarisk form og kun udsendes til personer eller virksomheder, der abonnerer på meddelelser fra bureauet. Publikationerne må ikke indeholde oplysninger om de registreredes personnummer.**

Stk. 3. **Summariske oplysninger om skyldforhold må kun videregives, hvis oplysningerne hidrører fra Statstidende, er indberettet af en offentlig myndighed efter reglerne i kapitel 5 a i lov om offentlige myndigheders registre, eller hvis oplysningerne vedrører skyldforhold til samme kreditor på mere end 1.000 kr. og kreditor har erhvervet den registreredes skriftlige erkendelse af en forfalden gæld, eller hvis der er foretaget retslige skridt mod den pågældende. Oplysninger om endeligt godkendt gældssanering må dog ikke videregives.**

Stk. 4. **Videregivelse af summariske oplysninger om enkeltpersoners skyldforhold må kun ske på en sådan måde, at oplysningerne ikke kan danne grundlag for vurderingen af økonomisk soliditet og kreditværdighed for andre end de pågældende enkeltpersoner.**

§ 13. Oplysninger eller bedømmelser, der viser sig urigtige eller vildledende, skal snarest muligt slettes af registeret eller berigtiges.

§ 14. Er en oplysning eller bedømmelse, der viser sig urigtig eller vildledende, forinden blevet videregivet, skal bureauet straks give skriftlig underretning om berigtigelsen til den registrerede og til alle, der har modtaget oplysningen eller bedømmelsen inden for de sidste 6 måneder, før bureauet er blevet bekendt med forholdet. Den registrerede skal tillige have meddelelse om, hvem der har modtaget underretning efter 1. pkt., og hvorfra oplysningen eller bedømmelsen stammer.

§ 15. Henvendelser fra en registreret om slettelse eller berigtigelse af oplysninger eller bedømmelser, der angives at være urigtige eller vildledende, eller om slettelse af oplysninger, der ikke må registreres eller videregives, skal snarest og inden "4 uger efter modtagelsen besvares skriftligt af bureauet.

Stk. 2. **Nægter bureauet at foretage den begærede slettelse eller berigtigelse, kan den registrerede inden 4 uger efter modtagelsen af bureauets svar eller efter udløbet af den i stk. 1 nævnte svarfrist indbringe spørgsmålet for registertilsynet, der træffer afgørelse om, hvorvidt der skal foretages slettelse eller berigtigelse. Bestemmelsen i § 14 gælder tilsvarende.**

Stk. 3. **Bureauets svar skal i de i stk. 2 nævnte tilfælde indeholde oplysning om adgangen til at indbringe spørgsmålet for registertilsynet og om fristen herfor.**

§ 16. Overdragelse eller overgivelse i øvrigt af registre må kun ske til anmeldt kreditoplysningsbureau og skal anmeldes til registertilsynet uden ugrundet ophold.

Kapitel 4

Adresserings- og kuverteringsbureauer

§ 17. Virksomheder, der sælger adresser over grupper af personer, institutioner, foreninger eller virksomheder, eller som for tredjemand foretager kuvertering eller udsendelse af meddelelser til sådanne grupper, må kun registrere:

1) navn, adresse, stilling, erhverv og
2) oplysninger, der frit kan indhentes fra erhvervsregisteret.

Stk. 2. **Oplysninger om enkeltpersoners rent private forhold, herunder oplysninger om race, religion og hudfarve, om politiske, seksuelle og strafbare forhold samt oplysninger om helbredsforhold, væsentlige sociale problemer og misbrug af nydelsesmidler og lign., må ikke registreres. Justitsministeren kan fastsætte yderligere begrænsning i adgangen til at registrere bestemte typer af oplysninger.**

§ 18. Bureauet skal i sine registre slette enhver, der fremsætter skriftlig begæring herom.

Stk. 2. **Fremsættes begæringen over for den, der fremtræder som afsender, skal denne videresende begæringen til bureauet**

§ 19. Overlader foreninger og lignende medlemsfortegnelser til et bureau med henblik på udsendelse af meddelelser for for-

eningen m.v., må bureauet ikke uden foreningens samtykke videregive medlemsfortegnelsen til tredjemand eller benytte den til udsendelser af meddelelser for tredjemand.

Kapitel 5

Edb-servicebureauer

§ 20. Virksomheder, der for tredjemand, herunder for en offentlig myndighed, udfører elektronisk databehandling af oplysninger som nævnt i § 1, skal forinden foretage anmeldelse til registertilsynet.

Stk. 2. Virksomheden må ikke uden samtykke fra ejeren af registeret anvende de modtagne oplysninger i andet øjemed end til udførelsen af den opgave, aftalen vedrører, eller lade oplysningerne opbevare eller bearbejde hos andre eller i udlandet.

Stk. 3. Virksomheden skal træffe fornødne sikkerhedsforanstaltninger mod, at oplysningerne misbruges eller kommer til uvedkommendes kendskab.

Kapitel 6

Registrering og elektronisk databehandling i udlandet

§ 21. Oplysninger, der efter § 3, stk. 2, ikke må registreres her i landet, må ikke indsamles med henblik på registrering i udlandet. Systematisk indsamling af oplysninger i øvrigt med henblik på registrering i udlandet må kun ske med registertilsynets tilladelse, for så vidt registreringen her i landet ville kræve anmeldelse til registertilsynet eller tilladelse efter denne lov.

Stk. 2. Registre, der indeholder oplysninger som nævnt i § 3, stk. 2, må kun overlades til elektronisk databehandling i udlandet efter forudgående tilladelse fra registertilsynet. Det samme gælder systematisk indsamling af oplysninger som nævnt i § 3, stk. 2, med henblik på elektronisk databehandling i udlandet. Bestemmelsen i 1. pkt. gælder dog ikke, hvis registeret alene befinder sig her i landet for at blive undergivet elektronisk databehandling.

Stk. 3. Tilladelse efter stk. 1 og 2 kan kun meddeles, når registertilsynet finder, at overladeisen ikke vil medføre en væsentlig forringelse af den beskyttelse af den registrerede, loven tilsigter at sikre.

Stk. 4. Justitsministeren kan til opfyldelse af internationale aftaler eller i øvrigt til fremme af internationalt samarbejde om regulering af den art af virksomhed, der omfattes af loven, fastsætte, at bestemmelserne i stk. 1, 2. pkt., og stk. 2 ikke skal finde anvendelse i forhold til bestemte andre lande eller bestemte typer af registre. Det kan kun fastsættes efter indhentet udtalelse fra registertilsynet, og såfremt det ikke vil medføre en væsentlig forringelse af den beskyttelse af den registrerede, loven tilsigter at sikre.

Kapitel 7

Tilsyn og straf m. v.

§ 22. Registertilsynet fører tilsyn med, at der ikke sker overtrædelse af loven eller bestemmelser, der er fastsat i medfør af loven. Tilsynet påser herunder af egen drift eller efter klage fra en registreret, at registeret er oprettet og anvendes i overensstemmelse med loven og bestemmelser, der er fastsat i medfør af loven.

Stk. 2. Tilsynet kan kræve enhver oplysning, der er af betydning for dets virksomhed, herunder til afgørelse af, om et forhold falder ind under lovens bestemmelser.

Stk. 3. For så vidt angår virksomhed, der er anmeldelsespligtig eller omfattes af bestemmelserne i § 3, stk. 6, § 21 eller bestemmelser fastsat i medfør af § 3, stk. 8, har tilsynets medlemmer og personale til enhver tid mod behørig legitimation uden retskendelse adgang til alle lokaler, hvorfra registeret administreres eller kan benyttes, samt til lokaler, hvor registeret eller de tekniske hjælpemidler opbevares eller anvendes.

§ 23. Registertilsynet kan meddele pålæg om, at registrering eller videregivelse, der ikke må finde sted efter denne lov, skal ophøre, og at eksisterende registre, der føres i strid med loven eller et i henhold hertil meddelt pålæg, skal slettes.

Stk. 2. Tilsynet kan pålægge en virksomhed m.v. at foretage slettelse eller berigtigelse af en oplysning, som ikke må registreres, eller som tilsynet finder urigtig eller vildledende.

Stk. 3. Tilsynet kan pålægge en person eller en virksomhed m.v. at slette eller berig-

tige oplysninger, der er registreret før lovens ikrafttræden, og som ikke må registreres efter loven, eller som tilsynet finder urigtige eller vildledende.

Stk. 4. Tilsynet kan i særlige tilfælde pålægge en virksomhed m.v. at slette oplysninger, der på grund af alder eller af andre grunde har mistet deres betydning for varetagelsen af registerets opgaver.

Stk. 5. Tilsynet kan forbyde anvendelsen af en nærmere angiven fremgangsmåde i forbindelse med indsamling eller videregivelse af oplysninger, såfremt tilsynet finder, at den pågældende fremgangsmåde medfører en væsentlig risiko for, at der registreres eller videregives urigtige eller vildledende oplysninger eller oplysninger, som ikke må registreres eller videregives.

Stk. 6. Tilsynet kan pålægge virksomheden m.v. at foretage nærmere angivne kontrolforanstaltninger til sikring af, at der ikke er eller bliver registreret eller videregivet oplysninger, som ikke må registreres eller videregives, eller som er urigtige eller vildledende, samt foranstaltninger til sikring eller forebyggelse mod, at de registrerede oplysninger misbruges eller kommer til uvedkommendes kendskab.

§ 24. Justitsministeren kan til opfyldelse af internationale aftaler eller i øvrigt til fremme af internationalt samarbejde om kontrol med den art af virksomhed, der omfattes af loven, fastsætte regler bl.a. om registertilsynets forhold til udenlandske tilsynsmyndigheder, om anmeldelsespligt, om slettelse af registre og om, at bestemmelsen i § 22, stk. 3, også finder anvendelse på anden virksomhed end nævnt i bestemmelsen.

§ 25. Registertilsynets afgørelser efter denne lov kan ikke indbringes for anden administrativ myndighed.

§ 26. Registertilsynet kan fastsætte regler om form og indhold for anmeldelser og ansøgninger efter loven.

Stk, 2. For følgende anmeldelser og tilladelser i henhold til denne lov betales 1.000 kr. :

1) Tilladelse i henhold til § 2, stk. 5, 1. pkt., til, at retsinformationssystemer helt eller delvis undtages fra lovens bestemmelser.
2) Anmeldelse i henhold til § 3, stk. 4, af edb-registre, hvor der gøres brug af elektronisk databehandling, og som indeholder oplysninger om rent private forhold.
3) Tilladelse i henhold til § 3, stk. 6, til oprettelse af registre med henblik på at advare andre mod forretningsforbindelser med eller ansættelsesforhold til en registreret.
4) Tilladelse i henhold til § 4, stk. 5, til samkøring som nævnt i § 4, stk. 4, af forskellige virksomheders registre, hvor der gøres brug af elektronisk databehandling.
5) Tilladelse i henhold til § 7 f til automatisk registrering af, hvilke telefonnumre der er foretaget opkald til fra en virksomheds telefoner.
6) Anmeldelse i henhold til § 7 g, stk. 2, af registre, hvor der gøres brug af elektronisk databehandling, og som alene indeholder oplysninger, der er offentliggjort i et periodisk skrift
7) Anmeldelse i henhold til § 8 af kreditoplysningsbureauer.
8) Anmeldelse i henhold til § 20, stk. 1, af edb-servicebureauer.
9) Tilladelse i henhold til § 21, stk 1 og 2, jf. stk. 3, til indsamling og videregivelse af oplysninger med henblik på registrering i udlandet samt overladelse af registre til elektronisk databehandling i udlandet.
10) Anmeldelse af virksomheder, der erhvervsmæssigt yder bistand ved stillingsbesættelse i henhold til § 3, stk. 8.

§ 27. Medmindre højere straf er forskyldt efter den øvrige lovgivning, straffes med bøde eller hæfte den, der:

1) overtræder § 2, stk. 3, § 3, stk. 2,4 og 6, § 4, stk. 1, 1.pkt., stk. 2 og 4, § 4 a, § 4 b, § 5, stk. 2, 2. pkt., § 6, § 7 a, § 7 b, stk. 1 -2, § 7 c, § 7 f, §§ 8 og 9, § 10, stk. 1, § 11, stk. 1, 2 og 4, §§12-14, § 15, stk. 1, stk. 2, 2. pkt., og stk. 3, §§ 16-20 og § 21, stk. 1 og 2.
2) undlader at efterkomme registertilsynets afgørelse efter § 5, stk. 1, § 7 d eller § 15, stk. 2, 1. pkt.,
3) undlader at opfylde rcgistertilsynets krav efter § 22, stk. 2,
4) tilsidesætter vilkår som nævnt i § 2, stk. 3, 3. pkt., eller § 7 g, stk. 3, eller en betingelse eller et vilkår for en tilladelse i henhold til loven eller i henhold til forskrifter udstedt i medfør af loven eller

5) undlader at efterkomme forbud eller påbud, der er meddelt i henhold til loven eller i henhold til forskrifter udstedt i medfør af loven.

Stk. 2. I forskrifter, der udstedes i medfør af loven, kan der fastsættes straf af enten bøde eller hæfte for overtrædelse af bestemmelser i forskrifterne.

Stk. 3. Er en overtrædelse begået af et aktieselskab, andelsselskab eller lignende, kan bodeansvar pålægges selskabet som sådant.

§ 28. Den, der driver eller er beskæftiget med virksomhed som nævnt i § 3, stk. 6, § 8 og § 20, kan ved dom for strafbart forhold frakendes retten hertil, såfremt det udviste forhold begrunder en nærliggende fare for misbrug. I øvrigt finder straffelovens § 79, stk. I, 3. pkt., samt stk. 2 og 3, anvendelse.

Kapitel 8

Ikrafttrædelses- og overgangsbestemmelser

§ 29. Loven træder i kraft den 1. januar 1979.

Stk. 2. Bestemmelsen i § 1, stk. 1, nr. 3, i lov nr. 63 af 3. marts 1948 om ydelse af juridisk bistand samt om inkasso- og detektivvirksomhed m.v. ophæves.

§ 30. For edb-registre, der er taget i brug inden lovens ikrafttræden, får bestemmelsen i § 6 først virkning 1 år efter lovens ikrafttræden.

Stk. 2. Kreditoplysningsbureauer, der eksisterer ved lovens ikrafttræden, og virksomheder, der ved lovens ikrafttræden udfører elektronisk databehandling for tredjemand som nævnt i § 20, skal indgive anmeldelse senest 3 måneder efter lovens ikrafttræden.

Stk. 3. I forhold til personer og virksomheder m.v., der ved lovens ikrafttræden er registreret i et kreditoplysningsbureau, gælder reglen i § 10, stk. 1, første gang der efter lovens ikrafttræden registreres oplysninger, hvorom der skal gives meddelelse.

Stk. 4. En virksomhed, der ved lovens ikrafttræden foretager registrering som nævnt i § 3, stk. 3, og den, der udøver virksomhed som nævnt i § 21, stk. 1 og 2, skal indgive ansøgning om tilladelse hertil senest 3 måneder efter lovens ikrafttræden.

§ 31. Loven gælder ikke for Færøerne.

§ 3 og 4 i lov nr. 383 af 10. juni 1987 indeholder følgende bestemmelser:

§3

Loven træder i kraft den 1. april 1988.

Stk. 2. Anmeldelse af registre som nævnt i § 1, nr. 3 og nr. 5 (§ 2, stk. 3, og § 3, stk. 4) og i § 7 g, stk. 1, som indsat ved § 1, nr. 10, der er taget i brug inden lovens ikrafttræden, skal ske senest 6 måneder efter lovens ikrafttræden.

Stk. 3.....

§4

Stk. 1. § 1 gælder ikke for Færøerne og Grønland.

Stk. 2.....

Lov om offentlige myndigheders registre

Kapitel 1

Lovens område

§ 1. Loven gælder for edb-registre, der føres for den offentlige forvaltning, og som indeholder personoplysninger.

Stk. 2. **Ved edb-registre forstås registre eller andre systematiserede fortegnelser, hvor der gøres brug af elektronisk databehandling.**

Stk. 3. **Ved personoplysninger forstås oplysninger, som kan henføres til bestemte personer, selv om det forudsætter kendskab til personnummer, registreringsnummer eller lignende særlige identifikationer.**

Stk. 4. **Kapitel 5 a gælder også for edb-registre, der føres for den offentlige forvaltning, og som indeholder oplysninger om virksomheder m.v.**

Stk. 5. **Loven omfatter ikke edb-registre, der alene indeholder retskildemateriale (retsinformationssystemer), som indgår i det statslige retsinformationssystem, og som er offentligt tilgængelige.**

Stk. 6. **Justitsministeren kan efter indhentet udtalelse fra Registertilsynet tillade, at andre rctsinformationssystemer helt eller delvis undtages fra lovens bestemmelser, når dette skønnes ubetænkeligt. Justitsministeren kan fastsætte betingelser for tilladelsen til beskyttelse af de registreredes privatliv.**

Stk. 7. **Loven finder ikke anvendelse på edb-registre, der er omfattet af lov om massemediers informationsdatabaser.**

Stk 8. **Loven finder ikke anvendelse på edb-registre, hvori der udelukkende er indlagt allerede offentliggjorte periodiske skrifter eller lyd- og billedprogrammer, der er omfattet af medieansvarslovens § 1, nr. 1 eller 2, eller dele heraf, når indlæggelsen i informationsdatabasen er sket uændret i forhold til offentliggørelsen.**

Stk. 9. **Loven gælder endvidere ikke for informationsdatabaser, hvori der udelukkende er indlagt allerede offentliggjorte tekster, billeder og lydprogrammer, der omfattes af medieansvarslovens § 1, nr. 3, eller dele heraf, når indlæggelsen i informationsdatabasen er sket uændret i forhold til offentliggørelsen.**

§ 2. Vedkommende minister kan efter forhandling med justitsministeren fastsætte, at loven helt eller delvis skal gælde for registre, der føres for nærmere angivne selskaber, institutioner, foreninger m.v., som ikke kan henregnes til den offentlige forvaltning. Det gælder dog kun, hvis udgifterne ved deres virksomhed overvejende dækkes af statslige eller kommunale midler, eller i det omfang de ved eller i henhold til lov har fået tillagt beføjelse til at træffe afgørelser på statens eller en kommunes vegne. Vedkommende minister fastsætter forskrifter for registret i overensstemmelse med reglerne i §§ 4 og 5.

§ 3. Vedkommende minister kan efter indhentet udtalelse fra Registertilsynet bestemme. at andre registre med personoplysninger, der føres for de i § 1, stk. 1, og § 2 nævnte myndigheder og selskaber m.v., omfattes af loven.

Stk. 2. **Vedkommende minister kan efter indhentet udtalelse fra Registertilsynet bestemme, at loven helt eller delvis skal finde tilsvarende anvendelse på edb-registre, der føres for de i § 1, stk. 1, og § 2 nævnte myndigheder og selskaber m.v., og som indeholder oplysninger om erhvervsvirksomheder m.v.**

Kapitel 2

Oprettelse af registre

§ 4. Registre, der føres for en statslig myndighed, må kun oprettes i henhold til godkendelse af vedkommende minister efter forhandling med finansministeren.

Stk. 2. **Forinden et register tages i brug, skal der af vedkommende minister eller den. han**

bemyndiger dertil, være fastsat forskrifter om det pågældende registers opbygning og drift, der opfylder bestemmelserne herom i kapitel 3-6.

Sik. 3. Bestemmelserne i stk. 1 og 2 gælder tilsvarende ved samkøring af registre, der er oparbeidet med henblik på varetagelse af forskellige opgaver. Dette gælder dog ikke samkøring, der udelukkende foretages med henblik på uddrag i statistisk eller videnskabeligt øjemed.

§ 5. Forinden der meddeles godkendelse eller fastsættes forskrifter som nævnt i § 4, skal der indhentes en udtalelse fra Registertilsynet.

Sik. 2. I tilfælde, hvor kompetencen til at fastsætte forskrifter som nævnt i § 4, stk. 2, er henlagt til en underordnet myndighed og Registertilsynet ikke har kunnet tiltræde et forelagt udkast til sådanne forskrifter, forelægges sagen for vedkommende minister, der træffer den endelige administrative afgørelse.

§ 6. Registre, der føres for en kommunal myndighed, må kun oprettes i henhold til beslutning, der træffes i et møde af vedkommende kommunalbestyrelse.

Stk. 2. Forinden et register tages i brug, skal der af kommunalbestyrelsen eller af vedkommende kommunale myndighed være fastsat forskrifter om det pågældende registers opbygning og drift, der opfylder bestemmelserne herom i kapitel 3-6.

Stk. i. Forinden der træffes beslutning eller fastsættes forskrifter som nævnt i stk. 1 og 2. skal der indhentes en udtalelse fra Registertilsynet. Kan Registertilsynet ikke tiltræde et forelagt forslag, forelægges sagen for finansministeren, der træffer den endelige administrative afgørelse.

Stk, 4. Bestemmelserne i stk. 1-3 gælder tilsvarende ved samkøring af registre, der er oparbejdet med henblik på varetagelse af forskellige opgaver. Dette gælder dog ikke samkøring, der udelukkende foretages med henblik på uddrag i statistisk eller videnskabeligt øjemed.

§ 7. Tilslutning til et register eller et system af registre, der er indrettet med henblik på at kunne føres for kommunale myndigheder fra flere kommuner, må kun finde sted. når registret eller registersystemet er godkendt af finansministeren og denne eller efter dennes bestemmelse en anden minister har fastsat forskrifter om det pågældende registers eller registersystems opbygning og drift, der opfylder bestemmelserne herom i kapitel 3-6.

Stk. 2. Forinden der meddeles godkendelse eller fastsættes forskrifter som nævnt i stk. 1, skal der indhentes en udtalelse fra Registertilsynet.

Stk. 3. Bestemmelserne i stk. 1 og 2 gælder tilsvarende ved samkøring af registre, der er oprettet med henblik på varetagelse af forskellige opgaver. Dette gælder dog ikke samkøring, der udelukkende foretages med henblik på uddrag i statistisk eller videnskabeligt øjemed.

Stk. 4. Kommunalbestyrelsen eller den, kommunalbestyrelsen bemyndiger dertil, kan bestemme, at kommunen tilslutter sig et register eller et system af registre af den i stk. 1 nævnte karakter. Beslutningen skal inden 4 uger meddeles til Registertilsynet med oplysning om eventuelle særlige vilkår for tilslutningen.

§ 8. Forskrifter som nævnt i § 4, stk. 2, § 6, stk. 2, og § 7, stk. 1, samt ændringer heraf skal straks efter udfærdigelsen fremsendes til Registertilsynet.

Stk. 2. De forskrifter, der er fastsat for et register eller et system af registre, skal være tilgængelige for offentligheden ved henvendelse såvel til den eller de registeransvarlige myndigheder som til Registertilsynet. Dette gælder dog ikke i det omfang, hensynet til gennemførelsen af de foreskrevne kontrol- og sikkerhedsforanstaltninger eller afgørende hensyn til andre offentlige interesser gør hemmeligholdelse påkrævet.

Kapitel 2 a

Undtagelse af visse registertyper fra forskriftskravet m.v.

§ 8 *2.* Registre, der føres for en statslig myndighed, og som ikke indeholder oplysninger af fortrolig karakter, er undtaget fra bestemmelserne i § 4, stk. 2 og 3, jf. § 5.

Stk. 2. I de i stk. 1 nævnte registre kan der uden fastsættelse af forskrifter endvidere registreres idcntifikationsoplysninger, herunder personnummer, og oplysninger om betaling til og fra en offentlig myndighed.

Stk. 3. En statslig myndighed, der opretter et register uden registerforskrifter, jf. stk. 1, skal inden 4 uger efter oprettelsen anmelde registret

til Registertilsynet med angivelse af registrets formål, personkreds, dataindhold og størrelse.

Stk. 4. Registertilsynet kan bestemme, at der under hensyn til registrets formål, personkreds, dataindhold, størrelse og anvendelsesområde skal fastsættes forskrift for registret.

§ 8 b. Registre, der føres for en kommunal myndighed, og som ikke indeholder oplysninger af fortrolig karakter, er undtaget fra bestemmelserne i § 6, stk. 2-4, og § 7, stk. 1-3.

Stk. 2. I de i stk. 1 nævnte registre kan der uden fastsættelse af forskrifter endvidere registreres identifikationsoplysninger, herunder personnummer, og oplysninger om betaling til og fra en offentlig myndighed.

Stk. 3. Vedkommende kommunalbestyrelse kan uanset bestemmelsen i § 6, stk. 1, bestemme, at de i stk. 1, jf. stk. 2, nævnte registre, kan oprettes efter beslutning i kommunale udvalg eller i den kommunale forvaltning.

Stk. 4. Forinden et enkeltkommunalt register, som er omfattet af stk. 1, jf. stk. 2, tages i brug, skal den, der opretter registret, udarbejde en beskrivelse af registrets formål, personkreds, dataindhold og størrelse, der kan danne grundlag for udarbejdelsen af den i stk. 5 nævnte oversigt.

Stk. 5. Kommunalbestyrelsen skal hvert kvartal udarbejde en oversigt over de nye registre, der er oprettet i kommunen uden forskrifter. Oversigten skal indeholde en beskrivelse af det enkelte registers formål, personkreds, dataindhold og størrelse. Oversigten indberettes inden 4 uger efter kvartalets udløb til Registertilsynet.

Stk. 6. Finansministeren skal godkende oprettelsen af et fælleskommunalt register, som er omfattet af stk. 1. jf. stk. 2, og skal inden 4 uger efter godkendelsen anmelde registret til Registertilsynet med angivelse af registrets formål, personkreds, dataindhold og størrelse.

Stk. 7. Registertilsynet kan bestemme, at der under hensyn til et registers formål, personkreds, dataindhold, størrelse og anvendelsesområde skal udfærdiges forskrifter for registret.

§ 8 c Registertilsynet kan bestemme, at anmeldelser og indberetninger efter § 8 a, stk. 3, og § 8 b, stk. 5-6, skal ske på nærmere angiven måde, herunder ved anvendelse af blanketter, som udfærdiges af Registertilsynet.

§ 8 d. Samkøring af registre, der indeholder fortrolige oplysninger, jf. § 8 a, stk. 2, og § 8 b, stk. 2, må ikke finde sted uden forskrifter. Det gælder dog ikke samkøring, som udelukkende foretages med henblik på uddrag i statistisk eller videnskabeligt øjemed eller med henblik på opdatering af identifikationsoplysninger og betalingsoplysninger.

§ 8 e. Justitsministeren kan efter indhentet udtalelse fra Registertilsynet fastsætte regler om, at bestemte typer af registre undtages fra bestemmelserne i § 4, stk. 2 og 3, jf. § 5, § 6 samt § 7, stk. 1-3. Det gælder dog ikke registre, der indeholder oplysninger om rent private forhold, jf. § 9, stk 2.

Kapitel 3

Registrering og opbevaring af oplysninger

§ 9. Der må kun registreres oplysninger, der klart er af betydning for varetagelsen af vedkommende myndigheds opgaver. Der må endvidere registreres oplysninger, der klart er af betydning for varetagelsen af en anden myndigheds opgaver, såfremt registret indrettes således, at oplysningerne kun kan benyttes af den anden myndighed.

Stk. 2. Der må ikke registreres oplysninger om politiske forhold, som ikke er offentligt tilgængelige. Andre oplysninger om enkeltpersoners rent private forhold, herunder oplysninger om race, religion og hudfarve, om foreningsmæssige, seksuelle og strafbare forhold samt oplysninger om helbredsforhold, væsentlige sociale problemer og misbrug af nydelsesmidler og lign., må ikke registreres, medmindre dette er nødvendigt for varetagelse af registrets opgaver.

Stk. 3. Registrerede oplysninger, der på grund af deres alder eller af andre grunde har mistet deres betydning for varetagelsen af registrets opgaver, skal slettes. Registre, der anvendes løbende, skal indrettes således, at der foretages fornøden ajourføring af oplysningerne.

Stk. 4. Registertilsynet kan tillade, at registre, der føres for kommunale myndigheder, overføres til opbevaring i arkiv på nærmere angivne vilkår. Registre, der føres for statslige myndigheder, overføres til opbevaring i statens arkiver efter reglerne i lov om offentlige arkiver m.v.

§ 10. Det kan i forskrifterne for et register fastsættes, at der skal gives en registreret meddelelse om optagelse i registret.

Stk. 2. **Justitsministeren kan med hensyn til registre, som indeholder oplysninger som nævnt i § 9, stk. 2, efter indhentet udtalelse fra Registertilsynet fastsætte regler om, at den registeransvarlige myndighed inden 4 uger efter registreringen skal give meddelelse til den, der første gang optages i registret.**

Stk. 3. **Meddelelser efter stk. 1 og 2 skal indeholde oplysning om den registreredes adgang til at få oplysninger fra registret efter bestemmelserne i §§ 13-15.**

§ 11. Der skal foretages fornøden kontrol til sikring af, at der ikke registreres urigtige eller vildledende oplysninger. Oplysninger, der viser sig urigtige eller vildledende, skal snarest muligt slettes eller berigtiges.

§ 12. Der skal træffes de fornødne sikkerhedsforanstaltninger mod, at oplysningerne misbruges eller kommer til uvedkommendes kendskab.

Stk. 2. **Sikkerhedsforanstaltningerne skal om fornødent omfatte kopier og udskrifter af registret, herunder kopier og udskrifter, der er videregivet til andre myndigheder.**

Stk. 3. **For registre, der indeholder oplysninger af særlig interesse for fremmede magter, skal der træffes foranstaltninger, der muliggør bortskaffelse eller tilintetgørelse i tilfælde af krig eller lignende forhold.**

Kapitel 4

Registrerede personers adgang til oplysninger om sig selv

§ 13. Fremsætter en registreret person begæring herom, skal den registeransvarlige myndighed snarest muligt give den registrerede meddelelse om de oplysninger, der er registreret om ham.

Stk. 2. **Hvis en person, hvorom der er registreret oplysninger som nævnt i § 9, stk. 2, fremsætter begæring herom, skal den pågældende med mellemrum, der fastsættes i forskrifterne, have udskrift af de oplysninger, der er registreret om ham. Dette gælder dog kun, hvis den registrerede ikke på anden måde gøres bekendt med de registrerede oplysninger. Der kan fastsættes regler om betaling for meddelelser som nævnt i 1. pkt.**

Stk. 3. **Det kan i forskrifterne for registret fastsættes, at den registrerede med nærmere fastsatte mellemrum skal have udskrift af de oplysninger, der er registreret om ham, eller at den registrerede skal kunne fremsætte begæring herom. Der kan fastsættes regler om betaling herfor.**

Stk. 4. **Bestemmelserne i stk. 1 og 2 gælder ikke, hvis den registreredes interesse i at få kendskab til oplysningerne findes at burde vige for afgørende hensyn til offentlige eller private interesser, herunder hensynet til den pågældende selv. Gør sådanne hensyn sig kun gældende for en del af oplysningerne, skal den registrerede gøres bekendt med de øvrige oplysninger.**

Stk. 5. **Bestemmelserne i stk. 1-3 finder ikke anvendelse for registre, der udelukkende er oparbejdet med henblik på at foretage statistiske uddrag. For andre registre kan der fastsættes undtagelser fra retten til at få oplysninger efter stk. 1-2, for så vidt bestemmelserne i stk. 4 må antages at medføre, at sådanne begæringer i almindelighed må afslås.**

Stk. 6. **En registreret person, der har fået meddelelse efter stk. 1 og 3, har ikke krav på ny meddelelse før 6 måneder efter sidste meddelelse, medmindre han kan godtgøre en særlig interesse heri.**

§ 14. Meddelelser i henhold til § 13, stk. 1, jf. stk. 4, skal på forlangende gives skriftligt. I tilfælde, hvor hensynet til den registrerede taler derfor, kan meddelelserne dog gives i form af en mundtlig underretning om indholdet af oplysningerne.

§ 15. Tvivlsspørgsmål om retten til at få meddelt oplysninger efter § 13, stk. 1, 2, 4 og 6, § 14 samt efter forskrifter fastsat i henhold til § 13, stk. 2, 3 og 5, kan indbringes for Registertilsynet. Tilsynets afgørelse kan ikke indbringes for anden administrativ myndighed.

Kapitel 5

Videregivelse af oplysninger til private

§ 16. Oplysninger som nævnt i § 9, stk. 2, der kan henføres til bestemte personer, må ikke videregives til private personer og virksomheder m.v.

Stk. 2. **Videregivelse af de i stk. 1 nævnte oplysninger kan dog ske, når**

1) den. oplysningen angår, har givet samtykke.
2) det følger aflov eller bestemmelser fastsat i henhold til lov, at oplysningen skal videregives,
3) videregivelsen sker til varetagelse af private eller offentlige interesser, der klart overstiger hensynet til de interesser, der begrunder hemmeligholdelse, herunder hensynet til den. oplysningerne angår,
4) videregivelsen er nødvendig for udførelsen af en persons eller virksomheds opgaver for det offentlige eller
5) videregivelsen er nødvendig for udførelsen af videnskabelige eller statistiske undersøgelser af væsentlig samfundsmæssig betydning.

Stk. 3. Samtykke som nævnt i stk. 2, nr. 1, skal meddeles skriftligt og skal indeholde oplysning om,

1) hvilke typer oplysninger der må videregives,
2) hvem oplysningerne må videregives til, og
3) hvorledes oplysningerne må anvendes af den angivne modtager.

Stk. 4. Samtykke bortfalder senest efter 1 års forløb.

Stk. 5. Oplysninger, der er videregivet til brug i statistisk eller forskningsmæssigt øjemed, må ikke yderligere videregives.

§ 16 a. Med mundtligt eller skriftligt samtykke fra patienten kan der fra sygehusregistre og andre patient- eller sygdomsregistre videregives oplysninger om patienten til den alment praktiserende læge, som patienten har valgt, eller til en læge, der har den pågældende i behandling.

Stk. 2. Fra de i stk. 1 nævnte registre kan der også videregives identifikationsoplysninger og oplysninger om diagnoser m.v. til læger til brug ved konkrete forskningsprojekter. Der må kun ske efterfølgende henvendelse til de registrerede i det omfang, de læger, der har behandlet de pågældende, giver tilladelse hertil.

Stk. 3. Herudover kan der fra registre som nævnt i stk. 1 med Sundhedsstyrelsens godkendelse og på nærmere angivne vilkår videregives oplysninger til brug ved forskning eller planlægning.

Stk. 4. Oplysninger, der er videregivet til brug i statistisk eller forskningsmæssigt øjemed, må ikke yderligere videregives.

§ 17. Andre registrerede oplysninger end dem, der er nævnt i § 9, stk. 2, må ikke videregives til private personer og virksomheder m.v.

Stk. 2. Videregivelse af de i stk. 1 nævnte oplysninger kan dog ske i det omfang, der er nævnt i § 16, eller når oplysningerne i forvejen er offentligt tilgængelige.

Stk. 3. Til brug i konkrete retsforhold kan der videregives enkeltstående oplysninger som nævnt i stk. 1 til private personer og virksomheder m.v., som kan godtgøre at have en retlig interesse i at få de pågældende oplysninger, der klart overstiger hensynet til oplysningernes hemmeligholdelse. Dette gælder dog ikke oplysninger, om hvilke der ved lov er fastsat særlige tavshedsforskrifter.

Stk. 4. Der kan videregives oplysninger som nævnt i stk. 1 til brug ved forskning.

Stk. 5. Herudover kan videregivelse af oplysninger som nævnt i stk. 1 til private personer og virksomheder m.v. i særlige tilfælde ske efter forudgående tilladelse fra Registertilsynet, når dette på grund af oplysningernes karakter, mængde og formålet med videregivelsen skønnes ubetænkeligt Registertilsynet kan fastsætte nærmere vilkår for tilladelsen. Registertilsynets afgørelse kan ikke indbringes for anden administrativ myndighed.

§ 18. Fra registre, der udelukkende er oparbejdet med henblik på at foretage statistiske uddrag eller som led i en videnskabelig undersøgelse, må der ikke uden særlig hjemmel videregives oplysninger, der kan henføres til bestemte personer. Registertilsynet kan dog efter ansøgning i hvert enkelt tilfælde tillade, at sådanne oplysninger på nærmere angivne vilkår videregives til private registre, der udelukkende er oparbejdet i statistisk eller videnskabeligt øjemed. Registertilsynets afgørelse herom kan ikke indbringes for anden administrativ myndighed.

§ 19. Den registeransvarlige myndighed kan fastsætte vilkår for videregivelse af oplysninger efter bestemmelserne i dette kapitel, herunder om, at oplysningerne kun må benyttes til bestemte formål. Sådan videregivelse med henblik på samkøring med registre, der ikke omfattes aflov om private registre m.v., kan kun ske efter forud indhentet udtalelse fra Registertilsynet.

§ 20. Vedkommende minister kan fastsætte regler om betaling for udlevering af oplysninger-

Kapitel 5 a

Videregivelse til kreditnplysningsbureauer af oplysninger om gæld til det offentlige

§ 20 a. Oplysninger om gæld til det offentlige kan efter bestemmelserne i dette kapitel videregives til kreditoplysningsbureauer, jf. kapitel 3 i lov om private registre.

Stk. 2. Oplysninger som nævnt i § 9, stk. 2, må ikke videregives.

Stk. 3. Fortrolige oplysninger videregivet efter reglerne i dette kapitel anses ikke af den grund for offentligt tilgængelige i øvrigt.

§ 20 b. Oplysninger om gæld til det offentlige kan videregives til et kreditoplysningsbureau, hvis

1) det følger af lov eller bestemmelser fastsat i henhold til lov eller
2) den samlede gæld er forfalden og overstiger 7.500 kr., idet der dog ikke heri må indgå gældsposter, der er omfattet af en overholdt aftale om henstand eller afdragsvis betaling.

Stk. 2. Det er en betingelse, at den samlede gæld, jf. stk. 1, nr. 2, administreres af samme inddrivelsesmyndighed.

Stk. 3. Det er endvidere en betingelse for videregivelse efter stk. 1, nr. 2, at

1) gælden kan inddrives ved udpantning og der er fremsendt 2 rykkere til skyldneren,
2) der er foretaget eller forsøgt foretaget udlæg for kravet,
3) kravet er fastslået ved endelig dom eller
4) det offentlige har erhvervet skyldnerens skriftlige erkendelse af den forfaldne gæld.

§ 20 c. Myndigheden skal give skyldneren skriftlig meddelelse herom, forinden videregivelse finder sted. Videregivelse må tidligst ske 4 uger efter, at denne meddelelse er givet.

Stk. 2. Den i stk. 1 nævnte meddelelse skal indeholde oplysninger om,

1) hvilke oplysninger der vil blive videregivet,
2) til hvilket kreditoplysningsbureau videregivelse vil ske,
3) hvornår videregivelse vil finde sted, og
4) at videregivelse ikke vil ske, hvis betaling af gælden sker inden videregivelsen eller der indrømmes henstand eller indgås og overholdes en aftale om afdragsvis betaling.

§ 20 d. Vedkommende minister kan efter indhentet udtalelse fra Registertilsynet fastsætte nærmere regler om fremgangsmåden ved videregivelse til kreditoplysningsbureauer af oplysninger om gæld til det offentlige. Det kan i den forbindelse bestemmes, at oplysninger om visse former for gæld til det offentlige ikke må videregives eller kun må videregives, hvis yderligere betingelser end de i § 20 b nævnte er opfyldt.

Kapitel 6

Videregivelse af oplysninger til offentlige myndigheder

§ 21. Registrerede oplysninger som nævnt i § 9, stk. 2, må ikke videregives til anden offentlig myndighed.

Stk. 2. Videregivelse af de i stk. 1 nævnte oplysninger kan dog ske, når

1) den, oplysningen angår, har givet samtykke,
2) det følger af lov eller bestemmelser fastsat i henhold til lov, at oplysningen skal videregives,
3) videregivelsen sker til varetagelse af private eller offentlige interesser, der klart overstiger hensynet til de interesser, der begrunder hemmeligholdelse, herunder hensynet til den, oplysningen angår,
4) videregivelsen er nødvendig for udførelsen af en myndigheds virksomhed eller påkrævet for en afgørelse, som myndigheden skal træffe, eller
5) videregivelsen er nødvendig for udførelsen af videnskabelige eller statistiske undersøgelser af væsentlig samfundsmæssig betydning.

Stk. 3. Andre registrerede oplysninger må ud over de i stk. 2 nævnte tilfælde kun videregives til en offentlig myndighed, når oplysningerne i forvejen er offentligt tilgængelige, eller når det må antages, at oplysningen vil være af væsentlig betydning for myndighedens virksomhed eller for en afgørelse, myndigheden skal træffe, jf. dog § 9, stk. 1, 2. pkt.

Stk. 4. Samtykke efter stk. 2, nr. 1, skal opfylde kravene i § 16, stk. 3. Samtykke bortfalder senest efter 1 års forløb.

Stk, 5. Fra registre, der udelukkende er opar-

bejdet med henblik på at foretage statistiske uddrag eller som led i en videnskabelig undersøgelse, må ikke uden særlig hjemmel videregives oplysninger, der kan henføres til bestemte personer. Registertilsynet kan dog efter ansøgning i hvert enkelt tilfælde tillade, at sådanne oplysninger videregives til registre, derudelukkende er oparbejdet i statistisk eller videnskabeligt øjemed. Registertilsynets afgørelse herom kan ikke indbringes for anden administrativ myndighed.

Kapitel 7

Registertilsyn

§ 22. Registertilsynet, der består af et råd og et sekretariat, fører tilsyn med ethvert register, der omfattes af loven. Registertilsynet udøver endvidere de funktioner, der i henhold til lov om private registre m.v. er henlagt til tilsynet.

Stic 2. Registertilsynet påser af egen drift eller efter klage fra en registreret, at registret er oprettet og anvendes i overensstemmelse med lovens bestemmelser og de forskrifter, der er fastsat i medfør af loven.

§ 23. Rådet, der nedsættes af justitsministeren, består af en formand, der skal opfylde betingelserne for at kunne blive udnævnt til dommer, og af 6 andre medlemmer. Medlemmerne og stedfortrædere for disse udnavnes for 4 år.

§ 24. Registertilsynets daglige forretninger varetages af sekretariatet, der ledes af en direktør.

§ 25. Justitsministeren fastsætter rådets forretningsorden og de nærmere regler om arbejdets fordeling mellem råd og sekretariat

§ 26, Registertilsynet kan afkræve såvel den eller de for registret ansvarlige myndigheder som den, der fører registret, enhver oplysning af betydning for tilsynet.

Stk. 2. Tilsynets medlemmer og personale har til enhver tid mod behørig legitimation uden retskendelse adgang til alle lokaler, hvorfra registret administreres eller kan benyttes, samt til lokaler, hvor registret eller de tekniske hjælpemidler opbevares eller anvendes.

Stk. 3. Tilsynet afgiver indberetning til den eller de for registret ansvarlige myndigheder og vedkommende minister om konstaterede overtrædelser af loven eller de fastsatte forskrifter samt i øvrigt om forefundne mangler. Tilsynet skal have underretning om, hvad myndigheden foretager i anledning af indberetningen.

§ 27. Registertilsynet kan til enhver tid fremsætte forslag om ændring af gældende forskrifter over for den myndighed, der har fastsat forskrifterne. Bestemmelserne i § 5, stk. 2, og § 6, stk. 3, 2. pkt., gælder tilsvarende.

§ 28. Registertilsynet afgiver en årlig beretning om sin virksomhed til Folketinget. Beretningen offentliggøres.

Stk. 2. Registertilsynet kan i øvrigt offentliggøre udtalelser, som tilsynet har afgivet i medfør af § 1, stk. 6, § 5, stk. 1, § 6, stk. 3, § 7, stk. 2, § 8 a, stk. 4, § 8 b, stk. 7, § 8 e, og § 19, indberetninger, der er afgivet i medfør af § 26, stk. 3, og forslag, der er fremsat i medfør af § 27. Bestemmelsen i § 8, stk. 2, 2. pkt., gælder tilsvarende.

Kapitel 8

Straf

§ 29. Medmindre højere straf er forskyldt efter den øvrige lovgivning, straffes med bøde eller hæfte den, der:

1) tilsidesætter vilkår i et samtykke efter § 16, stk.2,nr. 1,
2) overtræder § 16, stk. 5, § 16 a, stk. 2, 2. pkt., og§ 16 a, stk. 4, eller
3) tilsidesætter vilkår fastsat i medfør af § 16 a, stk. 3, § 17, stk. 5, § 18 og §19.

*Stk. 2.*1 forskrifter, der udstedes i medfør af lovens kapitel 2, kan der fastsættes straf af bøde for overtrædelse af bestemmelser i forskrifterne.

Stk. 3. Er overtrædelsen begået af et aktieselskab, andelsselskab eller lignende, kan bødeansvar pålægges selskabet som sådant

Kapitel 9

Ikrafttrædelses- og overgangsbestemmelser m.v.

§ 30. Loven træder i kraft den 1. januar 1979.

Stk. 2. For registre og registersystemer, der er taget i brug inden lovens ikrafttræden, får loven

først virkning 1 år efter lovens ikrafttræden. For de pågældende registre indsendes udkast til forskrifter om registrenes opbygning og drift. der opfylder bestemmelserne i kapitel 3-6, til Registertilsynet senest 6 måneder efter lovens ikrafttræden. Bestemmelserne i § 5, stk. 2, og § 6, stk. 3, 2. pkt., gælder tilsvarende. Justitsministeren kan forlænge fristerne for bestemte registre.

Stk. 3. **For registre, der er taget i brug eller er under opbygning ved lovens ikrafttræden, og for hvilke det ikke uden væsentlige systemtekniske ændringer er muligt at give udskrift af de registrerede oplysninger, får bestemmelserne i § 13, stk. 1 og 3, først virkning 3 år efter lovens ikrafttræden.**

§ 31. Loven gælder ikke for registre, der føres for politiets og forsvarets efterretningstjenester.

§ 32. Loven gælder ikke for registre, der fores for det færøske hjemmestyres myndigheder eller for rigsmyndighederne på Færøerne. Loven kan ved kgl. anordning sættes i kraft for rigsmyndighedernes registre med de afvigelser, som de særlige færøske forhold tilsiger.

§§ 3 og 4 i lov nr. 383 af 10. juni 1987 indeholder følgende bestemmelser:

§3

Stk. 1. **Loven træder i kraft den 1. april 1988. Bestemmelsen i § 2, nr. 5 (§ 13, stk. 2, om automatisk registerindsigt) træder dog først i kraft efter justitsministerens nærmere bestemmelse.**

Stk. 2. **(vedrørende lov om private registre)**

Stk. 3. **For offentlige myndigheders registre, der er taget i brug før lovens ikrafttræden, skal ændring af forskrifterne, således at disse opfylder bestemmelserne i § 2, ske senest 1 år efter lovens ikrafttræden. Justitsministeren kan forlænge fristen for bestemte registre.**

§4

Stk. 1. **(vedrørende lov om private registre)**

Stk. **2. § 2 (ændring af lov om offentlige myndigheders registre) gælder ikke for registre, der føres for det færøske eller grønlandske hjemmestyres myndigheder eller for rigsmyndighederne på Færøerne eller Grønland. Lovens § 2 kan ved kgl. anordning sættes i kraft for rigsmyndighedernes registre med de afvigelser, som de særlige færøske eller grønlandske forhold tilsiger.**

§§ 2 og 3 i lov nr. 346 af 6. juni 1991 indeholder følgende bestemmelser:

§2

Loven træder i kraft den 1. september 1991.

§3

Loven gælder ikke for registre, der føres for det færøske eller grønlandske hjemmestyres myndigheder eller for rigsmyndighedeme på Færøerne eller i Grønland. Lovens § 1 kan ved kgl. anordning sættes i kraft for rigsmyndighedernes registre med de afvigelser, som de særlige færøske eller grønlandske forhold tilsiger.

BILAG 3

Lov om massemediers informationsdatabaser

Kapitel 1

Almindelige bestemmelser

§ 1. Loven gælder for informationsdatabaser, der er massemedier, eller som drives i tilknytning til en eller flere virksomheder, der udgiver massemedier.

Stk. 2. Loven gælder dog ikke for informationsdatabaser, hvori der udelukkende er indlagt allerede offentliggjorte periodiske skrifter eller lyd- og billedprogrammer, der er omfattet af medieansvarslovens § 1, nr. 1 eller 2, eller dele heraf, når indlæggelsen i informationsdatabasen er sket uændret i forhold til offentliggørelsen.

Stk. 3. Loven gælder endvidere ikke for informationsdatabaser, hvori der udelukkende er indlagt allerede offentliggjorte tekster, billeder og lydprogrammer, der omfattes af medieansvarslovens § 1, nr. 3, eller dele heraf, når indlæggelsen i informationsdatabasen er sket uændret i forhold til offentliggørelsen.

§ 2. Ved massemedier forstås de af medieansvarslovens § 1 omfattede massemedier.

Stk. 2. Ved informationsdatabaser forstås informationssystemer, hvor der gøres brug af elektronisk databehandling i forbindelse med formidling af nyheder og andre informationer.

Stk. 3. Ved redaktionelle informationsdatabaser forstås informationsdatabaser eller klart adskilte dele heraf, der alene drives som led i journalistisk eller redaktionelt arbejde med henblik på offentliggørelse i et massemedie.

Kapitel 2

Redaktionelle informationsdatabaser

§ 3. En redaktionel informationsdatabase skal for at blive omfattet af loven være anmeldt til Registertilsynet.

Stk. 2. Et massemedie kan indgive en anmeldelse omfattende samtlige massemediets redaktionelle informationsdatabaser.

Stk. 3. Registertilsynet offentliggør hvert år en fortegnelse over anmeldte redaktionelle informationsdatabaser.

§ 4. En redaktionel informationsdatabase må ikke være tilgængelig for andre end massemediets journalister og redaktionsmedarbejdere.

Stk. 2. Journalister og redaktionsmedarbejdere må ikke få adgang til eller benytte informationsdatabasen til andet end journalistisk eller redaktionelt arbejde.

§ 5. Der skal træffes de fornødne sikkerhedsforanstaltninger mod, at uvedkommende får adgang til en redaktionel informationsdatabase, og mod, at informationsdatabasen benyttes til uvedkommende formål.

Kapitel 3

Offentligt tilgængelige informationsdatabaser

§ 6. En offentligt tilgængelig informationsdatabase skal for at blive omfattet af loven ud over at være tilgængelig for enhver på almindelige forretningsvilkår være anmeldt til Pressenævnet og Registertilsynet med angivelse af,

hvem der er ansvarlig for informationsdatabasen.

Stk. 2. Sker der anmeldelse efter stk. 1, er informationsdatabasen ikke samtidig omfattet af medieansvarsloven, jf. dog § 10, stk. 1, og § 13, stk. 3.

§ 7. Den, der driver en offentligt tilgængelig informationsdatabase, skal efter anmodning oplyse, hvem der er ansvarlig for informationsdatabasen.

§ 8. En offentligt tilgængelig informationsdatabase må ikke indeholde informationer, der ikke lovligt kan offentliggøres i et massemedie.

Stk. 2. Informationsdatabasen må ikke indeholde informationer, hvis offentliggørelse ville være i strid med god presseskik.

Stk. 3. Informationer om enkeltpersoners rent private forhold, herunder oplysninger om race, religion og hudfarve, om politiske, foreningsmæssige, seksuelle og strafbare forhold samt oplysninger om helbredsforhold, væsentlige sociale problemer og misbrug af nydelsesmidler og lignende, må ikke opbevares i informationsdatabasen, når der er forløbet 3 år efter, at den begivenhed, der har givet anledning til optagelsen i databasen, fandt sted, eller, hvis et sådant tidspunkt ikke kan fastsættes, 3 år efter, at informationerne er optaget i databasen.

Stk. 4. Bestemmelsen i stk. 3 finder dog ikke anvendelse, hvis der består en sådan interesse i. at de pågældende informationer er offentligt tilgængelige, at hensynet til den enkeltes interesse i, at informationerne slettes, findes at burde vige for hensynet til informationsfriheden.

§ 9. I informationsdatabaser, der er offentligt tilgængelige, skal der efter anmodning fra den, informationerne angår, foretages sletning, rettelse eller ajourføring, når

1) informationerne er urigtige eller vildledende,
2) en tidligere omtalt retsafgørelse eller administrativ afgørelse er blevet ændret eller
3) strafforfølgning i en tidligere omtalt sag opgives, eller når der i en sådan sag sker frifindelse.

§ 10. Den, oplysningerne vedrører, eller efter dennes død de nærmeste pårørende kan i stedet for at fremsætte anmodning om sletning, rettelse eller ajourføring tage til genmæle. Bestemmelserne i medieansvarslovens kapitel 6 om genmæle finder tilsvarende anvendelse, jf. dog stk. 2-4 og § 12, stk. 2.

Stk. 2. De pligter, der efter medieansvarslovens bestemmelser om genmæle påhviler redaktøren, påhviler efter denne lov den ansvarlige for informationsdatabasen.

Stk. 3. Anmodning om genmæle kan fremsættes, så længe de oplysninger, der ønskes imødegået, befinder sig i informationsdatabasen.

Stk. 4. Genmæle offentliggøres i den informationsdatabase, hvori de oplysninger, der begmnder genmælet, er bragt. Er de oplysninger, der begrunder genmælet, forinden slettet, berigtiget eller ajourført, bortfalder pligten til at offentliggøre genmælet.

§ 11. Fra en offentligt tilgængelig informationsdatabase skal der til enhver, der fremsætter anmodning herom, gives skriftlig meddelelse om de informationer, der er optaget i databasen om vedkommende selv, medmindre det er forbundet med uforholdsmæssigt store vanskeligheder at finde frem til informationerne.

Stk. 2. Den, der har fået meddelelse efter stk. 1, har ikke krav på ny meddelelse før 1 år efter sidste meddelelse.

Stk. 3. Den, der er ansvarlig for informationsdatabasen, skal inden 4 uger besvare anmodninger som nævnt i stk. 1.

Stk. 4. Justitsministeren kan fastsætte regler om betaling for skriftlige meddelelser om indholdet af offentligt tilgængelige informationsdatabaser.

Kapitel 4

Klager, straf m.v.

§ 12. Undlader den, der er ansvarlig for en offentligt tilgængelig informationsdatabase, efter anmodning at slette informationer, der strider mod god presseskik, jf. § 8, stk. 2, eller som befinder sig i databasen i strid med tidsfristen i § S. stk. 3, jf. stk. 4, eller nægter den ansvarlige at optage et genmæle, eller har vedkommende ikke inden 4 uger besvaret en henvendelse om sletning eller genmæle, kan den, informationerne angår, eller efter dennes død de nærmeste pårørende, indbringe spørgsmålet for Pressenævnet.

Stk. 2. Sagen skal indbringes for Pressenævnet senest 4 uger efter, at afslaget er kommet

frem, eller 4 uger efter udløbet af den i stk. 1 nævnte svarfrist.

§ 13. Pressenævnet kan efter anmodning give påbud om, at der foretages sletning af informationer, der strider mod bestemmelserne i § 8, stk. 2-4.

Stk. 2. Pressenævnet kan efter anmodning give påbud om, at der optages et genmæle i en offentligt tilgængelig informationsdatabase, herunder fastsætte genmælets indhold, form og placering.

Stk. 3. Bestemmelserne i medieansvarslovens § 42, § 43, stk. 2 og 3, § 44, stk. 1, §§ 45-48 og § 52, stk. 3, finder tilsvarende anvendelse.

§ 14. Pressenævnet kan af enhver kræve alle oplysninger, der er af betydning for nævnets virksomhed efter denne lov.

§ 15. Pressenævnets afgørelser efter denne lov kan ikke indbringes for anden administrativ myndighed.

§ 16. Med bøde eller hæfte straffes den, der

1) overtræder § 4, § 5, § 7, § 8, stk. 1, § 9, nr. 2 og 3, og § 11, stk. 1 og 3,
2) undlader at efterkomme påbud, der er givet af Pressenævnet i medfør af § 13, stk. 1 og 2, eller
3) undlader at efterkomme krav fra Pressenævnet efter § 14.

Stk. 2. Den, der uberettiget udnytter eller videregiver oplysninger, som den pågældende har fået kendskab til gennem benyttelse af en redaktionel informationsdatabase, straffes med bøde eller hæfte, medmindre højere straf er forskyldt i medfør af anden lovgivning.

§ 17. Lovgivningens almindelige straf- og erstatningsregler finder anvendelse på sager omfattet af denne lov.

Stk. 2. Er en overtrædelse begået af et selskab, en forening, en selvejende institution, en fond eller lignende, kan der pålægges den juridiske person som sådan bødeansvar. Er overtrædelsen begået af staten, en kommune eller et kommunalt fællesskab, jf. § 60 i lov om kommunernes styrelse, kan der pålægges staten, kommunen eller det kommunale fællesskab bødeansvar.

Kapitel 5

Ikrafttrædelsesbestemmelser m.v.

§ 18. I lov om private registre, jf. lovbekendtgørelse nr. 622 af 2. oktober 1987, som ændret ved lov nr. 386 af 20. maj 1992, foretages følgende ændringer:

1. I *§ 2* indsættes efter stk. 3 som nye stykker:

»*Stk. 4.* Loven finder ikke anvendelse på edb-registre, der er omfattet af lov om massemediers informationsdatabaser.

Stk. 5. Loven finder ikke anvendelse på edb-registre, hvori der udelukkende er indlagt allerede offentliggjorte periodiske skrifter eller lyd- og billedprogrammer, der er omfattet af medieansvarslovens § 1, nr. 1 eller 2, eller dele heraf, når indlæggelsen i informationsdatabasen er sket uændret i forhold til offentliggørelsen.

Stk. 6. Loven gælder endvidere ikke for informationsdatabaser, hvori der udelukkende er indlagt allerede offentliggjorte tekster, billeder og lydprogrammer, der omfattes af medieansvarslovens § 1, nr. 3, eller dele heraf, når indlæggelsen i informationsdatabasen er sket uændret i forhold til offentliggørelsen.

Stk. 7. Loven finder ikke anvendelse på ma-, nuelle arkiver over udklip fra offentliggjorte, trykte publikationer.«

Stk. 4 og 5 bliver herefter stk. 8 og 9.

2. *Kapitel 2 c* ophæves.

3. I *§ 27, stk. 1, nr. 1,* udgår »§ 7 g, stk. 1 og 2, § 7 h, § 7 i,«.

§ 19. I lov om offentlige myndigheders registre, jf. lovbekendtgørelse nr. 654 af 20. september 1991, som ændret ved § 37 i lov nr. 337 af 14. maj 1992, indsættes i *§ 1* som *stk. 6-8:*

»*Stk. 6.* Loven finder ikke anvendelse på edb-registre, der er omfattet af lov om massemediers informationsdatabaser.

Stk. 7. Loven finder ikke anvendelse på edb-registre, hvori der udelukkende er indlagt allerede offentliggjorte periodiske skrifter eller lyd- og billedprogrammer, der er omfattet af medieansvarslovens § 1, nr. 1 eller 2, eller dele heraf, når indlæggelsen i informationsdatabasen er sket uændret i forhold til offentliggørelsen.

Stk. 8. Loven gælder endvidere ikke for informationsdatabaser, hvori der udelukkende er indlagt allerede offentliggjorte tekster, billeder og lydprogrammer, der omfattes af medieansvarslovens § 1, nr. 3, eller dele heraf, når indlæggelsen i informationsdatabasen er sket uændret i forhold til offentliggørelsen.«

§ 20. Loven træder i kraft den 1. oktober 1994.

§ 21. Loven gælder ikke for Færøerne og Grønland.

Givet på Christiansborg Slot, den 1. juni 1994

Under Vor Kongelige Hånd og Segl

MARGRETHE R.

/ Erling Olsen

Lovbekendtgørelse nr. 622 af 15. september 1986

om tinglysning

som ændret ved lov nr. 138 af 7.3. 1990, lov nr. 398 af 13.6. 1990, lov nr. 322 af 31.5. 1991, lov nr. 281 af 29.4. 1992, lov nr. 153 af 8.3. 1994, lov nr. 389 af 14.6. 1995, lov nr. 1072 af 20.12. 1995, lov nr. 382 og 385 af 22.5. 1996

III. Administrative bestemmelser, gebyr- og strafbestemmelser m.v.

Kapitel 8

§ 50. Alle adkomstdokumenter og pantebreve vedrørende fast ejendom, der anmeldes til tinglysning, skal snarest muligt gøres offentligt tilgængelige. Det samme gælder pantebreve, der anmeldes til tinglysning i bilbogen, samt dokumenter, der anmeldes til tinglysning i personbogen. Justitsministeren fastsætter nærmere regler herom.

Stk. 2. Justitsministeren fastsætter nærmere regler om grundlaget for tinglysning, herunder eventuelt om oplysning om personnumre ved tinglysning i bilbog eller personbog, indleveringstid for dokumenter og indretning og førelse af dagbog, tingbog, bilbog og personbog samt videregivelse af oplysninger, herunder efter § 50 c.

Stk. 3. Dagbogen, tingbogen, bilbogen og personbogen kan føres ved hjælp af edb. Anvendes edb i tinglysningen, gælder reglerne i § 50 a-e.

§ 50 a. Formålet med edb-registrering efter § 50, stk. 3, er at tilvejebringe et arbejdsregister for tinglysningsvæsenet og et grundlag for formidling af tinglysningsoplysninger til offentligheden samt for udarbejdelse af statistik.

§ 50 b. Der må kun registreres oplysninger, der har betydning for varetagelsen af tinglysningsopgaverne, samt oplysninger, der har væsentlig betydning for de i § 50 c, stk. 3, nr. 1 og 2, nævnte myndigheders og erhvervsdrivendes brug af tinglysningsoplysninger.

§ 50 c. Oplysninger i edb-registrene om perssonnumre må ikke videregives.

Stk. 2. Oplysninger i edb-registrene i øvrigt er tilgængelige for enhver ved personlig henvendelse til tinglysningskontoret. Oplysningerne kan gives via terminaler, der opstilles på tinglysningskontorerae eller andre steder efter justitsministerens bestemmelse.

Stk. 3. Oplysninger i edb-registrene kan ved terminaladgang i øvrigt (ekstern terminaladgang) kun videregives til

1) offentlige myndigheder, såfremt tinglysningsoplysninger har betydning for udøvelsen af myndighedens virksomhed,
2) kreditinstitutter, ejendomsmæglere og ejendomshandlere, advokater, forsikringsselskaber, landinspektører og andre, der i erhvervsmæssigt øjemed udfører opgaver vedrørende overdragelse, forsikring, retsforfølgning, retsforhold i øvrigt, belåning af fast ejendom og løsøre samt fysisk råden over fast ejendom, og

3) organisationer, der varetager forbruger- eller brancheinteresser med henblik på rådgivning vedrørende de i nr. 2 nævnte forhold.

Stk. 4. Oplysninger, der slettes eller aflyses, overføres til et særligt register (historisk register). Adkomstoplysninger fra dette register kan videregives efter reglerne i stk. 2 og 3. Andre oplysninger fra det særlige register kan kun videregives til brug i konkrete retsforhold. Fuldstændige oplysninger skal dog efter anmodning videregives til den, som oplysningerne angår.

Stk. 5. Tinglysninsregistrene må ikke samkøres med private eller andre offentlige edb-registre, medmindre andet er fastsat ved lov. Der kan dog foretages samkøring med offentlige registre med henblik på overførelse af oplysninger til tinglysningsregistrene som led i etableringen af disse eller som led i tinglysningsregistrenes løbende ajourføring samt til statistiske og videnskabelige formål. Endvidere kan der ske sammenstilling via terminal med offentligt tilgængelige oplysninger fra andre offentlige registre vedrørende faste ejendomme.

Stk. 6. Der må ikke videregives masse-oplysninger, jfr. dog § 50, stk. 1.

Stk. 7. Videregivelse efter § 50, stk. 1, af oplysninger vedrørende bestemt angivne faste ejendomme og løsøregenstande kan ske løbende til de myndigheder og erhvervsdrivende, der er nævnt i stk. 3, nr. 1 og 2. Sådanne oplysninger må ikke udleveres på edb.

Stk. 8. Oplysninger, der videregives efter stk. 2-7, må ikke anvendes med henblik på at skaffe nye kunder eller i øvrigt med henblik på andre formål end overdragelse, forsikring, retsforfølgning og retsforhold i øvrigt, belåning af fast ejendom og løsøre, kreditvurdering, fysisk råden over fast ejendom samt rådgivning i forbindelse med disse formal.

Stk. 9. Afgørelser vedrørende terminaladgang og anden videregivelse efter stk. 3 og stk. 5-7 træffes ved retten i Århus. Kære af dommerens afgørelser sker til den landsret, i hvis kreds den-, som anmoder om videregivelse, har hjemting.

§ 50 d. Justitsministeren fastsætter efter drøftelse med Registertilsynet nærmere regler med henblik på at sikre, at oplysninger i tinglysningsregistrene ikke tilintetgøres, forvanskes eller uberettiget indføjes, slettes eller ændres, jfr. §§ 20, 42 g, stk. 2, og 49, samt med henblik på at sikre, at oplysninger ikke misbruges eller kommer til uvedkommendes kendskab.

Stk. 2. Landsretternes præsidenter fører tilsyn med tinglysningsregistrene. Præsidenternes afgørelser er endelige.

Stk. 3. Justitsministeren fastsætter nærmere regler om dette tilsyn efter forhandling med landsretternes præsidenter og Registertilsynet.

§ 50 e. Med bøde straffes den, der anvender en oplysning i strid med bestemmelsen i § 50 c, stk. 8. For overtrædelser, der begås af aktieselskaber, anpartsselskaber eller lignende, kan der pålægges selskabet som sådant bødeansvar.

§ 50 f. Pantebreve, der anmeldes til tinglysning, skal være oprettet på blanketter, der er godkendt af justitsministeren (justitsministeriets pantebrevsformularer).

Stk. 2. Justitsministeren kan bestemme, at andre dokumenter, der anmeldes til tinglysning, skal være oprettet på blanketter, som er godkendt af justitsministeren.

Stk. 3. Justitsministeren kan bestemme, at dokumenter, der anmeldes til tinglysning i bilbogen eller personbogen, skal være oprettet således, at de kan aflæses maskinelt.

Stk. 4. Justitsministeren kan uanset bestemmelserne i § 50 c, stk. 5-7, fastsætte regler om forsøg med tinglysning på grundlag af elektronisk overførelse af oplysninger samt om forsøg med elektronisk videregivelse af oplysninger til et realkreditinstitut. Det kan-i disse regler fastsættes, at tinglysning af elektroniske dokumenter skal have samme retsvirkning som tinglysning af andre dokumenter.

§ 50 g. Justitsministeren kan fastsætte regler om betaling for elektroniske forespørgsler til tinglysningskontorets bøger m.v. Krav på betaling kan i reglerne tillægges udpantningsret

Forvaltningslov

Kapitel 1
Loven almindelige anvendelsesområde

§ 1. Loven gælder for alle dele af den offentlige forvaltning.

Stk. 2. Vedkommende minister kan efter forhandling med justitsministeren fastsætte regler om, at loven helt eller delvis skal gælde for nærmere angivne selskaber, institutioner, foreninger m.v., som ikke kan henregnes til den offentlige forvaltning. Det gælder dog kun, hvis udgifterne ved deres virksomhed overvejende dækkes af statslige eller kommunale midler, eller i det omfang de ved eller i henhold til lov har fået tillagt beføjelse til at træffe afgørelser på statens eller en kommunes vegne. Vedkommende minister kan herunder fastsætte nærmere regler om opbevaring af dokumenter m.v. og om tavshedspligt.

§ 2. Loven gælder for behandlingen af sager, hvori der er eller vil blive truffet afgørelse af en forvaltningsmyndighed.

Stk. 2. Bestemmelserne i kapitel 2 om inhabilitet gælder også for behandlingen af sager om indgåelse af kontraktsforhold eller lignende privatretlige dispositioner.

Stk. 3. Bestemmelserne i kapitel 8 gælder for al virksomhed, der udøves inden for den offentlige forvaltning.

Stk. 4. Vedkommende minister kan efter forhandling med justitsministeren fastsætte regler om, at lovens bestemmelser i øvrigt helt eller delvist skal gælde for anden forvaltningsvirksomhed end nævnt i stk. 1.

Kapitel 4
Partens aktindsigt

§ 9. Den, der er part i en sag, hvori der er eller vil blive truffet afgørelse af en forvaltningsmyndighed, kan forlang at blive gjort bekendt med sagens dokumenter. Begæringen skal angive den sag, hvis dokumenter den pågældende ønsker at blive gjort bekendt med.

Stk. 2. Bestemmelser om tavshedspligt for personer, der virker i offentlig tjeneste eller hverv, begrænser ikke pligten til at give aktindsigt efter dette kapitel.

Stk. 3. Bestemmelserne i dette kapitel gælder ikke sager om strafferetlig forfølgning af lovovertrædelser, jfr. dog § 18.

Omfanget af aktindsigt

§ 10. En parts ret til aktindsigt omfatter med de i §§ 12-15 nævnte undtagelser

1) alle dokumenter, der vedrører sagen, herunder genpart af de skrivel-

ser, der er udgået fra myndigheden, når skrivelserne må antages at være kommet frem til adressaten, og
2) indførelser i journaler, registre og andre fortegnelser vedrørende den pågældende sags dokumenter.

Stk. 2. Den, der ansøger eller har ansøgt om ansættelse eller forfremmelse i det offentliges tjeneste, kan dog kun forlange at blive gjort bekendt med de dokumenter m.v., der vedrører den pågældendes egne forhold.

Udsættelse af sagen

§ 11. Fremsætter en part under sagens behandling begæring om aktindsigt, og denne begæring efter loven skal imødekommes, udsættes sagens afgørelse, indtil der er givet parten adgang til at gøre sig bekendt med dokumenterne.
Stk. 2. Bestemmelsen i stk. 1 gælder dog ikke, hvis udsættelse vil medføre overskridelse af en lovbestemt frist for sagens afgørelse, eller hvis partens interesse i, at sagens afgørelse udsættes, findes at burde vige for væsentlige hensyn til offentlige eller private interesser, der taler imod en sådan udsættelse.

Undtagelse af dokumenter

§ 12. Retten til aktindsigt omfatter ikke en myndigheds interne arbejdsdokumenter. Som interne arbejdsdokumenter anses

1) dokumenter, der udarbejdes af en myndighed til eget brug ved behandlingen af en sag.
2) brevveksling mellem forskellige enheder inden for samme myndighed og
3) brevveksling mellem en kommunalbestyrelse og dennes udvalg, afdelinger og andre administrative organer eller mellem disse organer indbyrdes.

Stk. 2. Oplysninger vedrørende sagens faktiske omstændigheder, der er af væsentlig betydning for sagens afgørelse, og som alene indeholdes i interne arbejdsdokumenter, skal uanset bestemmelsen i stk. 1 meddeles i overensstemmelse med reglerne i dette kapitel.

§ 13. Retten til aktindsigt omfatter uanset bestemmelserne i § 12 interne arbejdsdokumenter, som foreligger i endelig form, når

1) dokumenterne alene gengiver indholdet af myndighedens endelige beslutning vedrørende en sags afgørelse,
2) dokumenterne alene indeholder en gengivelse af oplysninger, som myndigheden har haft pligt til at notere efter lov om offentlighed i forvaltningen, eller
3) dokumenterne er selvstændige dokumenter, der er udarbejdet af en myndighed for at tilvejebringe bevismæssig eller anden tilsvarende klarhed med hensyn til en sags faktiske omstændigheder.

§ 14. Retten til aktindsigt omfatter ikke:

1) Statsrådsprotokoller, referater af møder mellem ministre og dokumenter, der udarbejdes af en myndighed til brug for sådanne møder.
2) Dokumenter, der udveksles i forbindelse med, at en myndighed udfører sekretariatsopgaver for en anden myndighed.
3) Myndigheders brevveksling med sagkyndige til brug i retssager eller ved overvejelse af, om retssag bør føres.

Stk. 2. Oplysninger vedrørende sagens faktiske omstændigheder, der er af væsentlig betydning for sagens afgørelse, og som alene indeholdes i de i stk. 1 nævnte dokumenter, skal uanset bestemmelsen i stk. 1 meddeles i overensstemmelse med reglerne i dette kapitel.

Undtagelse af oplysninger

§ 15. Retten til aktindsigt kan i øvrigt begrænses, i det omfang partens interesse i at kunne benytte kendskab til sagens dokumenter til varetagelse af sit tarv findes at burde vige for afgørende hensyn til den pågældende selv eller til andre private eller offentlige interesser, herunder

1) statens sikkerhed eller rigets forsvar,
2) rigets udenrigspolitiske eller udenrigsøkonomiske interesser, herunder forholdet til fremmende magter eller mellemfolkelige institutioner,
3) forebyggelse, opklaring og forfølgning af lovovertrædelser, straffuldbyrdelse og lignende samt beskyttelse af sigtede, vidner eller andre i sager om strafferetlig eller disciplinær forfølgning,
4) gennemførelse af offentlig kontrol-, regulerings- eller planlægningsvirksomhed eller af påtænkte foranstaltninger i henhold til skatte- og afgiftslovgivningen, eller
5) det offentliges økonomiske interesser, herunder udførelsen af det offentliges forretningsvirksomhed

Stk. 2. Gør hensyn som nævnt i stk. 1 sig kun gældende for en el af et dokument, skal parten gøres bekendt med dokumentets øvrige indhold.

Afgørelse af sager om aktindsigt

§ 16. Afgørelsen af, om og i hvilken form en begæring om aktindsigt skal imødekommes, træffes af den myndighed, der i øvrigt har afgørelsen af den pågældende sag.

Stk. 2. Myndigheden afgør snarest, om en begæring kan imødekommes. Er begæringen ikke imødekommet eller afslået inden 10 dage efter, at begæringen er modtaget af myndigheden, skal denne underrette parten om grunden hertil samt om, hvornår afgørelsen kan forventes at foreligge.

Stk. 3. Har det betydning for en parts mulighed for at varetage sine interesser at få afskrift eller kopi af sagens dokumenter, skal en begæring herom imødekommes. Dette gælder dog ikke, hvis dokumenternes karakter, antallet af dokumenter eller deres form med afgøren-

de vægt taler herimod. Justitsministeren fastsætter regler om betaling for afskrifter og kopier.

Stk. 4. Afgørelser om aktindsigtsspørgsmål kan påklages særskilt til den myndighed, som er klageinstans i forhold til afgørelsen af den sag, begæringen om aktindsigt vedrører. Bestemmelsen i § 11 gælder tilsvarende.

Stk. 5. Vedkommende minister kan fastsætte regler, der fraviger bestemmelserne i stk. 1 og stk. 4, 1. pkt.

§ 17. Hvor adgangen til at påklage afgørelsen i en sag er tidsbegrænset og begæringen om aktindsigt fremsættes efter, at afgørelsen er meddelt parten, men inden klagefristens udløb, kan myndigheden bestemme, at klagefristen afbrydes. Klagefristen løber i så fald videre fra det tidspunkt, hvor aktindsigt er meddelt parten eller er afslået, dog med mindst 14 dage. Underretning om, hvornår klagefristen herefter udløber, skal samtidig gives til andre klageberettigede, der har fået skriftlig meddelelse om selve afgørelsen.

Aktindsigt i straffesager

§ 18. En part i en straffesag kan, når sagen er afgjort, forlange at blive gjort bekendt med sagens dokumenter i det omfang, dette er rimeligt begrundet af hensyn til varetagelse af den pågældendes interesser, og hensynet til forebyggelse, opklaring og forfølgning af lovovertrædelser eller særlige hensyn til beskyttelse af sigtede, vidner eller andre ikke taler herimod. Bestemmelserne i §§ 12-14 gælder tilsvarende.

Stk. 2. Bestemmelsen i stk. 1 omfatter ikke retsbogsudskrifter vedrørende straffesagen og dokumenter, der har været fremlagt i retten i forbindelse med sagen. Det samme gælder retsbogsudskrifter og i retten fremlagte dokumenter vedrørende andre straffesager, der har været benyttet under sagens behandling.

Stk. 3. Afgørelsen af, om og i hvilken form en begæring om aktindsigt kan imødekommes efter stk. 1, træffes af den myndighed, der har truffet den administrative beslutning i straffesagen. Afgørelsen kan påklages til vedkommende overordnede forvaltningsmyndighed. Justitsministeren fastsætter regler om betaling for afskrifter og kopier.

Kapitel 8
Tavshedspligt
Tavshedspligt

§ 27. Den, der virker inden for den offentlige forvaltning, har tavshedspligt, jfr. borgerlig straffelov § 152 og §§ 152 c-152 f, når en oplysninger ved lov eller anden gyldig bestemmelse er betegnet som fortrolig, eller når det i øvrigt er nødvendigt at hemmeligholde den for at varetage væsentlige hensyn til offentlige eller private interesser, herunder navnlig til:

1) statens sikkerhed eller rigets forsvar,
2) rigets udenrigspolitiske eller udenrigsøkonomiske interesser, herunder forholdes til fremmende magter el-

1er mellemfolkelige institutioner,

3) forebyggelse, efterforskning og forfølgning af lovovertrædelser samt straffuldbyrdelse og beskyttelse af sigtede, vidner eller andre i sager om strafferetlig eller disciplinær forfølgning,
4) gennemførelse af offentlig kontrol-, regulerings- eller planlægningsvirksomhed eller af påtænkte foranstaltninger i henhold til skatte- og afgiftslovgivningen,
5) det offentliges økonomiske interesser, herunder udførelsen af det offentliges forretningsvirksomhed,
6) enkeltepersoners eller private selskabers eller foreningers interesse i at beskytte oplysninger om deres personlige eller interne, herunder økonomiske, forhold, eller
7) enkeltpersoners eller private selskabers eller foreningers økonomiske interesse i at beskytte oplysninger om tekniske indretninger eller fremgangsmåder eller om drifts- eller forretningsforhold.

Stk. 2. Inden for den offentlige forvaltning kan der kun pålægges tavshedspligt med hensyn til en oplysning, når det er nødvendigt at hemmeligholde den for at varetage væsentlige hensyn til bestemte offentlige eller private interesser som nævnt i stk. 1.

Stk. 3. En forvaltningsmyndighed kan bestemme, at en person uden for den offentlige forvaltning har tavshedspligt med hensyn til fortrolige oplysninger, som myndigheden videregiver til den pågældende uden at være forpligtet hertil.

Stk. 4. Fastsættes der i henhold til § 1, stk. 2, regler om tavshedspligt, eller pålægges der tavshedspligt efter stk. 3, finder straffelovens § 152 og §§ 152 c-152 f tilsvarende anvendelse på overtrædelse af sådanne regler eller pålæg.

Videregivelse af oplysninger til en anden forvaltningsmyndighed

§ 28. Oplysninger om enkeltpersoners rent private forhold, herunder oplysninger om race, religion og hudfarve, om politiske, foreningsmæssige, seksuelle og strafbare forhold samt oplysninger om helbredsforhold, væsentlige sociale problemer og misbrug af nydelsesmidler og lignende, må ikke videregives til en anden forvaltningsmyndighed

Stk. 2. Videregivelse af de i stk. 1 nævnte oplysninger kan dog ske, når

1) den, oplysningen angår, har givet samtykke,
2) det følger af lov eller bestemmelser fastsat i henhold til lov, at oplysningen skal videregives,
3) videregivelsen sker til varetagelse af private eller offentlige interesser, der klart overstiger hensynet til de interesser, der begrunder hemmeligholdelse, herunder hensynet til den, oplysningen angår, eller
4) videregivelsen er et nødvendigt led i sagens behandling eller er nødvendig for, at en myndighed kan gennemføre tilsyns eller kontrolopgaver.

Stk. 3. Andre fortrolige oplysninger må ud over de i stk. 2 nævnte tilfælde

kun videregives til en anden forvaltningsmyndighed, når det må antages, at oplysningen vil være af væsentlig betydning for myndighedens virksomhed eller for en afgørelse, myndigheden skal træffe.

Stk. 4. Samtykke efter stk. 2, nr. 1, skal meddeles skriftligt og indeholde oplysning om, hvilken type oplysninger der må videregives, til hvem oplysninger må videregives og til hvilket formål. Kravet om skriftlighed kan dog fraviges, når sagens karakter eller omstændighederne i øvrigt taler derfor.

Stk. 5. Samtykke efter stk. 2, nr. 1, bortfalder senest et år efter det er givet.

Stk. 6. Lokale administrative organer, som ved lov er tillagt en selvstændig kompetence, anses som en selvstændig myndighed efter stk. 1 og 3.

§ 29. I sager, der rejses ved ansøgning, må oplysninger om ansøgerens rent private forhold ikke indhentes fra andre dele af forvaltningen eller fra en anden forvaltningsmyndighed.

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

1) ansøgeren har givet samtykke hertil,
2) andet følger af lov eller bestemmelser fastsat i henhold til lov eller
3) særlige hensyn til ansøgeren eller tredjemand klart overstiger ansøgerens interesse i, at oplysningen ikke indhentes.

§ 30. Fortrolige oplysninger, der udelukkende er indhentet med henblik på statistiske uddrag eller som led i en videnskabelig undersøgelse, må ikke videregives til en forvaltningsmyndighed til anden anvendelse.

§ 31. I det omfang en forvaltningsmyndighed berettiget til at videregive en oplysning, skal myndigheden på begæring af en anden forvaltningsmyndighed videregive oplysningen, hvis den er af betydning for myndighedens virksomhed eller for en afgørelse, som myndigheden skal træffe.

Stk. 2. Bestemmelsen i stk. 1 finder dog ikke anvendelse, hvis videregivelsen påfører myndigheden et merarbejde, der væsentligt overstiger den interesse, den anden myndighed har i at få oplysningerne.

§ 32. Den, der virker inden for den offentlige forvaltning, må ikke i den forbindelse skaffe sig fortrolige oplysninger, som ikke er af betydning for udførelsen af den pågældendes opgaver.

Kapitel

Ikrafttræden, forholdet til anden lovgivning m.v.

§ **33.** Loven træder i kraft den 1. januar 1987. For kommunerne træder reglerne i §§ 19 og 20 samt kapitel 6 dog først i kraft den 1. januar 1989.

§ 34. Bestemmelser i andre love eller bestemmelser fastsat i henhold til lov, som i videre omfang end bestemmelserne i kapitel 2 medfører inhabilitet, opretholdes.

§ 35. Bestemmelserne i lovens kapitel 4 finder anvendelse på dokumenter, der er udfærdiget af en myndighed eller er

kommet i en myndigheds besiddelse den 1. oktober 1964 eller senere. Bestemmelserne i lovens § 18 kommer ikke til anvendelse på straffesager, der er afgjort inden lovens ikrafttræden.

Stk. 2. Oplysninger om faktiske omstændigheder, der indeholdes i dokumenter, der er udfærdiget af en myndighed eller er kommet i en myndigheds besiddelse før den 1. oktober 1964, er dog omfattet af bestemmelserne i kapitel 4, hvis dokumenterne er indgået i en sag, der er eller har været under behandling af en forvaltningsmyndighed efter det nævnte tidspunkt, og oplysningerne er eller har været af væsentlig betydning for sagens afgørelse.

Stk. 3. Bestemmelserne i andre love om parters aktindsigt opretholdes. Dette gælder dog ikke bestemmelser, der i snævrere omfang end denne lovs kapitel 4 giver parten adgang til aktindsigt, medmindre de er trådt i kraft den 1. oktober 1964 eller senere.

§ 36. Bestemmelser i andre love eller bestemmelser fastsat i medfør af lov, som stiller mere omfattende krav til begrundelsens indhold end de, der følger af § 24, opretholdes.

§ 37. Loven gælder ikke for sager om færøske og grønlandske anliggender, men kan ved kgl. anordning sættes i kraft for sådanne sager med de afvigelser, som de særlige færøske og grønlandske forhold tilsiger. Dette gælder dog kun for sager, der er eller har været under behandling af rigsmyndigheder.

Lov om offentlighed i forvaltningen

Kapitel 1

Lovens almindelige anvendelsesområde

§ 1. Loven gælder for al virksomhed, der udøves af den offentlige forvaltning, jf. dog §§ 2 og 3.

Stk. 2. Loven gælder endvidere for

1) elforsyningsvirksomheder, der producerer, transmitterer eller distribuerer elektricitet ved spænding på 500 V eller derover,
2) selskaber, institutioner, foreninger m.v., der driver naturgasforsyningsvirksomhed, og
3) kollektive varmeforsyningsanlæg, som er omfattet af varmeforsyningsloven og har en kapacitet på mere end 10 M J/s.

Stk. 3. Vedkommende minister kan efter forhandling med justitsministeren fastsætte regler om, at loven skal gælde for nærmere angivne selskaber, institutioner, foreninger m.v., som ikke kan henregnes til den offentlige forvaltning. Det gælder dog kun, såfremt udgifterne ved deres virksomhed overvejende dækkes af statslige eller kommunale midler eller i det omfang, de ved eller i henhold til lov har fået tillagt beføjelse til at træffe afgørelser på statens eller en kommunes vegne. Vedkommende minister kan herunder fastsætte nærmere regler om opbevaring m.v. af dokumenter.

§ 2. Loven gælder ikke for sager inden for strafferetsplejen. For sager om ansættelse eller forfremmelse i det offentliges tjeneste gælder kun bestemmelsen i § 6.

Stk. 2. Sager om lovgivning, herunder bevillingslove, er kun omfattet af loven, for så vidt lovforslaget er fremsat for Folketinget.

§ 3. Vedkommende minister kan efter forhandling med justitsministeren fastsætte regler om, at nærmere angivne myndigheder, sagsområder eller arter af dokumenter, for hvilke bestemmelserne i §§ 7-14 i almindelighed vil medføre, at begæring om aktindsigt kan afslås, skal være undtaget fra loven.

Stk. 2. Vedkommende minister kan fastsætte regler om, at der efter et vist åremål skal være ret til at blive gjort bekendt med nærmere angivne dokumenter, der ikke er undergivet retten til aktindsigt efter reglerne i denne lov.

Kapitel 2

Retten til aktindsigt

§ 4. Enhver kan med de undtagelser, der er nævnt i §§ 7-14, forlange at blive gjort bekendt med dokumenter, der er indgået til eller oprettet af en forvaltningsmyndighed som led i administrativ sagsbehandling i forbindelse med dens virksomhed. En forvaltningsmyndighed kan give aktindsigt i videre omfang, medmindre andet følger af regler om tavshedspligt m.v.

Stk. 2. Den, hvis personlige forhold er omtalt i et dokument, kan med de undtagelser, der er nævnt i §§ 7-11 og § 14, forlange at blive gjort bekendt med oplysningerne herom. Det gælder dog ikke i det omfang de hensyn, der er nævnt i § 13 eller hensynet til den pågældende selv eller andre med afgørende vægt taler imod.

Stk. 3. Begæring efter stk. 1 og 2 skal angive de dokumenter eller den sag, som den pågældende ønsker at blive gjort bekendt med.

§ 5. Retten til aktindsigt omfatter

1) alle dokumenter, der vedrører sagen, herunder genpart af de skrivelser, der er udgået fra myndigheden, når skrivelserne må antages at være kommet frem til adressaten, og
2) indførelser i journaler, registre og andre fortegnelser vedrørende den pågældende sags dokumenter.

Stk. 2. Retten til aktindsigt omfatter ikke registre eller andre systematiserede fortegnelser, hvor der gøres brug af elektronisk databehandling, dog bortset fra fortegnelser som nævnt i stk. 1, nr. 2.

Stk. 3. Vedkommende minister kan fastsætte regler om offentlighedens adgang til at blive gjort bekendt med oplysninger i edb-registre m.v., der ikke er omfattet af loven om offentlige myndigheders registre. Der kan herunder fastsættes regler om betaling.

Notatpligt m. v.

§ 6. I sager, hvor der vil blive truffet afgørelse af en forvaltningsmyndighed, skal en myndighed, der mundtligt modtager oplysninger vedrørende en sags faktiske omstændigheder, der er af betydning for sagens afgørelse, eller som på anden måde er bekendt med sådanne oplysninger, gøre notat om indholdet af oplysningerne. Det gælder dog ikke, såfremt oplysningerne i øvrigt fremgår af sagens dokumenter.

Stk. 2. Justitsministeren kan for nærmere angivne områder af forvaltningsvirksomhed fastsætte regler om opbevaring m.v. af meddelelser, der udfærdiges eller modtages ved hjælp af elektronisk databehandling.

Stk. 3. Vedkommende minister kan efter forhandling med justitsministeren fastsætte regler om notatpligt for nærmere angivne grupper af sager om udøvelse af anden forvaltningsvirksomhed end nævnt i stk. 1.

Kapitel 3

Undtagelser fra retten til aktindsigt

Undtagelse af interne arbejdsdokumenter

§ 7. Retten til aktindsigt omfatter ikke en myndigheds interne arbejdsdokumenter. Som interne arbejdsdokumenter anses

1) dokumenter, der udarbejdes af en myndighed til eget brug,
2) brevveksling mellem forskellige enheder inden for samme myndighed og
3) brevveksling mellem en kommunalbestyrelse og dennes udvalg, afdelinger og andre organer eller mellem disse organer indbyrdes.

§ 8. Retten til aktindsigt omfatter, uanset bestemmelsen i § 7, interne arbejdsdokumenter, som foreligger i endelig form, når

1) dokumenterne alene gengiver indholdet af myndighedens endelige beslutning vedrørende en sags afgørelse,
2) dokumenterne alene indeholder en gengivelse af oplysninger, som myndigheden har haft pligt til at notere efter bestemmelsen i § 6,
3) dokumenterne er selvstændige dokumenter, der er udarbejdet af en myndighed for at tilvejebringe bevismæssig eller anden tilsvarende klarhed med hensyn til en sags faktiske omstændigheder, eller
4) dokumenterne indeholder generelle retningslinier for behandlingen af bestemte sagstyper.

§ 9. (Ophævet).

Undtagelse af andre dokumenter

§ 10. Retten til aktindsigt omfatter ikke:

1) Statsrådsprotokoller, referater af møder mellem ministre og dokumenter, der udarbejdes af en myndighed til brug for sådanne møder.
2) Brevveksling mellem ministerier om lovgivning, herunder bevillingslove.
3) Dokumenter, der udveksles i forbindelse med, at en myndighed udfører sekretariatsopgaver for en anden myndighed.
4) Myndigheders brevveksling med sagkyndige til brug i retssager eller ved overvejelse af, om retssag bør føres.
5) Materiale, der tilvejebringes som grundlag for udarbejdelse af offentlig statistik eller videnskabelige undersøgelser.

Meddelelse af faktiske oplysninger

§ 11. Oplysninger i dokumenter, der er omfattet af § 7 og § 10, nr. 1-5, om faktiske omstændigheder, der er af væsentlig betydning for sagsforholdet, skal, uanset disse bestemmelser, meddeles i overensstemmelse med lovens almindelige regler.

Stk. 2. Vedkommende minister kan efter forhandling med justitsministeren fastsætte regler om, at pligten efter stk. 1 ikke skal

gælde nærmere angivne grupper af sager om udøvelse af faktisk forvaltningsvirksomhed.

Undtagelse af oplysninger

§ 12. Retten til aktindsigt omfatter ikke oplysninger om

1) enkeltpersoners private, herunder økonomiske, forhold,
2) tekniske indretninger eller fremgangsmåder eller om drifts- eller forretningsforhold eller lignende, for så vidt det er af væsentlig økonomisk betydning for den person eller virksomhed, oplysningen angår, at begæringen ikke imødekommes.

Stk. 2. Omfattes kun en del af et dokument af bestemmelsen i stk. 1, skal den pågældende gøres bekendt med dokumentets øvrige indhold.

§ 13. Retten til aktindsigt kan begrænses i det omfang, det er nødvendigt til beskyttelse af væsentlige hensyn til

1) statens sikkerhed eller rigets forsvar,
2) rigets udenrigspolitiske eller udenrigsøkonomiske interesser, herunder forholdet til fremmede magter eller mellemfolkelige institutioner,
3) forebyggelse, opklaring og forfølgning af lovovertrædelser, straffuldbyrdelse og lignende samt beskyttelse af sigtede, vidner eller andre i sager om strafferetlig eller disciplinær forfølgning,
4) gennemførelse af offentlig kontrol, regulerings- eller planlægningsvirksomhed eller af påtænkte foranstaltninger i henhold til skatte- og afgiftslovgivningen,
5) det offentliges økonomiske interesser, herunder udførelsen af det offentliges forretningsvirksomhed, eller
6) private og offentlige interesser, hvor hemmeligholdelse efter forholdets særlige karakter er påkrævet.

Stk. 2. Gør hensyn som nævnt i stk. 1 sig kun gældende for en del af et dokument, skal den pågældende gøres bekendt med dokumentets øvrige indhold.

Forholdet til tavshedspligt

§ 14. Pligten til at meddele oplysninger er begrænset af særlige bestemmelser om tavshedspligt fastsat ved lov eller med hjemmel i lov for personer, der virker i offentlig tjeneste eller hverv. Det gælder ikke, for så vidt angår den almindelige tavshedspligt efter straffeloven, forvaltningsloven og tjenestemandslovgivningen.

Kapitel 4

Behandlingen og afgørelsen af begæringer om aktindsigt

§ 15. Fremsættes der begæring om aktindsigt vedrørende dokumenter, der indgår i en sag, hvori der er eller vil blive truffet afgørelse af en forvaltningsmyndighed, af-

gør denne myndighed, om begæringen kan imødekommes. I andre tilfælde afgøres sager om aktindsigt af den myndighed, der har dokumentet i sin besiddelse.
Stk. 2. Afgørelser om aktindsigtsspørgsmål kan påklages særskilt til den myndighed, som er klageinstans i forhold til afgørelsen eller behandlingen i øvrigt af den sag, begæringen om aktindsigt vedrører.
Stk. 3. Vedkommende minister kan fastsætte bestemmelser, der fraviger reglerne i stk. 1 og 2.

§ 16. Vedkommende myndighed afgør snarest, om en begæring kan imødekommes, og om den, der har fremsat begæringen, skal gøres bekendt med dokumenterne ved, at der gives adgang til gennemsyn på stedet, eller ved, at der udleveres en afskrift eller kopi.
Stk. 2. Er en begæring om aktindsigt ikke imødekommet eller afslået inden 10 dage efter, at den er modtaget af vedkommende myndighed, skal myndigheden underrette den begærende om grunden hertil samt om, hvornår en afgørelse kan forventes at foreligge.
Stk. 3. Justitsministeren fastsætter regler om betaling for afskrifter og kopier.

Kapitel 5

Ikrafttræden, forholdet til anden lovgivning m.v.

§ 17. Loven træder i kraft den 1. januar 1987.
Stk. 2. Lov nr. 280 af 10. juni 1970 om offentlighed i forvaltningen ophæves.
Stk. 3. Loven gælder ikke for dokumenter, der er udfærdiget af en myndighed eller er kommet i en myndigheds besiddelse før den 1. januar 1971. Oplysninger om faktiske omstændigheder, der indeholdes i sådanne dokumenter, er dog omfattet af retten til aktindsigt efter reglerne i denne lov, hvis dokumenterne er indgået i en sag, der er eller har været under behandling af en forvaltningsmyndighed efter det nævnte tidspunkt, og oplysningerne er eller har været af betydning for sagen. Bestemmelsen i § 8, nr. 4, gælder for dokumenter, der anvendes efter lovens ikrafttræden. Bestemmelsen i § 9 gælder for sygehusjournaler oprettet efter lovens ikrafttræden og for tilførsler til eksisterende journaler, der er foretaget efter lovens ikrafttræden. Adgangen til aktindsigt efter § 1, stk. 2, gælder ikke for dokumenter, der er udfærdiget af eller er indkommet til de i bestemmelsen nævnte selskaber, institutioner, foreninger m.v. før lovens ikrafttræden.
Stk. 4. Bestemmelser i andre love om adgang til at blive gjort bekendt med dokumenter hos den offentlige forvaltning opretholdes, uanset om de giver ret til aktindsigt i snævrere omfang end denne lov.

§ 18. Loven gælder ikke sager om færøske og grønlandske anliggender. Loven kan ved kgl. anordning sættes i kraft for sådanne sager ved de afvigelser, som de særlige

færøske og grønlandske forhold tilsiger. Dette gælder dog kun sager, der er eller har været under behandling af rigsmyndigheder.

EUROPA-PARLAMENTET OG RÅDETS DIREKTIV 95/46/EF

af 24. oktober 1995

om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger

EUROPA-PARLAMENTET OG RÅDET FOR DEN EUROPÆISKE UNION HAR —

under henvisning til traktaten om oprettelse af Det Europæiske Fællesskab, særlig artikel 100 A,

under henvisning til forslag fra Kommissionen [1],

under henvisning til udtalelse fra Det Økonomiske og Sociale Udvalg [2],

i henhold til fremgangsmåden i traktatens artikel 189 B, stk.3 [3], og

ud fra følgende betragtninger:

(1) Fællesskabets målsætninger, der er nedfældet i traktaten, som ændret ved traktaten om Den Europæiske Union, er at gennemføre en stadig snævrere sammenslutning mellem de europæiske folk, at skabe snævrere forbindelser mellem de stater, som det forener, gennem fælles handling at sikre økonomiske og sociale fremskridt ved at fjerne de skranker, der deler Europa, stadig at forbedre dets folks levevilkår, at bevare og styrke freden og friheden samt at fremme demokratiet på grundlag af de grundlæggende rettigheder, der er anerkendt i medlemsstaternes forfatninger og love, samt i den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder;

(2) databehandlingssystemer er til for menneskets 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;

(3) det indre markeds oprettelse og funktion, som i henhold til traktatens artikel 7 A indebærer fri bevægelighed for varer, personer, tjenesteydelser, og kapital, forudsætter ikke blot, at personoplysninger kan cirkulere frit fra én medlemsstat til en anden, men også, at det enkelte menneskes grundlæggende rettigheder beskyttes;

(4) personoplysninger benyttes stadigt hyppigere inden for de forskellige områder af det økonomiske liv og samfundslivet i Fællesskabet; fremskridtene på det informationsteknologiske område gør det betydeligt nemmere at behandle og udveksle sådanne oplysninger;

(5) den økonomiske og sociale integration, der er en følge af det indre markeds oprettelse og funktion efter traktatens artikel 7 A, vil uvægerligt medføre en kraftig vækst i strømmen af personoplysninger på tværs af landegrænserne mellem alle aktører i medlemsstaternes økonomiske liv og samfundslivet, både inden for den private og den offentlige sektor; udvekslingen af personoplysninger mellem virksomheder i de forskellige medlemsstater kan ikke undgå at tage til i omfang; medlemsstaternes myndigheder vil som led i gennemførelsen af fællesskabsretten skulle samarbejde og udveksle personoplysninger indbyrdes for at kunne varetage deres opgaver og udføre hverv på vegne af en anden medlemsstats myndighed inden for det område uden indre grænser, som det indre marked indebærer;

(6) udbygningen af det teknisk-videnskabelige samarbejde og den koordinerede etablering af nye telekommunikationsnet i Fællesskabet gør det endvidere nødvendigt og nemmere at udveksle personoplysninger på tværs af landegrænserne;

(7) forskellen i den beskyttelse af personers rettigheder og frihedsrettigheder, og navnlig retten til privatlivets fred, som de enkelte medlemsstater yder i forbindelse med behandling af personoplysninger, kan forhindre, at oplysninger af denne art videregives fra én medlemsstats område til en anden medlemsstats område; denne forskel kan derved udgøre en hindring for udøvelsen af en række økonomiske aktiviteter på fællesskabsplan, virke konkurrence-

[1] EFT nr. C 277 af 5. 11. 1990, s. 3, og EFT nr. C 311 af 27. 11. 1992, s. 30.
[2] EFT nr. C 159 af 17. 6. 1991, s. 38.
[3] Europa-Parlamentets udtalelse af 11. 3. 1992 (EFT nr. C 94 af 13. 4. 1992, s. 198), bekræftet den 2. december 1993 (EFT nr. C 342 af 20. 12. 1993, s. 30);
Rådets fælles holdning af 20. 2. 1995 (EFT nr. C 93 af 13. 4. 1995, s. 1) og Europa-Parlamentets afgørelse af 15. 6. 1995 (EFT nr. C 166 af 3. 7. 1995).

fordrejende og hindre de nationale myndigheder i at udføre de opgaver, som påhviler dem i henhold til fællesskabsretten; denne forskel i beskyttelsesniveauet hidrører fra forskellene i de nationale love og administrative bestemmelser;

(8) for at hindringerne for udveksling af personoplysninger kan fjernes, skal beskyttelsen af det enkelte menneskes rettigheder og frihedsrettigheder i forbindelse med behandling af sådanne oplysninger være ensartet i alle medlemsstaterne; denne målsætning er af grundlæggende betydning for det indre marked, men kan ikke realiseres af medlemsstaternes alene, navnlig på grund af omfanget af de nuværende forskelle mellem de nationale love på området, og fordi det er nødvendigt at samordne medlemsstaternes lovgivninger, så udveksling af personoplysninger på tværs af landegrænserne underlægges et samlet regelsæt, der er i overensstemmelse med målsætningen om det indre marked som fastsat i traktatens artikel 7 A; det er derfor nødvendigt, at Fællesskabet tager skridt til at gennemføre en indbyrdes tilnærmelse af lovgivningerne;

(9) med den ensartede beskyttelse, som vil følge af den indbyrdes tilnærmelse af de nationale lovgivninger, vil medlemsstaterne ikke længere under henvisning til det enkelte menneskes rettigheder og frihedsrettigheder, navnlig retten til privatlivest fred, kunne lægge hindringer i vejen for den frie udveksling af personoplysninger medlemsstaterne imellem; medlemsstaterne vil få en manøvremargen, som erhvervslivet og arbejdsmarkedets parter kan benytte sig af i forbindelse med direktivets gennemførelse; de vil således i deres nationale lovgivning kunne fastsætte de generelle betingelser for lovlig behandling af personoplysninger; medlemsstaterne skal derved tilsigte en forbedring af den beskyttelse, som deres nuværende lovgivning sikrer; inden for rammerne af denne manøvremargen og i overensstemmelse med fællesskabsretten kan der forekomme forskelle i gennemførelsen af direktivet, og dette kan få konsekvenser for udvekslingen af oplysninger såvel inden for den enkelte medlemsstat som på fællesskabsplan;

(10) medlemsstaternes lovgivning om behandling af personoplysninger skal sikre overholdelsen af de grundlæggende rettigheder og frihedsrettigheder, navnlig den ret til privatlivets fred, der er fastslået i artikel 8 i den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder og i fællesskabsrettens generelle principper; af denne grund må en indbyrdes tilnærmelse af lovgivningerne ikke medføre en forringelse af den beskyttelse, disse yder, men skal tværtimod have til formål at sikre et højt beskyttelsesniveau overalt i Fællesskabet;

(11) dette direktivs princip om beskyttelse af personers rettigheder og frihedsrettigheder, og navnlig retten til privatlivets fred, er en præcisering og udvidelse af principperne i Europarådets konvention af 28. januar 1981 om beskyttelse af det enkelte menneske i forbindelse med databehandling af personoplysninger;

(12) principperne om beskyttelse skal finde anvendelse på enhver behandling af personoplysninger, foretaget af en person, hvis aktiviteter falder ind under fællesskabsrettens anvendelsesområde; en fysisk persons behandling af oplysninger som led i rent personlige eller familiemæssige aktiviteter som f. eks. korrespondance og føring af en adressefortegnelse, bør dog ikke være omfattet;

(13) aktiviteterne i afsnit V og VI i traktaten om Den Europæiske Union vedrørende offentlig sikkerhed, forsvar, statens sikkerhed og statens aktiviteter på det strafferetlige område hører ikke under fællesskabsrettens anvendelsesområde, uden at dette berører de forpligtelser, der påhviler medlemsstaterne i henhold til traktatens artikel 56, stk. 2, artikel 57 og artikel 100 A; den behandling af personoplysninger, som kræves for at beskytte statens økonomiske interesser, er ikke omfattet af dette direktiv, når behandlingen er forbundet med spørgsmål vedrørende statens sikkerhed;

(14) der gøres for tiden betydelige fremskridt inden for informationssamfundet med hensyn til udvikling af metoder til at registrere, udsende, bearbejde, lagre, opbevare og videresende oplysninger om fysiske personer via lyd og billede, og det er derfor nødvendigt, at dette direktiv finder anvendelse på behandling af sådanne oplysninger;

(15) behandling af sådanne oplysninger er kun omfattet af dette direktiv, hvis den foregår ved hjælp af elektronisk databehandling, eller hvis de pågældende oplysninger er indeholdt i eller skal indgå i et register, der er struktureret efter bestemte kriterier vedrørende personerne for at lette adgangen til de pågældende personoplysninger;

(16) behandling af lyd- og billeddata, som f.eks. i forbindelse med video-overvågning, er ikke omfattet af dette direktiv, hvis den iværksættes med henblik på den offentlige sikkerhed, forsvar, statens sikkerhed eller statens aktiviteter på det strafferetlige område eller andre aktiviteter, der ikke falder ind under fællesskabsretten;

(17) med hensyn til behandling af lyd- og billeddata, der finder sted i journalistisk øjemed eller med

henblik på kunstnerisk eller litterær virksomhed, navnlig på det audiovisuelle omrade, finder direktivets principper begrænset anvendelse i henhold til bestemmelserne i artikel 9;

(18) for at forhindre, at en person unddrages den beskyttelse, der sikres ved dette direktiv, skal enhver behandling af personoplysninger inden for Fællesskabet være i overensstemmelse med lovgivningen i en af medlemsstaterne; med henblik herpå bør enhver behandling af oplysninger være underkastet lovgivningen i den medlemsstat, hvor den registeransvarlige, under hvis myndighed behandlingen udføres, er etableret;

(19) ved etablering på en medlemsstats område forstås faktisk udøvelse af aktiviteter gennem en mere permanent struktur; den pågældende strukturs retlige form, hvad enten det blot er en filial eller et datterselskab med status som juridisk person, har ikke afgørende betydning i denne forbindelse; en registeransvarlig, som er etableret på flere medlemsstaters område, især i form af datterselskaber, skal, navnlig for at undgå omgåelse, sikre sig, at hver enkelt struktur opfylder kravene i den gældende nationale lovgivning;

(20) den omstændighed, at den registeransvarlige er etableret i et tredjeland, må ikke hindre personer i at nyde den beskyttelse, der fastsættes ved dette direktiv; den pågældende behandling bør i så fald underkastes lovgivningen i den medlemsstat, hvor de hjælpemidler, der benyttes til behandlingen, befinder sig, og der bør stilles garanti for, ar de rettigheder og forpligtelser, der følger af dette direktiv, også overholdes;

(21) dette direktiv berører ikke de territorialbestemmelser, der gælder i straffesager;

(22) medlemsstaterne fastsætter i deres lovgivning eller i de bestemmelser i øvrigt, der vedtages til gennemførelse af dette direktiv, nærmere bestemmelser om, på hvilke generelle betingelser en behandling er lovlig; især artikel 5 giver i forbindelse med artikel 7 og 8 medlemsstaterne mulighed for uafhængigt af de generelle regler at fastsætte særlige betingelser for databehandling på specifikke områder og med hensyn til de særlige kategorier af de oplysninger, der omhandles i artikel 8;

(23) medlemsstaterne er bemyndigede til at gennemføre beskyttelsen af personer såvel ved en generel lov om beskyttelse af personer i forbindelse med behandling af personoplysninger som ved særlove, f. eks. for statistikinstitutter;

(24) dette direktiv berører ikke national lovgivning, der beskytter juridiske personer i forbindelse med behandlingen af oplysninger, som vedrører dem;

(25) principperne om beskyttelse skal dels afspejles i de forskellige forpligtelser, der påhviler personer, offentlige myndigheder, virksomheder, organer eller andre databehandlingsansvarlige, navnlig for så vidt angår oplysningernes pålidelighed, den tekniske sikkerhed, anmeldelse til tilsynsmyndigheden og de omstændigheder, hvorunder behandlingen må udføres, og dels i de rettigheder, der tilkommer de personer, hvis personoplysninger gøres til genstand for behandling, bl. a. retten til at blive underrettet om en behandling, til indsigt, til at kunne kræve oplysninger bengtiget, men også til under visse omstændigheder at gøre indsigelse mod en behandling;

(26) beskyttelsesprincipperne skal gælde enhver oplysning om en identificeret eller identificerbar person; for at afgøre, om en person er identificerbar, tages alle de hjælpemidler i betragtning, der med rimelighed kan tænkes bragt.i anvendelse for at identificere den pågældende enten af den registeransvarlige eller af enhver anden person; beskyttelsesprincipperne gælder ikke oplysninger, som er gjort anonyme på en sådan måde, at den registrerede ikke længere kan identificeres; adfærdskodekser i henhold til artikel 27 kan være et nyttigt instrument til at angive måder, hvorpå oplysningerne kan gøres anonyme og opbevares i en sådan form, at den registrerede ikke længere kan identificeres;

(27) fysiske personer skal beskyttes såvel i forbindelse med elektronisk databehandling af oplysninger som i forbindelse med ikke-elektronisk behandling; omfanget af beskyttelsen må i praksis ikke afhænge af de anvendte teknikker, da der ellers vil være alvorlig risiko for omgåelse; for så vidt angår manuel behandling omfatter dette direktiv dog kun registre og ikke sagsmapper, der ikke er strukturerede; navnlig skal indholdet af et register være struktureret efter bestemte kriterier vedrørende personer for at lette adgangen til personoplysningerne; i overensstemmelse med definitionen i artikel 2, litra c), kan de forskellige kriterier, der gør det muligt at bestemme de enkelte dele i en struktureret samling af personoplysninger, samt de forskellige kriterier for adgang til denne samling af

oplysninger defineres af hver enkelt medlemsstat; sagsmapper eller samlinger af sagsmapper eller deres forsider, som ikke er struktureret efter bestemte kriterier, hører under ingen omstændigheder ind under dette direktivs anvendelsesområde;

(28) enhver behandling af personoplysninger skal udføres rimeligt og lovligt i- forhold til de registrerede; oplysninger, der behandles, skal være tilstrækkelige, relevante og nødvendige i forhold til behandlingsformålene; behandlingsformålene skal være udtrykkeligt angivet, legitime og skal fastlægges ved indsamlingen af oplysningerne; behandlingsformål, der fastlægges senere end indsamlingen, må ikke være uforenelige med de oprindeligt angivne formål;

(29) senere behandling af personoplysninger navnlig i historisk, statistisk eller videnskabeligt øjemed er generelt ikke uforenelig med de formål, som den tidligere indsamling af oplysningerne havde, såfremt medlemsstaterne giver de fornødne garantier; disse garantier skal især udelukke, at oplysningerne bliver anvendt til at underbygge foranstaltninger eller afgørelser, der træffes over for en bestemt person;

(30) for at være lovlig skal en behandling af personoplysninger desuden bero på den registreredes samtykke eller være nødvendig med henblik på indgåelse eller opfyldelse af en kontrakt, der har bindende virkning for den registrerede, eller være begrundet i et lovkrav, i udførelsen af opgaver i almenhedens interesse, i udøvelsen af embedsmyndighed eller i en persons legitime interesse, medmindre den registreredes interesser, grundlæggende rettigheder og frihedsrettigheder går forud herfor; med særligt henblik på at tilgodese de involverede interesser ligeligt og samtidig sikre en effektiv konkurrence kan medlemsstaterne fastsætte nærmere bestemmelser om, på hvilke betingelser anvendelse og videregivelse af personoplysninger til tredjemand kan finde sted i forbindelse med legitime aktiviteter udøvet af virksomheder og andre organer som led i den daglige drift; de kan ligeledes fastsætte nærmere bestemmelser om, på hvilke betingelser videregivelse af personoplysninger til tredjemand kan finde sted i forbindelse med markedsføring eller markedsundersøgelser, der udføres af velgørende organisationer eller andre sammenslutninger eller stiftelser, f. eks. af politisk karakter, under overholdelse af bestemmelser, som har til formål at give den registrerede mulighed for uden begrundelse og udgifter at gøre indsigelse mod, at sådanne oplysninger behandles;

(31) behandling af personoplysninger, der har til formål at beskytte et hensyn af fundamental betydning for den registreredes liv, anses ligeledes for lovlig;

(32) medlemsstaterne træffer afgørelse om, hvorvidt den registeransvarlige, der udfører en opgave i samfundets interesse eller henhørende under offentlig myndighedsudøvelse, skal være en offentlig myndighed eller en anden offentligretlig eller privatretlig person, f. eks. en faglig sammenslutning;

(33) oplysninger, som ifølge deres art kan krænke de grundlæggende frihedsrettigheder .eller privatlivets fred, må ikke gøres til genstand for behandling uden den registreredes udtrykkelige samtykke; der skal dog udtrykkeligt gives mulighed for undtagelser fra dette forbud for at imødekomme visse behov, navnlig i sådanne tilfælde, hvor databehandlingen udføres med bestemte sundhedsmæssige formål og af personer, der er underkastet tavshedspligt, eller i forbindelse med visse foreningers eller stifteisers legitime aktiviteter, hvis formål er at sikre udøvelsen af grundlæggende frihedsrettigheder;

(34) når hensynet til vigtige samfundsmæssige interesser berettiger det, skal medlemsstaterne ligeledes kunne fravige forbuddet mod at behandle følsomme kategorier af data på områder som f. eks. folkesundhed og social sikring — navnlig for at sikre kvaliteten og rentabiliteten af de procedurer, der anvendes i forbindelse med ansøgninger om ydelser og tjenester inden for en sygesikringsordning — videnskabelig forskning og offentlig statistik; det påhviler imidlertid medlemsstaterne at sørge for de fornødne specifikke garantier for beskyttelsen af det enkelte menneskes grundlæggende rettigheder og privatliv;

(35) offentlige myndigheders behandling af personoplysninger for officielt anerkendte religiøse sammenslutninger for at opfylde mål, der er fastsat i forfatningsretten eller i folkeretten, udføres af hensyn til vigtige samfundsmæssige interesser;

(36) hvis det i forbindelse med afholdelse af valg i visse medlemsstater er nødvendigt, for at det demokratiske system kan fungere, at politiske partier indsamler oplysninger om enkeltpersoners politiske holdning, kan behandling af sådanne oplysninger tillades af hensyn til varetagelsen af vigtige samfundsmæssige interesser, forudsat, at der fastsættes bestemmelser om de fornødne garantier;

(37) der bør fastsættes undtagelser fra eller begrænsninger af visse bestemmelser i dette direktiv i forbindelse med behandling af personoplysninger i journalistisk øjemed eller med henblik på kunstnerisk eller litterær virksomhed, navnlig på det audiovisuelle område, for så vidt sådanne undtagelser er

nødvendige for at forene det enkelte menneskes grundlæggende rettigheder med ytringsfriheden, herunder retten til at modtage og give oplysninger, som fastslået bl. a. i artikel 10 i den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder; det påhviler derfor medlemsstaterne med henblik på afvejning mellem de grundlæggende rettigheder at fastsætte de nødvendige undtagelser og begrænsninger for så vidt angår de generelle foranstaltninger vedrørende lovligheden af behandling af oplysninger, foranstaltningerne til overførsel af oplysninger til tredjelande samt tilsynsmyndighedernes beføjelser. Dette må dog ikke føre til, at medlemsstaterne fastsætter undtagelser fra de foranstaltninger, der tager sigte på at garantere behandlingssikkerheden. Der bør endvidere gives den kontrolmyndighed, der er ansvarlig for dette område, i det mindste visse efterfølgende beføjelser, som f. eks. beføjelsen til med jævne mellemrum at offentliggøre en rapport eller at indbringe sager for de retslige myndigheder;

(38) en rimelig behandling af oplysninger forudsætter, at de registrerede kan få kendskab til en behandlings eksistens og, når der indsamles oplysninger hos dem, kan få nøjagtig og fyldestgørende oplysninger med hensyn til de nærmere omstændigheder ved indsamlingen;

(39) visse behandlinger vedrører oplysninger, som den ansvarlige ikke har indsamlet direkte hos den registrerede; endvidere kan der berettiget videregives oplysninger til tredjemand, selv om dette ikke var hensigten, da oplysningerne blev indsamlet hos den registrerede; i disse tilfælde skal den pågældende underrettes, når oplysningerne registreres, eller senest når oplysningerne første gang videregives til tredjemand;

(40) det er imidlertid ikke nødvendigt at pålægge en sådan underretningspligt, hvis den registrerede allerede er bekendt med de registrerede oplysninger, eller hvis registreringen eller videregivelsen udtrykkeligt er fastsat i loven, eller hvis det viser sig umuligt eller uforholdsmæssigt vanskeligt at underrette den pågældende, hvilket kan være tilfældet i forbindelse med behandlinger i historisk, statistisk eller videnskabeligt øjemed; i denne forbindelse kan der tages hensyn til antallet af registrerede, oplysningernes alder samt de kompensatoriske foranstaltninger, der kan træffes;

(41) enhver skal have ret til indsigt i de oplysninger om sig selv, som gøres til genstand for behandling, så den pågældende kan forvisse sig om oplysningernes rigtighed og behandlingens lovlighed; af samme årsag skal enhver have ret til at kende den logik, der ligger bag edb-behandlingen af oplysningerne om sig selv, i det mindste i forbindelse med edb-baserede afgørelser, som omhandlet i artikel 15, stk. 1; denne ret ma ikke krænke forretningshemmeligheden eller den intellektuelle ejendomsret, navnlig den ophavsret, som programmerne er beskyttet af; dette ma dog ikke resultere i, at den registrerede nægtes alle oplysninger;

(42) medlemsstaterne kan af hensyn til den registreredes interesser eller med henblik på at beskytte andres rettigheder og frihedsrettigheder begrænse retten til indsigt og til underretning; de kan f. eks. fastsætte, at adgang til medicinske oplysninger kun kan finde sted via en person, der udøver en profession inden for sundhedsvæsenet;

(43) medlemsstaterne kan ligeledes indskrænke retten til indsigt og underretning samt visse af den registeransvarliges forpligtelser, såfremt dette er nødvendigt af hensyn til statens sikkerhed, forsvaret, den offentlige sikkerhed eller væsentlige økonomiske og finansielle interesser i medlemsstaten eller Unionen samt efterforskning og retsforfølgning i straffesager eller i forbindelse med brud på etiske regler for lovregulerede erhverv; undtagelser og begrænsninger bør omfatte kontrol-, tilsyns- og reguleringsopgaver, der er nødvendige på de tre sidstnævnte områder vedrørende den offentlige sikkerhed, de økonomiske og finansielle interesser og retsforfølgning i straffesager; dette berører ikke det berettigede i undtagelser og begrænsninger af hensyn til statens sikkerhed eller forsvaret;

(44) medlemsstaterne kan i medfør af fællesskabsrettens bestemmelser blive nødt til at fravige bestemmelserne i dette direktiv vedrørende indsigt, underretning af de registrerede og oplysningernes kvalitet for at sikre visse af ovenstående mål;

(45) hvor behandling af personoplysninger kan foregå fuldt lovligt i almenvellets interesse, af hensyn til offentlig myndighedsudøvelse eller i en persons legitime interesse, bør enhver ikke desto mindre være berettiget til, hvis han på grund af egne særlige forhold har tungtvejende og legitime grunde hertil, at gøre indsigelse mod, at oplysningerne om ham selv gøres til genstand for behandling; medlemsstaterne har imidlertid mulighed for at vedtage nationale bestemmelser om det modsatte;

(46) beskyttelsen af de registreredes rettigheder og frihedsrettigheder i forbindelse med behandling af personoplysninger forudsætter, at der træffes de

fornødne tekniske og organisatoriske foranstaltninger bade under selve udfonningen og under iværksættelsen af en behandling, navnlig for at varetage sikkerheden og derved forhindre enhver form for ubeføjet behandling; det påhviler medlemsstaterne at sørge for, at de registeransvarlige overholder disse foranstaltninger; disse foranstaltninger skal under hensyn til det aktuelle tekniske niveau og de omkostninger, som er forbundet med deres iværksættelse, tilvejebringe et tilstrækkeligt sikkerhedsniveau i forhold til de risici, som behandlingen indebærer, og arten af de oplysninger, der skal beskyttes;

(47) når en meddelelse, der indeholder personoplysninger, fremsendes via en telekommunikations- eller elektronisk posttjeneste, hvis eneste formål er at sende meddelelser af denne type, er det den person, som er ophavsmand til meddelelsen, og ikke den person, der tilbyder tjenesten, der normalt vil blive betragtet som ansvarlig for behandlingen af de personoplysninger, der er indeholdt i meddelelsen; de personer, som udbyder disse tjenester, vil dog normalt blive betragtet som ansvarlige for behandlingen af de supplerende personoplysninger, der er nødvendige for tjenestens udførelse;

(48) anmeldelsesprocedurerne tager sigte på at gøre en behandlings formål samt dens vigtigste karakteristika offentlig kendt med henblik på kontrol af behandlingens overholdelse af de nationale bestemmelser, der vedtages til gennemførelse af dette direktiv;

(49) for at undgå overflødige administrative formaliteter kan medlemsstaterne fastsætte fritagelser for og lempelser af anmeldelsespligten for behandlinger, der ikke vil kunne krænke de registreredes rettigheder og frihedsrettigheder, og som er i overensstemmelse med en retsakt, der er udstedt af en medlemsstat, og som fastsætter begrænsningerne herfor; medlemsstaten kan ligeledes give mulighed for forenklet anmeldelse eller fritagelse for anmeldelse, hvor en person med ansvar for databeskyttelse, der udpeges af den registeransvarlige, har kunnet fastslå, at den foretagne behandling ikke vil kunne krænke de registreredes rettigheder og frihedsrettigheder; den person, der har ansvar for databeskyttelse, skal, uanset om han er ansat hos den registeransvarlige eller ej, være i stand til at udøve sit hverv i fuld uafhængighed;

(50) der kan fastsættes fritagelse for anmeldelse eller forenklet anmeldelse i forbindelse med behandlinger, hvis eneste formål er at føre registre, som er udarbejdet i henhold til national ret med henblik på at stille oplysninger til rådighed for offentligheden eller for personer, der kan godtgøre en legitim interesse heri;

(51) den omstændighed, at den registeransvarlige er omfattet af den forenklede anmeldelsespligt eller fritaget for anmeldelsespligt, fritager ikke den registeransvarlige for de øvrige forpligtelser, der følger af dette direktiv;

(52) efterfølgende kontrol fra myndighedernes side skal i den forbindelse generelt betragtes som tilstrækkelig;

(53) dog vil visse behandlinger på grund af deres art, omfang eller formål kunne indebære en særlig risiko for at krænke de registreredes rettigheder og frihedsrettigheder, f. eks. behandlinger, der har til formål at udelukke den registrerede fra at udøve en ret, modtagen en ydelse eller opnå en kontrakt, eller som indebærer anvendelse af ny teknologi; medlemsstaterne må, hvis de ønsker det, præcisere denne risiko i deres lovgivning;

(54) i forhold til alle de behandlinger, der iværksættes i samfundet, skulle det antal behandlinger, der indebærer en særlig risiko, være meget begrænset; medlemsstaterne skal fastsætte bestemmelser om, at tilsynsmyndigheden eller den person, der har ansvar for databeskyttelse, i samråd med tilsynsmyndigheden skal foretage en kontrol af disse behandlinger, inden de iværksættes; tilsynsmyndigheden kan, efter at kontrollen er foretaget, og i overensstemmelse med den nationale lovgivning udtale sig om eller give tilladelse til den pågældende behandling; den forudgående kontrol kan også foretages som led i udarbejdelsen af en lov, der vedtages af det nationale parlament, eller af en anden foranstaltning med hjemmel i en sådan lov, som fastlægger karakteren af behandlingen og fastsætter de fornødne garantier;

(55) krænker den registeransvarlige en registrerets rettigheder, skal der i medlemsstaternes lovgivning gives adgang til at indbringe sagen for en retsinstans; personer, som lider skade som følge af en ulovlig behandling, skal have ret til erstatning fra den registeransvarlige; denne kan fritages for erstatningsansvar, hvis det bevises, at han ikke er skyld i den forvoldte skade, navnlig hvis der kan henvises til en fejl fra den registreredes side eller et tilfælde af force majeure; der skal iværksættes sanktioner over for såvel privatretlige som offentlige personer, der overtræder nationale bestemmelser vedtaget med henblik på gennemførelsen af dette direktiv;

(56) strømmen af personoplysninger på tværs af landegrænserne er nødvendig af hensyn til udbygningen af den internationale samhandel; den beskyttelse, der ved dette direktiv garanteres personer inden for Fællesskabet, er ikke til hinder for, at der videregi-

ves personoplysninger til tredjelande, for så vidt disse sikrer er tilstrækkeligt beskyttelsesniveau; vurderingen af, om beskyttelsesniveauet i et tredjeland er tilstrækkeligt, skal foretages på grundlag af samtlige de forhold, der har indflydelse på en videregivelse eller en type videregivelse af oplysninger;

(57) hvis et tredjeland derimod ikke sikrer et tilstrækkeligt beskyttelsesniveau, skal videregivelse af personoplysninger til det pågældende land forbydes;

(58) der skal dog kunne undtages fra dette forbud under bestemte omstændigheder, hvor den registrerede har meddelt sit samtykke, hvor videregivelsen er nødvendig i forbindelse med en kontrakt eller en retssag, hvor beskyttelsen af væsentlige samfundsinteresser kræver det, f. eks. ved international udveksling af oplysninger mellem skatte- eller toldforvaltninger eller mellem socialsikringsmyndigheder, eller hvor videregivelsen sker fra et register, der er oprettet ved lov, og som offentligheden eller personer med en legitim interesse heri skal kunne konsultere; en sådan videregivelse bør ikke omfatte alle oplysningerne eller hele kategorier af oplysninger i dette register; når et register er beregnet til at blive konsulteret af personer, der har en legitim interesse heri, bør videregivelse kun ske på anmodning af disse personer, eller hvis de selv er modtageren;

(59) der kan træffes særlige foranstaltninger til at afhjælpe et utilstrækkeligt beskyttelsesniveau i et tredjeland, hvis den registeransvarlige stiller de fornødne garantier; endvidere skal der fastsættes bestemmelser om forhandlingsprocedurer mellem Fællesskabet og de pågældende tredjelande;

(60) videregivelse til tredjelande må under alle omstændigheder kun finde sted under fuld overholdelse af de bestemmelser, som medlemsstaterne vedtager i medfør af dette direktiv, særlig artikel 8;

(61) medlemsstaterne og Kommissionen skal inden for deres respektive kompetenceområder opfordre de berørte erhvervskredse til at udarbejde adfærdskodekser med henblik på, under hensyn til de særlige former for behandling, der udføres i bestemte sektorer, at fremme iværksættelsen af dette direktiv under overholdelse af de bestemmelser, medlemsstaterne har truffet til gennemførelse deraf;

(62) oprettelsen af en uafhængig tilsynsmyndighed i hver medlemsstat, har afgørende betydning for beskyttelsen af fysiske personer i forbindelse med behandling af personoplysninger;

(63) denne myndighed skal tildeles de fornødne beføjelser til at varetage denne opgave, herunder undersøgelses- og interventionsbeføjelser, navnlig nar det drejer sig om klager, samt beføjelse til at indbringe sager for en retsinstans; myndigheden skal bidrage til at tilvejebringe gennemsigtighed i de databehandlinger, der udføres i den medlemsstat, hvorunder den hører;

(64) tilsynsmyndighederne i de enkelte medlemsstater skal yde hinanden bistand i forbindelse med varetagelsen af deres opgaver for at sikre, at beskyttelsesreglerne overholdes fuldt ud overalt i Den Europæiske Union;

(65) der skal på fællesskabsplan nedsættes en arbejdsgruppe om beskyttelse af personer i forbindelse med behandling af personoplysninger; gruppen skal være fuldt uafhængig i udøvelsen af sine funktioner; i kraft af denne uafhængighed skal den rådgive Kommissionen og navnlig bidrage til, at de nationale regler, der vedtages til gennemførelse af dette direktiv, anvendes ensartet;

(66) for så vidt angår videregivelse af oplysninger til tredjelande, er det nødvendigt at tillægge Kommissionen beføjelse til at udstede gennemførelsesbestemmelser og indføre en procedure i henhold til retningslinjerne i Rådets afgørelse nr. 87/373/EØF [1] for at kunne anvende dette direktiv;

(67) Europa-Parlamentet, Rådet og Kommissionen nåede den 20. december 1994 til enighed om en modus vivendi vedrørende gennemførelsesforanstaltningerne til retsakter vedtaget efter fremgangsmåden i artikel 189 B i EF-traktaten;

(68) de principper om beskyttelse af personers rettigheder og frihedsrettigheder, og navnlig retten til privatlivets fred, i forbindelse med behandling af personoplysninger, som opstilles i dette direktiv, vil for visse sektorers vedkommende kunne suppleres med eller præciseres i særregler, der skal være i overensstemmelse med disse principper;

(69) der bør gives medlemsstaterne en frist på højst tre år regnet fra datoen for ikrafttrædelsen af de nationale foranstaltninger, der træffes til gennemførelse af dette direktiv, for at de gradvis kan bringe de nye nationale bestemmelser i anvendelse på samtlige behandlinger, der allerede er iværksat; af hensyn til en omkostningsbevidst gennemførelse

[1] EFT nr. L 197 af 18. 7. 1987, s. 33.

indrømmes der medlemsstaterne en yderligere periode, der udløber tolv år efter datoen for vedtagelsen af dette direktiv, til at sikre, at eksisterende ikke-elektromske registre bringes i overensstemmelse med visse af direktivets bestemmelser; data, der er indeholdt i disse registre, og som behandles manuelt i denne udvidede overgangsperiode, skal dog på det tidspunkt, hvor de er genstand for en sådan yderligere behandling, være bragt i overensstemmelse med disse bestemmelser;

(70) den registrerede skal ikke på ny give sit samtykke, for at den registeransvarlige efter ikrafttrædelsen af de nationale bestemmelser i forbindelse med gennemførelsen af dette direktiv kan fortsætte behandlingen af følsomme oplysninger, når denne er nødvendig for udførelsen af en kontrakt, der er indgået på grundlag af frit og informeret samtykke inden ikrafttrædelsen af ovennævnte bestemmelser;

(71) dette direktiv er ikke til hinder for, at en medlemsstat vedtager regler for markedsføring, der henvender sig til forbrugere, der er bosiddende på dens område, for så vidt sådanne regler ikke berører beskyttelsen af personer i forbindelse med behandlingen af personoplysninger;

(72) dette direktiv giver mulighed for, at der i gennemførelsen af dets bestemmelser kan tages hensyn til princippet om aktindsigt i offentlige dokumenter —

UDSTEDT FØLGENDE DIREKTIV:

KAPITEL I

ALMINDELIGE BESTEMMELSER

Artikel 1

Direktivets formål

1. Medlemsstaterne sikrer i overensstemmelse med dette direktiv beskyttelsen af fysiske personers grundlæggende rettigheder og frihedsrettigheder, især retten til privatlivets fred, i forbindelse med behandling af personoplysninger.

2. Medlemsstaterne må ikke af grunde, der har forbindelse med den i stk. 1 foreskrevne beskyttelse, indskrænke eller forbyde fri udveksling af personoplysninger mellem medlemsstaterne.

Artikel 2

Definitioner

I dette direktiv forstås ved:

a) »personoplysninger« enhver form for information om en identificeret eller identificerbar fysisk person (»den registrerede«); ved identificerbar person forstås en person, der direkte eller indirekte kan identificeres, bl. a. ved et identifikationsnummer eller et eller flere elementer, der er særlige for denne persons fysiske, fysiologiske, psykiske, økonomiske, kulturelle eller sociale identitet

b) »behandling af personoplysninger« (»behandling«) enhver operation eller række af operationer — med eller uden brug af elektronisk databehandling — som personoplysninger gøres til genstand for, f. eks. indsamling, registrering, systematisering, opbevaring, tilpasning eller ændring, selektion, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring samt blokering, slettelse eller tilintetgørelse

»register med personoplysninger« (»register«) enhver struktureret samling af personoplysninger, der er tilgængelige efter bestemte kriterier, hvad enten denne samling er placeret centralt, decentralt eller er fordelt på et funktionsbestemt eller geografisk grundlag

d) »den registeransvarlige« 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 personoplysninger; er formålet med og hjælpemidlerne ved behandlingen fastlagt ved nationale love eller forskrifter eller på fællesskabsplan, kan den registeransvarlige, eller de specifikke kriterier for udpegelse af denne, angives i den pågældende nationale ret eller i fællesskabsretten

»registerfører« den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der behandler personoplysninger på den registeransvarliges vegne

i) »tredjemand« enhver anden fysisk eller juridisk person, offentlig myndighed, institution eller ethvert andet organ end den registrerede, den registeransvarlige, registerføreren og de personer under den registeransvarliges eller registerførerens direkte myndighed, der er beføjet til at behandle oplysningerne

g) »modtager« den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, hvortil oplysningerne meddeles, uanset om der er tale om en tredjemand; myndigheder, som vil kunne få meddelt oplysninger som led i en isoleret forespørgsel, betragtes ikke som modtagere

h) »den registreredes samtykke« enhver frivillig, specifik og informeret viljetilkendegivelse, hvorved den registrerede indvilliger i, at personoplysninger, der vedrører den pågældende selv, gøres til genstand for behandling.

Artikel 3

Anvendelsesområde

1. Dette direktivs bestemmelser anvendes på behandling af personoplysninger, der helt eller delvis foretages ved hjælp af edb, samt på ikke-elektronisk behandling af personoplysninger, der er eller vil blive indeholdt i et register.

2. Dette direktiv gælder ikke for sådan behandling af personoplysninger,

— som iværksættes med henblik på udøvelse af aktiviteter, der ikke er omfattet af fællesskabsretten, som f. eks. de aktiviteter, der er fastsat i afsnit V og VI i traktaten om Den Europæiske Union, og under ingen omstændigheder for behandling, der vedrører den offentlige sikkerhed, forsvar, statens sikkerhed (herunder statens økonomiske interesser, når behandlingen er forbundet med spørgsmål vedrørende statens sikkerhed) og statens aktiviteter på det strafferetlige område

— som foretages af en fysisk person med henblik på udøvelse af rent personlige eller familiemæssige aktiviteter.

Artikel 4

Gældende national ret

1. Medlemsstaterne anvender de nationale bestemmelser, de vedtager til gennemførelse af dette direktiv, på behandling af personoplysninger:

a) der foretages som led i en virksomheds eller et organs aktiviteter inden for den medlemsstats område, hvor den registeransvarlige er etableret; en registeransvarlig, som er etableret på flere medlemsstaters område, skal træffe de nødvendige foranstaltninger til at sikre, at hver af disse virksomheder eller organer opfylder kravene i den gældende nationale lovgivning

b) der foretages af en registeransvarlig, der ikke er etableret på den pågældende medlemsstats område, men på et sted, hvor dens nationale lovgivning gælder i henhold til folkeretten

c) der foretages af en registeransvarlig, der ikke er etableret på Fællesskabets område, og som med henblik på behandling af personoplysninger anvender midler, det være sig elektroniske eller ikke-elektroniske, som befinder sig på den pågældende medlemsstats område, medmindre disse midler kun benyttes med henblik på forsendelse gennem Det Europæiske Fællesskabs område.

2. I det i stk. 1, litra c), omhandlede tilfælde udpeger den registeransvarlige en repræsentant, der er etableret på den pågældende medlemsstats område, uden at dette i øvrigt berører eventuelle retslige skridt mod den registeransvarlige selv.

KAPITEL II

ALMINDELIGE BETINGELSER FOR LOVLIG BEHANDLING AF PERSONOPLYSNINGER

Artikel 5

Medlemsstaterne præciserer i henhold til bestemmelserne i dette kapitel, på hvilke betingelser behandling af personoplysninger er lovlig.

AFDELING I

PRINCIPPER VEDRØRENDE OPLYSNINGERNES PALIDELIGHED

Artikel 6

1. Medlemsstaterne fastsætter bestemmelser om, at personoplysninger

a) skal behandles rimeligt og lovligt

b) skal indsamles til udtrykkeligt angivne og legitime formål, samt at senere behandling heraf ikke må være uforenelig med disse formål; senere behandling af oplysninger i historisk, statistisk eller videnskabeligt øjemed anses ikke for at være uforenelig med disse formål, såfremt medlemsstaterne giver de fornødne garantier

c) skal være relevante og tilstrækkelige og ikke omfatte mere end, hvad der kræves til opfyldelse af de formål, hvortil de indsamles, og til de formål, hvortil de senere behandles

d) skal være korrekte og om nødvendigt ajourførte; der skal tages ethvert rimeligt skridt til at slette eller berigtige oplysninger, der er urigtige eller ufuldstændige i forhold til det formål, hvortil de indsamles, eller i forbindelse med hvilke de behandles på et senere tidspunkt

e) ikke må opbevares på en måde, der giver mulighed for at identificere de registrerede i et længere tidsrum end det, der er nødvendigt af hensyn til de formål, hvortil de indsamles, eller i forbindelse med hvilke de behandles på et senere tidspunkt. Medlemsstaterne fastsætter de fornødne garantier for personoplysninger, der i historisk, statistisk eller videnskabeligt øjemed opbevares længere end i ovennævnte periode.

2. Det påhviler den registeransvarlige at sikre, at bestemmelserne i stk. 1 overholdes.

AFDELING II

PRINCIPPER VEDRØRENDE GRUNDLAGET FOR BEHANDLING AF OPLYSNINGER

Artikel 7

Medlemsstaterne fastsætter bestemmelser om, at behandling af personoplysninger kun må finde sted hvis:

a) der ikke hersker tvivl om, at den registrerede har givet sit samrykke, eller

b) behandlingen er nødvendig af hensyn til opfyldelsen af en kontrakt, som den registrerede er part i, eller af hensyn til gennemførelse af foranstaltninger, der træffes på dennes anmodning forud for indgåelsen af en sådan kontrakt, eller

c) behandlingen er nødvendig for at overholde en retlig forpligtelse, som gælder for den registeransvarlige, eller

d) behandlingen er nødvendig for at beskytte den registreredes vitale interesser, eller

e) behandlingen er nødvendig af hensyn til udførelsen af en opgave i samfundets interesse eller henhørende under offentlig myndighedsudøvelse, som den registeransvarlige eller en tredjemand, til hvem oplysningerne videregives, har fået pålagt, eller

f) behandlingen er nødvendig, for at den registeransvarlige eller den tredjemand eller de tredjemænd, til hvem oplysningerne videregives, kan forfølge en legitim interesse, medmindre den registreredes interesser eller de grundlæggende rettigheder og frihedsrettigheder, der skal beskyttes i henhold til artikel 1, stk. 1, i dette direktiv, går forud herfor.

AFDELING III

SÆRLIGE KATEGORIER AF BEHANDLINGER

Artikel 8

Behandlinger, der vedrører særlige kategorier af oplysninger

1. Medlemsstaterne forbyder behandling af personoplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssigt tilhørsforhold og oplysninger om helbredsforhold og seksuelle forhold.

2. Stk. 1 finder ikke anvendelse, hvis

a) den registrerede udtrykkeligt har givet sit samrykke til en sådan behandling, medmindre det i medlemsstatens lovgivning fastsættes, at det i stk. 1 omhandlede forbud ikke kan hæves ved den registreredes samtykke, eller

b) behandlingen er nødvendig for overholdelsen af den registeransvarliges arbejdsretlige forpligtelser og specifikke rettigheder, for så vidt den er tilladt ifølge nationale lovbestemmelser, som fastsætter de fornødne garantier, eller

c) behandlingen er nødvendig for at beskytte den registreredes eller en anden persons vitale interesser i tilfælde, hvor den pågældende ikke fysisk eller juridisk er i stand til at give sit samtykke, eller

d) behandlingen foretages af en stiftelse, en forening eller et andet almennyttigt organ, hvis sigte er af politisk, filosofisk, religiøs eller faglig art, som led i organets legitime aktiviteter og med de fornødne garantier, på betingelse af, at behandlingen alene vedrører organets medlemmer eller personer, der på grund af organets

formål er i regelmæssig kontrakt hermed, og at oplysningerne ikke videregives til tredjemand uden den registreredes samtykke, eller

e) behandlingen vedrører oplysninger, som klart offentliggøres af den registrerede, eller er nødvendig for, at et retskrav kan fastlægges, gøres gældende eller forsåvidt som de er nødvendige for at forene rerten til privatlivets fred med reglerne for ytringsfrihed.

3. Stk. 1 finder ikke anvendelse, hvis behandlingen af oplysningerne er nødvendig med henblik på forebyggende medicin, medicinsk diagnose, sygepleje eller patientbehandling eller forvaltning af læge- og sundhedstjenester, og hvis behandlingen af disse oplysninger foretages af en erhvervsudøvende i sundhedssektoren, der i henhold til den nationale lovgivning eller til regler, der er fastsat af kompetente nationale organer, har tavshedspligt, eller af en anden person med tilsvarende tavshedspligt.

4. Med forbehold af, at der gives tilstrækkelige garantier, kan medlemsstaterne af grunde, der vedrører hensynet til vigtige samfundsmæssige interesser, fastsætte andre undtagelser end dem, der er nævnt i stk. 2, enten ved national lovgivning eller ved en afgørelse truffet af tilsynsmyndigheden.

5. Behandling af oplysninger om lovovertrædelser, straffedomme eller sikkerhedsforanstaltninger må kun foretages under kontrol af en offentlig myndighed, eller hvis der gælder tilstrækkelige, specifikke garantier i medfør af den nationale lovgivning med forbehold af de undtagelser, som medlemsstaten kan fastsætte på grundlag af nationale lovbestemmelser, hvorefter der gives tilstrækkelige, specifikke garantier. Et fuldstændigt register over straffedomme må dog kun føres under kontrol af en offentlig myndighed.

Medlemsstaterne kan fastsætte bestemmelser om, at behandling af oplysninger vedrørende administrative sanktioner eller civile retssager ligeledes skal foretages under en offentlig myndigheds kontrol.

6. Undtagelser fra stk. 1 som omhandlet i stk. 4 og 5 meddeles til Kommissionen.

7. Medlemsstaterne bestemmer, på hvilke betingelser et nationalt identifikationsnummer eller andre almene midler til identifikation kan gøres til genstand for behandling.

Artikel 9

Behandling af personoplysninger og ytringsfriheden

Medlemsstaterne fastsætter i forbindelse med behandling af personoplysninger, der udelukkende finder sted i journalistisk øjemed eller med henblik på kunstnerisk eller litterær virksomhed, kun fritagelser eller undtagelser fra bestemmelserne i dette kapitel og i kapitel IV og VI, for

AFDELING IV

OPLYSNINGSPLIGT OVER FOR DEN REGISTRERERE

Artikel 10

Oplysningspligt **ved** indsamling af oplysninger hos den registrerede

Medlemsstaterne fastsætter bestemmelser om, at den registeransvarlige eller dennes repræsentant skal give den person, hos og om hvem der indsamles oplysninger, mindst følgende informationer, medmindre den pågældende allerede er bekendt hermed, og for så vidt som disse yderligere informationer, under hensyn til de særlige omstændigheder hvorunder oplysningerne indsamles, er nødvendige for at sikre den registrerede en rimelig behandling af oplysningerne:

a) den registeransvarliges og eventuelt dennes repræsentants identitet

b) formålene med den behandling, hvortil oplysningerne er bestemt

c) alle yderligere informationer som f. eks.

— modtagerne eller kategorierne af modtagere

— om det er obligatorisk eller frivilligt at besvare spørgsmålene samt mulige følger af ikke at svare

— hvorvidt der gives ret til at få indsigt i og foretage berigtigelse af de oplysninger, der vedrører den registrerede.

Artikel 11

Oplysningspligt, når oplysningerne ikke er indsamlet hos den registrerede

1. Når oplysningerne ikke er indsamlet hos-den registrerede, fastsætter medlemsstaterne bestemmelser om, at den registeransvarlige eller dennes repræsentant allerede ved registreringen af oplysningerne, eller senest når oplysningerne første gang videregives til tredjemand, skal give den reigstrerede mindst følgende informationer, medmindre den pågældende allerede er bekendt hermed, og for så vidt som disse yderligere informationer, under hensyn til de særlige omstændigheder hvorunder oplysningerne indsamles, er nødvendige for at sikre den registrerede en rimelig behandling af oplysningerne:

a) den registeransvarliges og eventuelt dennes repræsentants identitet

b) formålene med behandlingen

c) alle yderligere informationer som f. eks.

— hvilken type oplysninger det drejer sig om

— modtagerne eller kategorierne af modtagere

— hvorvidt der gives ret til at få indsigt i og foretage berigtigelse af de oplysninger, der vedrører den registrerede.

2. Bestemmelserne i stk. 1 finder ikke anvendelse, navnlig ikke når behandlingen foretages i statistisk øjemed eller til historiske eller videnskabelige forskningsformål, hvis underretning af den registrerede viser sig umulig eller er uforholdsmæssig vanskelig, eller registreringen eller videregivelsen af oplysningerne er udtrykkeligt fastsat ved lov. I sådanne tilfælde fastsætter medlemsstaterne de fornødne garantier.

AFDELING V

DEN REGISTREREDES RET TIL INDSIGT

Artikel 12

Ret til indsigt

Medlemsstaterne sikrer enhver registreret ret til hos den registeransvarlige

a) frit og uhindret, med rimelige mellemrum og uden større ventetid eller større udgifter

— at få oplyst, om der behandles personoplysninger om den pågældende selv, samt mindst formålene med behandlingen, hvilken rype oplysninger dot drejer sig om, og modtagerne eller kategorierne af modtagere af oplysningerne

— at få meddelt letforståelig information om, hvilke oplysninger der er omfattet af behandlingerne, samt enhver tilgængelig information om, hvorfra disse oplysninger stammer

— at få at vide, hvilken logik der ligger bag edb-behandlingen af oplysningerne om den pågældende, i det mindste i forbindelse med edb-baserede afgørelser som omhandlet i artikel 15, stk. 1

b) efter omstændighederne at få oplysninger, som ikke er blevet behandlet i overensstemmelse med dette direktiv, berigtiget, slettet eller blokeret, navnlig hvis de er ufuldstændige eller urigtige

c) at få udvirket, at tredjemand, til hvem sådanne oplysninger er blevet videregivet, underrettes om enhver berigtigelse, sletning eller blokering, der er foretaget i overensstemmelse med litra b), medmindre underretning viser sig umulig eller er uforholdsmæssig vanske-**lig-**

AFDELING VI

UNDTAGELSER OG BEGRÆNSNINGER

Artikel 13

Undtagelser og begrænsninger

1. Medlemsstaterne kan træffe lovmæssige foranstaltninger med henblik på at begrænse rækkevidden af de forpligtelser og rettigheder, der er omhandlet i artikel 6, stk. 1, artikel 10, artikel 11, stk. 1, samt artikel 12 og 21, hvis en sådan begrænsning er en nødvendig foranstaltning af hensyn til:

a) statens sikkerhed

b) forsvaret

c) den offentlige sikkerhed

d) forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager eller i forbindelse med brud på etiske regler for lovregulerede erhverv

e) væsentlige økonomiske eller finansielle interesser hos en medlemsstat eller Den Europæiske Union, herunder valuta-, budget- og skatteanliggender

f) en kontrol-, tilsyns- eller reguleringsopgave, selv af midlertidig karakter, der er et led i den offentlige myndighedsudøvelse på de i litra c), d) og e) nævnte områder

g) beskyttelsen af den registreredes interesser eller andres rettigheder og frihedsrettigheder.

2. Medlemsstaterne kan med forbehold af de fornødne lovhjemlede garantier, navnlig for at oplysningerne ikke anvendes til at træffe foranstaltninger eller afgørelser vedrørende bestemte personer, i tilfælde, hvor der klart ikke er nogen risiko for, at den registreredes ret til privatlivets fred krænkes, ved lov begrænse de i artikel 12 omhandlede rettigheder, hvis oplysningerne udelukkende behandles med videnskabelig forskning for øje eller kun opbevares i form af personopylsninger i det tidsrum, som kræves for at udarbejde statistikker.

AFDELING VII

DEN REGISTREREDES INDSIGELSESRET

Artikel 14

Den registreredes indsigelsesret

Medlemsstaterne indrømmer den registrerede ret til

a) i det mindste i de i artikel 7, litra e) og f), omhandlede tilfælde af vægtige legitime grunde, der vedrører den pågældendes særlige situation, til enhver tid at gøre indsigelse mod, at personoplysninger om ham

selv gøres til genstand for behandling, medmindre andet er bestemt i den nationale lovgivning; i tilfælde af berettiget indsigelse må den af den registeransvarlige iværksatte behandling ikke længere omfatte de pågældende oplysninger

b) efter anmodning og uden udgifter at modsætte sig en behandling af personoplysninger, der vedrører den pågældende, og som den registeransvarlige agter at foretage med henblik på markedsføring, eller at blive underrettet, inden personoplysningerne første gang videregives til tredjemand eller anvendes på tredjemands vegne med henblik på markedsføring, og udtrykkelig få tilbud om uden udgifter at gøre indsigelse mod en sådan videregivelse eller anvendelse.

Medlemsstaterne træffer de nødvendige foranstaltninger til at sikre, at de registrerede er bekendt med den i litra b), første afsnit, omhandlede ret.

Artikel 15

Edb-behandlede individuelle afgørelser

1. Medlemsstaterne indrømmer enhver person ret til ikke at være undergivet afgørelser, der har retsvirkning for ham, eller som berører ham i væsentlig grad, og som alene er truffet på grundlag af edb-behandling af oplysninger, der er bestemt til at vurdere bestemte personlige forhold, såsom erhvervsevne, kreditværdighed, pålidelighed, adfærd osv.

2. Uden at dette berører de øvrige bestemmelser i dette direktiv, fastsætter medlemsstaterne bestemmelser om, at en person kan undergives en afgørelse af den art, der er omhandlet i stk. 1, når:

a) den pågældende afgørelse træffes som led i indgåelsen eller opfyldelsen af en kontrakt, såfremt den registreredes anmodning om indgåelse eller opfyldelse af kontrakten er blevet efterkommet, eller der findes passende foranstaltninger til at beskytte den registreredes legitime interesser, som f. eks. mulighed for denne til at gøre sit synspunkt gældende, eller når

b) den pågældende afgørelse er hjemlet i en lov, **der** indeholder bestemmelser til beskyttelse af den registreredes legitime interesser.

AFDELING VIII

FORTROLIGHED OG BEHANDLINGSSIKKERHED

Artikel 16

Behandlingernes fortrolige karakter

Enhver, der udfører arbejde under den registeransvarlige eller registerføreren, herunder registerføreren selv, og som far adgang til personoplysninger, ma kun behandle disse efter instruks fra den registeransvarlige, bortset fra tilfælde der er fastsat i lovgivningen.

Artikel 17

Behandlingssikkerhed

1. Medlemsstaterne fastsætter bestemmelser om, at den registeransvarlige skal iværksætte de fornødne tekniske og organisatoriske foranstaltninger til at beskytte personoplysninger mod hændelig eller ulovlig tilintetgørelse, mod hændeligt tab, mod forringelse, ubeføjet udbredelse eller ikke-autoriseret adgang, navnlig hvis behandlingen omfatter fremsendelser af oplysninger i et net, samt mod enhver anden form for ulovlig behandling.

Disse foranstaltninger skal under hensyn til det aktuelle tekniske niveau og de omkostninger, som er forbundet med deres iværksættelse, tilvejebringe et tilstrækkeligt sikkerhedsniveau i forhold til de risici, som behandlingen indebærer, og arten af de oplysninger, som skal beskyttes.

2. Medlemsstaterne fastsætter bestemmelser om, at den registeransvarlige, hvis oplysninger behandles for dennes regning, skal vælge en registerfører, som frembyder den fornødne garanti med hensyn til de tekniske sikkerhedsforanstaltninger og organisatoriske foranstaltninger, der skal træffes, og skal påse, at disse foranstaltninger overholdes.

3. Gennemførelse af en behandling ved en registerfører skai ske i henhold til en kontrakt eller et andet retligt bindende dokument mellem registerføreren og den registeransvarlige, hvori det navnlig fastsættes

— at registerføreren alene handler efter instruks fra den registeransvarlige

— at forpligtelserne i henhold til stk. 1, som fastlagt i lovgivningen i den medlemsstat, hvor registerføreren er etableret, ligeledes påhviler denne.

4. Med henblik på opbevaring af beviserne skal de dele i kontrakten eller det retlige dokument, der vedrører beskyttelse af oplysninger, og de krav, der vedrører de i stk. 1 omhandlede foranstaltninger, foreligge skriftligt eller i en anden tilsvarende form.

AFDELING IX

ANMELDELSE

Artikel 18

Anmeldesespligt over for tilsynsmyndigheden

1. Medlemsstaterne **fastsætter** bestemmelser om, at den registeransvarlige eller dennes eventuelle repræsentant

forud for iværksættelsen af en behandling, der helt eller delvis udføres ved brug af elektronisk databehandling, eller en række sådanne behandlinger, hvis formål er identiske eller indbyrdes relaterede, skal foretage anmeldelse til den i artikel 28 omhandlede tilsynsmyndighed.

2. Medlemsstaterne må kun give mulighed for forenklet anmeldelse eller fritagelse for anmeldelse i følgende tilfælde og på følgende betingelser:

— medlemsstaterne anfører for de ryper behandling, hvor det i betragtning af de behandlede oplysninger ikke er sandsynligt, at de registreredes rettigheder eller frihedsrettigheder krænkes, behandlingens formål, hvilke oplysninger eller typer oplysninger der behandles, hvilke registrerede eller kategorier af registrerede der er tale om, til hvilke modtagere eller kategorier af modtagere oplysningerne videregives, samt hvor længe oplysningerne opbevares, og/eller

— de registeransvarlige udpeger i overensstemmelse med den nationale lovgivning, som de er underlagt, en person med ansvar for beskyttelse af personoplysninger, som bl. a. har til opgave

  — i fuld uafhængighed at sikre den interne anvendelse af de nationale bestemmelser, der er truffet i medfør af direktivet

  — at føre et register over. de behandlinger, der gennemføres af den registeransvarlige, og som omfatter de i artikel 21, stk. 2, omhandlede oplysninger

  for på denne måde at sikre, at det er ikke sandsynligt, at de registreredes rettigheder og frihedsrettigheder vil kunne krænkes som følge af behandlingen.

3. Medlemsstaterne kan fastsætte, at stk. 1 ikke finder anvendelse på behandlinger, hvis eneste formål er at føre et register, der ifølge love eller administrative bestemmelser er beregnet til at informere offentligheden, og som er tilgængeligt for offentligheden generelt eller for personer, der kan godtgøre at have en legitim interesse heri.

4. Medlemsstaterne kan fritage de behandlinger, der er omhandlet i artikel 8, stk. 2, litra d), for anmeldelsespligt eller fastsætte en forenklet anmeldelse.

5. Medlemsstaterne kan bestemme, at ikke-elektroniske behandlinger af personoplysninger eller nogle af disse behandlinger skal anmeldes, eller foreskrive forenklet anmeldelse af sådanne behandlinger.

Artikel 19

Anmeldelsens indhold

1. Medlemsstaterne præciserer, hvilke oplysninger anmeldelsen skal indeholde. Anmeldelsen skal mindst indeholde følgende oplysninger:

a) navn og adresse på den registeransvarlige og dennes eventuelle repræsentant

b) behandlingens formål

c) en beskrivelse af kategorien eller kategorierne af registrerede og af de oplysninger eller ryper af oplysninger, der vedrører dem

d) de modtagere eller kategorier af modtagere, som oplysningerne kan videregives

e) påtænkte overførsler af oplysninger til tredjelande

f) en generel beskrivelse, der giver mulighed for foreløbigt at vurdere, om foranstaltningerne med henblik på behandlingssikkerheden i henhold til artikel 17 er passende.

2. Medlemsstaterne præciserer, efter hvilke procedurer ændringer i de i stk. 1 omhandlede oplysninger skal anmeldes til tilsynsmyndigheden.

Artikel 20

Forudgående kontrol

1. Medlemsstaterne præciserer, hvilke behandlinger der kan indebære særlige risici for personers rettigheder og frihedsrettigheder, og sikrer, at disse behandlinger kontrolleres, inden de iværksættes.

2. En sådan forudgående kontrol foretages af tilsynsmyndigheden efter modtagelsen af anmeldelsen fra den registeransvarlige, eller den foretages af den person, der har ansvar for databeskyttelse, som i tvivlstilfælde skal høre tilsynsmyndigheden.

3. Medlemsstaterne kan også gennemføre en sådan kontrol som led i udarbejdelsen af en foranstaltning, der vedtages af det nationale parlament, eller af en anden foranstaltning med hjemmel i en sådan lov, som fastlægger karakteren af behandlingen og fastsætter de fornødne garantier.

Artikel 21

Behandlingernes offentlige tilgængelighed

1. Medlemsstaterne træffer foranstaltninger til at sikre, at behandlingerne er offentligt tilgængelige.

2. Medlemsstaterne fastsætter bestemmelser om, at tilsynsmyndigheden fører et register over de behandlinger, der er anmeldt i henhold til artikel 18.

Registret omfatter mindst de oplysninger, der er anført i artikel 19, stk. 1, litra a)-e).

Registret er offentligt tilgængeligt.

3. For så vidt angår behandlinger, som ikke er omfattet af anmeldelsespligt, fastsætter medlemsstaterne bestemmelser om, at de registeransvarlige eller enhver anden myndighed, som medlemsstaterne udpeger, på passende måde mindst skal stille de i artikel 19, stk. 1, litra a)-e), omhandlede oplysninger til rådighed for enhver person, der anmoder herom.

Medlemsstaterne kan fastsætte, at denne bestemmelse ikke finder anvendelse på behandlinger, hvis eneste formål er at føre et register, der ifølge love eller administrative bestemmelser er beregnet til at informere offentligheden, og som er tilgængeligt for offentligheden generelt eller for personer, der kan godtgøre at have en legitim interesse heri.

KAPITEL III

RETSMIDLER, ANSVAR OG SANKTIONER

Artikel 22

Klageadgang

Uden at foregribe muligheden for at iværksætte administrativ klage, herunder for den tilsynsmyndighed, der er nævnt i artikel 28, inden forelæggelse for retsinstanser, fastsætter medlemsstaterne bestemmelser om, at enhver har ret til for en domstol at indbringe en klage over krænkelser af de rettigheder, der garanteres i henhold til de nationale love, der gælder for den pågældende behandling.

Artikel 23

Ansvar

1. Medlemsstaterne fastsætter bestemmelser om, at enhver, som har lidt skade som følge af en ulovlig behandling eller enhver anden handling, der er uforenelig med de nationale bestemmelser, der vedtages til gennemførelse af dette direktiv, har ret til erstatning for den forvoldte skade fra den registeransvarlige.

2. Den registeransvarlige kan helt eller delvis fritages for erstatningsansvar for skade, hvis han beviser, at han ikke er skyld i den begivenhed, der medførte skaden.

Artikel 24

Sanktioner

Medlemsstaterne træffer de nødvendige foranstaltninger til at sikre, at dette direktiv gennemføres i fuldt omfang, og de fastsætter bl. a. de sanktioner, der skal finde anvendelse i tilfælde af overtrædelse af de bestemmelser, der vedtages til dette direktivs gennemførelse.

KAPITEL IV

VIDEREGIVELSE AF PERSONOPLYSNINGER TIL TREDJELANDE

Artikel 25

incipp r

1. Medlemsstaterne fastsætter bestemmelser om, at videregivelse til et tredjeland af personoplysninger, der gøres til genstand for behandling, eller som skal gøres til genstand for behandling efter videregivelsen, kun må finde sted, hvis det pågældende tredjeland sikrer et tilstrækkeligt beskyttelsesniveau, og forudsat at de nationale bestemmelser, der vedtages til gennemførelse af direktivets øvrige bestemmelser, overholdes.

2. Vurderingen af, om beskyttelsesniveauet i et tredjeland er tilstrækkeligt, sker på grundlag af samtlige de forhold, der har indflydelse på en videregivelse eller en type videregivelse af oplysninger; til grund for vurderin-

gen lægges navnlig oplysningernes art, den eller de påtænkte behandlingers formål og varighed, oprindelseslandet og det endelige bestemmelsesland, de retsregler — almindelige regler eller sektorregler — der er i kraft i det pågældende tredjeland, samt de regler for god forretningsskik og de sikkerhedsforanstaltninger, der gælder i landet.

3. Medlemsstaterne og Kommissionen underretter gensidigt hinanden, hvis de mener, at et tredjeland ikke sikrer et tilstrækkeligt beskyttelsesniveau i overensstemmelse med stk. 2.

4. Konstaterer Kommissionen efter proceduren i artikel 31, stk. 2, at et tredjeland ikke sikrer et tilstrækkeligt beskyttelsesniveau i overensstemmelse med denne artikels stk. 2, træffer medlemsstaterne de foranstaltninger, der er nødvendige for at hindre enhver videregivelse af oplysninger af samme art til det pågældende tredjeland.

5. Kommissionen indleder på det rette tidspunkt forhandlinger med henblik på at afhjælpe den situation, der opstår som følge af en konstatering efter stk. 4.

6. Kommissionen kan efter proceduren i artikel 31, stk. 2, fastslå, at et tredjeland sikrer et tilstrækkeligt beskyttelsesniveau i overensstemmelse med denne artikels stk. 2, pa grundlag af dets nationale lovgivning eller dets internationale forpligtelser med henblik på at beskytte privatlivet og personers grundlæggende rettigheder og frihedsrettigheder, herunder de forpligtelser, der er indgået efter de i stk. 5 nævnte forhandlinger.

Medlemsstaterne træffer de foranstaltninger, der er nødvendige for at efterkomme Kommissionens afgørelse.

Artikel 26

Undtagelser

1. Som undtagelse fra bestemmelserne i artikel 25, fastsætter medlemsstaterne, medmindre andet er bestemt i deres nationale lovgivning, at videregivelse eller en type videregivelse af personoplysninger til et tredjeland, der ikke sikrer et tilstrækkeligt beskyttelsesniveau i overensstemmelse med artikel 25, stk. 2, kan finde sted, hvis

a) der ikke hersker tvivl om, at den registrerede har givet sit samtykke, eller

b) videregivelsen er nødvendig af hensyn til opfyldelsen af en kontrakt mellem den registrerede og den registeransvarlige eller af hensyn til gennemførelse af foranstakninger, der træffes på den registreredes anmodning forud for indgåelse af en sådan kontrakt, eller

c) videregivelsen er nødvendig af hensyn til indgåelsen eller udførelsen af en kontrakt, der i den registreredes interesse er indgået mellem den registeransvarlige og tredjemand, eller

d) videregivelsen er nødvendig eller følger af lov eller bestemmelser fastsat med hjemmel i lov for at beskytte en vigtig samfundsinteresse eller for, at et retskrav kan fastlægges, gøres gældende eller forsvares, eller

videregivelsen er nødvendig for at beskytte den registreredes vitale interesser, eller

videregivelsen finder sted fra et offentligt register, der ifølge love eller administrative bestemmelser er beregnet til at informere offentligheden, og som er tilgængeligt for offentligheden generelt eller for personer, der kan godtgøre at have en legitim interesse heri, i det omfang de ved lov fastsatte betingelser for offentlig tilgængelighed er opfyldt i det specifikke tilfælde.

2. Med forbehold af stk. 1, kan en medlemsstat give tilladelse til videregivelse eller en type videregivelse af personoplysninger til et tredjeland, der ikke sikrer et tilstrækkeligt beskyttelsesniveau i overensstemmelse med artikel 25, stk. 2, hvis den registeransvarlige yder tilstrækkelige garantier for beskyttelse af privatlivets fred, personers grundlæggende rettigheder og frihedsrettigheder samt for udøvelsen af de dertil knyttede rettigheder; sådanne garantier kan især fremgå af passende kontraktbestemmelser.

3. Den pågældende medlemsstat underretter Kommissionen og de øvrige medlemsstater om de tilladelser, den giver i henhold til stk. 2.

Rejses der indsigelse herimod fra en anden medlemsstat eller Kommissionen, og er denne berettiget ud fra hensynet til beskyttelse af privatlivets fred eller personers grundlæggende rettigheder og frihedsrettigheder, vedtager Kommissionen passende foranstaltninger efter proceduren i artikel 31, stk. 2.

Medlemsstaterne træffer de foranstaltninger, der er nødvendige for at efterkomme Kommissionens afgørelse.

4. Fastslår Kommissionen efter proceduren i artikel 31, stk. 2, at visse standardkontraktbestemmelser frembyder tilstrækkelige garantier i henhold til stk. 2, træffer medlemsstaterne de foranstaltninger, der er nødvendige for at efterkomme Kommissionens afgørelse.

KAPITEL V

ADFÆRDSKODEKSER

Artikel 27

1. Medlemsstaterne og Kommissionen tilskynder til udarbejdelsen af adfærdskodekser, der afhængigt af de særlige forhold i de forskellige sektorer skal bidrage til en korrekt anvendelse af de nationale bestemmelser, medlemsstaterne vedtager til gennemførelse af dette direktiv.

2. Medlemsstaterne fastsætter bestemmelser om, at de brancheforeninger eller andre organer, som repræsenterer andre kategorier af registeransvarlige, som har udarbejdet udkast til nationale adfærdskodekser, eller som agter at ændre eller forlænge gældende nationale kodekser, skal kunne forelægge dem for den nationale myndighed til udtalelse.

Medlemsstaterne fastsætter bestemmelser om, at denne myndighed bl. a. skal kontrollere, at de udkast, den får forelagt, er i overensstemmelse med de nationale bestemmelser, der vedtages til gennemførelse af dette direktiv. Hvis myndigheden finder det hensigtsmæssigt, kan den indhente bemærkninger fra de registrerede eller disses repræsentanter.

3. Udkast til EF-kodeks og forslag til ændring eller forlængelse af eksisterende EF-kodekser kan forelægges den i artikel 29 omhandlede gruppe. Denne udtaler sig bl. a. om, hvorvidt de udkast, den har fået forelagt, er i overensstemmelse med de nationale bestemmelser til gennemførelse af dette direktiv. Hvis den finder det nødvendigt, indhenter den bemærkninger fra de registrerede eller disses repræsentanter. Kommissionen kan tilse, at de kodekser, som gruppen har godkendt, offentliggøres på passende vis.

KAPITEL VI

TILSYNSMYNDIGHED SAMT GRUPPE TIL BESKYTTELSE AF PERSONER I FORBINDELSE MED BEHANDLING AF PERSONOPLYSNINGER

Artikel 28

Tilsynsmyndighed

1. Hver medlemsstat drager omsorg for, at der udpeges en eller flere offentlige myndigheder, der har til opgave på dens område at påse overholdelsen af de bestemmelser, medlemsstaten vedtager til gennemførelse af dette direktiv.

Disse myndigheder udøver fuld uafhængighed de funktioner, der tillægges dem.

2. Hver medlemsstat drager omsorg for, at tilsynsmyndighederne høres ved udarbejdelsen af administrative foranstaltninger eller retsforskrifter om beskyttelse af personers rettigheder og frihedsrettigheder i forbindelse med behandling af personoplysninger.

3. Hver tilsynsmyndighed skal bl. a. kunne:

iværksætte undersøgelser og bl. a. have adgang til de oplysninger, der gøres til genstand for en behandling, og til at indsamle alle oplysninger, der er nødvendige for at varetage dens tilsynsopgaver

gribe effektivt ind ved f. eks. at afgive udtalelser forud for iværksættelsen af behandlingerne i henhold til artikel 20 og sikre en passende offentliggørelse af disse udtalelser, at beordre oplysninger blokeret, slettet eller tilintetgjort, midlertidigt eller definitivt at forbyde en behandling, at udstede en advarsel til den registeransvarlige eller påtale en overtrædelse over for den registeransvarlige eller ved at høre parlamenter eller andre nationale politiske institutioner

indbringe overtrædelser af de nationale bestemmelser, som vedtages til gennemførelse af dette direktiv, for retsinstanserne eller gøre retsinstanserne opmærksom på disse overtrædelser.

Afgørelser truffet af tilsynsmyndigheden, som går en involveret part imod, kan indbringes for en retsinstans.

4. Enhver kan, eventuelt repræsenteret ved en sammenslutning, til tilsynsmyndigheden indgive en anmodning om beskyttelse af sine rettigheder og frihedsrettigheder i forbindelse med behandling af personoplysninger. Den pågældende underrettes om, hvorledes sagen følges op.

Enhver kan til tilsynsmyndigheden især indgive en anmodning om at få kontrolleret en behandlings lovlighed, når de nationale bestemmelser, der er truffet i henhold til artikel 13 i dette direktiv, finder anvendelse. Den pågældende underrettes i alle tilfælde om, at der er blevet foretaget en kontrol.

5. Hver tilsynsmyndighed udarbejder med regelmæssige mellemrum en rapport om sin virksomhed. Denne rapport offentliggøres.

6. Den enkelte tilsynsmyndighed er, uanset hvilken national lov der måtte gælde for den pågældende behandling, kompetent til på sin medlemsstats område at udøve de beføjelser, der tillægges den i overensstemmelse med stk. 3 i denne artikel. Myndigheden kan blive anmodet om at udøve sine beføjelser af en myndighed i en anden medlemsstat.

Tilsynsmyndighederne samarbejder med hinanden i det omfang, det er nødvendigt for at opfylde deres pligter, navnlig ved at udveksle alle nyttige oplysninger.

7. Medlemsstaterne fastsætter bestemmelser i deres lovgivning om, at tilsynsmyndighedernes medlemmer og ansatte også efter deres aktiviteters ophør har tavshedspligt for så vidt angår de fortrolige oplysninger, de har adgang til.

Artikel 29

Gruppe vedrørende beskyttelse af personer i forbindelse med behandling af personoplysninger

1. Der nedsættes en gruppe vedrørende beskyttelse af personer i forbindelse med behandling af personoplysninger, i det følgende benævnt »gruppen«.

Denne gruppe er rådgivende og uafhængig.

2. Gruppen består af en repræsentant for den eller de tilsynsmyndigheder, hver medlemsstat har udpeget, og af en repræsentant for den eller de myndigheder, der er oprettet for fællesskabsinstitutionerne og -organerne, samt af en repræsentant for Kommissionen.

Hvert medlem af gruppen udpeges af den institution eller den eller de myndigheder, det repræsenterer. Når en medlemsstat har udpeget flere tilsynsmyndigheder, udnævner disse en fælles repræsentant. Det samme gælder de myndigheder, der er oprettet for fællesskabsinstitutionerne og -organerne.

3. Gruppen træffer sine afgørelser med simpelt flertal blandt repræsentanterne for tilsynsmyndighederne.

4. Gruppen vælger selv sin formand. Formandens mandat gælder for en penode af to år. Mandatet kan fornyes.

5. Gruppens sektretariatsopgaver varetages af Kommissionen.

6. Gruppen fastsætter selv sin forretningsorden.

7. Gruppen behandler de spørgsmål, der sættes pd dagsordenen af dens formand, enten på dennes initiativ, efter anmodning fra en repræsentant for tilsynsmyndighederne eller efter anmodning fra Kommissionen.

Artikel 30

1. Gruppen har til opgave:

a) at undersøge ethvert spørgsmål vedrørende anvendelse af de nationale bestemmelser, der vedtages til gennemførelse af dette direktiv, med henblik på at bidrage til en ensartet anvendelse heraf

b) at give Kommissionen en udtalelse om beskyttelsesniveauet i Fællesskabet og i tredjelande

c) at rådgive Kommissionen om ethvert udkast til ændring af dette direktiv og om, hvilke supplerende eller specifikke foranstaltninger der bør træffes for at sikre fysiske personers rettigheder og frihedsrettigheder for så vidt angår behandling af personoplysninger, samt om ethvert andet udkast til fællesskabsforanstaltninger, der har indvirkning på sådanne rettigheder og frihedsrettigheder

d) at afgive udtalelse om de adfærdskodekser, der udarbejdes på fællesskabsplan.

2. Konstaterer gruppen forskelle mellem medlemsstaternes lovgivning eller praksis, der kan være til fare for en ensartet beskyttelse af personer i forbindelse med behandling af personoplysninger inden for Fællesskabet, underretter den Kommissionen herom.

3. Gruppen kan på eget initiativ fremsætte henstillinger om ethvert spørgsmål vedrørende beskyttelsen af personer i forbindelse med behandling af personoplysninger inden for Fællesskabet.

4. Gruppens udtalelser og henstillinger forelægges for Kommissionen og for det i artikel 31 omhandlede udvalg.

5. Kommissionen underretter gruppen om, hvorledes den har taget hensyn til dens udtalelser og henstillinger. Kommissionen udarbejder med henblik herpå en beret-

ning, som også forelægges for Europa-Parlarnentet og Rådet. Denne beretning offentliggøres.

6. Gruppen udarbe|der en årsberetning om situationen vedrørende beskyttelsen af fysiske personer i forbindelse med behandling af personoplysninger inden for Fællesskabet og i tredjelande; den forelægger beretningen for Europa-Parlamentet. Rådet og Kommissionen. Beretningen offentliggøres.

KAPITEL VII

EF-GENNEMFØRELSESFORANSTALTNINGER

Artikel 31

Udvalget

1. Kommissionen bistås af et udvalg, der består af repræsentanter for medlemsstaternes regeringer, og som har Kommissionens repræsentant som formand.

2. Kommissionens repræsentant forelægger udvalget et udkast til de foranstaltninger, der skal træffes. Udvalget afgiver en udtalelse om dette udkast inden for en frist, som formanden kan fastsætte under hensyn til, hvor meget det pågældende spørgsmål haster.

Udtalelsen afgives med det flertal, som er fastsat i traktatens artikel 148, stk. 2. Ved afstemninger i udvalget tildeles medlemsstaternes stemmer den vægt, som er fastsat i nævnte artikel. Formanden deltager ikke i afstemningen.

Kommissionen vedtager foranstaltninger, der straks finder anvendelse. Hvis de ikke er i overensstemmelse med den afgivne udtalelse, underrettes Rådet dog straks af Kommissionen om disse foranstaltninger. I så fald gælder følgende:

— Kommissionen udsætter gennemførelsen af de foranstaltninger, den har truffet afgørelse om, i et tidsrum pa tre måneder regnet fra datoen for underretningen

— Rådet kan med kvalificeret flertal træffe en anden afgørelse inden for det tidsrum, der er nævnt i ovenstående led.

AFSLUTTENDE BESTEMMELSER

Artikel 32

1. Medlemsstaterne sætter de nødvendige love og administrative bestemmelser i kraft for at efterkomme dette direktiv senest tre år efter dets vedtagelse.

Når medlemsstaterne vedtager disse love og administrative bestemmelser, skal de indeholde en henvisning til dette direktiv, eller de skal ved offentliggørelsen ledsages at en sådan henvisning. De nærmere regler for denne henvisning fastsættes af medlemsstaterne.

2. Medlemsstaterne påser, at behandlinger, der allerede er iværksat på ikrafttrædelsesdatoen for de nationale bestemmelser, der vedtages til gennemførelse af dette direktiv, bringes i overensstemmelse med disse bestemmelser senest tre år efter denne dato. Som en undtagelse fra foregående afsnit kan medlemsstaterne fastsætte, at behandlingen af oplysninger, som allerede findes i manuelle registre, der føres på ikrafttrædelsesdatoen for de nationale bestemmelser, der vedtages til gennemførelse af dette direktiv, senest tolv år efter vedtagelsen af direktivet skal bringes i overensstemmelse med direktivets artikel 6, 7 og 8. Medlemsstaterne indrømmer dog den registrerede ret til efter anmodning og navnlig i forbindelse med udøvelse af retten til indsigt at få berigtiget, slettet eller blokeret oplysninger, der er ufuldstændige eller urigtige, eller som opbevares på en måde, der er uforenelig med de legitime formål, som den registeransvarlige forfølger.

3. Som en undtagelse fra stk. 2 kan medlemsstaterne, hvis der gives passende garantier, fastsætte, at oplysninger, der kun opbevares med henblik på historisk

forskning, ikke skal bringes i overensstemmelse med artikel 6, 7 og 8 i dette direktiv.

4. Medlemsstaterne meddeler Kommissionen teksten til de nationale retsforskrifter, som de udsteder på det område, der er omfattet af dette direktiv.

Artikel 33

Kommissionen forelægger med jævne mellemrum, første gang senest tre år efter det i artikel 32, stk. 1, nævnte tidspunkt, Europa-Parlamentet og Rådet en beretning om anvendelsen af dette direktiv, eventuelt ledsaget af passende ændringsforslag. Beretningen offentliggøres.

Kommissionen undersøger navnlig direktivets anvendelse på behandling af lyd og billeddata om fysiske personer og forelægger passende forslag, der matte være nødvendige i betragtning af udviklingen inden for informationsteknologien og informationssamfundet.

Artikel 34

Dette direktiv er rettet til medlemsstaterne.

Udfærdiget i Luxembourg, den 24. oktober 1995.

For Europa-Parlamentet	*For Rådet*
K. HÄNSCH	L. ATIENZA SERNA
Formand	*Formand*

DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 24 October 1995

on the protection of individuals with regard to the processing of personal data and on the free movement of such data

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treat)' establishing the European Community, and in particular Article 100a thereof,

Having regard to the proposal from the Commission (1),

Having regard to the opinion of the Economic and Social Committee (2),

Acting in accordance with the procedure referred to in Article 189b of the Treaty (3),

(1) Whereas the objectives of the Community, as laid down in the Treaty, as amended by the Treaty on European Union, include creating an ever closer union among the peoples of Europe, fostering closer relations between the States belonging to the Community, ensuring economic and social progress by common action to eliminate the barriers which divide Europe, encouraging the constant improvement of the living conditions of its peoples, preserving and strengthening peace and liberty and promoting democracy on the basis of the fundamental rights recognized in the constitution and laws of the Member States and in the European Convention for the Protection of Human Rights and Fundamental Freedoms;

(2) Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals;

(3) Whereas the establishment and functioning of an internal market in which, in accordance with Article 7a of the Treaty, the free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded;

(4) Whereas increasingly frequent recourse is being had in the Community to the processing of personal data in the various spheres of economic and social activity; whereas the progress made in information technology is making the processing and exchange of such data considerably easier;

(5) Whereas the economic and social integration resulting from the establishment and functioning of the internal market within the meaning of Article 7a of the Treaty will necessarily lead to a substantial increase in cross-border flows of personal data between all those involved in a private or public capacity in economic and social activity in the Member States; whereas the exchange of personal data between undertakings in different Member States is set to increase; whereas the national authorities in the various Member States are being called upon by virtue of Community law to collaborate and exchange personal data so as to be able to perform their dunes or carry out tasks on behalf of an authority in another Member State within the context of the area without internal frontiers as constituted by the internal market;

(6) Whereas, furthermore, the increase in scientific and technical cooperation and the coordinated introduction of new telecommunications networks in the Community necessitate and facilitate cross-border flows of personal data;

(7) Whereas the difference in levels of protection of the rights and freedoms of individuals, notably the right to privacy, with regard to the processing of personal data afforded in the Member States may prevent the transmission of such data from the territory of one Member State to that of another Member State; whereas this difference may therefore constitute an obstacle to the pursuit of a number of economic activities at Community level,

(1) OJ No C 277, 5. 11. 1990, p. 3 and OJ No C 311, 27. 11. 1992, p. 30.
(2) OJ No C 159, 17. 6. 1991, p 38.
(3) Opinion of the European Parliament of 11 March 1992 (OJ No C 94, 13. 4. 1992, p. 198), confirmed on 2 December 1993 (OJ No C 342, 20. 12. 1993, p. 30); Council common position of 20 February 1995 (OJ No C 93, 13. 4. 1995, p. 1) and Decision of the European Parliament of 15 June 1995 (OJ No C 166, 3. 7. 1995).

distort competition and impede authorities in the discharge of their responsibilities under Community law; whereas this difference in levels of protection is due to the existence of a wide variety of national laws, regulations and administrative provisions;

(8) Whereas, in order to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data must be equivalent in all Member States; whereas this objective is vital to the internal market but cannot be achieved by the Member States alone, especially in view of the scale of the divergences which currently exist between the relevant laws in the Member States and the need to coordinate the laws of the Member States so as to ensure that the cross-border flow of personal data is regulated in a consistent manner that is in keeping with the objective of the internal market as provided for in Article 7a of the Treaty; whereas Community action to approximate those laws is therefore needed;

(9) Whereas, given the equivalent protection resulting from the approximation of national laws, the Member States will no longer be able to inhibit the free movement between them of personal data on grounds relating to protection of the rights and freedoms of individuals, and in particular the right to privacy; whereas Member States will be left a margin for manoeuvre, which may, in the context of implementation of the Directive, also be exercised by the business and social partners; whereas Member States will therefore be able to specify in their national law the general conditions governing the lawfulness of data processing; whereas in doing so the Member States shall strive to improve the protection currently provided by their legislation; whereas, within the limits of this margin for manoeuvre and in accordance with Community law, disparities could arise in the implementation of the Directive, and this could have an effect on the movement of data within a Member State as well as within the Community;

(10) Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law; whereas, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community;

(11) Whereas the principles of the protection of the rights and freedoms of individuals, notably the right to privacy, which are contained in this Directive, give substance to and amplify those contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data;

(12) Whereas the protection principles must apply to all processing of personal data by any person whose activities are governed by Community law: whereas there should be excluded the processing of data earned out by a natural person in the exercise of activities which are exclusively personal or domestic, such as correspondence and the holding of records of addresses;

Whereas the acitivities referred to in Titles V and VI of the Treaty on European Union regarding public safety, defence, State security or the acitivities of the State in the area of criminal laws fall outside the scope of Community law, without prejudice to the obligations incumbent upon Member States under Article 56 (2), Article 57 or Article 100a of the Treaty establishing the European Community; whereas the processing of personal data that is necessary to safeguard the economic well-being of the State does not fall within the scope of this Directive where such processing relates to State security matters;

(14) Whereas, given the importance of the developments under way, in the framework of the information society, of the techniques used to capture, transmit, manipulate, record, store or communicate sound and image data relating to natural persons, this Directive should be applicable to processing involving such data;

(15) Whereas the processing of such data is covered by this Directive only if it is automated or if the data processed are contained or are intended to be contained in a filing system structured according to specific criteria relating to individuals, so as to permit easy access to the personal data in question;

(16) Whereas the processing of sound and image data, such as in cases of video surveillance, does not come within the scope of this Directive if it is carried out for the purposes of public security, defence, national security or in the course of State activities relating to the area of criminal law or of other activities which do not come within the scope of Community law;

(17) Whereas, as far as the processing of sound and image data carried out for purposes of journalism

or the purposes of literary or artistic expression is concerned, in particular in the audiovisual field, the principles of the Directive are to apply in a restricted manner according to the provisions laid down in Article 9;

(18) Whereas, in order to ensure that individuals are not deprived of the protection to which they are entitled under this Directive, any processing of personal data in the Community must be carried out in accordance with the law of one of the Member States; whereas, in this connection, processing carried out under the responsibility of a controller who is established in a Member State should be governed by the law of that State;

(19) Whereas establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements; whereas the legal form of such an establishment, whether simply branch or a subsidiary with a legal personality, is not the determining factor in this respect; whereas, when a single controller is established on the territory of several Member States, particularly by means of subsidiaries, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities;

(20) Whereas the fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive; whereas in these cases, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice;

(21) Whereas this Directive is without prejudice to the rules of territonality applicable in criminal matters;

(22) Whereas Member States shall more precisely define in the laws they enact or when bringing into force the measures taken under this Directive the general circumstances in which processing is lawful; whereas in particular Article 5, in conjunction with Articles 7 and 8, allows Member States, independently of general rules, to provide for special processing conditions for specific sectors and for the various categories of data covered by Article 8;

(23) Whereas Member States are empowered to ensure the implementation of the protection of individuals both by means of a general law on the protection of individuals as regards the processing of personal data and by sectonal laws such as those relating, for example, to statistical institutes;

(24) Whereas the legislation concerning the protection of legal persons with regard to the processing data which concerns them is not affected by this Directive;

(25) Whereas the principles of protection must be reflected, on the one hand, in the obligations imposed on persons, public authorities, enterprises, agencies or other bodies responsible for processing, in particular regarding data quality, technical security, notification to the supervisory authority, and the circumstances under which processing can be carried out, and, on the other hand, in the right conferred on individuals, the data on whom are the subject of processing, to be informed that processing is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances;

(26) Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data sub)ect is no longer identifiable; whereas codes of conduct within the meaning of Article 27 may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible;

(27) Whereas the protection of individuals must apply as much to automatic processing of data as to manual processing; whereas the scope of this protection must not in effect depend on the techniques used, otherwise this would create a serious risk of circumvention; whereas, nonetheless, as regards manual processing, this Directive covers only filing systems, not unstructured files; whereas, in particular, the content of a filing system must be structured according to specific criteria relating to individuals allowing easy access to the personal data; whereas, in line with the definition in Article 2 (c), the different criteria for determining the constituents of a structured set of personal data, and the different criteria governing access to such a set,

may be laid down by each Member State; whereas files or sets of files as well as their cover pages, which are not structured according to specific criteria, shall under no circumstances fall within the scope of this Directive;

(28) Whereas any processing of personal data must be lawful and fair to the individuals concerned; whereas, in particular, the data must be adequate, relevant and not excessive in relation to the purposes for which they are processed; whereas such purposes must be explicit and legitimate and must be determined at the time of collection of the data; whereas the purposes of processing further to collection shall not be incompatible with the purposes as they were originally specified;

(29) Whereas the further processing of personal data for historical, statistical or scientific purposes is not generally to be considered incompatible with the purposes for which the data have previously been collected provided that Member States furnish suitable safeguards; whereas these safeguards must in particular rule out the use of the data in support of measures or decisions regarding any particular individual;

(30) Whereas, in order to be lawful, the processing of personal data must in addition be carried out with the consent of the data subject or be necessary for the conclusion or performance of a contract binding on the data subject, or as a legal requirement, or for the performance of a task carried out in the public interest or in the exercise of official authority, or in the legitimate interests of a natural or legal person, provided that the interests or the rights and freedoms of the data subject are not overriding; whereas, m particular, in order to maintain a balance between the interests involved while guaranteeing effective competition, Member States may determine the circumstances in which personal data may be used or disclosed to a third party in the context of the legitimate ordinary business activities of companies and other bodies; whereas Member States may similarly specify the conditions under which personal data may be disclosed to a third party for the purposes of marketing whether carried out commercially or by a charitable organization or by any other association or foundation, of a political nature for example, subject to the provisions allowing a data subject to object to the processing of data regarding him, at no cost and without having to state his reasons;

(31) Whereas the processing of personal data must equally be regarded as lawful where it is carried out in order to protect an interest which is essential for the data subject's life;

(32) Whereas it is for national legislation to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public administration or another natural or legal person governed by public law, or by private law such as a professional association;

(33) Whereas data which are capable by their nature of infringing fundamental freedoms or privacy should not be processed unless the data subject gives his explicit consent; whereas, however, derogations from this prohibition must be explicitly provided for in respect of specific needs, in particular where the processing of these data is carried out for certain health-related purposes by persons sub)ect to a legal obligation of professional secrecy or in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms;

(34) Whereas Member States must also be authorized, when justified by grounds of important public interest, to derogate from the prohibition on processing sensitive categories of data where important reasons of public interest so justify in areas such as public health and social protection - especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system - scientific research and government statistics; whereas it is incumbent on them, however, to provide specific and suitable safeguards so as to protect the fundamental rights and the privacy of individuals;

(35) Whereas, moreover, the processing, of personal data by official authorities for achieving aims, laid down in constitutional law or international public law, of officially recognized religious associations is carried out on important grounds of public interest;

(36) Whereas where, in the course of electoral activities, the operation of the democratic system requires in certain Member States that political parties compile data on people's political opinion, the processing of such data may be permitted for reasons of important public interest, provided that appropriate safeguards are established;

(37) Whereas the processing of personal data for purposes of journalism or for purposes of literary of artistic expression, in particular in the audiovisual field, should qualify for exemption from the requirements of certain provisions of this Directive in so far as this is necessary to reconcile

the fundamental rights of individuals with freedom of information and notably the right to receive and impart information, as guaranteed in particular in Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; whereas Member States should therefore lay down exemptions and derogations necessary for the purpose of balance between fundamental rights as regards general measures on the legitimacy of data processing, measures on the transfer of data to third countries and the power of the supervisory authority; whereas this should not, however, lead Member States to lay down exemptions from the measures to ensure security of processing; whereas at least the supervisory authority responsible for this sector should also be provided with certain ex-post powers, e.g. to publish a regular report or to refer matters to the judicial authorities;

(38) Whereas, if the processing of data is to be fair, the data subject must be in a position to learn of the existence of a processing operation and, where data are collected from him, must be given accurate and full information, bearing in mind the circumstances of the collection;

(39) Whereas certain processing operations involve data which the controller has not collected directly from the data subject; whereas, furthermore, data can be legitimately disclosed to a third party, even if the disclosure was not anticipated at the time the data were collected from the data subject; whereas, in all these cases, the data subject should be informed when the data are recorded or at the latest when the data are first disclosed to a third party;

(40) Whereas, however, it is not necessary to impose this obligation of the data subject already has the information; whereas, moreover, there will be no such obligation if the recording or disclosure are expressly provided for by law or if the provision of information to the data subject proves impossible or would involve disproportionate efforts, which could be the case where processing is for historical, statistical or scientific purposes; whereas, in this regard, the number of data subjects, the age of the data, and any compensatory measures adopted may be taken into consideration;

(4.1) Whereas any person must be able to exercise the right of access to data relating to him which are processed, in order to verify in particular the accuracy of the data and the lawfulness of the processing; whereas, for the same reasons, every data subject must also have the right to know the logic involved in the automatic processing of data concerning him. at least in the case of the automated decisions referred to in Article 15 (1); whereas this right must not adversely affect trade secrets or intellectual property and in particular the copyright protecting the software; whereas these considerations must not, however, result in the data subject being refused all information;

(42) Whereas Member States may, in the interest of the data subject or so as to protect the rights and freedoms of others, restrict rights of access and information; whereas they may, for example, specify that access to medical data may be obtained only through a health professional;

(43) Whereas restrictions on the rights of access and information and on certain obligations of the controller may similarly be imposed by Member States in so far as they are necessary to safeguard, for example, national security, defence, public safety, or important economic or financial interests of a Member State or the Union, as well as criminal investigations and prosecutions and action in respect of breaches of ethics in the regulated professions; whereas the list of exceptions and limitations should include the tasks of monitoring, inspection or regulation necessary in the three last-mentioned areas concerning public security, economic or financial interests and crime prevention; whereas the listing of tasks in these three areas does not affect the legitimacy of exceptions or restrictions for reasons of State security or defence;

(44) Whereas Member States may also be led, by virtue of the provisions of Community law, to derogate from the provisions of this Directive concerning the right of access, the obligation to inform individuals, and the quality of data, in order to secure certain of the purposes referred to above;

(45) Whereas, in cases where data might lawfully be processed on grounds of public interest, official authority or the legitimate interests of a natural or legal person, any data subject should nevertheless be entitled, on legitimate and compelling grounds relating to his particular situation, to object to the processing of any data relating to himself; whereas Member States may nevertheless lay down national provisions to the contrary;

(46) Whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical

and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing; whereas it is incumbent on the Member States to ensure that controllers comply with these measures; whereas these measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected;

(47) Whereas where a message containing personal data is transmitted by means of a telecommunications or electronic mail service, the sole purpose of which is the transmission of such messages, the controller in respect of the personal data contained in the message will normally be considered to be the person from whom the message originates, rather than the person offering the transmission services; whereas, nevertheless, those offering such services will normally be considered controllers in respect of the processing of the additional personal data necessary for the operation of the service;

(48) Whereas the procedures for notifying the supervisory authority are designed to ensure disclosure of the purposes and main features of any processing operation for the purpose of verification that the operation is in accordance with the national measures taken under this Directive;

(49) Whereas, in order to avoid unsuitable administrative formalities, exemptions from the obligation to notify and simplification of the notification required may be provided for by Member States in cases where processing is unlikely adversely to affect the rights and freedoms of data subjects, provided that it is in accordance with a measure taken by a Member State specifying its limits; whereas exemption or simplification may similarly be provided for by Member States where a person appointed by the controller ensures that the processing carried out is not likely adversely to affect the rights and freedoms of data subjects; whereas such a data protection official, whether or not an employee of the controller, must be in a position to exercise his functions in complete independence;

(50) Whereas exemption or simplification could be provided for in cases of processing operations whose sole purpose is the keeping of a register intended, according to national law, to provide information to the public and open to consultation by the public or by any person demonstrating a legitimate interest;

(51) Whereas, nevertheless, simplification or exemption from the obligation to notify shall not release the controller from any of the other obligations resulting from this Directive;

(52) Whereas, in this context, *ex post facto* verification by the competent authorities must in general be considered a sufficient measure;

(53) Whereas, however, certain processing operation are likely to pose specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, such as that of excluding individuals from a right, benefit or a contract, or by virtue of the specific use of new technologies; whereas it is for Member States, if they so wish, to specify such risks in their legislation;

(54) Whereas with regard to all the processing undertaken in society, the amount posing such specific risks should be very limited; whereas Member States must provide that the supervisory authority, or the data protection official in cooperation with the authority, check such processing prior to it being carried out; whereas following this prior check, the supervisory authority may, according to its national law, give an opinion or an authorization regarding the processing; whereas such checking may equally take place in the course of the preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing and lays down appropriate safeguards;

(55) Whereas, if the controller fails to respect the rights of data subjects, national legislation must provide for a judicial remedy; whereas any damage which a person may suffer as a result of unlawful processing must be compensated for by the controller, who may be exempted from liability if he proves that he is not responsible for the damage, in particular in cases where he establishes fault on the part of the data subject or in case of *force majeure;* whereas sanctions must be imposed on any person, whether governed by private of public law, who fails to comply with the national measures taken under this Directive;

(56) Whereas cross-border flows of personal data are necessary to the expansion of international trade; whereas the protection of individuals guaranteed in the Community by this Directive does not stand in the way of transfers of personal data to third

countries which ensure an adequate level of protection; whereas the adequacy of the level of protection afforded by a third country must be assessed in the light of all the circumstances surrounding the transfer operation or set of transfer operations;

(57) Whereas, on the other hand, the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited;

(58) Whereas provisions should be made for exemptions from this prohibition in certain circumstances where the data subject has given his consent, where the transfer is necessary in relation to a contract or a legal claim, where protection of an important public interest so requires, for example in cases of international transfers of data between tax or customs administrations or between services competent for social security marters, or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest; whereas in this case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients;

(59) Whereas particular measures may be taken to compensate for the lack of protection in a third country in cases where the controller offers appropriate safeguards; whereas, moreover, provision must be made for procedures for negotiations between the Community and such third countries;

(60) Whereas, in any event, transfers to third countries may be effected only in full compliance with the provisions adopted by the Member States pursuant to this Directive, and in particular Article 8 thereof;

(61) Whereas Member States and the Commission, in their respective spheres of competence, must encourage the trade associations and other representative organizations concerned to draw up codes of conduct so as to facilitate the application of this Directive, taking account of the specific characteristics of the processing carried out in certain sectors, and respecting the national provisions adopted for its implementation;

(62) Whereas the establishment in Member States of supervisory authorities, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of personal data;

(63) Whereas such authorities must have the necessary means to perform their duties, including powers of investigation and intervention, particularly in cases of complaints from individuals, and powers to engage in legal proceedings; whereas such authorities must help to ensure transparency of processing in the Member States within whose jurisdiction thev fall;

(64) Whereas the authorities in the different Member States will need to assist one another in performing their duties so as to ensure that the rules of protection are properly respected throughout the European Union:

(65) Whereas, at Community level, a Working Party on the Protection of Individuals with regard to the Processing of Personal Data must be set up and be completely independent in the performance of its functions; whereas, having regard to its specific nature, it must advise the Commission and. in particular, contribute to the uniform application of the national rules adopted pursuant to this Directive;

(66) Whereas, with regard to the transfer of data to third countries, the application of this Directive calls for the conferment of powers of implementation on the Commission and the establishment of a procedure. as laid down in Council Decision 87/373/EEC (1);

(67) Whereas an agreement on a *modus vivendi* between the European Parliament, the Council and the Commission concerning the implementing measures for acts adopted in accordance with the procedure laid down in Article 189b of the EC Treaty was reached on 20 December 1994:

(68) Whereas the principles set out in this Directive regarding the protection of the rights and freedoms of individuals, notably their right to privacy, with regard to the processing of personal data may be supplemented or clarified, in particular as far as certain sectors are concerned, by specific rules based on those principles;

(69) Whereas Member States should be allowed a period of not more than three years from the entry into force of the national measures transposing this Directive in which to apply such new national rules progressively to all processing operations already under way; whereas, in order to facilitate their cost-effective implementation, a further period

(1) OJ No L 197, 18. 7. 1987, p. 33.

expiring 12 years after the date on which this Directive is adopted will be allowed to Member States to ensure the conformity of existing manual filing systems with certain of the Directive's provisions; whereas, where data contained in such filing systems are manually processed during this extended transition period, those systems must be brought into conformity with these provisions at the time of such processing;

(70) Whereas it is not necessary for the data subject to give his consent again so as to allow the controller to continue to process, after the national provisions taken pursuant to this Directive enter into force, any sensitive data necessary for the performance of a contract concluded on the basis of free and informed consent before the entry into force of these provisions;

(71) Whereas this Directive does not stand in the **way** of a Member State's regulating marketing activities aimed at consumers residing in territory in so far as such regulation does not concern the protection of individuals with regard to the processing of personal data;

(72) Whereas this Directive allows the principle of public access to official documents to be taken into account when implementing the principles set out in this Directive,

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I

GENERAL PROVISIONS

Article 1

Object of the Directive

1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.

2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.

Article 2

Definitions

For the purposes of this Directive:

(a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

(b) 'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

(c) 'personal data filing system' ('filing system') shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

(d) 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;

(e) 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

(f) 'third parr.-' shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data;

(g) 'recipient' shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authonnes which may receive data in the framework of a particular inquiry shall not be regarded as recipients;

(h) 'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

Article 3

Scope

1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Directive shall not apply to the processing of personal data:

— in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security marters) and the activities of the State in areas of criminal law,

— by a natural person in the course of a purely personal or household activitv.

Article 4

National law applicable

1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;

(b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;

(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

2. In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.

CHAPTER II

GENERAL RULES ON THE LAWFULNESS OF THE PROCESSING OF PERSONAL DATA

Article 5

Member States shall, within the limits of the provisions of this Chapter, determine more precisely the conditions under which the processing of personal data is lawful.

SECTION I

PRINCIPLES RELATING TO DATA QUALITY

Article 6

1. Member States shall provide that personal data must be:

(a) processed fairly and lawfully;

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;

(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

2. It shall be for the controller to ensure that paragraph 1 is complied with.

SECTION II

CRITERIA FOR MAKING DATA PROCESSING LEGITIMATE

Article 7

Member States shall provide that personal data may be processed only if:

(a) the data subject has unambiguously given his consent;

(b) processing is necessary for the performance of a contract to which the data subject is parry or in order to take steps at the request of the data subject prior to entering into a contract; or

(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or

(d) processing is necessary in order to protect the vital interests of the data subject; or

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third parry or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

SECTION III

SPECIAL CATEGORIES OF PROCESSING

Article 8

The processing of special categories of data

1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

2. Paragraph 1 shall not apply where:

(a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or

(b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or

(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or

(d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular

contact with it in connection with its purposes and that the data are not disclosed to a third parry without the consent of the data subjects; or

the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.

3. Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of

4. Subject to the provision of suitable safeguards. Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.

5. Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority.

Member States may provide that data relating to administrative sanctions or judgements in civil cases shall also be processed under the control of official authority.

6. Derogations from paragraph 1 provided for in paragraphs 4 and 5 shall be notified to the Commission.

7. Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed.

Article 9

Processing of personal data and freedom of expression

Member States shall . provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.

SECTION IV

INFORMATION TO BE GIVEN TO THE DATA SUBJECT

Article 10

Information in cases of collection of data from the data subject

Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:

(a) the identity of the controller and of his representative, if any;

(b) the purposes of the processing for which the data are intended;

(c) any further information such as

— the recipients or categories of recipients of the data,

— whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,

— the existence of the right of access to and the right to rectify the data concerning him

in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

Article 11

Information where the data have not been obtained from the data subject

1. Where the data have not been obtained from the data subject, Member States shall provide that the controller or his representative must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except where he already has it:

(a) the identity of the controller and of his representative, if any;

(b) the purposes of the processing;

(c) any further information such as

— the categories of data concerned,

— the recipients or categories of recipients,

— the existence of the right of access to and the right to rectify the data concerning him

in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.

2. Paragraph 1 shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law. In these cases Member States shall provide appropriate safeguards.

SECTION V

THE DATA SUBJECT'S RIGHT OF ACCESS TO DATA

Article 12

Right of access

Member States shall guarantee every data subject the right to obtain from the controller:

(a) without constraint at reasonable intervals and without excessive delay or expense:

— confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,

— communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,

— knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1);

(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;

(c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.

SECTION VI

EXEMPTIONS AND RESTRICTIONS

Article 13

Exemptions and restrictions

1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard:

(a) national security;

(b) defence;

(c) public security;

(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;

(e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;

(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);

(g) the protection of the data subject or of the rights and freedoms of others.

2. Subject to adequate legal safeguards, in particular that the data are not used for taking measures or decisions regarding any particular individual. Member States may, where there is clearly no risk of breaching the privacy of the data subject, restrict by a legislative measure the rights provided for in Article 12 when data are processed solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics.

SECTION VII

THE DATA SUBJECT'S RIGHT TO OBJECT

Article 14

The data subject's right to object

Member States shall grant the data subject the right:

(a) at least in the cases referred to in Article 7 (e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where

otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;

(b) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.

Member States shall take the necessary measures to ensure that data subjects are aware of the existence of the right referred to in the first subparagraph of (b).

Article 15

Automated individual decisions

1. Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.

2. Subject to the other Articles of this Directive, Member States shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision:

(a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or

(b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

SECTION VIII

CONFIDENTIALITY AND SECURITY OF PROCESSING

Article 16

Confidentiality of processing

Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so bv law.

Article 17

Security of processing

1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:

— the processor shall act only on instructions from the controller,

— the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.

4. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.

SECTION IX

NOTIFICATION

Article 18

Obligation to notify the supervisory authority

1. Member States shall provide that the controller or his representative, if any, must notify the supervisory

authonty referred to in Article 28 before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes.

2. Member States may provide for the simplification of or exemption from notification only in the following cases and under the following conditions:

— where, for categories of processing operations which are unlikely, taking account of the data to be processed, to affect adversely the rights and freedoms of data subjects, they specify the purposes of the processing, the data or categories of data undergoing processing, the category or categories of data subject, the recipients or categories of recipient to whom the data are to be disclosed and the length of time the data are to be stored, and/or

— where the controller, in compliance with the national law which governs him, appoints a personal data protection official, responsible in particular:

  — for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive

  — for keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21 (2),

  thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations.

3. Member States may provide that paragraph 1 does not apply to processing whose sole purpose is the keeping of a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person demonstrating a legitimate interest.

4. Member States may provide for an exemption from the obligation to notify or a simplification of the notification in the case of processing operations referred to in Article 8 (2) (d).

5. Member States may stipulate that certain or all non-automatic processing operations involving personal data shall be notified, or provide for these processing operations to be subject to simplified notification.

Article 19

Contents of notification

1. Member States shall specify the information to be given in the notification. It shall include at least:

(a) the name and address of the controller and of his representative, if any;

(b) the purpose or purposes of the processing;

(c) a description of the category or categories of data subject and of the data or categories of data relating to them;

(d) the recipients or categories of recipient to whom the data might be disclosed;

(e) proposed transfers of data to third countries;

(f) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 17 to ensure security of processing.

2. Member States shall specify the procedures under which any change affecting the information referred to in paragraph 1 must be notified to the supervisory authority.

Article 20

Prior checking

1. Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof.

2. Such prior checks shall be carried out by the supervisory authority following receipt of a notification from the controller or by the data protection official, who, in cases of doubt, must consult the supervisory authority.

3. Member States may also carry out such checks in the context of preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which define the nature of the processing and lay down appropriate safeguards.

Article 21

Publicizing of processing operations

1. Member States shall take measures to ensure that processing operations are publicized.

2. Member States shall provide that a register of processing operations notified in accordance with Article 18 shall be kept by the supervisory authority.

The register shall contain at least the information listed in Article 19 (1) (a) to (e).

The register may be inspected by any person.

3. Member States shall provide, in relation to processing operations not subject to notification, that controllers or another body appointed by the Member States make available at least the information referred to in Article 19 (1) (a) to (e) in an appropriate form to any person on request.

Member States may provide that this provision does not apply to processing whose sole purpose is the keeping of a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can provide proof of a legitimate interest.

CHAPTER III

JUDICIAL REMEDIES, LIABILITY AND SANCTIONS

Article 22

Remedies

Without prejudice to any administrative remedy for which provision may be made, *inter alia* before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question.

Article 23

Liability

1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.

2. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

Article 24

Sanctions

The Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive.

CHAPTER IV

TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

Article 25

Principles

1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration

shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.

4. Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.

5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.

6. The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.

Member States shall take the measures necessary to comply with the Commission's decision.

Article 26

Derogations

1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:

(a) the data subject has given his consent unambiguously to the proposed transfer; or

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subnet's request; or

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or

(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or

(e) the transfer is necessary in order to protect the vital interests of the data subject; or

(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

2. Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.

3. The Member State shall inform the Commission and the other Member States of the authorizations it grants pursuant to paragraph 2.

If a Member State or the Commission objects on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals, the Commission shall take appropriate measures in accordance with the procedure laid down in Article 31 (2).

Member States shall take the necessary measures to comply with the Commission's decision.

4. Where the Commission decides, in accordance with the procedure referred to in Article 31 (2), that certain standard contractual clauses offer sufficient safeguards as required by paragraph 2, Member States shall take the necessary measures to comply with the Commission's decision.

CHAPTER V

CODES OF CONDUCT

Article 27

1. The Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the specific features of the various sectors.

2. Member States shall make provision for trade associations and other bodies representing other categories of controllers which have drawn up draft national codes or which have the intention of amending or extending existing national codes to be able to submit them to the opinion of the national authority.

Member States shall make provision for this authority to ascertain, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives.

3. Draft Community codes, and amendments or extensions to existing Community codes, may be submitted to the Working Party referred to in Article 29. This Working Party shall determine, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives. The Commission may ensure appropriate publicity for the codes which have been approved by the Working Party.

CHAPTER VI

SUPERVISORY AUTHORITY AND WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

Article 28

Supervisory authority

1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.

These authorities shall act with complete independence in exercising the functions entrusted to them.

2. Each Member State shall provide that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data.

3. Each authority shall in particular be endowed with:

— investigative powers, such as powers of access to data forming the sub)ect-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,

effective powers of intervention, such as, for example, that of delivering opinions before processing operations are earned out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions,

the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities.

Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.

4. Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.

Each supervisory authority shall, in particular, hear claims for checks on the lawfulness of data processing lodged by any person when the national provisions adopted pursuant to Article 13 of this Directive apply. The person shall at any rate be informed that a check has taken place.

5. Each supervisory authority shall draw up a report on its activities at regular intervals. The report shall be made public.

6. Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.

The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

7. Member States shall provide that the members and staff of the supervisory authority, even after their employment has ended, are to be sub)ect to a duty of professional secrecy with regard to confidential •information to which they have access.

Article 29

Working Party on the Protection of Individuals with regard to **the** Processing of Personal Data

1. A Working Parry on the Protection of Individuals with regard to the Processing of Personal Data, hereinafter referred to as 'the Working Party', is hereby set up.

It shall have advisory status and act independently.

2. The Working Party shall be composed of a representative of the supervisory authority or authorities designated by each Member State and of a representative of the authority or authorities established for the Community institutions and bodies, and of a representative of the Commission.

Each member of the Working Party shall be designated by the institution, authority or authorities which he represents. Where a Member State has designated more than one supervisory authority, they shall nominate a joint representative. The same shall apply to the authorities established for Community institutions and bodies.

3. The Working Party shall take decisions by a simple majority of the representatives of the supervisory authorities.

4. The Working Party shall elect its chairman. The chairman's term of office shall be two years. His appointment shall be renewable.

5. The Working Party's secretariat shall be provided by the Commission.

6. The Working Parry shall adopt its own rules of procedure.

7. The Working Party shall consider items placed on its agenda by its chairman, either on his own initiative or at the request of a representative of the supervisory authorities or at the Commission's request.

Article 30

1. The Working Party shall:

(a) examine any question covering the application of the national measures adopted under this Directive in order to contribute to the uniform application of such measures;

(b) give the Commission an opinion on the level of protection in the Community and in third countries;

(c) advise the Commission on any proposed amendment of this Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms;

(d) give an opinion on codes of conduct drawn up at Communirv level.

2. If the Working Parry finds that divergences likely to affect the equivalence of protection for persons with regard to the processing of personal data in the Community are arising between the laws or practices of Member States, it shall inform the Commission accordingly.

3. The Working Party may, on its own initiative, make recommendations on all matters relating to the protection of persons with regard to the processing of personal data in the Community.

4. The Working Parry's opinions and recommendations shall be forwarded to the Commission and to **the** committee referred to in Article 31.

5. The Commission shall inform the Working Party of the action it has taken in response to its opinions and recommendations. It shall do so in a report which shall

also be forwarded to the European Parliament and the Council. The report shall be made public.

6. The Working Party shall draw up an annual report on the situation regarding the protection of natural persons with regard to the processing of personal data in the Community and in third countries, which it shall transmit to the Commission, the European Parliament and the Council. The report shall be made public.

CHAPTER VII

COMMUNITY IMPLEMENTING MEASURES

Article 31

The Committee

1. The Commission shall be assisted by a committee composed of the representatives of the Member States and chaired by the representative of the Commission.

2. The representative of the Commission shall submit to the committee a draft of the measures to be taken. The committee shall deliver its opinion on the draft within a time limit which the chairman may lay down according to the urgency of the maner.

The opinion shall be delivered by the majority laid down in Article 148 (2) of the Treaty. The votes of the representatives of the Member States within the committee shall be weighted in the manner set out in that Article. The chairman shall not vote.

The Commission shall adopt measures which shall apply immediately. However, if these measures are not in accordance with the opinion of the committee, they shall be communicated by the Commission to the Council forthwith. It that event:

— the Commission shall defer application of the measures which it has decided for a period of three months from the date of communication,

— the Council, acting by a qualified majority, may take a different decision within the time limit referred to in the first indent.

FINAL PROVISIONS

Article 32

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive at the latest at the end of a period of three years from the date of its adoption.

When Member States adopt these measures, they shall contain a reference to this Directive or be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by the Member States.

2. Member States shall ensure that processing already under way on the date the national provisions adopted pursuant to this Directive enter into force, is brought into conformity with these provisions within three years of this date.

By way of derogation from the preceding subparagraph, Member States may provide that the processing of data already held in manual filing systems on the date of entry into force of the national provisions adopted in implementation of this Directive shall be brought into conformity with Articles 6, 7 and 8 of this Directive within 12 years of the date on which it is adopted. Member States shall, however, grant the data subject the right to obtain, at his request and in particular at the time of exercising his right of access, the rectification, erasure or blocking of data which are incomplete, inaccurate or stored in a way incompatible with the legitimate purposes pursued by the controller.

3. By way of derogation from paragraph" 2, Member States may provide, subject to suitable safeguards, that data kept for the sole purpose of historical research need

not be brought into conformity with Articles 6, and 8 of this Directive.

4. Member States shall communicate to the Commission the text of the provisions of domestic law which they adopt in the field covered by this Directive.

Article 33

The Commission shall report to the Council and the European Parliament at regular intervals, starting not later than three years after the date referred to in Article 32 (1), on the implementation of this Directive, attaching to its report, if necessary, suitable proposals for amendments. The report shall be made public.

The Commission shall examine, in particular, the application of this Directive to the data processing of sound and image data relating to natural persons and shall submit any appropriate proposals which prove to be necessary, taking account of developments in information technology and in the light of the state of progress in the information societv.

Article 34

This Directive is addressed to the Member States.

Done at Luxembourg, 24 October 1995.

For the European Parliament	*For the Council*
The President	*The President*
K. HÄNSCH	L. ATIENZA SERNA

DIRECTIVE 95/46/CE DU PARLEMENT EUROPÉEN ET DU CONSEIL

du 24 octobre 1995

relative à la protection des personnes physiques a l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité instituant la Communauté européenne, et notamment son article 100 A,

vu la proposition de la Commission (1),

vu l'avis du Comité économique et social (2),

statuant conformément à la procédure visée à l'article 189 B du traité (3),

(1) considérant que les objectifs de la Communauté, énoncés dans le traité, tel que modifié par le traité sur l'Union européenne, consistent à réaliser une union sans cesse plus étroite entre les peuples européens, à établir des relations plus étroites entre les États que la Communauté réunit, à assurer par une action commune le progrès économique et social en éliminant les barrières qui divisent l'Europe, à promouvoir l'amélioration constante des conditions de vie de ses peuples, à préserver et conforter la paix et la liberté, et à promouvoir la démocratie en se fondant sur les droits fondamentaux reconnus dans les constitutions et les lois des États membres, ainsi que dans la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales;

(2) considérant que les systèmes de traitement de données sont au service de l'homme; qu'ils doivent, quelle que soit la nationalité ou la résidence des personnes physiques, respecter les libertés et droits fondamentaux de ces personnes, notamment la vie privée, et contribuer au progrès économique et social, au développement des échanges ainsi qu'au bien-être des individus;

(3) considérant que l'établissement et le fonctionnement du marché intérieur dans lequel, conformément à l'article 7 A du traité, la libre circulation des marchandises, des personnes, des services et des capitaux est assurée, nécessitent non seulement que des données à caractère personnel puissent circuler librement d'un État membre à l'autre, mais également que les droits fondamentaux des personnes soient sauvegardés;

(4) considérant que, dans la Communauté, il est fait de plus en plus fréquemment appel au traitement de données à caractère personnel dans les divers domaines de l'activité économique et sociale; que les progrès des technologies de l'information facilitent considérablement le traitement et l'échange de ces données;

(5) considérant que l'intégration économique et sociale résultant de l'établissement et du fonctionnement du marché intérieur au sens de l'article 7 A du traité va nécessairement entraîner une augmentation sensible des flux transfrontaliers de données à caractère personnel entre tous les acteurs de la vie économique et sociale des États membres, que ces acteurs soient privés ou publics; que l'échange de données à caractère personnel entre des entreprises établies dans des États membres différents est appelé à se développer; que les administrations des États membres sont appelées, en application du droit communautaire, à collaborer et à échanger entre elles des données à caractère personnel afin de pouvoir accomplir leur mission ou exécuter des tâches pour le compte d'une administration d'un autre État membre, dans le cadre de l'espace sans frontières que constitue le marché intérieur;

(6) considérant, en outre, que le renforcement de la coopération scientifique et technique ainsi que la mise en place coordonnée de nouveaux réseaux de télécommunications dans la Communauté nécessitent et facilitent la circulation transfrontalière de données à caractère personnel;

(7) considérant que les différences entre États membres quant au niveau de protection des droits et libertés des personnes, notamment du droit à la vie privée, à l'égard des traitements de données à caractère personnel peuvent empêcher la transmission de ces données du territoire d'un État membre à celui d'un autre État membre; que ces différences peuvent dès lors constituer un obstacle à l'exercice d'une série d'activités économiques à l'échelle communautaire, fausser la concurrence et empêcher les administrations de s'acquitter des responsabilités qui leur incombent en vertu du droit communau-

1) JO n° C 277 du 5. 11. 1990, p. 3.
JO n° C 311 du 27. 11. 1992, p. 30.
2) JO n° C 159 du 17. 6. 1991, p. 38.
3) Avis du Parlement européen du 11 mars 1992 (JO n° C 94 du 13. 4. 1992, p. 198), confirmé le 2 décembre 1993 (JO n° C 342 du 20. 12. 1993, p. 30); position commune du Conseil du 20 février 1995 (JO n° C 93 du 13. 4. 1995, p. 1) et décision du Parlement européen du 15 juin 1995 (JO n° C 166 du 3. 7. 1995).

taire; que ces différences de niveau de protection résultent de la disparité des dispositions nationales législatives, réglementaires et administratives;

(8) considérant que, pour éliminer les obstacles à la circulation des données à caractère personnel, le niveau de protection des droits et libertés des personnes à l'égard du traitement de ces données doit être équivalent dans tous les États membres; que cet objectif, fondamental pour le marché intérieur, ne peut pas être atteint par la seule action des États membres, compte tenu en particulier de l'ampleur des divergences qui existent actuellement entre les législations nationales applicables en la matière et de la nécessité de coordonner les législations des États membres pour que le flux transfrontalier de données à caractère personnel soit réglementé d'une manière cohérente et conforme à l'objectif du marché intérieur au sens de l'article 7 A du traité; qu'une intervention de la Communauté visant à un rapprochement des législations est donc nécessaire;

(9) considérant que, du fait de la protection équivalente résultant du rapprochement des législations nationales, les États membres ne pourront plus faire obstacle à la libre circulation entre eux de données à caractère personnel pour des raisons relatives à la protection des droits et libertés des personnes, notamment du droit à la vie privée; que les États membres disposeront d'une marge de manœuvre qui, dans le contexte de la mise en œuvre de la directive, pourra être utilisée par les partenaires économiques et sociaux; qu'ils pourront donc préciser, dans leur législation nationale, les conditions générales de licéité du traitement des données; que, ce faisant, les États membres s'efforceront d'améliorer la protection assurée actuellement par leur législation; que, dans les limites de cette marge de manœuvre et conformément au droit communautaire, des disparités pourront se produire dans la mise en œuvre de la directive et que cela pourra avoir des incidences sur la circulation des données tant à l'intérieur d'un État membre que dans la Communauté;

(10) considérant que l'objet des législations nationales relatives au traitement des données à caractère personnel est d'assurer le respect des droits et libertés fondamentaux, notamment du droit à la vie privée reconnu également dans l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et dans les principes généraux du droit communautaire; que, pour cette raison, le rapprochement de ces législations ne doit pas conduire à affaiblir la protection qu'elles assurent mais doit, au contraire, avoir pour objectif de garantir un niveau élevé de protection dans la Communauté;

(11) considérant que les principes de la protection des droits et des libertés des personnes, notamment du droit à la vie privée, contenus dans la présente directive précisent et amplifient ceux qui sont contenus dans la convention, du 28 janvier 1981, du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel;

(12) considérant que les principes de la protection doivent s'appliquer à tout traitement de données à caractère personnel dès lors que les activités du responsable du traitement relèvent du champ d'application du droit communautaire; que doit être exclu le traitement de données effectué par une personne physique dans l'exercice d'activités exclusivement personnelles ou domestiques, telles la correspondance et la tenue de répertoires d'adresses;

(13) considérant que les activités visées aux titres V et VI du traité sur l'Union européenne concernant la sécurité publique, la défense, la sûreté de l'État ou les activités de l'État dans le domaine pénal ne relèvent pas du champ d'application du droit communautaire, sans préjudice des obligations incombant aux États membres au titre de l'article 56 paragraphe 2 et des articles 57 et 100 A du traité; que le traitement de données à caractère personnel qui est nécessaire à la sauvegarde du bien-être économique de l'État ne relève pas de la présente directive lorsque ce traitement est lié à des questions de sûreté de l'État;

(14) considérant que, compte tenu de l'importance du développement en cours, dans le cadre de la société de l'information, des techniques pour capter, transmettre, manipuler, enregistrer, conserver ou communiquer les données constituées par des sons et des images, relatives aux personnes physiques, la présente directive est appelée à s'appliquer aux traitements portant sur ces données;

(15) considérant que les traitements portant sur de telles données ne sont couverts par la présente directive que s'ils sont automatisés ou si les données sur lesquelles ils portent sont contenues ou sont destinées à être contenues dans un fichier structuré selon des critères spécifiques relatifs aux personnes, afin de permettre un accès aisé aux données à caractère personnel en cause;

(16) considérant que les traitements des données constituées par des sons et des images, tels que ceux de vidéo-surveillance, ne relèvent pas du champ d'application de la présente directive s'ils sont mis en œuvre à des fins de sécurité publique, de défense, de sûreté de l'État ou pour l'exercice des activités de l'État relatives à des domaines du droit pénal ou pour l'exercice d'autres activités qui ne relèvent pas du champ d'application du droit communautaire;

(17) considérant que, pour ce qui est des traitements de sons et d'images mis en œuvre à des fins de

journalisme ou d'expression littéraire ou artistique, notamment dans le domaine audiovisuel, les principes de la directive s'appliquent d'une manière restreinte selon les dispositions prévues à l'article 9;

(18) considérant qu'il est nécessaire, afin d'éviter qu'une personne soit exclue de la protection qui lui est garantie en vertu de la présente directive, que tout traitement de données à caractère personnel effectué dans la Communauté respecte la législation de l'un des États membres; que, à cet égard, il est opportun de soumettre les traitements de données effectués par toute personne opérant sous l'autorité du responsable du traitement établi dans un État membre à l'application de la législation de cet État;

(19) considérant que l'établissement sur le territoire d'un État membre suppose l'exercice effectif et réel d'une activité au moyen d'une installation stable; que la forme juridique retenue pour un tel établissement, qu'il s'agisse d'une simple succursale ou d'une filiale ayant la personnalité juridique, n'est pas déterminante à cet égard; que, lorsqu'un même responsable est établi sur le territoire de plusieurs États membres, en particulier par le biais d'une filiale, il doit s'assurer, notamment en vue d'éviter tout contournement, que chacun des établissements remplit les obligations prévues par le droit national applicable aux activités de chacun d'eux;

(20) considérant que l'établissement, dans un pays tiers, du responsable du traitement de données ne doit pas faire obstacle à la protection des personnes prévue par la présente directive; que, dans ce cas, il convient de soumettre les traitements de données effectués à la loi de l'État membre dans lequel des moyens utilisés pour le traitement de données en cause sont localisés et de prendre des garanties pour que les droits et obligations prévus par la présente directive soient effectivement respectés;

(21) considérant que la présente directive ne préjuge pas des règles de territorialité applicables en matière de droit pénal;

(22) considérant que les États membres préciseront dans leur législation ou lors de la mise en œuvre des dispositions prises en application de la présente directive les conditions générales dans lesquelles le traitement de données est licite; que, en particulier, l'article 5, en liaison avec les articles 7 et 8, permet aux États membres de prévoir, indépendamment des règles générales, des conditions particulières pour les traitements de données dans des secteurs spécifiques et pour les différentes catégories de données visées à l'article 8;

(23) considérant que les États membres sont habilités à assurer la mise en œuvre de la protection des personnes, tant par une loi générale relative à la protection des personnes à l'égard du traitement des données à caractère personnel que par des lois sectorielles telles que celles relatives par exemple aux instituts de statistiques;

(24) considérant que les législations relatives à la protection des personnes morales à l'égard du traitement des données qui les concernent ne sont pas affectées par la présente directive;

(25) considérant que les principes de la protection doivent trouver leur expression, d'une part, dans les obligations mises à la charge des personnes, autorités publiques, entreprises, agences ou autres organismes qui traitent des données, ces obligations concernant en particulier la qualité des données, la sécurité technique, la notification à l'autorité de contrôle, les circonstances dans lesquelles le traitement peut être effectué, et, d'autre part, dans les droits donnés aux personnes dont les données font l'objet d'un traitement d'être informées sur celui-ci, de pouvoir accéder aux données, de pouvoir demander leur rectification, voire de s'opposer au traitement dans certaines circonstances;

(26) considérant que les principes de la protection doivent s'appliquer à toute information concernant une personne identifiée ou identifiable; que, pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne; que les principes de la protection ne s'appliquent pas aux données rendues anonymes d'une manière telle que la personne concernée n'est plus identifiable; que les codes de conduite au sens de l'article 27 peuvent être un instrument utile pour fournir des indications sur les moyens par lesquels les données peuvent être rendues anonymes et conservées sous une forme ne permettant plus l'identification de la personne concernée;

(27) considérant que la protection des personnes doit s'appliquer aussi bien au traitement de données automatisé qu'au traitement manuel; que le champ de cette protection ne doit pas en effet dépendre des techniques utilisées, sauf à créer de graves risques de détournement; que, toutefois, s'agissant du traitement manuel, la présente directive ne couvre que les fichiers et ne s'applique pas aux dossiers non structurés; que, en particulier, le contenu d'un fichier doit être structuré selon des critères déterminés relatifs aux personnes permettant un accès facile aux données à caractère personnel; que, conformément à la définition figurant à l'article 2 point c), les différents critères permettant de déterminer les éléments d'un ensemble structuré de données à caractère personnel et les différents critères régissant l'accès à cet ensemble de données peuvent être définis par chaque État

membre; que les dossiers ou ensembles de dossiers, de même que leurs couvertures, qui ne sont pas structurés selon des critères déterminés n'entrent en aucun cas dans le champ d'application de la présente directive;

(28) considérant que tout traitement de données à caractère personnel doit être effectué licitement et loyalement à l'égard des personnes concernées; qu'il doit, en particulier, porter sur des données adéquates, pertinentes et non excessives au regard des finalités poursuivies; que ces finalités doivent être explicites et légitimes et doivent être déterminées lors de la collecte des données; que les finalités des traitements ultérieurs à la collecte ne peuvent pas être incompatibles avec les finalités telles que spécifiées à l'origine;

(29) considérant que le traitement ultérieur de données à caractère personnel à des fins historiques, statistiques ou scientifiques n'est pas considéré en général comme incompatible avec les finalités pour lesquelles les données ont été auparavant collectées, dans la mesure où les États membres prévoient des garanties appropriées; que ces garanties doivent notamment empêcher l'utilisation des données à l'appui de mesures ou de décisions prises à l'encontre d'une personne;

(30) considérant que, pour être licite, un traitement de données à caractère personnel doit en outre être fondé sur le consentement de la personne concernée ou être nécessaire à la conclusion ou à l'exécution d'un contrat liant la personne concernée, ou au respect d'une obligation légale, ou à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, ou encore à la réalisation d'un intérêt légitime d'une personne à condition que ne prévalent pas l'intérêt ou les droits et libertés de la personne concernée; que, en particulier, en vue d'assurer l'équilibre des intérêts en cause, tout en garantissant une concurrence effective, les États membres peuvent préciser les conditions dans lesquelles des données à caractère personnel peuvent être utilisées et communiquées à des tiers dans le cadre d'activités légitimes de gestion courante des entreprises et autres organismes; que, de même, ils peuvent préciser les conditions dans lesquelles la communication à des tiers de données à caractère personnel peut être effectuée à des fins de prospection commerciale, ou de prospection faite par une association à but caritatif ou par d'autres associations ou fondations, par exemple à caractère politique, dans le respect de dispositions visant à permettre aux personnes concernées de s'opposer sans devoir indiquer leurs motifs et sans frais au traitement des données les concernant;

(31) considérant qu'un traitement de données à caractère personnel doit être également considéré comme licite lorsqu'il est effectué en vue de protéger un intérêt essentiel à la vie de la personne concernée;

(32) considérant qu'il appartient aux législations nationales de déterminer si le responsable du traitement investi d'une mission d'intérêt public ou d'une mission relevant de l'exercice de l'autorité publique doit être une administration publique ou une autre personne soumise au droit public ou au droit privé, telle qu'une association professionnelle;

(33) considérant que les données qui sont susceptibles par leur nature de porter atteinte aux libertés fondamentales ou à la vie privée ne devraient pas faire l'objet d'un traitement, sauf consentement explicite de la personne concernée; que, cependant, des dérogations à cette interdiction doivent être expressément prévues pour répondre à des besoins spécifiques, en particulier lorsque le traitement de ces données est mis en œuvre à certaines fins relatives à la santé par des personnes soumises à une obligation de secret professionnel ou pour la réalisation d'activités légitimes par certaines associations ou fondations dont l'objet est de permettre l'exercice de libertés fondamentales;

(34) considérant que les États membres doivent également être autorisés à déroger à l'interdiction de traiter . des catégories de données sensibles lorsqu'un motif d'intérêt public important le justifie dans des domaines tels que la santé publique et la protection sociale — particulièrement afin d'assurer la qualité et la rentabilité en ce qui concerne les procédures utilisées pour régler les demandes de prestations et de services dans le régime d'assurance maladie — et tels que la recherche scientifique et les statistiques publiques; qu'il leur incombe, toutefois, de prévoir les garanties appropriées et spécifiques aux fins de protéger les droits fondamentaux et la vie privée des personnes;

(35) considérant, en outre, que le traitement de données à caractère personnel par des autorités publiques pour la réalisation de fins prévues par le droit constitutionnel ou le droit international public, au profit d'associations à caractère religieux officiellement reconnues, est mis en œuvre pour un motif d'intérêt public important;

(36) considérant que, si, dans le cadre d'activités liées à des élections, le fonctionnement du système démocratique suppose, dans certains États membres, que les partis politiques collectent des données relatives aux opinions politiques des personnes, le traitement de telles données peut être autorisé en raison de l'intérêt public important, à condition que des garanties appropriées soient prévues;

(37) considérant que le traitement de données à caractère personnel à des fins de journalisme ou d'expression artistique ou littéraire, notamment dans le domaine audiovisuel, doit bénéficier de dérogations ou de limitations de certaines dispositions de la présente directive dans la mesure où elles sont nécessaires

à la conciliation des droits fondamentaux de la personne avec la liberté d'expression, et notamment la liberté de recevoir ou de communiquer des informations, telle que garantie notamment à l'article 10 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales; qu'il incombe donc aux États membres, aux fins de la pondération entre les droits fondamentaux, de prévoir les dérogations et limitations nécessaires en ce qui concerne les mesures générales relatives à la légalité du traitement des données, les mesures relatives au transfert des données vers des pays tiers ainsi que les compétences des autorités de contrôle, sans qu'il y ait lieu toutefois de prévoir des dérogations aux mesures visant à garantir la sécurité du traitement; qu'il conviendrait également de conférer au moins à l'autorité de contrôle compétente en la matière certaines compétences *a posteriori*, consistant par exemple à publier périodiquement un rapport ou à saisir les autorités judiciaires;

(38) considérant que le traitement loyal des données suppose que les personnes concernées puissent connaître l'existence des traitements et bénéficier, lorsque des données sont collectées auprès d'elles, d'une information effective et complète au regard des circonstances de cette collecte;

(39) considérant que certains traitements portent sur des données que le responsable n'a pas collectées directement auprès de la personne concernée; que, par ailleurs, des données peuvent être légitimement communiquées à un tiers, alors même que cette communication n'avait pas été prévue lors de la collecte des données auprès de la personne concernée; que, dans toutes ces hypothèses, l'information de la personne concernée doit se faire au moment de l'enregistrement des données ou, au plus tard, lorsque les données sont communiquées pour la première fois à un tiers;

(40) considérant que, cependant, il n'est pas nécessaire d'imposer cette obligation si la personne concernée est déjà informée; que, en outre, cette obligation n'est pas prévue si cet enregistrement ou cette communication sont expressément prévus par la loi ou si l'information de la personne concernée se révèle impossible ou implique des efforts disproportionnés, ce qui peut être le cas pour des traitements à des fins historiques, statistiques ou scientifiques; que, à cet égard, peuvent être pris en considération le nombre de personnes concernées, l'ancienneté des données, ainsi que les mesures compensatrices qui peuvent être prises;

(41) considérant que toute personne doit pouvoir bénéficier du droit d'accès aux données la concernant qui font l'objet d'un traitement, afin de s'assurer notamment de leur exactitude et de la licéité de leur traitement; que, pour les mêmes raisons, toute personne doit en outre avoir le droit de connaître la logique qui sous-tend le traitement automatisé des données la concernant, au moins dans le cas des décisions automatisées visées à l'article 15 paragraphe 1; que ce droit ne doit pas porter atteinte au secret des affaires ni à la propriété intellectuelle, notamment au droit d'auteur protégeant le logiciel; que cela ne doit toutefois pas aboutir au refus de toute information de la personne concernée;

(42) considérant que les États membres peuvent, dans l'intérêt de la personne concernée ou en vue de protéger les droits et libertés d'autrui, limiter les droits d'accès et d'information; qu'ils peuvent, par exemple, préciser que l'accès aux données à caractère médical ne peut être obtenu que par l'intermédiaire d'un professionnel de la santé;

(43) considérant que des restrictions aux droits d'accès et d'information, ainsi qu'à certaines obligations mises à la charge du responsable du traitement de données, peuvent également être prévues par les États membres dans la mesure où elles sont nécessaires à la sauvegarde, par exemple, de la sûreté de l'État, de la défense, de la sécurité publique, d'un intérêt économique ou financier important d'un État membre ou de l'Union européenne, ainsi qu'à la recherche et à la poursuite d'infractions pénales ou de manquements à la déontologie des professions réglementées; qu'il convient d'énumérer, au titre des exceptions et limitations, les missions de contrôle, d'inspection ou de réglementation nécessaires dans les trois derniers domaines précités concernant la sécurité publique, l'intérêt économique ou financier et la répression pénale; que cette enumeration de missions concernant ces trois domaines n'affecte pas la légitimité d'exceptions et de restrictions pour des raisons de sûreté de l'État et de défense;

(44) considérant que les États membres peuvent être amenés, en venu de dispositions du droit communautaire, à déroger aux dispositions de la présente directive concernant le droit d'accès, l'information des personnes et la qualité des données, afin de sauvegarder certaines finalités parmi celles visées ci-dessus;

(45) considérant que, dans le cas où des données pourraient faire l'objet d'un traitement licite sur le fondement d'un intérêt public, de l'exercice de l'autorité publique ou de l'intérêt légitime d'une personne, toute personne concernée devrait, toutefois, avoir le droit de s'opposer, pour des raisons prépondérantes et légitimes tenant à sa situation particulière, à ce que les données la concernant fassent l'objet d'un traitement; que les États membres ont, néanmoins, la possibilité de prévoir des dispositions nationales contraires;

(46) considérant que la protection des droits et libertés des personnes concernées à l'égard du traitement de données à caractère personnel exige que des

mesures techniques et d'organisation appropriées soient prises tant au moment de la conception qu'à celui de la mise en œuvre du traitement, en vue d'assurer en particulier la sécurité et d'empêcher ainsi tout traitement non autorisé; qu'il incombe aux États membres de veiller au respect de ces mesures par les responsables du traitement; que ces mesures doivent assurer un niveau de sécurité approprié tenant compte de l'état de l'art et du coût de leur mise en œuvre au regard des risques présentés par les traitements et de la nature des données à protéger;

(47) considérant que, lorsqu'un message contenant des données à caractère personnel est transmis *via* un service de télécommunications ou de courrier électronique dont le seul objet est de transmettre des messages de ce type, c'est la personne dont émane le message, et non celle qui offre le service de transmission, qui sera normalement considérée comme responsable du traitement de données à caractère personnel contenues dans le message; que, toutefois, les personnes qui offrent ces services seront normalement considérées comme responsables du traitement des données à caractère personnel supplémentaires nécessaires au fonctionnement du service;

(48) considérant que la notification à l'autorité de contrôle a pour objet d'organiser la publicité des finalités du traitement, ainsi que de ses principales caractéristiques, en vue de son contrôle au regard des dispositions nationales prises en application de la présente directive;

(49) considérant que, afin d'éviter des formalités administratives inadéquates, des exonérations ou des simplifications de la notification peuvent être prévues par les États membres pour les traitements de données qui ne sont pas susceptibles de porter atteinte aux droits et libertés des personnes concernées, à condition qu'ils soient conformes à un acte pris par l'État membre qui en précise les limites; que des exonérations ou simplifications peuvent pareillement être prévues par les États membres dès lors qu'une personne désignée par le responsable du traitement de données s'assure que les traitements effectués ne sont pas susceptibles de porter atteinte aux droits et libertés des personnes concernées; que la personne ainsi détachée à la protection des données, employée ou non du responsable du traitement de données, doit être en mesure d'exercer ses fonctions en toute indépendance;

(50) considérant que des exonérations ou simplifications peuvent être prévues pour le traitement de données dont le seul but est de tenir un registre destiné, dans le respect du droit national, à l'information du public et qui est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime;

(51) considérant que, néanmoins, le bénéfice de la simplification ou de l'exonération de l'obligation de notification ne dispense le responsable du traitement de données d'aucune des autres obligations découlant de la présente directive;

(52) considérant que, dans ce contexte, le contrôle *a posteriori* par les autorités compétentes doit être en général considéré comme une mesure suffisante;

(53) considérant que, cependant, certains traitements sont susceptibles de présenter des risques particuliers au regard des droits et des libertés des personnes concernées, du fait de leur nature, de leur portée ou de leurs finalités telles que celle d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat, ou du fait de l'usage particulier d'une technologie nouvelle; qu'il appartient aux États membres, s'ils le souhaitent, de préciser dans leur législation de tels risques;

(54) considérant que, au regard de tous les traitements mis en œuvre dans la société, le nombre de ceux présentant de tels risques particuliers devrait être très restreint; que les États membres doivent prévoir, pour ces traitements, un examen préalable à leur mise en œuvre, effectué par l'autorité de contrôle ou par le détaché à la protection des données en coopération avec celle-ci; que, à la suite de cet examen préalable, l'autorité de contrôle peut, selon le droit national dont elle relève, émettre un avis ou autoriser le traitement des données; qu'un tel examen peut également être effectué au cours de l'élaboration soit d'une mesure législative du Parlement national, soit d'une mesure fondée sur une telle mesure législative, qui définisse la nature du traitement et précise les garanties appropriées;

(55) considérant que, en cas de non-respect des droits des personnes concernées par le responsable du traitement de données, un recours juridictionnel doit être prévu par les législations nationales; que les dommages que peuvent subir les personnes du fait d'un traitement illicite doivent être réparés par le responsable du traitement de données, lequel peut être exonéré de sa responsabilité s'il prouve que le fait dommageable ne lui est pas imputable, notamment lorsqu'il établit l'existence d'une faute de la personne concernée ou d'un cas de force majeure; que des sanctions doivent être appliquées à toute personne, tant de droit privé que de droit public, qui ne respecte pas les dispositions nationales prises en application de la présente directive;

(56) considérant que des flux transfrontaliers de données à caractère personnel sont nécessaires au développement du commerce international; que la protection des personnes garantie dans la Communauté par la présente directive ne s'oppose pas aux

transferts de données à caractère personnel vers des pays tiers assurant un niveau de protection adéquat: que le caractère adéquat du niveau de protection offert par un pays tiers doit s'apprécier au regard de toutes les circonstances relatives à un transfert ou à une catégorie de transferts;

(57) considérant, en revanche, que, lorsqu'un pays tiers n'offre pas un niveau de protection adéquat, le transfert de données à caractère personnel vers ce pays doit être interdit;

(58) considérant que des exceptions à cette interdiction doivent pouvoir être prévues dans certaines circonstances lorsque la personne concernée a donné son consentement, lorsque le transfert est nécessaire dans le contexte d'un contrat ou d'une action en justice, lorsque la sauvegarde d'un intérêt public important l'exige, par exemple en cas d'échanges internationaux de données entre les administrations fiscales ou douanières ou entre les services compétents en matière de sécurité sociale, ou lorsque le transfert est effectué à partir d'un registre établi par la loi et destiné à être consulté par le public ou par des personnes ayant un intérêt légitime; que, dans ce cas, un tel transfert ne devrait pas porter sur la totalité des données ni sur des catégories de données contenues dans ce registre; que, lorsqu'un registre est destiné à être consulté par des personnes qui ont un intérêt légitime, le transfert ne devrait pouvoir être effectué qu'à la demande de ces personnes ou lorsqu'elles en sont les destinataires;

(59) considérant que des mesures particulières peuvent être prises pour pallier l'insuffisance du niveau de protection dans un pays tiers lorsque le responsable du traitement présente des garanties appropriées; que, en outre, des procédures de négociation entre la Communauté et les pays tiers en cause doivent être prévues;

(60) considérant que, en tout état de cause, les transferts vers les pays tiers ne peuvent être effectués que dans le plein respect des dispositions prises par les États membres en application de la présente directive, et notamment de son article 8;

(61) considérant que les États membres et la Commission, dans leurs domaines de compétence respectifs, doivent encourager les milieux professionnels concernés à élaborer des codes de conduite en vue de favoriser, compte tenu des spécificités du traitement de données effectué dans certains secteurs, la mise en œuvre de la présente directive dans le respect des dispositions nationales prises pour son application;

(62) considérant que l'institution, dans les États membres, d'autorités de contrôle exerçant en toute indépendance leurs fonctions est un élément essentiel de la protection des personnes à l'égard du traitement des données à caractère personnel;

(63) considérant que ces autorités doivent être dotées des moyens nécessaires à l'exécution de leurs tâches, qu'il s'agisse des pouvoirs d'investigation et d'intervention, en particulier lorsque les autorités sont saisies de réclamations, ou du pouvoir d'ester en justice; qu'elles doivent contribuer à la transparence du traitement de données effectué dans l'État membre dont elles relèvent;

(64) considérant que les autorités des différents États membres seront appelées à se prêter mutuellement assistance dans la réalisation de leurs tâches afin d'assurer le plein respect des règles de protection dans l'Union européenne;

(65) considérant que, au niveau communautaire, un groupe de travail sur la protection des personnes à l'égard du traitement des données à caractère personnel doit être instauré et qu'il doit exercer ses fonctions en toute indépendance; que, compte tenu de cette spécificité, il doit conseiller la Commission et contribuer notamment à l'application homogène des règles nationales adoptées en application de la présente directive;

(66) considérant que, pour ce qui est du transfert de données vers les pays tiers, l'application de la présente directive nécessite l'attribution de compétences d'exécution à la Commission et l'établissement d'une procédure selon les modalités fixées dans la décision 87/373/CEE du Conseil [1];

(67) considérant qu'un accord sur un *modus vivendi* concernant les mesures d'exécution des actes arrêtés selon la procédure visée à l'article 189 B du traité est intervenu, le 20 décembre 1994, entre le Parlement européen, le Conseil et la Commission;

(68) considérant que les principes énoncés dans la présente directive et régissant la protection des droits et des libertés des personnes, notamment du droit à la vie privée, à l'égard du traitement des données à caractère personnel pourront être complétés ou précisés, notamment pour certains secteurs, par des règles spécifiques conformes à ces principes;

(69) considérant qu'il convient de laisser aux États membres un délai ne pouvant pas excéder trois ans à compter de l'entrée en vigueur des mesures nationales de transposition de la présente directive, pour leur permettre d'appliquer progressivement à tout traitement de données déjà mis en œuvre les nouvelles dispositions nationales susvisées; que,

[1] JO nº L 197 du 18. 7. 1987, p. 33.

afin de permettre un bon rapport coût-efficacité lors de la mise en œuvre de ces dispositions, les États membres sont autorisés à prévoir une période supplémentaire, expirant douze ans après la date d'adoption de la présente directive, pour la mise en conformité des fichiers manuels existants avec certaines dispositions de la directive; que, lorsque des données contenues dans de tels fichiers font l'objet d'un traitement manuel effectif pendant cette période transitoire supplémentaire, la mise en conformité avec ces dispositions doit être effectuée au moment de la réalisation de ce traitement;

(70) considérant qu'il n'y a pas lieu que la personne concernée donne à nouveau son consentement pour permettre au responsable de continuer à effectuer, après l'entrée en vigueur des dispositions nationales prises en application de la présente directive, un traitement de données sensibles nécessaire à l'exécution d'un contrat conclu sur la base d'un consentement libre et informé avant l'entrée en vigueur des dispositions précitées;

(71) considérant que la présente directive ne s'oppose pas à ce qu'un État membre réglemente les activités de prospection commerciale visant les consommateurs qui résident sur son territoire, dans la mesure où cette réglementation ne concerne pas la protection des personnes à l'égard du traitement de données à caractère personnel;

(72) considérant que la présente directive permet de prendre en compte, dans la mise en œuvre des règles qu'elle pose, le principe du droit d'accès du public aux documents administratifs,

ONT ARRÊTÉ LA PRÉSENTE DIRECTIVE:

CHAPITRE PREMIER

DISPOSITIONS GÉNÉRALES

Article premier

Objet de la directive

1. Les États membres assurent, conformément à la présente directive, la protection des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel.

2. Les États membres ne peuvent restreindre ni interdire la libre circulation des données à caractère personnel entre États membres pour des raisons relatives à la protection assurée en vertu du paragraphe 1.

Article 2

Définitions

Aux fins de la présente directive, on entend par:

a) «données à caractère personnel»: toute information concernant une personne physique identifiée ou identifiable (personne concernée); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale;

b) «traitement de données à caractère personnel» (traitement): toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction;

«fichier de données à caractère personnel» (fichier): tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique;

d) «responsable du traitement»: la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel; lorsque les finalités et les moyens du traitement sont déterminés par des dispositions législatives ou réglementaires nationales ou communautaires, le responsable du traitement ou les critères spécifiques pour le désigner peuvent être fixés par le droit national ou communautaire;

e) «sous-traitement»: la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement;

f) «tiers»: la personne physique ou morale, l'autorité publique, le service ou tout autre organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont habilitées à traiter les données;

g) «destinataire»: la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données, qu'il s'agisse ou non d'un tiers; les autorités qui sont susceptibles de recevoir communication de données dans le cadre d'une mission d'enquête particulière ne sont toutefois pas considérées comme des destinataires;

h) «consentement de la personne concernée»: toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement.

Article 3

Champ d'application

1. La présente directive s'applique au traitement de données à caractère personnel, automatisé en tout **ou** en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier.

2. La présente directive ne s'applique pas au traitement de données à caractère personnel:

— mis en œuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire, telles que celles prévues aux titres V et VI du traité sur l'Union européenne, et, en tout état de cause, aux traitements ayant pour objet la sécurité publique, la défense, la sûreté de **l'État** (y compris le bien-être économique de l'État lorsque ces traitements sont liés à des questions de sûreté de l'État) et les activités de l'État relatives à des domaines du droit pénal,

— effectué par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques.

Article 4

Droit national applicable

1. Chaque État membre applique les dispositions nationales qu'il arrête en vertu de la présente directive aux traitements de données à caractère personnel lorsque:

a) le traitement est effectué dans le cadre des activités d'un établissement du responsable du traitement sur le territoire de l'État membre; si un même responsable du traitement est établi sur le territoire de plusieurs États membres, il doit prendre les mesures nécessaires pour assurer le respect, par chacun de ses établissements, des obligations prévues par le droit national applicable;

b) le responsable du traitement n'est pas établi sur le territoire de l'État membre mais en un lieu où sa loi nationale s'applique en vertu du droit international public;

c) le responsable du traitement n'est pas établi sur le territoire de la Communauté et recourt, à des fins de traitement de données à caractère personnel, à des moyens, automatisés ou non, situés sur le territoire dudit État membre, sauf si ces moyens ne sont utilisés qu'à des fins de transit sur le territoire de la Communauté.

2. Dans le cas visé au paragraphe 1 point c), le responsable du traitement doit désigner un représentant établi **sur** le territoire dudit État membre, sans préjudice d'actions qui pourraient être introduites contre le responsable du traitement lui-même.

CHAPITRE **II**

CONDITIONS GÉNÉRALES DE LICÉITÉ DES TRAITEMENTS DE DONNÉES À CARACTÈRE PERSONNEL

Article 5

Les États membres précisent, dans les limites des dispositions du présent chapitre, les conditions dans lesquelles les traitements de données à caractère personnel sont licites.

SECTION I

PRINCIPES RELATIFS À LA QUALITÉ DES DONNÉES

Article 6

1. Les États membres prévoient que les données à caractère personnel doivent être:

a) traitées loyalement et licitement;

b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités. Un traitement ultérieur à des fins historiques, statistiques ou scientifiques n'est pas réputé incompatible pour autant que les États membres prévoient des garanties appropriées;

c) adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement;

d) exactes et, si nécessaire, mises à jour; toutes les mesures raisonnables doivent être prises pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées;

e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement. Les États membres prévoient des garanties appropriées pour les données à caractère personnel qui sont conservées au-delà de la période précitée, à des fins historiques, statistiques ou scientifiques.

2. Il incombe au responsable du traitement d'assurer le respect du paragraphe 1.

SECTION II

PRINCIPES RELATIFS À LA LÉGITIMATION DES TRAITEMENTS DE DONNÉES

Article 7

Les États membres prévoient que le traitement de données à caractère personnel ne peut être effectué que si:

a) la personne concernée a indubitablement donné son consentement

b) il est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci

il est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis

d) il est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée

e) il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées

ou

f) il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée, qui appellent une protection au titre de l'article 1" paragraphe 1.

SECTION III

CATÉGORIES PARTICULIÈRES DE TRAITEMENTS

Article 8

Traitements portant sur des catégories particulières de données

1. Les États membres interdisent le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle.

2. Le paragraphe 1 ne s'applique pas lorsque:

a) la personne concernée a donné son consentement explicite à un tel traitement, sauf dans le cas où la législation de l'Etat membre prévoit que l'interdiction visée au paragraphe 1 ne peut être levée par le consentement de la personne concernée

b) le traitement est nécessaire aux fins de respecter les obligations et les droits spécifiques du responsable du traitement en matière de droit du travail, dans la mesure où il est autorisé par une législation nationale prévoyant des garanties adéquates

c) le traitement est nécessaire à la défense des intérêts vitaux de la personne concernée ou d'une autre personne dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement

d) le traitement est effectué dans le cadre de leurs activités légitimes et avec des garanties appropriées par une fondation, une association ou tout autre organisme à but non lucratif et à finalité politique, philosophique, religieuse ou syndicale, à condition que le traitement se rapporte aux seuls membres de cet organisme ou aux personnes entretenant avec lui des contacts réguliers liés à sa finalité et que les

données ne soient pas communiquées à des tiers sans le consentement des personnes concernées

e) le traitement porte sur des données manifestement rendues publiques par la personne concernée ou est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice.

3. Le paragraphe 1 ne s'applique pas lorsque le traitement des données est nécessaire aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements ou de la gestion de services de santé et que le traitement de ces données est effectué par un praticien de la santé soumis par le droit national ou par des réglementations arrêtées par les autorités nationales compétentes au secret professionnel, ou par une autre personne également soumise à une obligation de secret équivalente.

4. Sous réserve de garanties appropriées, les Etats membres peuvent prévoir, pour un motif d'intérêt public important, des dérogations autres que celles prévues au paragraphe 2, soit par leur législation nationale, soit sur décision de l'autorité de contrôle.

5. Le traitement de données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté ne peut être effectué que sous le contrôle de l'autorité publique ou si des garanties appropriées et spécifiques sont prévues par le droit national, sous réserve des dérogations qui peuvent être accordées par l'État membre sur la base de dispositions nationales prévoyant des garanties appropriées et spécifiques. Toutefois, un recueil exhaustif des condamnations pénales ne peut être tenu que sous le contrôle de l'autorité publique.

Les États membres peuvent prévoir que les données relatives aux sanctions administrativesou aux jugements civils sont également traitées sous le contrôle de l'autorité publique.

6. Les dérogations au paragraphe 1 prévues aux paragraphes 4 et 5 sont notifiées à la Commission.

7. Les États membres déterminent les conditions dans lesquelles un numéro national d'identification ou tout autre identifiant de portée générale peut faire l'objet d'un traitement.

Article 9

Traitements de données à caractère personnel et liberté d'expression

Les États membres prévoient, pour les traitements de données à caractère personnel effectués aux seules fins de journalisme ou d'expression artistique ou littéraire, des exemptions et dérogations au présent chapitre, au chapitre IV et au chapitre VI dans la seule mesure où elles s'avèrent nécessaires pour concilier le droit à la vie privée avec les règles régissant la liberté d'expression.

SECTION IV

INFORMATION DE LA PERSONNE CONCERNÉE

Article 10

Informations en cas de collecte de données auprès de la personne concernée

Les États membres prévoient que le responsable du traitement ou son représentant doit fournir à la personne auprès de laquelle il collecte des données la concernant au moins les informations énumérées ci-dessous, sauf si la personne en est déjà informée:

a) l'identité du responsable du traitement et, le cas échéant, de son représentant;

b) les finalités du traitement auquel les données sont destinées;

c) toute information supplémentaire telle que:

— les destinataires ou les catégories de destinataires des données,

— le fait de savoir si la réponse aux questions est obligatoire ou facultative ainsi que les conséquences éventuelles d'un défaut de réponse.

l'existence d'un droit d'accès aux données la concernant et de rectification de ces données,

dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont collectées, ces informations supplémentaires sont nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données.

Article 11

Informations lorsque les données n'ont pas été collectées auprès de la personne concernée

1. Lorsque les données n'ont pas été collectées auprès de la personne concernée, les États membres prévoient que le responsable du traitement ou son représentant doit, dès l'enregistrement des données ou, si une communication de données à un tiers est envisagée, au plus tard lors de la première communication de données, fournir à la personne concernée au moins les informations énumérées ci-dessous, sauf si la personne en est déjà informée:

a) l'identité du responsable du traitement et, le cas échéant, de son représentant;

b) les finalités du traitement;

c) toute information supplémentaire telle que:

— les catégories de données concernées,

— les destinataires ou les catégories de destinataires des données,

— l'existence d'un droit d'accès aux données la concernant et de rectification de ces données,

dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont collectées, ces informations supplémentaires sont nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données.

2. Le paragraphe 1 ne s'applique pas lorsque, en particulier pour un traitement à finalité statistique ou de recherche historique ou scientifique, l'information de la personne concernée se révèle impossible ou implique des efforts disproportionnés ou si la législation prévoit expressément l'enregistrement ou la communication des données. Dans ces cas, les États membres prévoient des garanties appropriées.

SECTION V

DROIT D'ACCÈS DE LA PERSONNE CONCERNÉE AUX DONNÉES

Article 12

Droit d'accès

Les États membres garantissent à toute personne concernée le droit d'obtenir du responsable du traitement:

a) sans contrainte, à des intervalles raisonnables et sans délais ou frais excessifs:

— la confirmation que des données la concernant sont ou ne sont pas traitées, ainsi que des informations portant au moins sur les finalités du traitement, les catégories de données sur lesquelles il porte et les destinataires ou les catégories de destinataires auxquels les données sont communiquées,

— la communication, sous une forme intelligible, des données faisant l'objet des traitements, ainsi que de toute information disponible sur l'origine des données,

— la connaissance de la logique qui sous-tend tout traitement automatisé des données la concernant, au moins dans le cas des décisions automatisées visées à l'article 15 paragraphe 1;

b) selon le cas, la rectification, l'effacement ou le verrouillage des données dont le traitement n'est pas conforme à la présente directive, notamment en raison du caractère incomplet ou inexact des données;

c) la notification aux tiers auxquels les données ont été communiquées de toute rectification, tout effacement ou tout verrouillage effectué conformément au point b), si cela ne s'avère pas impossible ou ne suppose pas un effort disproportionné.

SECTION VI

EXCEPTIONS ET LIMITATIONS

Article 13

Exceptions et limitations

1. Les États membres peuvent prendre des mesures législatives visant à limiter la portée des obligations et des droits prévus à l'article 6 paragraphe 1, à l'article 10, à l'article 11 paragraphe 1 et aux articles 12 et 21, lorsqu'une telle limitation constitue une mesure nécessaire pour sauvegarder:

a) la sûreté de l'État;

b) la défense;

c) la sécurité publique;

d) la prévention, la recherche, la détection et la poursuite d'infractions pénales ou de manquements à la déontologie dans le cas des professions réglementées;

e) un intérêt économique ou financier important d'un État membre ou de l'Union européenne, y compris dans les domaines monétaire, budgétaire et fiscal;

f) une mission de contrôle, d'inspection ou de réglementation relevant, même à titre occasionnel, de l'exercice de l'autorité publique, dans les cas visés aux points c), d) et e);

g) la protection de la personne concernée ou des droits et libertés d'autrui.

2. Sous réserve de garanties légales appropriées, excluant notamment que les données puissent être utilisées aux fins de mesures ou de décisions se rapportant à des personnes précises, les États membres peuvent, dans le cas où il n'existe manifestement aucun risque d'atteinte à la vie privée de la personne concernée, limiter par une mesure législative les droits prévus à l'article 12 lorsque les données sont traitées exclusivement aux fins de la recherche scientifique ou sont stockées sous la forme de données à caractère personnel pendant une durée n'excédant pas celle nécessaire à la seule finalité d'établissement de statistiques.

SECTION VII

DROIT D'OPPOSITION DE LA PERSONNE CONCERNÉE

Article 14

Droit d'opposition de la personne concernée

Les États membres reconnaissent à la personne concernée le droit:

a) au moins dans les cas visés à l'article 7 points e) et f), de s'opposer à tout moment, pour des raisons prépondérantes et légitimes tenant à sa situation particulière, à ce que des données la concernant fassent l'objet

d'un traitement, sauf en cas de disposition contraire du droit national. En cas d'opposition justifiée, le traitement mis en œuvre par le responsable du traitement ne peut plus porter sur ces données;

b) de s'opposer, sur demande et gratuitement, au traitement des données à caractère personnel la concernant envisagé par le responsable du traitement à des fins de prospection

d'être informée avant que des données à caractère personnel ne soient pour la première fois communiquées à des tiers ou utilisées pour le compte de tiers à des fins de prospection et de se voir expressément offrir le droit de s'opposer, gratuitement, à ladite communication ou utilisation.

Les États membres prennent les mesures nécessaires pour garantir que les personnes concernées ont connaissance de l'existence du droit visé au point b) premier alinéa.

Article 15

Décisions individuelles automatisées

1. Les États membres reconnaissent à toute personne le droit de ne pas être soumise à une décision produisant des effets juridiques à son égard ou l'affectant de manière significative, prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité, tels que son rendement professionnel, son crédit, sa fiabilité, son comportement, etc.

2. Les États membres prévoient, sous réserve des autres dispositions de la présente directive, qu'une personne peut être soumise à une décision telle que celle visée au paragraphe 1 si une telle décision:

a) est prise dans le cadre de la conclusion ou de l'exécution d'un contrat, à condition que la demande de conclusion ou d'exécution du contrat, introduite par la personne concernée, ait été satisfaite ou que des mesures appropriées, telles que la possibilité de faire valoir son point de vue, garantissent la sauvegarde de son intérêt légitime

b) est autorisée par une loi qui précise les mesures garantissant la sauvegarde de l'intérêt légitime de la personne concernée.

SECTION VIII

CONFIDENTIALITÉ ET SÉCURITÉ DES TRAITEMENTS

Article 16

Confidentialité des traitements

Toute personne agissant sous l'autorité du responsable du traitement ou celle du sous-traitant, ainsi que le sous-traitant lui-même, qui accède à des données à caractère personnel ne peut les traiter que sur instruction du responsable du traitement, sauf en vertu d'obligations légales.

Article 17

Sécurité des traitements

1. Les États membres prévoient que le responsable du traitement doit mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite.

Ces mesures doivent assurer, compte tenu de l'état de l'art et des coûts liés à leur mise en œuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger.

2. Les États membres prévoient que le responsable du traitement, lorsque le traitement est effectué pour son compte, doit choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements à effectuer et qu'il doit veiller au respect de ces mesures.

3. La réalisation de traitements en sous-traitance doit être régie par un contrat ou un acte juridique qui lie le sous-traitant au responsable du traitement et qui prévoit notamment que:

— le sous-traitant n'agit que sur la seule instruction du responsable du traitement,

— les obligations visées au paragraphe 1, telles que définies par la législation de l'État membre dans lequel le sous-traitant est établi, incombent également à celui-ci.

4. Aux fins de la conservation des preuves, les éléments du contrat ou de l'acte juridique relatifs à la protection des données et les exigences portant sur les mesures visées au paragraphe 1 sont consignés par écrit ou sous une autre forme équivalente.

SECTION IX

NOTIFICATION

Article 18

Obligation de notification à l'autorité de contrôle

1. Les États membres prévoient que le responsable du traitement, ou le cas échéant son représentant, doit

adresser une notification à l'autorité de contrôle visée à l'article 28 préalablement à la mise en œuvre d'un traitement entièrement ou partiellement automatisé ou d'un ensemble de tels traitements ayant une même finalité ou des finalités liées.

2. Les États membres ne peuvent prévoir de simplification de la notification ou de dérogation à cette obligation que dans les cas et aux conditions suivants:

— lorsque, pour les catégories de traitement qui, compte tenu des données à traiter, ne sont pas susceptibles de porter atteinte aux droits et libertés des personnes concernées, ils précisent les finalités des traitements, les données ou catégories de données traitées, la ou les catégories de personnes concernées, les destinataires ou catégories de destinataires auxquels les données sont communiquées et la durée de conservation des données

et/ou

— lorsque le responsable du traitement désigne, conformément au droit national auquel il est soumis, un détaché à la protection des données à caractère personnel chargé notamment:

— d'assurer, d'une manière indépendante, l'application interne des dispositions nationales prises en application de la présente directive,

— de tenir un registre des traitements effectués par le responsable du traitement, contenant les informations visées à l'article 21 paragraphe 2,

et garantissant de la sorte que les traitements ne sont pas susceptibles de porter atteinte faux droits et libertés des personnes concernées.

3. Les États membres peuvent prévoir que le paragraphe 1 ne s'applique pas aux traitements ayant pour seul objet la tenue d'un registre qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime.

4. Les États membres peuvent prévoir une dérogation à l'obligation de notification ou une simplification de la notification pour les traitements visés à l'article 8 paragraphe 2 point d).

5. Les États membres peuvent prévoir que les traitements non automatisés de données à caractère personnel, ou certains d'entre eux, font l'objet d'une notification, éventuellement simplifiée.

Article 19

Contenu de la notification

1. Les États membres précisent les informations qui doivent figurer dans la notification. Elles comprennent au minimum:

a) le nom et l'adresse du responsable du traitement et, le cas échéant, de son représentant;

b) la ou les finalités du traitement;

c) une description de la ou des catégories de personnes concernées et des données ou des catégories de données s'y rapportant;

d) les destinataires ou les catégories de destinataires auxquels les données sont susceptibles d'être communiquées;

e) les transferts de données envisagés à destination de pays tiers;

f) une description générale permettant d'apprécier de façon préliminaire le caractère approprié des mesures prises pour assurer la sécurité du traitement en application de l'article 17.

2. Les États membres précisent les modalités de notification à l'autorité de contrôle des changements affectant les informations visées au paragraphe 1.

Article 20

Contrôles préalables

1. Les États membres précisent les traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées et veillent à ce que ces traitements soient examinés avant leur mise en œuvre.

2. De tels examens préalables sont effectués par l'autorité de contrôle après réception de la notification du responsable du traitement ou par le détaché à la protection des données, qui, en cas de doute, doit consulter l'autorité de contrôle.

3. Les États membres peuvent aussi procéder à un tel examen dans le cadre de l'élaboration soit d'une mesure du Parlement national, soit d'une mesure fondée sur une telle mesure législative, qui définisse la nature du traitement et fixe des garanties appropriées.

Article 21

Publicité des traitements

1. Les États membres prennent des mesures pour assurer la publicité des traitements.

2. Les États membres prévoient que l'autorité de contrôle tient un registre des traitements notifiés en vertu de l'article 18.

Le registre contient au minimum les informations énumérées à l'article 19 paragraphe 1 points a) à e).

Le registre peut être consulté par toute personne.

3. En ce qui concerne les traitements non soumis à notification, les États membres prévoient que le responsable du traitement ou une autre instance qu'ils désignent communique sous une forme appropriée à toute personne qui en fait la demande au moins les informations visées à l'article 19 paragraphe 1 points a) à e).

Les États membres peuvent prévoir que la présente disposition ne s'applique pas aux traitements ayant pour seul objet la tenue d'un registre qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime.

CHAPITRE III

RECOURS JURIDICTIONNELS, RESPONSABILITÉ ET SANCTIONS

Article 22

Recours

Sans préjudice du recours administratif qui peut être organisé, notamment devant l'autorité de contrôle visée à l'article 28, antérieurement à la saisine de l'autorité judiciaire, les États membres prévoient que toute personne dispose d'un recours juridictionnel en cas de violation des droits qui lui sont garantis par les dispositions nationales applicables au traitement en question.

Article 23

Responsabilité

1. Les États membres prévoient que toute personne ayant subi un dommage du fait d'un traitement illicite ou de toute action incompatible avec les dispositions nationales prises en application de la présente directive a le droit d'obtenir du responsable du traitement réparation du préjudice subi.

2. Le responsable du traitement peut être exonéré partiellement ou totalement de cette responsabilité s'il prouve que le fait qui a provoqué le dommage ne lui est pas imputable.

Article 24

Sanctions

Les États membres prennent les mesures appropriées pour assurer la pleine application des dispositions de la présente directive et déterminent notamment les sanctions à appliquer en cas de violation des dispositions prises en application de la présente directive.

CHAPITRE IV

TRANSFERT DE DONNÉES À CARACTÈRE PERSONNEL VERS DES PAYS TIERS

Article 25

Principes

1. Les États membres prévoient que le transfert vers un pays tiers de données à caractère personnel faisant l'objet d'un traitement, ou destinées à faire l'objet d'un traitement après leur transfert, ne peut avoir keu que si, sous réserve du respect des dispositions nationales prises en application des autres dispositions de la présente directive, le pays tiers en question assure un niveau de protection adéquat.

2. Le caractère adéquat du niveau de protection offert par un pays tiers s'apprécie au regard de toutes les circonstances relatives à un transfert ou à une catégorie

de transferts de données; en particulier, sont prises en considération la nature des données, la finalité et la durée du ou des traitements envisagés, les pays d'origine et de destination finale, les règles de droit, générales ou sectorielles, en vigueur dans le pays tiers en cause, ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées.

3. Les États membres et la Commission " s'informent mutuellement des cas dans lesquels ils estiment qu'un pays tiers n'assure pas un niveau de protection adéquat au sens du paragraphe 2.

4. Lorsque la Commission constate, conformément à la procédure prévue à l'article 31 paragraphe 2, qu'un pays tiers n'assure pas un niveau de protection adéquat au sens du paragraphe 2 du présent article, les États membres prennent les mesures nécessaires en vue d'empêcher tout transfert de même nature vers le pays tiers en cause.

5. La Commission engage, au moment opportun, des négociations en vue de remédier à la situation résultant de la constatation faite en application du paragraphe 4.

6. La Commission peut constater, conformément à la procédure prévue à l'article 31 paragraphe 2, qu'un pays tiers assure un niveau de protection adéquat au sens du paragraphe 2 du présent article, en raison de sa législation interne ou de ses engagements internationaux, souscrits notamment à l'issue des négociations visées au paragraphe 5, en vue de la protection de la vie privée et des libertés et droits fondamentaux des personnes.

Les États membres prennent les mesures nécessaires pour se conformer à la décision de la Commission.

Article 26

Dérogations

1. Par dérogation à l'article 25 et sous réserve de dispositions contraires de leur droit national régissant des cas particuliers, les États membres prévoient qu'un transfert de données à caractère personnel vers un pays tiers n'assurant pas un niveau de protection adéquat au sens de l'article 25 paragraphe 2 peut être effectué, à condition que:

a) la personne concernée ait indubitablement donné son consentement au transfert envisagé

b) le transfert soit nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou à l'exécution de mesures précontractuelles prises à la demande de la personne concernee

le transfert soit nécessaire à la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers

d) le transfert soit nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important, ou pour la constatation, l'exercice ou la défense d'un droit en justice

le transfert soit nécessaire à la sauvegarde de l'intérêt vital de la personne concernée

f) le transfert intervienne au départ d'un registre public qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime, dans la mesure où les conditions légales pour la consultation sont remplies dans le cas particulier.

2. Sans préjudice du paragraphe 1, un État membre peut autoriser un transfert, ou un ensemble de transferts, de données à caractère personnel vers un pays tiers n'assurant pas un niveau de protection adéquat au sens de l'article 25 paragraphe 2, lorsque le responsable du traitement offre des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants; ces garanties peuvent notamment résulter de clauses contractuelles appropriées.

3. L'État membre informe la Commission et les autres États membres des autorisations qu'il accorde en application du paragraphe 2.

En cas d'opposition exprimée par un autre État membre ou par la Commission et dûment justifiée au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, la Commission arrête les mesures appropriées, conformément à la procédure prévue à l'article 31 paragraphe 2.

Les États membres prennent les mesures nécessaires pour se conformer à la décision de la Commission.

4. Lorsque la Commission décide, conformément à la procédure prévue à l'article 31 paragraphe 2, que certaines clauses contractuelles types présentent les garanties suffisantes visées au paragraphe 2, les États membres prennent les mesures nécessaires pour se conformer à la décision de la Commission.

CHAPITRE V

CODES DE CONDUITE

Article 27

1. Les États membres et la Commission encouragent l'élaboration de codes de conduite destinés à contribuer, en fonction de la spécificité des secteurs, à la bonne application des dispositions nationales prises par les États membres en application de la présente directive.

2. Les États membres prévoient que les associations professionnelles et les autres organisations représentant d'autres catégories de responsables du traitement qui ont élaboré des projets de codes nationaux ou qui ont l'intention de modifier ou de proroger des codes nationaux existants peuvent les soumettre à l'examen de l'autorité nationale.

Les États membres prévoient que cette autorité s'assure, entre autres, de la conformité des projets qui lui sont soumis avec les dispositions nationales prises en application de la présente directive. Si elle l'estime opportun, l'autorité recueille les observations des personnes concernées ou de leurs représentants.

3. Les projets de codes communautaires, ainsi que les modifications ou prorogations de codes communautaires existants, peuvent être soumis au groupe visé à l'article 29. Celui-ci se prononce, entre autres, sur la conformité des projets qui lui sont soumis avec les dispositions nationales prises en application de la présente directive. S'il l'estime opportun, il recueille les observations des personnes concernées ou de leurs représentants. La Commission peut assurer une publicité appropriée aux codes qui ont été approuvés par le groupe.

CHAPITRE VI

AUTORITÉ DE CONTRÔLE ET GROUPE DE PROTECTION DES PERSONNES L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

Article 28

Autorité de contrôle

1. Chaque État membre prévoit qu'une ou plusieurs autorités publiques sont chargées de surveiller l'application, sur son territoire, des dispositions adoptées par les États membres en application de la présente directive.

Ces autorités exercent en toute indépendance les missions dont elles sont investies.

2. Chaque État membre prévoit que les autorités de contrôle sont consultées lors de l'élaboration des mesures réglementaires ou administratives relatives à la protection des droits et libertés des personnes à l'égard du traitement de données à caractère personnel.

3. Chaque autorité de contrôle dispose notamment:

— de pouvoirs d'investigation, tels que le pouvoir d'accéder aux données faisant l'objet d'un traitement et de recueillir toutes les informations nécessaires à l'accomplissement de sa mission de contrôle,

— de pouvoirs effectifs d'intervention, tels que, par exemple, celui de rendre des avis préalablement à la mise en œuvre des traitements, conformément à l'article 20, et d'assurer une publication appropriée de ces avis ou celui d'ordonner le verrouillage, l'effacement ou la destruction de données, ou d'interdire temporairement ou définitivement un traitement, ou celui d'adresser un avertissement ou une admonestation au responsable du traitement ou celui de saisir les parlements nationaux ou d'autres institutions politiques,

— du pouvoir d'ester en justice en cas de violation des dispositions nationales prises en application de la présente directive ou du pouvoir de porter ces violations à la connaissance de l'autorité judiciaire.

Les décisions de l'autorité de contrôle faisant grief peuvent faire l'objet d'un recours juridictionnel.

4. Chaque autorité de contrôle peut être saisie par toute personne, ou par une association la représentant, d'une demande relative à la protection de ses droits et libertés à l'égard du traitement de données à caractère personnel. La personne concernée est informée des suites données à sa demande.

Chaque autorité de contrôle peut, en particulier, être saisie par toute personne d'une demande de vérification de la licéité d'un traitement lorsque les dispositions nationales prises en vertu de l'article 13 de la présente directive sont d'application. La personne est à tout le moins informée de ce qu'une vérification a eu lieu.

5. Chaque autorité de contrôle établit à intervalles réguliers un rapport sur son activité. Ce rapport est publié.

6. Indépendamment du droit national applicable au traitement en cause, chaque autorité de contrôle a compétence pour exercer, sur le territoire de l'État membre dont elle relève, les pouvoirs dont elle est investie conformément au paragraphe 3. Chaque autorité peut être appelée à exercer ses pouvoirs sur demande d'une autorité d'un autre État membre.

Les autorités de contrôle coopèrent entre elles dans la mesure nécessaire à l'accomplissement de leurs missions, notamment en échangeant toute information utile.

7. Les États membres prévoient que les membres et agents des autorités de contrôle sont soumis, y compris après cessation de leurs activités, à l'obligation du secret professionnel à l'égard des informations confidentielles auxquelles ils ont accès.

Article 29

Groupe de protection des personnes à l'égard du traitement des données à caractère personnel

1. Il est institué un groupe de protection des personnes à l'égard du traitement des données à caractère personnel, ci-après dénommé «groupe».

Le groupe a un caractère consultatif et indépendant.

2. Le groupe se compose d'un représentant de l'autorité ou des autorités de contrôle désignées par chaque État membre, d'un représentant de l'autorité ou des autorités créées pour les institutions et organismes communautaires et d'un représentant de la Commission.

Chaque membre du groupe est désigné par l'institution, l'autorité ou les autorités qu'il représente. Lorsqu'un État membre a désigné plusieurs autorités de contrôle, celles-ci procèdent à la nomination d'un représentant commun. Il en va de même pour les autorités créées pour les institutions et organismes communautaires.

3. Le groupe prend ses décisions à la ma|onté simple des représentants des autorités de contrôle.

4. Le groupe élit son président. La durée du mandat du président est de deux ans. Le mandat est renouvelable.

5. Le secrétariat du groupe est assuré par la Commission.

6. Le groupe établit son règlement intérieur.

7. Le groupe examine les questions mises à l'ordre du jour par son président, soit à l'initiative de celui-ci, soit à la demande d'un représentant des autorités de contrôle ou de la Commission.

Article 30

1. Le groupe a pour mission:

a) d'examiner toute question portant sur la mise en œuvre des dispositions nationales prises en application de la présente directive, en vue de contribuer à leur mise en œuvre homogène;

b) de donner à la Commission un avis sur le niveau de protection dans la Communauté et dans les pays tiers;

c) de conseiller la Commission sur tout projet de modification de la présente directive, sur tout projet de mesures additionnelles ou spécifiques à prendre pour sauvegarder les droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel, ainsi que sur tout autre projet de mesures communautaires ayant une incidence sur ces droits et libertés;

d) de donner un avis sur les codes de conduite élaborés au niveau communautaire.

2. Si le groupe constate que des divergences, susceptibles de porter atteinte à l'équivalence de la protection des personnes à l'égard du traitement des données à caractère personnel dans la Communauté, s'établissent entre les législations et pratiques des États membres, il en informe la Commission.

3. Le groupe peut émettre de sa propre initiative des recommandations sur toute question concernant la protection des personnes à l'égard du traitement de données à caractère personnel dans la Communauté.

4. Les avis et recommandations du groupe sont transmis à la Commission et au comité visé à l'article 31.

5. La Commission informe le groupe des suites qu'elle a données à ses avis et recommandations. Elle rédige à cet

effet un rapport qui est transmis également au Parlement européen et au Conseil. Ce rapport est publié.

6. Le groupe établit un rapport annuel sur l'état de la protection des personnes physiques à l'égard du traitement des données à caractère personnel dans la Communauté et dans les pays tiers, qu'il communique à la Commission, au Parlement européen et au Conseil. Ce rapport est publié.

CHAPITRE Vil

MESURES D'EXÉCUTION COMMUNAUTAIRES

Article 31

Comité

1. La Commission est assistée par un comité composé des représentants des États membres et présidé par le représentant de la Commission.

2. Le représentant de la Commission soumet au comité un projet des mesures à prendre. Le comité émet son avis sur ce projet, dans un délai que le président peut fixer en fonction de l'urgence de la question en cause.

L'avis est émis à la majorité prévue à l'article 148 paragraphe 2 du traité. Lors des votes au sein du comité, les voix des représentants des États membres sont affectées de la pondération définie à l'article précité. Le président ne prend pas part au vote.

La Commission arrête des mesures qui sont immédiatement applicables. Toutefois, si elles ne sont pas conformes à l'avis émis par le comité, ces mesures sont aussitôt communiquées par la Commission au Conseil. Dans ce cas:

— la Commission diffère l'application des mesures décidées par elle d'un délai de trois mois à compter de la date de la communication,

— le Conseil, statuant à la majorité qualifiée, peut prendre une décision différente dans le délai prévu au premier tiret.

DISPOSITIONS FINALES

Article 32

1. Les États membres mettent en vigueur les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la présente directive au plus tard à l'issue d'une période de trois ans à compter de son adoption.

Lorsque les États membres adoptent ces dispositions, celles-ci contiennent une référence à la présente directive ou sont accompagnées d'une telle référence lors de leur publication officielle. Les modalités de cette référence sont arrêtées par les États membres.

2. Les États membres veillent à ce que les traitements dont la mise en œuvre est antérieure à la date d'entrée en vigueur des dispositions nationales prises en application de la présente directive soient rendus conformes à ces dispositions au plus tard trois ans après cette date.

Par dérogation à l'alinéa précédent, les États membres peuvent prévoir que les traitements de données déjà contenues dans des fichiers manuels à la date d'entrée en vigueur des dispositions nationales prises en application de la présente directive seront rendus conformes aux articles 6, 7 et 8 de la présente directive dans un délai de douze ans à compter de la date d'adoption de celle-ci. Les États membres permettent toutefois à la personne concernée d'obtenir, à sa demande et notamment lors de l'exercice du droit d'accès, la rectification, l'effacement ou le verrouillage des données incomplètes, inexactes ou conservées d'une manière qui est incompatible avec les fins légitimes poursuivies par le responsable du traitement.

3. Par dérogation au paragraphe 2, les États membres peuvent prévoir, sous réserve des garanties appropriées, que les données conservées dans le seul but de la recher-

ehe historique ne soient pas rendues conformes aux articles 6, 7 et 8 de la présente directive.

4. Les États membres communiquent à la Commission le texte des dispositions de droit interne qu'ils adoptent dans le domaine régi par la présente directive.

Article 33

Périodiquement, et pour la première fois au plus tard trois ans après la date prévue à l'article 32 paragraphe 1, la Commission fait un rapport au Parlement européen et au Conseil sur l'application de la présente directive et l'assortit, le cas échéant, des propositions de modification appropriées. Ce rapport est publié.

La Commission examine, en particulier, l'application de la présente directive aux traitements de données constituées par des sons et des images, relatives aux personnes physiques, et elle présente les propositions appropriées qui pourraient s'avérer nécessaires en tenant compte des développements de la technologie de l'information et à la lumière de l'état des travaux sur la société de l'information.

Article 34

Les États membres sont destinataires de la présente directive.

Fait à Luxembourg, le 24 octobre 1995.

Par le Parlement européen	*Par le Conseil*
Le président	*Le président*
K. HÄNSCH	L. ATIENZA SERNA

BILAG 10

Bekendtgørelse af europæisk konvention af 28. januar 1981 om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger

I henhold til kgl. resolution af 6. oktober 1989 har Danmark ratificeret en den 28. januar 1981 i Strasbourg udfærdiget europæisk konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger.

Konventionens ordlyd er som følger:

Oversættelse

CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA

Preamble

The member States of the Council of Europe, signatory hereto,

Considering that the aim of the Council of Europe is to achieve greater unity between its members, based in particular on respect for the rule of law, as well as human rights and fundamental freedoms;

Considering that it is desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing;

Reaffirming at the same time their commitment to freedom of information regardless of frontiers ;

Recognising that it is necessary to reconcile the fundamental values of the respect for privacy and free flow of information between peoples,

Have agreed as follows:

CHAPTER I

General provisions

Article 1

Object and purpose

The purpose of this convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection").

Article 2

Definitions

For the purposes of this convention:

a. "personal data" means any information relating to an identified or identifiable individual ("data subject");

KONVENTION OM BESKYTTELSE AF DET ENKELTE MENNESKE I FORBINDELSE MED ELEKTRONISK DATABEHANDLING AF PERSONOPLYSNINGER

Præambel

Undertegnede medlemsstater af Europarådet har,

i betragtning af at Europarådets sigte er at opnå større enhed blandt dets medlemsstater, især med hensyn til respekt for lov og ret, for menneskerettighederne og for de grundlæggende frihedsrettigheder;

i betragtning af det ønskelige i at styrke beskyttelsen af den enkeltes grundlæggende frihedsrettigheder og andre rettigheder, især den enkeltes ret til privatlivets fred, og i erkendelse af den voksende grænseoverskridende strøm af personoplysninger, der gennemgår elektronisk databehandling;

idet de samtidigt bekræfter deres tilslutning til princippet om informationsfrihed uanset landegrænser; og

i erkendelse af at det er nødvendigt at forene de grundlæggende værdier bag respekten for privatlivets fred med den frie udveksling af informationer landene imellem,

indgået følgende aftale :

KAPITEL I

Almindelige bestemmelser

Artikel 1

Genstand og formål

Denne konvention har til formål inden for de kontraherende staters territorier, uanset statsborgerskab og bopæl at sikre det enkelte menneske respekt for dettes grundlæggende rettigheder og andre rettigheder, især for retten til privatlivets fred, i forbindelse med elektronisk databehandling af personoplysninger om den pågældende (»databeskyttelse«).

Artikel 2

Definitioner

I denne konvention betyder:

a. »personoplysninger»: enhver oplysning vedrørende en fysisk person hvis identitet er fastslået eller kan fastslås (»den registrerede«);

b. "automated data file" means any set of data undergoing automatic processing;

c. "automatic processing" includes the following operations if carried out in whole or in part by automated means : storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination ;

d. "controller of the file" means the natural or legal person, public authority, agency or any other body who is competent according to the national law to decide what should be the purpose of the automated data file, which categories of personal data should be stored and which operations should be applied to them.

Article 3

Scope

1. The Parties undertake to apply this convention to automated personal data files and automatic processing of personal data in the public and private sectors.

2. Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, or at any later time, give notice by a declaration addressed to the Secretary General of the Council of Europe:

a. that it will not apply this convention to certain categories of automated personal data files, a list of which will be deposited. In this list it shall not include, however, categories of automated data files subject under its domestic law to data protection provisions. Consequently, it shall amend this list by a new declaration whenever additional categories of automated personal data files are subjected to data protection provisions under its domestic law;

b. that it will also apply this convention to information relating to groups of persons, associations, foundations, companies, corporations and any other bodies consisting directly or indirectly of individuals, whether or not such bodies possess legal personality;

c. that it will also apply this convention to personal data files which are not processed automatically.

3. Any State which has extended the scope of this convention by any of the declarations provided for in sub-paragraph 2. b or c above may give notice in the said declaration that such ex-

fa, »elektronisk register« : enhver samling af oplysninger som behandles elektronisk;

c. »elektronisk databehandling« (foretaget helt eller delvist elektronisk: lagring af oplysninger, logisk og/eller aritmetisk behandling af lagrede oplysninger, ændring, sletning, genfinding og videregivelse eller spredning af lagrede oplysninger;

d. »den registeransvarlige« : den fysiske eller juridiske person, offentlige myndighed, institution eller anden instans, som i henhold til landets gældende lov bestemmer, hvilke formål det elektroniske register skal anvendes til, hvilke arter af personoplysninger, der skal lagres, og hvordan de skal behandles.

Artikel 3

Anvendelsesområde

1. De kontraherende parter forpligter sig til i den offentlige og den private sektor at anvende konventionen på elektroniske registre med personoplysninger og på elektronisk behandling af personoplysninger.

2. Enhver stat kan ved konventionens undertegnelse eller ved deponeringen af sit ratifikations-, accept-, godkendelses-, eller tiltrædelsesinstrument eller senere i en erklæring stilet til Europarådets generalsekretær meddele :

a. at den ikke vil anvende denne konvention på visse arter af elektroniske registre med personoplysninger, over hvilke en liste vil blive deponeret. Listen må dog ikke omfatte elektroniske registre af en art, som ifølge landets gældende lov er underkastet databeskyttelse. Den skal derfor ændre listen ved en ny erklæring, hver gang landets gældende bestemmelser om databeskyttelse bringes til anvendelse på nye arter elektroniske registre med personoplysninger;

b. at den vil anvende konventionen også på data vedrørende persongrupper, foreninger, stiftelser, selskaber, sammenslutninger og enhver anden form for institutioner, som direkte eller indirekte består af fysiske personer, uanset om sådanne institutioner har rets- og handleevne;

c. at den vil anvende konventionen også på personoplysninger, der ikke behandles elektronisk.

3. Enhver stat, der har udvidet konventionens anvendelsesområde ved en erklæring i henhold til stk. 2, b eller c, kan i erklæringen meddele, at udvidelsen kun omfatter visse arter

tensions shall apply only to certain categories of personal data files, a list of which will be deposited.

4. Any Party which has excluded certain categories of automated personal data files by a declaration provided for in sub-paragraph 2. a above may not claim the application of this convention to such categories by a Party which has not excluded them.

5. Likewise, a Party which has not made one or other of the extensions provided for in sub-paragraphs 2. b and c above may not claim the application of this convention on these points with respect to a Party which has made such extensions.

6. The declarations provided for in paragraph 2 above shall take effect from the moment of the entry into force of the convention with regard to the State which has made them if they have been made at the time of signature or deposit of its instrument of ratification, acceptance, approval or accession, or three months after their receipt by the Secretary General of the Council of Europe if they have been made at any later time. These declarations may be withdrawn, in whole or in part, by a notification addressed to the Secretary General of the Council of Europe. Such withdrawals shall take effect three months after the date of receipt of such notification.

elektroniske registre med personoplysninger, over hvilke en liste vil blive deponeret.

4. En kontraherende stat, som ved erklæring i henhold til stk. 2, a, har undtaget visse arter elektroniske registre med personoplysninger fra konventionens anvendelsesområde, kan ikke kræve, at en anden kontraherende stat, som ikke har udelukket dem, skal anvende konventionen på disse arter.

5. En kontraherende part, som ikke har foretaget nogen af de ved stk. 2, b og c, muliggjorte udvidelser kan tilsvarende ikke over for en kontraherende part, som har foretaget sådanne udvidelser, kræve konventionen anvendt på disse punkter.

6. De i stk. 2 anførte erklæringer har virkning fra den dato konventionen træder i kraft for den stat, som har afgivet dem, hvis de er afgivet ved undertegnelsen eller ved deponeringen af dens ratifikations-, accept-, godkendelses-, eller tiltrædelsesinstrument eller, hvis erklæringerne er afgivet på et senere tidspunkt, tre måneder efter at Europarådets generalsekretær har modtaget dem. Erklæringerne kan tilbagekaldes helt eller delvis ved meddelelse stilet til Europarådets generalsekretær. Tilbagekaldelse træder i kraft tre måneder efter at meddelelse derom er modtaget.

CHAPTER II

Basic principles for data protection

Article 4

Duties of the Parties

1. Each Party shall take the necessary measures in its domestic law to give effect to the basic principles for data protection set out in this chapter.

2. These measures shall be taken at the latest at the time of entry into force of this convention in respect of that Party.

Article 5

Quality of data

Personal data undergoing automatic processing shall be:

a. obtained and processed fairly and lawfully;

KAPITEL II

Grundprincipper for beskyttelsen

Artikel 4

De kontraherende parters pligter

1. Hver kontraherende part skal i deres nationale lovgivning træffe de nødvendige foranstaltninger for at gennemføre de grundprincipper for databeskyttelse, som opstilles i dette kapitel.

2. Disse foranstaltninger skal træffes senest, når konventionen træder i kraft for den pågældende kontraherende part.

Artikel 5

Oplysningernes beskaffenhed

Personoplysninger som behandles elektronisk skal :

a. indsamles og behandles rimeligt og lovligt;

b. stored for specified and legitimate purposes and not used in a way incompatible with those purposes;

c. adequate, relevant and not excessive in relation to the purposes for which they are stored;

d. accurate and, where necessary, kept up to date;

e. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

b. lagres til nærmere bestemte og lovlige formål, og må ikke anvendes på en måde, som er uforenelig med disse formål;

c. være relevante og tilstrækkelige, og ikke omfatte mere end, hvad der kræves til opfyldelsen af de formål, de er lagret til;

d. være nøjagtige og, om nødvendigt føres ajour;

e. opbevares i en form, som ikke muliggør identifikation af de registrerede personer længere end nødvendigt til det formål, de er lagret til.

Article 6

Special categories of data

Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.

Artikel 6

Særlige typer af oplysninger

Personoplysninger vedrørende race, politisk overbevisning, religiøs eller anden trosbekendelse, såvel som personoplysninger om helbred og seksuelle forhold, må ikke behandles elektronisk, medmindre national gældende lovgivning yder fornøden beskyttelse. Det samme gælder personoplysninger vedrørende straffedomme.

Article 7

Data security

Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.

Artikel 7

Sikkerhedsforanstaltninger

Elektroniske registre med personoplysninger skal sikres i fornødent omfang mod uagtsom eller uautoriseret ødelæggelse og tab ved uagtsomhed såvel som mod uautoriseret adgang, ændring og spredning.

Article 8

Additional safeguards for the data subject

Any person shall be enabled:

a. to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;

b. to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;

c. to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention;

Artikel 8

Yderligere beskyttelse af den registrerede

Enhver skal have mulighed for:

a. at få kendskab til tilstedeværelsen af et elektronisk register med personoplysninger og dets hovedformål, samt hvem den registeransvarlige er, dennes faste bopæl eller hovedforretningssted;

b. med passende mellemrum og uden unødig forsinkelse eller omkostning at få bekræftet, om der i det elektroniske register er lagret personoplysninger vedrørende den pågældende selv, samt til at blive underrettet om disse data i en forståelig form;

c. at få rettet, henholdsvis slettet, disse oplysninger, hvis de er blevet behandlet i strid med de bestemmelser i national lovgivning, der omhandler de i artikel 5 og 6 anførte grundlæggende principper;

d. to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with.

Article 9

Exceptions and restrictions

1. No exception to the provisions of Articles 5, 6 and 8 of this convention shall be allowed except within the limits defined in this article.

2. Derogation from the provisions of Articles 5, 6 and 8 of this convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of:

a. protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;

b. protecting the data subject or the rights and freedoms of others.

3. Restrictions on the exercise of the rights specified in Article 8, paragraphs b, c and d, may be provided by law with respect to automated personal data files used for statistics or for scientific research purposes when there is obviously no risk of an infringement of the privacy of the data subjects.

Article 10

Sanctions and remedies

Each Party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter.

Article 11

Extended protection

None of the provisions of this chapter shall be interpreted as limiting or otherwise affecting the possibility for a Party to grant data subjects a wider measure of protection than that stipulated in this convention.

d. klageadgang, hvis anmodning om bekræftelse, underreting, rettelse eller sletning, som anført i litra b og c ikke imødekommes.

Artikel 9

Undtagelser og begrænsninger

1. Artikel 5,6 og 8 må kun fraviges inden for de i denne artikel anførte grænser.

2. Artikel 5,6 og 8 kan fraviges, når den kontraherende parts gældende lovgivning hjemler det og undtagelsen er en nødvendig forholdsregel i et demokratisk samfund for at:

a. beskytte statens sikkerhed, offentlighedens sikkerhed, statens økonomiske interesser eller for at bekæmpe strafbare forhold;

b. beskytte den registrerede eller andres frihedsrettigheder og andre rettigheder.

3. Udøvelsen af de i artikel 8, b, c og d, fastlagte rettigheder kan ved lov begrænses for elektroniske registre med personoplysninger, der benyttes til statistiske eller forskningsmæssige formål, når der ikke åbenbart er fare for, at de registreredes retsbeskyttelse og ret til privatlivets fred herved krænkes.

Artikel 10

Sanktioner og retsmidler

Enhver kontraherende part forpligter sig til at indføre de fornødne sanktioner og retsmidler mod krænkelse af de bestemmelser i national lovgivning, der gennemfører de grundlæggende principper om databeskyttelse, der er anført i dette kapitel.

Artikel 11

Videregående beskyttelse

Ingen bestemmelser i dette kapitel kan fortolkes således, at de begrænser eller på anden måde indvirker på en kontraherende parts adgang til at yde de registrerede større beskyttelse end den, der er foreskrevet i denne konvention.

CHAPTER III

Transborder dataflows

Article 12

Transborder flows of personal data and domestic law

1. The following provisions shall apply to the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed.

2. A Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorisation transborder flows of personal data going to the territory of another Party.

3. Nevertheless, each Party shall be entitled to derogate from provisions of paragraph 2 :

a. insofar as its legislation includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other Party provide an equivalent protection;

b. when the transfer is made from its territory to the territory of a non-Contracting State through the intermediary of the territory of another Party, in order to avoid such transfers resulting in circumvention of the legislation of the Party referred to at the beginning of this paragraph.

KAPITEL III

International overførsel af personoplysninger

Artikel 12

Overførsel mellem landene af personoplysninger og national lovgivning

1. Følgende bestemmelser gælder for enhver form for international overførsel - uanset, hvilket medium, der anvendes - af personoplysninger, der undergives elektronisk databehandling eller er indsamlet med henblik på elektronisk databehandling.

2. En kontraherende part må ikke, med det ene formål at beskytte privatlivets fred, forbyde overførsel af personoplysninger til en anden kontraherende parts territorium eller gøre sådan overførsel betinget af særlig tilladelse.

3. Enhver kontraherende part kan dog fravige bestemmelsen i stk. 2:

a. i det omfang dens lovgivning indeholder udtrykkelige bestemmelser for visse kategorier af personoplysninger eller elektroniske registre med personoplysninger på grund af disses særlige karakter, medmindre den anden kontraherende parts lovgivning yder tilsvarende beskyttelse;

b. for at undgå, at overførsler resulterer i en omgåelse af dens lovgivning, som følge af, at overførslen sker gennem en kontraherende part til en part, der ikke er medunderskriver af konventionen.

CHAPTER IV

Mutual assistance

Article 13

Co-operation between Parties

1. The Parties agree to render each other mutual assistance in order to implement this convention.

2. For that purpose :

a. each Party shall designate one or more authorities, the name and address of each of which it shall communicate to the Secretaty General of the Council of Europe;

b. each Party which has designated more than one authority shall specify in its communication referred to in the previous subparagraph the competence of each authority.

3. An authority designated by a Party shall at the request of an auhority designated by another Party:

KAPITEL IV

Gensidig bistand

Artikel 13

Samarbejde mellem de kontraherende parter

1. De kontraherende parter er enige om at bistå hinanden med konventionens gennemførelse.

2. Med dette formål skal:

a. hver kontraherende part udpege en eller flere myndigheder og meddele Europarådets generalsekretær disse myndigheders betegnelse og adresse;

b. hver kontraherende part, der har udpeget mere end en myndighed, angive hver enkelt myndigheds kompetenceområde i den i litra a nævnte meddelelse.

3. En myndighed, der er udpeget af en kontraherende part, skal efter anmodning fra en myndighed udpeget af en anden kontraherende part:

a. furnish information on its law and administrative practice in the field of data protection;

b. take, in conformity with its domestic law and for the sole purpose of protection of privacy, all appropriate measures for furnishing factual information relating to specific automatic processing carried out in its territory, with the exception however of the personal data being processed.

a. give oplysninger om landets gældende lovgivning og administrative praksis vedrørende databeskyttelse;

b. i overensstemmelse med den nationale lovgivning og med det ene formål at beskytte privatlivets fred, træffe egnede foranstaltninger med henblik på at tilvejebringe faktiske oplysninger om en bestemt elektronisk databehandling, der udføres på den pågældende parts territorium, dog med undtagelse af oplysninger om de behandlede personoplysninger.

Article 14

Assistance to data subjects resident abroad

1. Each Party shall assist any person resident abroad to exercise the rights conferred by its domestic law giving effect to the principles set out in Articled of this convention.

2. When such a person resides in the territory of another Party he shall be given the option of submitting his request the intermediary of the authority designated by that Party.

3. The request for assistance shall contain all the necessary particulars, relating *inter alia* to :

a. the name, address and any other relevant particulars identifying the person making the request;

b. the automated personal data file to which the request pertains, or its controller;

c. the purpose of the request.

Artikel 14

Bistand til registrerede der er bosat i udlandet

1. Enhver kontraherende part skal bistå personer bosat i udlandet i udøvelsen af rettigheder, de nyder ifølge den kontraherende parts gældende lovgivning, som gennemfører de grundlæggende principper, der er anført i denne konventions artikel 8.

2. Personer bosat i en anden kontraherende part kan valgfrit lade deres anmodninger formidle gennem den myndighed, der er udpeget af denne kontraherende part.

3. Anmodning om bistand skal indeholde alle nødvendige oplysninger, herunder især oplysninger om:

a. navn, adresse og andre oplysninger, der er nødvendige for at identificere den person, som anmoder om bistand;

b. det elektroniske register med personoplysninger, som anmodningen angår, eller den registeransvarlige;

c. formålet med anmodningen.

Article 15

Safeguards concerning assistance rendered by designated authorities

1. An authority designated by a Party which has received information from an authority designated by another Party either accompanying a request for assistance or in reply to its own request for assistance shall not use that information for purposes other than those specified in the request for assistance.

2. Each Party shall see to it that the persons belonging to or acting on behalf of the designated authority shall be bound by appropriate obligations of secrecy or confidentiality with regard to that information.

Artikel 15

Sikkerhedsforanstaltninger i forbindelse med bistand, der ***er*** *ydet* ***af*** *de udpegede myndigheder*

1. En myndighed, der er udpeget af en kontraherende part, som i anledning af en anmodning om bistand eller som svar på myndighedens egen anmodning modtager oplysninger fra en myndighed, der er udpeget af en anden kontraherende part, må kun anvende disse oplysninger til de formål, der er anført i anmodningen om bistand.

2. Enhver kontraherende part skal sørge for, at de personer, der er tilknyttet den udpegede myndighed eller som handler på dennes vegne, er underkastet den fornødne tavshedspligt med hensyn til de i stk. 1 nævnte oplysninger.

3. In no case may a designated authority be allowed to make under Article 14, paragraph 2, a request for assistance on behalf of a data subject resident abroad, of its own accord and without the express consent of the person concerned.

Article 16

Refusal of requests for assistance

A designated authority to which a request for assistance is addressed under Article 13 or 14 of this convention may not refuse to comply with it unless:

a. the request is not compatible with the powers in the field of data protection of the authorities responsible for replying;

b. the request does not comply with the provisions of this convention;

c. compliance with the request would be incompatible with the sovereignty, security or public policy *(ordre public)* of the Party by which it was designated, or with the rights and fundamental freedoms of persons under the jurisdiction of the Party.

Article 17

Costs and procedures of assistance

1. Mutual assistance which the Parties render each other under Article 13 and assistance they render to data subjects abroad under Article 14 shall not give rise to the payment of any costs or fees other than those incurred for experts and interpreters. The latter costs or fees shall be borne by the Party which has designated the authority making the request for assistance.

2. The data subject may not be charged costs or fees in connection with the steps taken on his behalf in the territory of another Party other than those lawfully payable by residents ofthat Party.

3. Other details concerning the assistance relating in particular to the forms and procedures and the languages to be used, shall be established directly between the Parties concerned.

3. En udpeget myndighed må under ingen omstændigheder på eget initiativ anmode om bistand i henhold til artikel 14, stk. 2, for en registreret person bosat i udlandet uden den pågældendes udtrykkelige samtykke.

Artikel 16

Afvisning af anmodninger om bistand

En udpeget myndighed, der modtager en anmodning om bistand i henhold til artikel 13 eller 14, må ikke afvise at efterkomme anmodningen, medmindre:

a. anmodningen falder uden for de beføjelser på databeskyttelsesområdet, som er tillagt de myndigheder, der er ansvarlige for besvarelsen;

b. anmodningen ikke er i overensstemmelse med bestemmelserne i denne konvention ;

c. efterkommelse af anmodningen ville være uforenelig med den udpegede kontraherende parts suverænitet, sikkerhed eller ordre public, eller med de grundlæggende frihedsrettigheder og andre rettigheder som tilkommer de personer, der er undergivet denne kontraherende parts jurisdiktion.

Artikel 17

Omkostninger og fremgangsmåde i forbindelse med bistand

1. For den gensidige bistand, som de kontraherende parter yder hinanden i henhold til artikel 13, eller den bistand, som de yder registrerede personer i udlandet i henhold til artikel 14, kan der ikke kræves betaling af omkostninger eller gebyrer, medmindre der er tale om udgifter til eksperthjælp og tolkning. Sidstsnævnte udgifter afholdes af den kontraherende part, der har udpeget den myndighed, der har fremsat anmodningen om bistand.

2. En registreret må ikke afkræves omkostninger eller gebyrer i forbindelse med de foranstaltninger, der er truffet for hans skyld af en anden kontraherende part på dennes territorium, bortset fra hvad personer bosat i denne anden kontraherende part lovligt kan afkræves.

3. Øvrige enkeltheder i forbindelse med bistand, især med hensyn til form og fremgangsmåde samt med hensyn til hvilke sprog, der skal anvendes, fastlægges direkte mellem de berørte kontraherende parter.

CHAPTER V

Consultative committee

Article 18

Composition of the committee

1. A Consultative Committee shall be set up after the entry into force of this convention.

2. Each Party shall appoint a representative to the committee and a deputy representative. Any member State of the Council of Europe which is not a Party to the convention shall have the right to be represented on the committee by an observer.

3. The Consultative Committee may, by unanimous decision, invite any non-member State of the Council of Europe which is not a Party to the convention to be represented by an observer at a given meeting.

Article 19

Functions of the committee

The Consultative Committee:

a. may make proposals with a view to facilitating or improving the application of the convention;

b. may make proposals for amendment of this convention in accordance with Article 21 ;

c. shall formulate its opinion on any proposal for amendment of this convention which is referred to it in accordance with Article 21, paragraph 3 ;

d. may, at the request of a Party, express an opinion on any question concerning the application of this convention.

Article 20

Procedure

1. The Consultative Committee shall be convened by the Secretary General of the Council of Europe. Its first meeting shall be held within twelve months of the entry into force of this convention. It shall subsequently meet at least once every two years and in any case when one-third of the representatives of the Parties requests its convocation.

2. A majority of representatives of the Parties shall constitute a quorum for a meeting of the Consultative Committee.

3. After each of its meetings, the Consultative Committee shall submit to the Committee of Ministers of the Council of Europe a report on its work and on the functioning of the convention.

KAPITEL V

Rådgivende komité

Artikel 18

Komiteens sammensætning

1. Efter denne konventions ikrafttræden nedsættes en rådgivende komité.

2. Enhver kontraherende part udpeger en repræsentant og en stedfortræder for denne til komiteen. Enhver af Europarådets medlemsstater, der ikke har tilsluttet sig denne konvention, kan lade sig repræsentere i komiteen ved en observatør.

3. Den rådgivende komité kan ved enstemmighed opfordre en part, der ikke er medlem af Europarådet og som ikke har tilsluttet sig konventionen, til at lade sig repræsentere ved en observatør på et nærmere bestemt møde.

Artikel 19

Komiteens opgaver

Den rådgivende komité:

a. kan stille forslag med henblik på at lette eller forbedre konventionens anvendelse;

b. kan i overensstemmelse med artikel 21 stille forslag til ændring af konventionen ;

c. skal udtale sig om ethvert forslag om ændring af konventionen, som den får forelagt i henhold til artikel 21, stk. 3;

d. kan efter anmodning fra en kontraherende part udtale sig om ethvert spørgsmål angående konventionens anvendelse.

Artikel 20

Procedure

1. Den rådgivende komité indkaldes af Europarådets generalsekretær. Dens første møde afholdes senest tolv måneder efter konventionens ikrafttræden. Derefter holder komiteen møde mindst en gang hvert andet år, og i øvrigt når en tredjedel af de kontraherende parters repræsentanter anmoder derom.

2. Den rådgivende komité er beslutningsdygtig, når et flertal af de kontraherende parters repræsentanter er til stede på mødet.

3. Efter hvert møde afgiver den rådgivende komité en beretning til Europarådets ministerkomité om sit arbejde, og om hvordan konventionen virker.

4. Subject to the provisions of this convention, the Consultative Committee shall draw up its own Rules of Procedure.

CHAPTER VI

Amendments

Article 21

Amendments

1. Amendments to this convention may be proposed by a Party, the Committee of Ministers of the Council of Europe or the Consultative Committee.

2. Any proposal for amendment shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe and to every non-member State which has acceded to or has been invited to accede to this convention in accordance with the provisions of Article 23.

3. Moreover, any amendment proposed by a Party or the Committee of Ministers shall be communicated to the Consultative Committee, which shall submit to the Committee of Ministers its opinion on that proposed amendment.

4. The Committee of Ministers shall consider the proposed amendment and any opinion submitted by the Consultative Committee and may approve the amendment.

5. The text of any amendment approved by the Committee of Ministers in accordance with paragraph 4 of this article shall be forwarded to the Parties for acceptance.

6. Any amendment approved in accordance with paragraph 4 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

CHAPTER VII

Final clauses

Article 22

Entry into force

1. This convention shall be open for signature by the member States of the Council of Europe. It is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

2. This convention shall enter into force on the first day of the month following the expiration of a period of three months after the date

4.1 overensstemmelse med bestemmelserne i denne konvention fastlægger den rådgivende komité selv sin forretningsorden.

KAPITEL VI

Ændringer

Artikel 21

Ændringer

1. Forslag til ændring af denne konvention kan fremsættes af en kontraherende part, Europarådets ministerkomité, eller den rådgivende komité.

2. Ethvert forslag til ændring sendes af Europarådets generalsekretær til Europarådets medlemsstater og desuden til enhver part, der ikke er medlem af Europarådet, som i henhold til artikel 23 har tiltrådt eller er blevet opfordret til at tiltræde denne konvention.

3. Endvidere sendes ethvert ændringsforslag, der fremsættes af en kontraherende part eller af ministerkomiteen, til den rådgivende komité, der skal afgive en udtalelse til ministerkomiteen om den forestående ændring.

4. Ministerkomiteen behandler den foreslåede ændring og udtalelsen fra den rådgivende komité og vil kunne godkende ændringen.

5. Enhver ændring, som ministerkomiteen har godkendt i henhold til stk. 4, forelægges de kontraherende parter med henblik på deres tiltrædelse.

6. Enhver ændring, som er godkendt i henhold til stk. 4, træder i kraft den 30. dag efter, at alle kontraherende parter har meddelt generalsekretæren deres tiltrædelse.

KAPITEL VII

Afsluttende bestemmelser

Artikel 22

Ikrafttræden

1. Denne konvention er åben for undertegnelse af Europarådets medlemsstater. Den er betinget af ratifikation, accept eller godkendelse. Ratifikations-, accept-, eller godkendelsesinstrumenter deponeres hos Europarådets generalsekretær.

2. Konventionen træder i kraft den første dag i den måned, der følger efter udløbet af tre måneder fra den dag, da fem af Europarådets

on which five member States of the Council of Europe have expressed their consent to be bound by the convention in accordance with the provisions of the preceding paragraph.

3. In respect of any member State which subsequently expresses its consent to be bound by it, the convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the deposit of the instrument of ratification, acceptance or approval.

medlemsstater i henhold til stk. 1 har tilkendegivet at ville være bundet af konventionen.

3. For medlemsstater, der på et senere tidspunkt tilkendegiver at ville være bundet af konventionen, træder denne i kraft den første dag i den måned, der følger efter udløbet af tre måneder, fra den dag ratifikations-, accept-, eller godkendelsesinstrumentet er blevet deponeret.

Article 23
Accession by non-member States

1. After the entry into force of this convention, the Committee of Ministers of the Council of Europe may invite any State not a member of the Council of Europe to accede to this convention by a decision taken by the majority provided for in Article 20.d of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the committee.

2. In respect of any acceding State, the convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Artikel 23
Ikke-medlemsstaters tiltrædelse

1. Efter denne konventions ikrafttræden kan Europarådets ministerkomité ved en beslutning truffet med det i artikel 20, d, i vedtægten for Europarådet fastsatte flertal og med enstemmig tilslutning fra repræsentanterne for de kontraherende parter, der har ret til en plads i komiteen, opfordre enhver part, som ikke er medlem af Europarådet, til at tiltræde konventionen.

2. For enhver part, som tiltræder konventionen, træder denne i kraft den første dag i den måned, der følger efter udløbet af tre måneder, fra den dag tiltrædelsesinstrumentet er blevet deponeret hos Europarådets generalsekretær.

Article 24
Territorial clause

1. Any State may at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this convention shall apply.

2. Any State may at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this convention to any other territory specified in the declaration. In respect of such territory the convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of such declaration by the Secretary General.

3. Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secre-

Artikel 24
Geografisk gyldighedsområde

1. Enhver part kan ved undertegnelsen eller ved deponeringen af sit ratifikations-, accept-, godkendelses- eller tiltrædelsesinstrument nærmere angive det territorium eller de territorier, for hvilke denne konvention finder anvendelse.

2. Enhver part kan til enhver tid derefter ved en erklæring til Europarådets generalsekretær udvide anvendelsen af denne konvention til et hvilket som helst territorium, der er anført i erklæringen. For et sådant territorium træder konventionen i kraft den første dag i den måned, der følger efter udløbet af tre måneder, fra den dag en sådan erklæring er modtaget af Europarådets generalsekretær.

3. Enhver erklæring, der er afgivet i henhold til stk. 1 og stk. 2, kan, hvad angår de territorier, der er anført i erklæringen, tilbagekaldes ved en meddelelse til Europarådets generalsekre-

tary General. The withdrawal shall become effective on the first day of the month following the expiration of a period of six months after the date of receipt of such notification by the Secretary General.

Article 25
Reservations

No reservation may be made in respect of the provisions of this convention.

Article 26
Denunciation

1. Any Party may at any time denounce this convention by means of a notification addressed to the Secretary General of the Council of Europe.

2. Such denunciation shall become effective on the first day of the month following the expiration of a period of six months after the date of receipt of the notification by the Secretary General.

Article 27
Notifications

The Secretary General of the Council of Europe shall notify the member States of the Council and any State which has acceded to this convention of:

a. any signature,

b. the deposit of any instrument of ratification, acceptance, approval or accession;

c. any date of entry into force of this convention in accordance with Articles 22, 23 and 24;

d. any other act, notification or communication relating to this convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

Done at Strasbourg, the 28th day of January 1981, in English and in French, both texts being equally authoritative, in a single copy which shall remain deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe and to any State invited to accede to this Convention.

tær. Tilbagekaldelsen har virkning fra den første dag i den måned, der følger efter udløbet af seks måneder, fra den dag meddelelse derom er modtaget af generalsekretæren.

Artikel 25
Forbehold

Der kan ikke tages forbehold over for konventionens bestemmelser.

Artikel 26
Opsigelse

1. Enhver kontraherende part kan til enhver tid opsige denne konvention ved en meddelelse til Europarådets generalsekretær.

2. Opsigelsen har virkning fra den første dag i den måned, der følger efter udløbet af seks måneder, fra den dag meddelelse derom er modtaget af Europarådets generalsekretær.

Artikel 27
Meddelelser

Europarådets generalsekretær giver Europarådets medlemsstater og enhver part, der har tiltrådt denne konvention, meddelelse om:

a. enhver undertegnelse;

b. enhver deponering af ratifikations-, accept-, godkendelses- eller tiltrædelsesinstrumenter;

c. enhver ikrafttrædelsesdato for denne konvention i henhold til artikel 22, 23 og 24;

d. enhver anden handling eller meddelelse som vedrører denne konvention.

Til bekræftelse heraf har undertegnede, som er behørigt befuldmægtiget dertil, underskrevet denne konvention.

Udfærdiget i Strasbourg den 28. januar 1981, med engelsk og fransk tekst, som begge har samme gyldighed, i ét eksemplar, som skal opbevares i Europarådets arkiver. Europarådets generalsekretær skal fremsende bekræftede genparter til hver af Europarådets medlemsstater og til hver af de parter, som er blevet opfordret til at tiltræde denne konvention.

Europarådets konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger trådte i medfør af art. 22 i kraft den 1. oktober 1985 for følgende lande: Frankrig, Forbundsrepublikken Tyskland, Norge, Spanien og Sverige.

Danmarks ratifikationsinstrument deponeredes hos Europarådet den 23. oktober 1989, og konventionen trådte i medfør af art. 22, stk. 2, i kraft for Danmark den 1. februar 1990.

Endvidere har følgende lande med virkning fra de anførte datoer ratificeret, accepteret eller godkendt konventionen:

Storbritannien . . . . . 1. december 1987
Luxembourg . . . . . 1. juni 1988
Østrig . . . . . 1. juli 1988
Irland . . . . . 1. august 1990

Idet bemærkes at betegnelse og adresse for den ansvarlige myndighed i henhold til art. 13, stk. 2, a, kun er angivet for Danmarks vedkommende, har nedennævnte lande ved ratifikationen, accepten eller godkendelsen afgivet erklæringer som følger:

Danmark

Konventionsforpligtelsen i henhold til art. 13, stk. 2, a, vil blive varetaget af Registertilsynet, Christians Brygge 28,4. sal, 1559 København V.

I henhold til art. 24 er angivet, at konventionen ikke gælder for Færøerne og Grønland.

Frankrig

I henhold til den franske oversættelse af konventionens art. 9, stk. 2, a, fortolkes ordene »Sécurité d'Etat« som betydende »Sûreté de l'Etat« og ordene »Sûreté publique« som betydende »Sécurité publique«.

I henhold til bestemmelsen i art. 3, stk. 2, c, vil Frankrig tillige anvende nærværende konvention på personregistre, som ikke behandles elektronisk.

Forbundsrepublikken Tyskland

Ved konventionens art. 8, b, forudsættes, at en forespørgsel om personoplysninger ikke kan efterkommes, såfremt den registrerede er ude af stand til fyldestgørende at beskrive sin anmodning.

Med henvisning til konventionens forarbejder antages det, at konventionens art. 12, stk. 2, giver den kontraherende stat adgang til i dens nationale lov om databeskyttelse at indarbejde regler, der i særlige tilfælde forbyder overførsel af personoplysninger under hensyntagen til den registreredes interesser, der berettiger beskyttelse.

I henhold til art. 24, finder konventionen tillige anvendelse for Land Berlin med virkning fra den dato, hvor konventionen træder i kraft for Forbundsrepublikken Tyskland.

Luxembourg

Inden for rammerne afart. 3, stk. 2, a, forbeholdes retten til ikke at lade konventionen finde anvendelse på a) databanker, der i kraft af en lov eller anden bestemmelse er tilgængelige for offentligheden, b) databanker, som udelukkende indeholder data i forbindelse med databankens ejerskab, c) databanker, der er etableret for folkeretlige institutioner.

Norge

I henhold til art. 3, stk. 2, a, meddeles, at konventionen ikke skal finde anvendelse på private personregistre, som hverken bruges af den private sektor eller foreninger eller stiftelser.

I henhold til art. 3, stk. 2, b, meddeleles, at konventionen tillige vil finde anvendelse på informationer vedrørende foreninger og stiftelser.

I henhold til konventionens art. 24, stk. 1, vil konventionen ikke være anvendelig for Svalbard.

Storbritannien

I henhold til art. 3, stk. 2, a, vil konventionen ikke finde anvendelse på følgende kategorier af elektroniske personregistre: a) lønninger og pensioner: personoplysninger, som udelukkende opbevares med henblik på at udregne arbejdsvederlag eller pension eller betaling af fradrag fra samme, b) regnskabs- og overførselsesfortegnelser: personoplysninger, som udelukkende opbevares med henblik på at føre regnskab eller fortegnelser over overførelser, c) informationer, der er offentligt tilgængelige i henhold til lov: personoplysninger, som skal være offentligt tilgængelige i henhold til lovbestemmelse.

I henhold til art. 24 vil konventionen tillige finde anvendelse inden for Jerseys og Guernseys retsområder.

Østrig

For så vidt angår formuleringen i art. 2, c, antages, at udtrykket »spredning« omfatter udtrykket »kommunikation« samt »gøre tilgængeligt« som anvendt i afsnit 3, stk. 9 og 10, i tillægget til den østrigske lov om databeskyttelse, nr. 370/1986.

Med hensyn til art. 5, e, antager Østrig, at denne betingelse fuldt ud imødekommes ved bestemmelsen i den østrigske lov om databeskyttelse angående slettelse af oplysninger efter ansøgning fra den registrerede.

Østrig antager, at betydningen af ordene »når den kontraherende parts gældende lovgivning hjemler det« indeholdt i den første sætning i konventionens art. 9, stk. 2, svarer til betydningen af ordene »i overensstemmelse med loven« som anført i den europæiske menneskerettighedskonventions art. 8, stk. 2, og at det derfor er i overensstemmelse med konventionen, såfremt det under den østriske lov om databeskyttelse kun er tilladt at begrænse den fundamentale ret til databeskyttelse når hjemlet ved loven.

Endvidere antager Østrig, at begrænsningen i konventionens art. 9, stk. 2, a, vedrørende »statens økonomiske interesser« sammenholdt med stk. 2, b, svarer til begrænsningen i art. 8, stk. 2, i den europæiske menneskerettighedskonvention af hensyn til »landets økonomiske velfærd«.

I henhold til art. 3, stk. 2, b, har Østrig meddelt, at konventionen tillige vil finde anvendelse på oplysninger om grupper af personer, foreninger, stiftelser, selskaber, sammenslutninger eller enhver anden form for institutioner, som direkte eller indirekte består af fysiske personer, uanset om disse institutioner er retssubjekter.

Irland

I henhold til art. 3, stk. 2, a, vil konventionen ikke finde anvendelse på følgende katego "ier af elektroniske personregistre, opført i paragraf 1 (4) i databeskyttelsesloven fra 1988: a) personoplysninger, som ifølge justitsministeren eller forsvarsministeren er eller har været registreret med det formål at beskytte statens sikkerhed; b) personoplysninger i form af oplysninger som den, der opbevarer de pågældende data ved lov er forpligtet til at gøre tilgængelige for offentligheden; c) personoplysninger, som opbevares af en enkeltperson, og som alene har at gøre med dennes personlige, familie- eller husholdningsmæssige forhold, eller som opbevares af en enkeltperson alene for rekreative formål.

Udenrigsministeriet, den 16. maj 1991

UFFE ELLEMANN-JENSEN

BILAG 1 1

EUROPA-KOMMISSIONEN
GENERALDIREKTORAT XV
Det Indre Marked og Finansielle Tjenesteydelser
Fri bevægelighed for information. Selskabsret og finansiel information
Fri bevægelighed for information, databeskyttelse og internationale aspekter i forbindelse hermed

XV/5012/97-DA

Arbejdsgruppen vedrørende beskyttelse af personer

i forbindelse med behandling af personoplysninger

HENSTILLING 1/97

Databeskyttelseslovgivningen og medierne

Vedtaget af arbejdsgruppen den 25. februar 1997

INDHOLDSFORTEGNELSE

1. INDLEDNING 3

2. GENERELLE ASPEKTER 4

2.1 Ytringsfrihed og beskyttelse af privatlivets fred 4

2.2 Lovgivningsmæssig baggrund for direktivets artikel 9 5

2.3 Oversigt over den nuværende situation i den nationale ret 6

3. KONKLUSIONER 7

ARBEJDSGRUPPEN VEDRØRENDE BESKYTTELSE AF PERSONER I FORBINDELSE MED BEHANDLING AF PERSONOPLYSNINGER

som blev nedsat ved Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995[1], og

som henviser til artikel 29 og artikel 30, stk. 3, i dette direktiv,

har under henvisning til sin forretningsorden, særlig artikel 12 og 14, vedtaget følgende henstilling:

1. INDLEDNING

Artikel 9 i direktiv 95/46/EF om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (i det følgende benævnt "direktivet") har følgende ordlyd:

> "Medlemsstaterne fastsætter i forbindelse med behandling af personoplysninger, der udelukkende finder sted i journalistisk øjemed eller med henblik på kunstnerisk eller litterær virksomhed, kun fritagelser eller undtagelser fra bestemmelserne i dette kapitel og i kapitel IV og VI, for så vidt som de er nødvendige for at forene retten til privatlivets fred med reglerne for ytringsfrihed."

Arbejdsgruppen indledte på sit første møde på basis af mandatet i direktivets artikel 30, stk. 1, litra a), en drøftelse af, hvorledes artikel 9 vil kunne implementeres. Der blev fremlagt arbejdsdokumenter af den britiske og den tyske delegation. Under drøftelsen viste det sig, at der er forskelle i de nationale lovgivninger med hensyn til anvendelsen af databeskyttelsesbestemmelserne på medierne[2].

Der var enighed om, at det kunne være nyttigt, hvis arbejdsgruppen formulerede visse retningslinjer for fortolkningen af artikel 9 i direktivet. Som et første skridt blev det aftalt, at sekretariatet skulle indsamle oplysninger om den nuværende lovgivningssituation og udarbejde en rapport under hensyntagen til Europarådets rapport "Databeskyttelse og medierne" fra 1991[3].

Den 21. februar 1996 runddeltes et spørgeskema udarbejdet af arbejdsgruppen.

[1] EFT L 281 af 23.11.1995, s. 31.

[2] Medmindre andet er anført, forstås ved udtrykket "medierne" alle de forskellige massekommunikationsmidler, bl.a. pressen, radio, tv osv.

[3] *"Databeskyttelse og medierne"*, undersøgelse udarbejdet af ekspertkomitéen om databeskyttelse (CJ-PD) på grundlag ai' et kommissorium fra den europæiske komité om retligt samarbejde (CDCJ), Europarådet, Strasbourg, 1991.

Arbejdsgruppen drøftede et arbejdsdokument på sit tredje møde og nåede visse konklusioner, som blev drøftet nærmere på gruppens fjerde møde. I lyset af disse konklusioner blev der nået enighed om at vedtage dokumentet som en henstilling, jf. direktivets artikel 30, stk. 3. Henstillingen blev vedtaget af arbejdsgruppen den 25. februar 1997.

I næste afsnit redegøres der for nogle generelle aspekter af anvendelsen af databeskyttelseslovgivningen på medierne, herunder den lovgivningsmæssige baggrund for direktivets artikel 9. Afsnit 3 gennemgår nogle af hovedtrækkene i den nuværende lovgivningssituation i medlemsstaterne[4]. Fjerde afsnit redegør for konklusionerne af drøftelserne i arbejdsgruppen vedrørende anvendelsen af databeskyttelseslovgivningen på medierne.

Artikel 9 giver mulighed for fritagelser og undtagelser fra anvendelsen af visse bestemmelser i direktivet i forbindelse med behandling af oplysninger i journalistisk øjemed samt med henblik på kunstnerisk eller litterær virksomhed. Denne henstilling fokuserer som følge heraf på undtagelserne og fritagelserne i forbindelse med behandling af oplysninger i journalistisk øjemed[5].

2. GENERELLE **ASPEKTER**

2.1 Ytringsfrihed og beskyttelse af privatlivets fred

I artikel 10 i den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder hedder det bl.a.:

> "Enhver har ret til ytringsfrihed. Denne ret omfatter meningsfrihed og frihed til at give eller modtage meddelelser eller tanker, uden indblanding fra offentlig myndighed og uden hensyn til grænser.[..]"

Denne ret er en af de grundlæggende menneskerettigheder, der følger af medlemsstaternes fælles forfatningsmæssige traditioner, og er et af de mest typiske karakteristika ved demokratiske samfunds retlige arv. Historisk var den en af de første menneskerettigheder, der blev krævet og garanteret ved lov. Specielt pressen fik tildelt særlige retlige og forfatningsmæssige garantier, bl.a. mod censur.

Retten til privatlivets fred er tilsvarende garanteret ved artikel 8 i menneskerettighedskonventionen. Databeskyttelse falder ind under den beskyttelse af privatlivets fred, der er garanteret ved denne artikel. Fravigelser af principperne om databeskyttelse og af artikel 8 i menneskerettighedskonventionen skal være i overensstemmelse med loven og respektere proportionalitetsprincippet[6] Tilsvarende skal begrænsninger i ytringsfriheden, f.eks.

[4] Nærmere oplysninger om situationen i de enkelte medlemsstater gives i dok. XV D 5027/96.

Den svenske delegation ønskede at understrege, at denne henstilling ikke berører den enkeltes grundlovssikrede ret til at give udtryk for sin holdning i medierne i Sverige.

[6] F.eks. Den Europæiske Menneskerettighedsdomstol, *Sunday Times*, serie A, nr. 30.

begrænsninger, der følger af anvendelsen af principperne for databeskyttelse, være i overensstemmelse med loven og respektere proportionalitetsprincippet[7].

De to grundlæggende rettigheder må dog ikke opfattes som grundlæggende modstridende. Hvis der ikke foreligger tilstrækkelige garantier for beskyttelse af privatlivets fred, vil den enkelte være tilbøjelig til at være tilbageholdende med frit at give udtryk for sine tanker. Tilsvarende vil en identificering og profilering af læsere og brugere af informationstjenester formentlig mindske den enkeltes ønske om at give og modtage meddelelser.

2.2 Lovgivningsmæssig baggrund for direktivets artikel 9

Ifølge artikel F, stk. 2, i traktaten om Den Europæiske Union skal EU respektere de grundlæggende rettigheder, således som de garanteres ved menneskerettighedskonventionen og medlemsstaternes fælles forfatningsmæssige traditioner.

EU-lovgiveme har anerkendt, at medierne repræsenterer et særtilfælde, og at der er behov for at sikre en passende balance mellem hensynet til beskyttelsen af privatlivets fred og hensynet til beskyttelsen af ytringsfriheden.[8]

Artikel 19 i det oprindelige kommissionsforslag[9] indeholdt bestemmelser om, at medlemsstaterne kunne give dispensation fra direktivets bestemmelser for pressen og de audiovisuelle medier. Begrundelsen fastslog, at hovedelementet i denne artikel er forpligtelsen til at foretage en passende afvejning af de implicerede interesser, og at denne afvejning skal tage højde for muligheden for brug af andre retsmidler eller en ret til at tage til genmæle, eksistensen af faglige etiske regler samt de begrænsninger, der følger af menneskerettighedskonventionen og de generelle retsprincipper.

Artikel 9 i Kommissionens ændrede forslag[10] gjorde det obligatorisk at give dispensation for medierne. Ordlyden blev desuden ændret med henblik på at inkludere journalister og begrænse dispensationen til aktiviteter i journalistisk øjemed.

Artiklens ordlyd blev ændret yderligere, inden den fik sin nuværende ordlyd, hvor der ikke over én bank gives dispensation for alle databeskyttelsesbestemmelserne. Ifølge den nuværende ordlyd gives der kun obligatorisk fritagelser eller undtagelser, "for så vidt som de er nødvendige", hvilket betyder, at fritagelser eller undtagelser fra hvert enkelt specifikt princip i direktivet kun må gives, for så vidt som (på fransk er ordlyden "dans la seule mesure", og på tysk er den "nur insofern vor, als sich dies als notwendig erweist") de er nødvendige for at sikre en passende balance mellem beskyttelsen af privatlivets fred og

[7] Se senest Den Europæiske Menneskerettighedsdomstol, *Goodwin mod Det Forenede Kongerige*, 27.3.1996, endnu ikke offentliggjort.

[8] Behovet for at sikre en passende balance mellem de interesser, der beskyttes ved de to sæt af normer, blev også anerkendt ved konvention 108/81. I begrundelsen *(begrundelse for konventionen om beskyttelse af personer i forbindelse med automatiseret behandling af persondata,* Europarådet, Strasbourg, 1991) betegnes ytringsfriheden som henhørende under "andres ret og frihed", med henblik på hvis beskyttelse de nationale lovgivere ifølge konventionens artikel 9, stk. 2, litra b), kan fravige de grundlæggende principper for databeskyttelse.

[9] KOM(90) 314 endelig udg. - SYN 287.

[10] KOM(92) 422 endelig udg. - SYN 287.

beskyttelsen af ytringsfriheden. Fritagelserne og undtagelserne må desuden kun vedrøre de generelle regler om lovlig behandling af personoplysninger, reglerne om videregivelse af oplysninger til tredjelande og reglerne om tilsynsmyndighedernes beføjelser. Ifølge betragtning 37 må der ikke gives dispensation fra reglerne om behandlingssikkerhed, og tilsynsmyndighederne på dette område bør i det mindste tildeles visse ex post facto-beføjelser til f.eks. regelmæssigt at offentliggøre rapporter eller indbringe sager for de retslige myndigheder.

2.3 Oversigt over den nuværende situation i den nationale ret

De forskellige nationale love behandler på nuværende tidspunkt spørgsmålet ud fra én af følgende synsvinkler:

a) I nogle lande indeholder databeskyttelseslovgivningen ingen udtrykkelig dispensation fra bestemmelserne for medierne. Dette er tilfældet i Belgien, Spanien, Portugal, Sverige og Det Forenede Kongerige.

b) I andre lande gives der dispensation for medierne fra en række bestemmelser i databeskyttelseslovgivningen. Dette er tilfælde i Tyskland[11], Frankrig, Nederlandene, Østrig og Finland. Der opereres med en tilsvarende dispensation i det italienske lovudkast.

c) I andre lande igen gives der dispensation fra den generelle databeskyttelseslovgivning for medierne, som i stedet er underlagt særlige databeskyttelsesbestemmelser. Dette er tilfældet i Danmark for alle mediers vedkommende og i Tyskland for offentlige tv- og radioselskaber, der ikke er omfattet af forbundsstatslige eller delstatslige databeskyttelseslove, men er underlagt særlige databeskyttelsesbestemmelser i de traktater mellem delstaterne, som regulerer dem.

Forskellene mellem de tre modeller skal dog ikke overvurderes. I de fleste tilfælde finder databeskyttelseslovgivningen uafhængigt af de udtrykkelige dispensationer, der måtte forefindes, ikke fuld anvendelse på medierne på grund af den særlige forfatningsmæssige status, som reglerne om ytrings- og pressefrihed har. Disse regler sætter en reel grænse for anvendelsen af materielle databeskyttelsesbestemmelser eller i det mindste deres håndhævelse i praksis.

Derimod gælder den almindelige databeskyttelsesordning generelt for mediernes ikke-redaktionelle aktiviteter.

Ved anvendelsen af databeskyttelseslovgivningen anerkender tilsynsmyndighederne inden for databeskyttelse, at medierne repræsenterer et særtilfælde, både hvor der findes en særlig retlig ordning, og hvor der ikke gør det.

Dispensationernes reelle omfang kan endvidere ikke vurderes abstrakt, men afhænger af databeskyttelseslovgivningens generelle opbygning i det enkelte land. Det siger sig selv, at dispensationernes omfang afhænger af, i hvor høj grad de materielle retsregler har reel betydning for mediernes aktiviteter.

[11] Med én nævneværdig undtagelse, se herom litra c).

Forskellene i anvendelsen af databeskyttelseslovgivningen på medierne kan muligvis også tilskrives de ændrede perspektiver med hensyn til databeskyttelseslovgivningens rolle og mediernes brug af informationsteknologi. I databeskyttelsens tidlige fase var man tilbøjelig til at rette opmærksomheden mod de store mainframebaserede databaser. I denne fase syntes medierne næppe at være berørt af reglerne, og det forekom derfor ikke nødvendigt med nogen dispensationer for dem. Den omstændighed, at vægten i databeskyttelseslovgivningen er blevet forskudt i retning af databehandling og omfattende brug af informationsteknologi i medierne, har fuldstændig vendt op og ned på situationen.

Et vigtigt element i den nuværende lovgivningssituation i medlemsstaterne er, at medierne, eller i det mindste pressen, er bundet af visse regler, som, selv om de ikke er en del af databeskyttelseslovgivningen i egentlig forstand, bidrager til at beskytte privatlivets fred for den enkelte. Disse regler og den ofte omfattende retspraksis på området giver mulighed for at trække på specifikke retsmidler, som undertiden opfattes som en erstatning for mangelen på forebyggende foranstaltninger i databeskyttelseslovgivningen.

Retten til at tage til genmæle og muligheden for at få urigtige oplysninger berigtiget, journalisters faglige forpligtelser og de særlige selvregulerende procedurer, der er knyttet hertil, samt loven om ærekrænkende udtalelser (straffe- og civilretlige bestemmelser om injurier) skal tages i betragtning ved vurderingen af, hvordan privatlivets fred er beskyttet i relation til medierne[12].

Den forskydning, der sker med de traditionelle medier i retning af elektronisk udgiver-virksomhed og levering af online-tjenester, føjer tilsyneladende yderligere brikker til overvejelserne. Sondringen mellem redaktionelle og ikke-redaktionelle aktiviteter antager en ny dimension i relation til online-tjenester, som modsat alle de traditionelle medier giver mulighed for at identificere modtagerne af tjenesterne.

3. KONKLUSIONER

Det foregående synes at bekræfte, at der er behov for en nyvurdering af lovrammerne for anvendelsen af databeskyttelseslovgivningen på medierne i de enkelte medlemsstater. I denne forbindelse er det nødvendigt at vurdere, i hvor høj grad anvendelsen af de enkelte bestemmelser i kapitel II, IV og VI i direktivet skal begrænses for at beskytte ytringsfriheden.

I denne forbindelse skal der tages hensyn til en række forhold:

- Databeskyttelseslovgivningen gælder principielt for medierne. Der må kun ydes fritagelser og undtagelser i relation til kapitel II om de almindelige betingelser for lovlig

[12] Et af resultaterne af Europarådets arbejde på dette felt er, at den omstændighed, at der findes særlige retsmidler ifølge medielovgivningen, kan retfærdiggøre dispensationer fra databeskyttelseslovgivningen og derved fra artikel 8 i menneskerettighedskonventionen, men dog kun under visse omstændigheder. Europarådet foreslog i begrundelsen (se ovenfor), at for at opveje den manglende anvendelse af visse principper for databeskyttelse, skal medielovgivningen overholde Europarådets Parlamentariske Forsamlings resolution 428 (1970) om massemedier og menneskerettigheder og Ministerkomitéens resolution om retten til at tage til genmæle. Retten til at tage til genmæle er blevet inkorporeret i artikel 8 i den europæiske konvention om grænseoverskridende fjernsyn (europæisk traktatserie, nr. 132/89).

behandling af oplysninger, kapitel IV om videregivelse af oplysninger til tredjelande og kapitel VI om tilsynsmyndighedernes beføjelser. Der må ikke ydes fritagelser eller undtagelser i relation til behandlingssikkerheden. De tilsynsmyndigheder, der er ansvarlige på området, skal under alle omstændigheder bevare visse ex post facto-beføjelser.

- Fritagelserne og undtagelserne i henhold til artikel 9 skal være i overensstemmelse med proportionalitetsprincippet. Der må kun gives fritagelser og undtagelser for de bestemmelser, der vil kunne udgøre en fare for ytringsfriheden, og i så fald kun i det omfang det er nødvendigt for, at denne ret kan udøves effektivt, samtidig med at der sikres en passende balance i forhold til retten til privatlivets fred for datasubjektet.

- Fritagelser og undtagelser i henhold til artikel 9 er muligvis ikke nødvendige i tilfælde, hvor andre bestemmelser i direktivet på grund af deres fleksibilitet eller de undtagelser, der er mulighed for i henhold til andre særbestemmelser (som selvfølgelig også skal fortolkes snævert), i forvejen sikrer en passende balance mellem privatlivets fred og ytringsfriheden[13].

- Artikel 9 i direktivet respekterer den enkeltes ret til ytringsfrihed. Der kan ikke ydes fritagelser og undtagelser i henhold til artikel 9 for medier eller journalister som sådanne, men for enhver, der behandler oplysninger i journalistisk øjemed.

- Det er tilladt kun at yde fritagelser og undtagelser for databehandling i journalistisk øjemed, herunder elektronisk udgivervirksomhed. Enhver anden form for databehandling fra journalisters eller mediers side er underlagt de almindelige bestemmelser i direktivet. Denne sondring har særlig relevans i forhold til elektronisk udgivervirksomhed. Behandling af abonnentoplysninger til faktureringsformål eller behandling med henblik på direkte markedsføring (herunder behandling af oplysninger med henblik på brug af medier til profilering) falder ind under den almindelige databeskyttelsesordning.

- Direktivet stiller krav om, at der skal findes en passende balance mellem to grundlæggende friheder. For at kunne vurdere, om begrænsningerne i de rettigheder og forpligtelser, der følger af direktivet, er proportionale i forhold til målsætningen om at beskytte ytringsfriheden, skal man i særlig grad være opmærksom på de særlige garantier, den enkelte nyder i relation til medierne. Begrænsninger i retten til indsigt og berigtigelse inden offentliggørelse kan kun betragtes som proportionale, hvis den enkelte har ret til indsigelse og berigtigelse af urigtige oplysninger efter offentliggørelse.

- Den enkelte har under alle omstændigheder ret til passende afhjælpning i tilfælde af, at hans rettigheder krænkes[14].

[13] F.eks. skal det, når det skal vurderes, om undtagelserne fra artikel 11 skal ydes, tages i betragtning, at oplysningspligten over for datasubjekterne ikke gælder, hvis dens overholdelse indebærer en uforholdsmæssig stor indsats.

[14] Der er ingen mulighed for fritagelse eller undtagelse fra bestemmelserne i direktivets kapitel III.

Ved vurderingen af, om fritagelser eller undtagelser er proportionale, skal man være opmærksom på, hvilke etiske regler og faglige forpligtelser journalister er underlagt, samt hvilke selvregulerende former for kontrol professionen selv udøver.

Udfærdiget i Bruxelles, den 25. februar 1997

For Arbejdsgruppen

Formand

P.J. HUSTINX

KAPITTEL 22

Lovforslaget

Lov om behandling av personopplysninger (personopplysningsloven)

Kapittel 1 Lovens formål og område

§ 1 Lovens formål

Lovens formål er å bidra til at behandling av personopplysninger skjer i samsvar med grunnleggende personvernhensyn, herunder behovet for tilstrekkelig opplysningskvalitet, personlig integritet og privatlivets fred.

Alternativt forslag til § 1:

Denne lovens hensikt er å sikre at personopplysninger, knyttet til den enkeltes private livsområde, blir innhentet, bearbeidet, oppbevart og benyttet på grunnlag av samtykke, lovhjemmel eller rettslig beslutning. De samme krav stilles til registrering av adferd.

Den enkeltes ukrenkelighet skal respekteres både i privatliv, arbeidsliv og i offentlige sammenhenger.

Enhver har i utgangspunktet råderett over kunnskap denne gir fra seg om seg selv. Opplysninger, eller et materiale som gir grunnlag for opplysninger, skal bare benyttes til det eller de oppgitte formål de innhentes eller samles for.

Unntak skal være hjemlet i lov.

Lovens regler omfatter fysiske personer. De kommer også til anvendelse hvis opplysninger om døde eller juridiske personer kan knyttes til individ eller slekt og opplysningene må antas å være følsomme.

§ 2 Definisjoner

1) Med «personopplysning» menes opplysninger og vurderinger som direkte eller indirekte kan knyttes til en identifiserbar, fysisk person (den registrerte).
2) Med «behandling av personopplysninger» menes enhver operasjon eller serie av operasjoner som utføres på personopplysninger, som for eksempel innsamling og registrering herunder elektronisk overvåkning, systematisering, oppbevaring, endring, søking, utlevering, sammenstilling, blokkering og sletting.
3) Med «personregister menes registre, fortegnelser mm der personopplysninger er lagret systematisk slik at opplysninger om den enkelte person kan finnes igjen.
4) Med «behandlingsansvarlig» menes den som bestemmer formålet med en elektronisk behandling eller formålet med et manuelt personregister, samt hvilke operasjoner som skal eller kan utføres på personopplysninger.
5) Med «databehandler» menes den som i henhold til avtale behandler personopplysninger på vegne av den behandlingsansvarlige.
6) Med «elektronisk overvåkning» menes vedvarende eller regelmessig gjentatt personovervåkning ved hjelp av fjernbetjent eller automatisk virkende utstyr.
7) Med «samtykke» menes en uttrykkelig og informert erklæring fra den registrerte om at han eller hun godtar at opplysninger om en selv blir behandlet.
8) Med «sensitive personopplysninger» menes personopplysninger om
   a) rasemessig eller etnisk bakgrunn, eller politisk eller religiøs oppfatning
   b) at en person har vært mistenkt, siktet, tiltalt eller dømt for straffbare forhold
   c) helseforhold, herunder opplysninger om arveegenskaper og misbruk av rusmidler
   d) seksuelle forhold
   e) medlemsskap i fagforeninger.
9) Med «enkeltavgjørelse» menes
   a) enkeltvedtak, jf forvaltningsloven § 2 bokstavene b) og a), og
   b) andre avgjørelser som er bestemmende for bestemte private personers rettigheter eller plikter.

§ 3 Lovens saklige virkeområde

Loven gj elder for helt eller delvis elektronisk behandling av personopplysninger og for manuell behandling når personopplysningene inngår eller skal inngå i et personregister.

Loven gjelder ikke behandling av personopplysninger for rent personlige formål.

Kongen kan gi forskrift om at loven eller deler av denne ikke skal gjelde for bestemte former for elektronisk behandling av personopplysninger.

§ 4 Fjernsynsovervåkning og billedopptak

For fjernsynsovervåkning og billedopptak i forbindelse med slik overvåkning som ikke er elektronisk behandling av personopplysninger gjelder §§7, 24,40.41og 42 nr 6.

For billedopptak i forbindelse med fjernsynsovervåkning som ikke er elektronisk behandling gjelder også §§ 31, 32 og 38 tilsvarende.

Med fjernsynsovervåkning menes vedvarende eller regelmessig gjentatt personovervåkning ved hjelp av fjernbetjent eller automatisk virkende fjemsynskamera. fotografiapparat eller lignende apparat.

§ 5 Forholdet til ytnngsfriheten

Loven gjelder for behandling av personopplysninger som utelukkende finner sted i journalistisk øyemed eller for kunstnerisk eller litterær virksomhet. Det skal gjøres unntak fra bestemmelsene i den grad det er nødvendig for å forene hensynet til ytringsfrihet med hensynet til personvern.

§ 6 Lovens geografiske virkeområde

Loven gjelder for behandling av personopplysninger når den behandlingsansvarlige er etablert i riket, herunder Svalbard og Jan Maven.

Loven gjelder også for behandling av personopplysninger som skjer i riket og som forestås av en behandlingsansvarlig som er etablert i stater utenfor EØS-området dersom den behandlingsansvarlige benytter hjelpemidler i Norge. Den behandlingsansvarlige skal i så fall utpeke en representant som er etablert i Norge. Regiene om den behandlingsansvarlige gjelder tilsvarende for representanten.

Annet ledd gjelder ikke dersom hjelpemidlene utelukkende benyttes til å transportere personopplysninger via Norge.

Kapittel 2 Alminnelige regler om behandling av personopplysninger

§ 7 Krav til saklighet

Personopplysninger kan bare behandles til lovlige og uttrykkelig angitte formål. Formålet skal være saklig begrunnet ut fra den behandlingsansvarliges virksomhet.

Personopplysningene skal være relevante ut fra det angine formålet.

Elektronisk overvåkning av sted hvor en begrenset krets av personer jevnlig ferdes, er bare tillatt dersom det ut fra hensynet til virksomheten er et særskilt behov for overvåkningen.

§ 8 Anvendelse av personopplysninger til andre formål enn det opprinnelige

Personopplysninger som er samlet inn til behandling for et formål kan bare anvendes til andre formål dersom

1) den registrene samtykker i det nye behandlingsformålet
2) det er fastsatt i lov at det er adgang til å bruke opplysningene til det nye behandlingsformålet, eller'
3) fordelene med den nye behandlingen er klart større enn ulempene som den volder for den enkelte og den nye behandlingen ikke er uforenlig med det opprinnelige formålet.

Kongen kan gi forskrift om anvendelse av personopplysninger til nye formål.

§ 9 Behandling av sensitive personopplysninger

Sensitive personopplysninger (jf § 2 nr 8) kan bare behandles dersom

1) den registrene samtykker
2) det er fastsatt i lov at det er adgang til slik behandling
3) den behandlingsansvarlige plikter å foreta behandlingen i henhold til avtale mellom partene i arbeidslivet
4) behandlingen er nødvendig for å beskytte den registrenes eller en annen persons vesentlige interesser, og vedkommende selv ikke er i stand til å gi samtykke som nevnt i nr 1
5) behandlingen utføres av en ideeli organisasjon som ledd i organisasjonens rettmessige virksomhet. Behandlingen kan kun omfatte opplysninger om organisasjonens medlemmer eller personer som på grunn av organisasjonens formål er i regelmessig kontakt med den. Personopplysningene kan ikke videreformidles uten den registrenes samtykke
6) behandlingen gjelder opplysninger som den registrerte selv har gjort alminnelig kjent
7) behandlingen er nødvendig for at et rettskrav kan fastsettes. gjøres gjeldende eller forsvares
8) behandlingen er nødvendig for medisinske formål eller for forvaltning av helsetjenester og opplysningene behandles av en helsearbeider med taushetsplikt
9) behandlingen er nødvendig for statistiske formål eller forskning og behandlingen ikke kan få direkte virkninger for den enkelte.

Datatilsynet kan bestemme at sensitive personopplysninger også i andre tilfeller kan behandles dersom viktige samfunnsinteresser tilsier det og det settes i verk tiltak for å sikre de registrenes interesser.

§ 10 Bruk av fødselsnummer

Bruk av fødselsnummer må være saklig begrunnet ut i fra behovet for sikker identifisering.

Datatilsynet kan gi pålegg om at fødselsnummer skal brukes for å sikre tilstrekkelig kvalitet på personopplysninger.

§11 Sikring av personopplysninger

Den behandlingsansvarlige og databehandleren skal sørge for at personopplysningene til enhver tid er sikret tilstrekkelig konfidensialitet og har den kvalitet og tilgjengelighet som formålet med behandlingen tilsier.

Den behandlingsansvarlige plikter å gjennomføre sikkerhetsvurderinger og etablere og holde vedlike planlagte og systematiske sikkerhetstiltak for å oppnå kravene i første ledd. Sikkerhetstiltakene skal være bygget opp i henhold til alminnelige anerkjente metoder.

Sikkerhetsvurderingen og tiltakene skal dokumenteres og ved forespørsel være tilgjengelig for Datatilsynet og Personvernnemnda. De ansatte i Datatilsynet og medlemmene i Personvernnemnda plikter å hindre at andre får adgang eller kjennskap til opplysninger om sikkerhetsvurderinger og sikkerhetstiltak

dersom slike opplysninger kan svekke sikkerhetstiltakene.

Kongen kan gi forskrift om sikring av personopplysninger.

Alternativt tredje ledd annet punktum:

De ansatte i Datatilsynet, styremedlemmene og medlemmene i Personvernnemnda plikter å hindre at andre får adgang eller kjennskap til opplysninger om sikkerhetsvurderinger og sikkerhetstiltak dersom slike opplysninger kan svekke sikkerhetstiltakene.

§ 12 Internkontroll

Den behandlingsansvarlige skal kunne dokumentere at det er etablert systemer og rutiner som sikrer overholdelse av regiene i loven samt vilkår og pålegg etter §§ 35 og 40.

Kongen kan gi forskrift om internkontroll.

§ 13 Databehandlerens rådighet over personopplysninger

Databehandleren kan ikke uten avtale med den behandlingsansvarlige anvende opplysningene til andre formål enn det oppdraget gjelder. Opplysningene kan heller ikke uten slik avtale overlates til næn andre for lagring eller bearbeidelse.

§ 14 Frist for oppfyllelse av plikter

Den behandlingsansvarlige skal sørge for at den registrertes krav etter loven §§ 16, 18, 22, 25, 26, 27 og 28 gjennomføres uten ugrunnet opphold og senest innen én måned.

Dersom særlige grunner gjør det umulig å oppfylle pliktene innen en måned kan gjennomføring skje senere. I slike tilfeller skal midlertidig skriftlig svar gis innen fristen. I det midlertidige svaret skal det opplyses om grunnen til forsinkelsen og sannsynlig tidspunkt for gjennomføring.

§ 15 Betaling

Rettighetene etter §§ 16, 18, 22, 25, 26, 27 og 28 utøves vederlagsfritt for den registrerte. Dersom særlige grunner gjør det nødvendig, kan Kongen gi forskrift om at den registrerte må betale vederlag til den behandlingsansvarlige.

Kapittel 3 Innsynsrett og varslingsplikt m v

§ 16 Rett til generell informasjon om behandling av personopplysninger

Den som ber om det skal få vite hvilke behandlinger av personopplysninger en behandlingsansvarlig , et «a» n som ber om det skal dessuten få følgende informasjon om en bestemt behandling av personopplysninger:

1) navn og adresse på den behandlingsansvarlige og på dennes eventuelle representant, jf § 6
2) hvem som har det daglige ansvaret for å oppfylle pliktene som hviler på den behandlingsansvarlige
3) behandlingens formål
4) definisjoner og andre beskrivelser av de typer personopplysninger som inngår i behandlingen
5) kilde for opplysningene
6) hvem personopplysningene blir eller vil bli utlevert til, herunder planlagt utlevering av personopplysningene til mottakere i andre stater.

Informasjon kan kreves hos den behandlingsansvarlige eller dennes representant som nevnt i § 6. Den som ber om informasjon kan kreve at informasjonen gis skriftlig.

Kongen kan gi forskrift om unntak fra første ledd dersom dette er nødvendig av hensyn til rikets sikkerhet eller forebyggelse og etterforskning av straffbare handlinger.

§ 17 Offentlig fortegnelse over konsesjoner og meldinger

Datatilsynet skal føre en systematisk fortegnelse over alle behandlinger som er innmeldt etter § 31 eller gitt konsesjon i medhold av § 33. Av fortegnelsen skal det minst fremgå opplysninger som nevnt i § 16 annet ledd.

Fortegnelsen skal være offentlig på den maten Datatilsynet bestemmer.

Kongen kan gi forskrift om fortegnelsen og gjøre slike unntak fra første ledd som er nødvendig ut fra beredskapshensyn eller hensynet til rikets sikkerhet.

§18 Den registrertes rett til innsyn

Den registrerte skal på forespørsel få opplyst:

1) hvilke opplysninger om en selv som behandles ved elektroniske hjelpemidler eller som er tan inn i et manuelt register
2) behandlingens formål
3) hvem opplysningene om en selv blir eller vil bli utlevert til
4) kilden for disse opplysningene
5) hvilke sikkerhetstiltak som er knyttet til behandlingen, dersom innsyn ikke svekker sikkerheten.

Innsyn kan kreves hos den behandlingsansvarlige eller dennes representant som nevnt i § 6. Den registrene kan kreve at opplysningene skal gis skriftlig.

§ 19 Unntak fra den registrertes rett til innsyn

Innsynsretten etter § 18 gjelder ikke opplysninger som bare brukes til statistikk, forskning eller generelle planleggingsformål dersom behandlingen ikke får noen direkte betydning for den registrerte.

Innsynsretten gjelder ikke opplysninger som det må anses utilrådelig at den registrerte får kjennskap til, av hensyn til vedkommendes helse eller forholdet til personer som står dem nær. upplysningen kan på anmodning likevel gjøres kjent for en representant for den registrerte når ikke særlige grunner taler mot det.

Den registrerte kan ikke kreve innsyn i opplysninger i dokumenter som er unntatt fra innsyn etter forvaltningsloven § 18. Overfor behandlingsansvarlige som ikke er organ for stat eller kommune kan det ikke

kreves innsyn i opplysrunger i dokumenter som er uiarbeidet for den interne saksforberedelse av

1) den behandlingsansvarlige selv
2) særskilte rådgivere eller sakkyndige, eller
3) annen sammenslutning eller stiftelse innenfor eget konsern eller organisasjon.

Selv om opplysninger er unntatt etter regiene i fjerde ledd, har den registrene rett til innsyn i faktiske opplysninger eller sammendrag eller annen bearbeidelse av faktum. Dette gjelder likevel ikke når den registrene på annen mate har tilgang til de faktiske opplysningene.

Dersom innsyn kan motvirke muligheten for å få en sak som er under behandling avklart, kan den som kravet om innsyn retter seg mot bestemme at den registrene ikke skal gis innsyn så lenge undersøkelser pågår.

Kongen kan gi forskrift om unntak fra og vilkår for bruk av innsynsretten.

§ 20 Informasjonsplikt ved innsamling av personopplysninger fra den registrene

Ved innsamling av personopplysninger fra den registrene skal den behandlingsansvarlige opplyse den registrene om hvem som er behandlingsansvarlig, formålet med innsamlingen av opplysningene samt om det er frivillig å levere fra seg opplysningene. Informasjonsplikten gjelder ikke dersom den registrene må antas allerede å kjenne til dette.

Ytterligere informasjon skal gis dersom det må antas å være nødvendig for at den registrene skal kunne ivareta egne interesser. Eksempler på slik informasjon er hvem opplysningene kan bli utleven til, samt i hvilken grad den registrene kan kreve innsyn, retting eller sletting av opplysningene.

§ 21 Varslingsplikt ved innsamling av personopplysninger fra andre enn den registrene

Dersom personopplysningene innhentes fra andre enn den registrene, skal den behandlingsansvarlige gi informasjon som nevnt i § 15 annet ledd til den registrene når registrering skjer. Dersom opplysningene skal videregis innen rimelig tid, kan varslingen utsettes til første gangs videregivelse av opplysningene.

Første ledd gjelder ikke dersom

1) varslingen er umulig eller uforholdsmessig vanskelig,
2) den registrene må antas å være kjent med behandlingen, eller
3) det er fastsatt i lov at det er adgang til å registrere eller videregi opplysningene.

§ 22 Rett til begrunnelse for fullstendig automatisene avgjørelser

Dersom det foreligger en avgjørelse som definen i § 2 nr 9 som fullt ut er basen på automatisk behandling av personopplysninger. kan den som avgjørelsen retter seg mot kreve å få begrunnet resultatet. I begrunnelsen skal den behandlingsansvarlige redegjøre for regelinnholdet i datamaskinprogrammene som ligger til grunn for avgjørelsen.

§ 23 Varslingsplikt ved bruk av personprofiler

Når det treffes enkeltavgjørelser som definen i § 2 nr 9 eller gjøres henvendelser til den registrene på grunnlag av personprofiler som er ment å beskrive atferd, preferanser. evner eller behov, skal den behandlingsansvarlige opplyse den registrene om hvem som er behandlingsansvarlig, hvilke opplysningsryper som er anvendt, samt kildene for disse opplysningene.

§ 24 Varslingsplikt ved elektronisk overvåkning

Ved elektronisk overvåkning på offentlig sted eller arbeidssted skal det ved skilting eller på annen mate gjøres tydelig oppmerksom på at stedet blir overvåket og hvem som er behandlingsansvarlig.

Kapittel 4 Retting og sletting mv

§ 25 Plikt til å rette, slette, supplere og sperre mangelfulle personopplysninger

Dersom det er registren personopplysninger som er uriktige, ufullstendige eller som det ikke er adgang til å registrere, skal den behandlingsansvarlige sørge for at opplysningene rettes, slettes eller suppleres såframt mangelen kan få betydning for den registrene. Har mangelen ført til at det er gitt eller brukt slike opplysninger, skal den behandlingsansvarlige såvidt mulig sørge for at feilen ikke får betydning for den registrene.

Dersom opplysningene på grunn av annen lovgivning ikke kan slettes eller rettes kan Datatilsynet gi pålegg om at opplysningene skal sperres for å forhindre at de blir brukt.

§ 26 Sletting og sperring av personopplysninger

Den behandlingsansvarlige plikter, når det ikke lenger er saklig grunn for oppbevaring, å slette personopplysninger som behandles elektronisk eller som inngår eller skal inngå i et manuelt personregister. Med saklig grunn forstås blant annet at oppbevaring er pålagt i eller i medhold av lov eller at den behandlingsansvarlige behandler opplysningene til det formål de er innsamlet for.

Den registrene kan, dersom dette ikke strider mot annen lov, likevel kreve slike opplysninger om seg selv sperret eller slettet dersom opplysningene er belastende for den registrene og sperring eller sletting finnes forsvarlig ut fra en samlet vurdering av andres interesser, personvemintersser, samfunnsmessige interesser og den ressursinnsats som kravet forutsetter. Datatilsynet kan gi pålegg om slik sperring eller sletting. Slikt pålegg går foran bestemmelsene om kassasjon i lov 4 desember 1992 nr 126 om arkiv § 9.

§27 Rett til å kreve manuell behandling av personopplysninger

Den som en avgjørelse retter seg mot eller som

saken ellers direkte gjelder, kan kreve at personopplysningene behandles manuelt dersom avgjørelsen

1) er en enkeltavgjørelse som definert i § 2 nr 9 eller som på annen mate har vesentlig betydning for vedkommende, og
2) fullt ut er basert på automatisk behandling, og
3) karakteriserer personlige egenskaper.

Retten til å kreve en manuell behandling som nevnt i første ledd gjelder ikke dersom det er truffet tilstrekkelige tiltak for å ivareta vedkommendes personverninteresser, og

1) avgjørelsen er hjemlet i lov, eller
2) avgjørelsen knytter seg til inngåelse eller oppfyllelse av kontrakt.

§ 28 Rett til å kreve sitt navn sperret mot bruk i markedsføringsøyemed

Kongen kan gi forskrift om at det skal opprettes et sentralt reservasjonsregister samt nærmere regler for registeret.

Den registrerte kan kreve sitt navn sperret mot bruk til direkte markedsføring. Sperring kan kreves både i det sentrale reservasjonsregisteret og i markedsførerens adresseregister.

En behandlings ans varlig som markedsfører direkte plikter å oppdatere adresseregisteret i henhold til det sentrale reservasjonsregisteret før første gangs utsendelse og minst to ganger pr år. Kongen kan i forskrift gjøre unntak fra denne plikten.

Mottakere av direkte reklame skal få opplyst hvem som har oppgitt personopplysningene som ligger til grunn for henvendelsen.

Denne bestemmelsen gjelder ikke for markedsføring av egne produkter fra den behandlingsansvarlige hvor den registrerte har et løpende kundeforhold.

Kapittel 5 Videregivelse av personopplysninger til utlandet

§ 29 Vilkår for videregivelse av personopplysninger til utlandet - hovedregel

Videregivelse av personopplysninger til utlandet kan bare skje dersom staten som mottakeren skal behandle personopplysningene i regulerer behandling av personopplysninger på en tilstrekkelig forsvarlig mate. Stater som har gjennomført direktiv 95/46/EF oppfyller kravet til tilstrekkelig forsvarlig regulering.

I vurderingen av om stater som ikke har gjennomført direktiv 95/46/EF regulerer behandling av personopplysninger på en tilstrekkelig forsvarlig mate, skal det bl a legges vekt på opplysningenes art, de planlagte behandlingenes formal og varighet, den aktuelle statens rettsreglerom behandling av personopplysninger. regler for god forretningsskikk og sikkerhetsforanstaltninger hos mottakeren. Det skal også legges vekt på om den aktuelle staten har tiltrådt Europarådets konvensjon 28 januar 1981 nr 108.

§ 30 Videregivelse av personopplysninger til stater som ikke regulerer behandling av personopplysninger på en tilstrekkelig forsvarlig mate

Videregivelse av personopplysninger til utlandet kan skje selv om den aktuelle staten ikke regulerer behandling av personopplysninger på en tilstrekkelig forsvarlig mate dersom

1) den registrerte har gitt sitt samtykke til videregivelsen
2) Norge har plikt til å foreta slik videregivelse etter folkerettslig overenskomst eller som følge av medlemsskap i internasjonal organisasjon
3) det er fastsatt i lov at det er adgang til å videregi opplysningene
4) videregivelsen er nødvendig for å inngå eller oppfylle en kontrakt mellom den registrerte og den behandlingsansvarlige
5) videregivelsen er nødvendig for å inngå eller oppfylle en kontrakt i den registrertes interesse
6) videregivelsen er nødvendig for å beskytte den registrertes vesentlige interesser.

Dersom særlig grunner taler for det, kan Datatilsynet tillate videregivelse selv om vilkårene i første ledd ikke er oppfylt.

Kongen kan gi forskrift om videregivelse av personopplysninger til utlandet.

Kapittel 6 Meldeplikt og konsesjonsplikt m v

§ 31 Meldeplikt

Enhver behandlinesansvarlig som benytter elektroniske systemer ror benandling av personopplysninger skal gi melding til Datatilsynet på fastsatt skjema i god tid før behandlingen tar til.

Slik melding skal også sendes ved opprettelse av et manuelt personregister dersom det skal inneholde sensitive personopplysninger, jf § 2 nr 8.

Meldeplikten gjelder ikke for behandinger som utelukkende gjør bruk av aliment tilgjengelige personopplysninger.

Kongen kan gi forskrift om at visse typer behandlinger skal være unntatt fra meldeplikten etter første og annet ledd. underlagt en forenklet meldeplikt eller underlagt konsesjonsplikt. For behandlinger som unntas fra meldeplikt kan det gis forskrift om forhold som nevnt i § 35 annet ledd. Det kan også gis forskrift for å begrense de ulemper behandlingen ellers kunne medføre for den enkelte.

§ 32 Meldingens innhold

Meldingen skal inneholde opplysninger om

1) navn og adresse på den behandlingsansvarlige og på dennes eventuelle representant, jf § 6
2) hvem som har det daglige ansvaret for å oppfylle pliktene som hviler på den behandlingsansvarlige
3) behandlingens formål
4) definisjoner og andre beskrivelser av de typer personopplysninger som inngår i behandlingen

5) kildene for personopplysningene
6) grunnlaget for innhenting av opplysningene
7) hvem personopplysningene blir eller vil bli utlevert til
8) planlagt utlevering av personopplysningene til mottakere i andre stater, og
9) hvilke sikkerhetstiltak som er knyttet til behandlingen.

Kongen kan gi forskrift om hvilke opplysninger meldingene skal inneholde. samt regler om gjennomføringen av meldepliktsordningen.

Den behandlingsansvarlige er ansvarlig for at det til enhver tid er innsendt melding som gir riktige opplysninger. Ny melding med oppdaterte opplysninger skal sendes etter 3 år, med mindre det i løpet av denne tiden er sendt endringsmelding. Kongen kan gi forskrift som skal sikre meldingenes kvalitet og kan for enkelte typer av behandlinger fastsette andre regler for når ny melding skal sendes.

§ 33 Konsesjonsplikt

Det kreves samtykke fra Datatilsynet (konsesjon) for å behandle sensitive personopplysninger (jf § 2 nr 8) når formålet med behandlingen er å treffe enkeltavgjørelser som definert i § 2 nr 9.

Kongen kan gi forskrift om at visse typer behandlinger skal være unntatt fra konsesjonsplikten etter første ledd, og i stedet underlagt meldeplikt etter §31. For slik behandling skal det gis forskrift om forhold som nevnt i § 35 annet ledd. Det kan også gis forskrift for å begrense de ulemper behandlingen ellers kunne medføre for den enkelte.

§ 34 Vurderingen av om konsesjon skal gis

Ved vurderingen av om konsesjon skal gis, skal det innenfor den rammen som er fastsatt i loven kapittel 2, vurderes om behandlingen av de sensitive personopplysningene kan volde ulemper for den registrerte som ikke løses tilfredsstillende av vilkår fastsatt i medhold av § 35 første ledd. Dersom slike ulemper kan oppstå, må det overveies om de blir oppveid av hensyn som taler for at behandlingen kan finne sted.

§ 35 Vilkår for konsesjonsplikiige behandlinger

Når det blir gitt samtykke etter § 33, skal det fastsettes nærmere vilkår for behandlingen dersom slike vilkår anses nødvendige for å begrense de ulempene behandlingen ellers kunne medføre.

I vurderingen av om det er nødvendig å sette vilkår etter første ledd bør det blant annet tas i betraktning om

1) det er lagt til rene for at de registrerte kan gjøre nytte av rettighetene etter loven, herunder om de vil bli gitt tilstrekkelig informasjon om sine rettigheter og mulighetene til å gjøre nytte av dem
2) personopplysningene vil bli tilstrekkelig korrekte, dekkende og ajourførte i forhold til formålet med behandlingen, jf § 7
3) personopplysningene vil bli behandlet med den diskresjon som regler om taushetsplikt og formålet med behandlingen gjør nødvendig
4) det er planlagt informasjons- og veiledningstiltak som står i et rimelig forhold til kontrolltiltak
5) det er etablert tilstrekkelig sikkerhet i forhold til formålene med behandlingen av personopplysninger.

Kapittel 7 Tilsyn og sanksjoner

§ 36 Datatilsynets organisering og oppgaver

Datatilsynet skal være et uavhengig forvaltningsorgan administrativt underordnet Kongen og det departement Kongen fastsetter. Datatilsynet ledes av en direktør som utnevnes av Kongen. Direktøren kan utnevnes for en tidsavgrenset periode.

Kongen kan ikke gi Datatilsynet instrukser om håndhevingen av loven, og heller ikke om myndighetsutøvelsen i enkelttilfeller. Datatilsynets enkeltvedtak kan ikke omgjøres av Kongen.

Datatilsynet skal

1) behandle søknader om konsesjoner, motta meldinger og vurdere om det skal gis pålegg der loven gir hjemmel for dette
2) kontrollere at lover og forskrifter som gjelder for behandling av personopplysninger blir fulgt, og at feil eller mangler blir rettet
3) holde seg orientert om den generelle nasjonale og internasjonale utviklingen i behandlingen av personopplysninger og om de problemer som knytter seg tu slik behandling, samt gi informasjon om dette
4) identifisere og formulere personverntrusler, og gi råd om hvorledes de kan unngås eller begrenses
5) gi råd og rettledning i spørsmål om personvem og sikring av personopplysninger til dem som planlegger å behandle personopplysninger eller utvikle systemer for slik behandling, herunder gi bistand i utarbeidelsen av bransjevise atferdsnormer
6) etter henvendelse eller av eget tiltak gi uttalelse i spørsmål om behandling av personopplysninger, herunder være høringsinstans ved utarbeidelsen av lover og forskrifter som har direkte betydning for personvem
7) gi Kongen eller det departement Kongen fastsetter årlig melding om sin virksomhet.

Alternativt forslag til § 36 forste ledd:

Datatilsynet skal være et uavhengig forvaltningsorgan administrativt underordnet Kongen og det departement Kongen fastsetter. Datatilsynet ledes av et styre som skal ha syv medlemmer. Medlemmene blir oppnevnt av Kongen som også fastsetter hvem som skal være styrets leder og nestleder. Datatilsynets direktør kan utnevnes for en tidsavgrenset periode.

§ 37 Personvernnemndas oppgaver og organisering

Personvemnemnda avgjør klager over Datatilsynets avgjørelser. Nemnda kan bestemme at tre av

nemndas medlemmer, herav leder og/eller nestleder kan behandle klager over avgjørelser som etter sin an må avgjøres uten opphold. Nemnda orienterer årlig Kongen om behandlingen av klagesakene.

Personvernnemnda skal være et uavhengig forvaltningsorgan administrativt underordnet Kongen og det departement Kongen fastsetter. Paragraf 36 annet ledd gjelder tilsvarende.

Personvernnemnda har fem medlemmer som oppnevnes for fire år. Medlemmene blir oppnevnt av Kongen, som også fastsetter hvem som skal være nemndas leder og nestleder. Leder og nestleder skal ha kompetanse som nevnt i domstolloven § 54 annet ledd.

Alternativt forslag til § 37 tredje ledd:

Personvernnemnda har syv medlemmer som oppnevnes for fire år. Fem av medlemmene oppnevnes av Kongen. Lederen og nestlederen oppnevnes av Stortinget. Lederen og nestlederen skal ha kompetanse som nevnt i domstolloven § 54 annet ledd.

§ 38 Tilsynsmyndighetens tilgang til opplysninger m v

Datatilsynet og Personvernnemnda kan kreve de opplysningene som trengs for at det kan gjennomføre sine oppgaver.

Datatilsynetilsynet kan kreve å få adgang til de stedene der personregistre, billedopptak som nevnt i § 4, personopplysninger som behandles elektronisk og hjelpemidlene for elektronisk behandling av personopplysninger fins. Tilsynet kan gjennomføre de prøver eller kontroller som det mener er nødvendige og kreve nødvendig bistand fra personalet slike steder for å få utført prøvene eller kontrollene. Beslutninger om stedlig kontroll kan påklages til Personvernemnda.

Datatilsynets rett til å kreve opplysninger og tilgang til lokaler og hjelpemidler er ikke begrenset av taushetsplikt.

Kongen kan gjøre unntak fra første til tredje ledd som er nødvendige av hensyn til rikets sikkerhet. Kongen kan også gi forskrift om dekning av utgiftene ved kontroll. Skyldig bidrag til dekning av utgiftene er tvangsgrunnlag for utlegg.

§ 39 Unntak fra taushetsplikt

Datatilsynets ansatte og medlemmer av Personvernnemnda kan uten hinder av lovbestemt taushetsplikt gi opplysninger til utenlandske tilsynsmyndigheter når dette er nødvendig for at tilsynsmyndigheten eller utenlandske tilsynsmyndigheter skal kunne treffe vedtak, eller for å gjennomføre slike vedtak.

Alternativt forslag til § 39:

Datatilsynets ansatte, styremedlemmer og medlemmer av Personvernnemnda kan uten hinder av lovbestemt taushetsplikt gi opplysninger til utenlandske tilsynsmyndigheter når dette er nødvendig for at tilsynsmyndigheten eller utenlandske tilsynsmyndigheter skal kunne treffe vedtak, eller for å gjennomføre slike vedtak.

§ 40 Pålegg om opphør av ulovlige behandlinger m v

Datatilsynet kan gi pålegg om at behandling av personopplysninger i strid med denne loven skal opphøre eller stille vilkår som må oppfylles for at behandlingen skal være i samsvar med loven. Pålegg kan påklages til Personvernnemnda.

Ved vurderingen av om det skal gis pålegg ener første ledd skal det særlig tas i betraktning forhold som nevnt i § 35 annet ledd nr 1-5.

§ 41 Tvangsmulkt

Dersom pålegg i medhold av §§ 10, 25, 26 eller 40 ikke overholdes, kan Datatilsynet bestemme at den avgjørelsen retter seg mot skal betale en daglig løpende mulkt til staten inntil forholdet rettes.

Mulkten løper ikke før klagefristen er ute. Hvis vedtaket om tvangsmulkt påklages, løper ingen mulkt før vedtak om mulkt treffes av Personvernnemnda.

Mulkten er tvangsgrunnlag for utlegg.

§ 42 Straff

Med bøter eller fengsel inntil ett år eller begge deler straffes den som forsettlig eller aktløst

1) unnlater å innhente samtykke etter §§ 33 eller 46
2) unnlater å sende melding etter §§31 eller 46
3) overtrer vilkår fastsatt etter § 35 eller § 40
4) behandler personopplysninger i strid med §§11. 13 eller 28
5) unnlater å varsle etter §§ 20, 21, 23 eller 24
6) unnlater å etterkomme pålegg fra Datatilsynet etter §§ 10, 25, 26 eller 40
7) unnlater å gi opplysninger etter §§16 eller 18 jf 19.

Ved særdeles skjerpende omstendigheter kan fengsel inntil to år idømmes. Ved avgjørelsen av om det foreligger særdeles skjerpende omstendigheter skal det blant annet legges vekt på faren for stor skade eller ulempe for den registrerte, den tilsiktede vinning ved overtredelsen, overtredelsens varighet og omfang, utvist skyld, og på om den skyldige tidligere er straffet for overtredelse av tilsvarende bestemmelser.

Medvirkning straffes på samme mate.

I forskrift som gis i medhold av loven, kan det fastsettes at overtredelse av forskriften skal straffes med bøter eller fengsel inntil ett år eller begge deler.

§ 43 Erstatning

Har den behandlingsansvarlige eller dennes databehandler behandlet personopplysninger i strid med denne loven eller vedtak gitt i medhold av den, skal den behandlingsansvarlige erstatte det økonomiske tapet som skaden påfører den registrene. Den behandlingsansvarlige kan fritas for ansvar dersom han godtgjør at tapet ikke skyldes feil eller forsømmelse på den behandlingsansvariiges side.

Kongen kan gi forskrift om objektivt ansvar for virksomheter som formidler personopplysninger (§ 45) og som har meddelt opplysninger som viser seg uriktige eller åpenbart misvisende.

Kapittel 8 Forholdet til andre lover. Ikraftsetting. Overgangsregler, m v

§ 44 Forholdet til andre lover

Loven gjelder også for behandling av personopplysninger som er regulert i armen lov i den utstrekning ikke annet følger av hjemmelsloven.

§ 45 Forskriftsregulering av bestemte former for virksomheter

Kongen kan gi forskrift om behandling av personopplysninger for særskilte virksomheter og bransjer.

§ 46 Overgangsregler

Innehavere av konsesjon etter lov om personregistre mm § 9 som blir meldepliktige eller konsesjonspliktige i medhold av denne lov kapittel 6, skal sende melding etter § 31 eller søke konsesjon etter § 33 innen tre år fra loven trer i kraft. Konsesjonsvilkårene gjelder i den utstrekning de ikke strider mot denne loven.

Behandlingsansvarlige som ikke har konsesjon etter lov om personregistre mm § 10 og som foretar behandling av personopplysninger som blir meldepliktige eller konsesjonspliktige i medhold av denne lov kapittel 6, skal sende melding etter § 31 eller søke konsesjon etter § 33 innen ett år fra loven trer i kraft.

Kongen kan gi forskrift med utfyllende overgangsregler.

§ 47 Ikrafttredelse

Loven trer i kraft fra den tiden Kongen bestemme. De ulike paragrafene kan settes i kraft til ulik tid.

FÖRFATTNINGSFÖRSLAG

a) Förslag till

Persondatalag (1998:000)

Härmed föreskrivs[1] följande.

Inledande bestämmelser

Syftet med lagen

1 § Syftet med denna lag är att skydda människor mot otillbörligt intrång i den personliga integriteten vid behandling av personuppgifter.

Avvikande bestämmelser i annan lagstiftning

2 § Om det i en annan lag eller i en förordning finns bestämmelser som avviker från denna lag, skall dessa bestämmelser gälla.

[1] Jfr Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (EGT nr L 281. 23.11.1995. s. 31, Celex 395L0046).

Definitioner

3 § I denna lag används följande beteckningar med nedan angiven betydelse.

Beteckning	*Betydelse*
Behandling (av personuppgifter)	Varje åtgärd som vidtas beträffande personuppgifter.
Blockering (av personuppgifter)	Varje åtgärd som kan vidtas för att personuppgifterna i alla sammanhang skall vara förknippade med tydlig information om att de är spärrade och om anledningen till spärren och för att personuppgifterna inte skall lämnas ut till tredje man annat än med stöd av 2 kap. tryckfrihetsförordningen.
Den registrerade	Den som en personuppgift avser.
Känsliga personuppgifter	Sådana personuppgifter som avses i 13 §.
Mottagare	Den till vilken personuppgifter lämnas ut. När personuppgifter lämnas ut för att en myndighet skall kunna utföra sådan tillsyn, kontroll eller revision som åligger den, anses dock inte myndigheten som mottagare.
Persondataansvarig	Den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter.
Persondatabiträde	Den som behandlar personuppgifter för den persondataansvariges räkning.
Personuppgifter	All slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet.
Samtycke	Varje slag av frivillig, särskild och informerad viljeyttring genom vilken den registrerade godtar behandling av personuppgifter som rör honom eller henne.
Tillsynsmyndigheten	Den myndighet som regeringen utser.
Tredje land	En stat som inte ingår i Europeiska unionen eller är ansluten till Europeiska ekonomiska samarbetsområdet.

Beteckning	*Betydelse*
Tredje man	Någon annan än den registrerade, den personuppgiftsansvarige, personuppgiftsbiträdet och sådana personer som under den personuppgiftsansvariges eller personuppgiftsbiträdets direkta ansvar har befogenhet att behandla personuppgifter. Ett sådant personuppgiftsombud som avses i 37 § anses inte som tredje man.

Tillämpningsområdet

Det territoriella tillämpningsområdet

4 § Denna lag gäller för sådana personuppgiftsansvariga som är etablerade i Sverige.

Lagen tillämpas också när den personuppgiftsansvarige är etablerad i tredje land men för behandlingen av personuppgifter använder sig av utrustning som finns i Sverige. Vad som nu sagts gäller dock inte om utrustningen bara används för att överföra uppgifter mellan ett tredje land och ett annat sådant land.

I det fall som avses i andra stycket skall den personuppgiftsansvarige utse en företrädare för sig som är etablerad i Sverige. Den personuppgiftsansvarige skall, innan utrustningen börjar användas, till tillsynsmyndigheten skriftligen anmäla vem som har utsetts och därvid bifoga ett skriftligt medgivande från den utsedde. Vad som anges i denna lag om den personuppgiftsansvarige skall också gälla den företrädare som har anmälts på detta sätt.

Vilken behandling av personuppgifter omfattas av lagen

5 § Denna lag gäller för sådan behandling av personuppgifter som helt eller delvis är automatisk.

Lagen gäller även för annan behandling av personuppgifter, om uppgifterna ingår i eller är avsedda att ingå i ett register. Med register avses varje strukturerad samling av personuppgifter vilka är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

Undantag för privat användning av personuppgifter

6 § Denna lag gäller inte för sådan behandling av personuppgifter som en fysisk person utför som ett led i en verksamhet av rent privat natur.

Undantag med hänsyn till yttrandefriheten

7 § Bestämmelserna i 9-29 och 33-46 §§ samt 47 § första stycket och 49 § skall inte tillämpas på

a) sådana förfaranden som är skyddade enligt tryckfrihetsförordningen eller yttrandefrihetsgrundlagen,
b) spridningen av sådana yttranden som är skyddade enligt tryckfrihetsförordningen eller yttrandefrihetsgrundlagen, eller
c) sådan behandling av personuppgifter som annars sker uteslutande för journalistiska ändamål eller konstnärligt eller litterärt skapande.

Förhållandet till offentlighetsprincipen

8 § **Bestämmelserna** i **denna** lag skall inte tillämpas i den utsträckning det **skulle inskränka en myndighets** skyldighet enligt 2 kap. tryckfrihetsförordningen **att lämna ut personuppgifter.**

Bestämmelserna hindrar inte heller att en myndighet arkiverar och bevarar sina **allmänna uppgifter eller att** arkivmaterial tas om hand av en arkivmyndighet. **Bestämmelserna i 9** § tredje stycket gäller inte för personuppgifter i en **myndighets arkiv.**

Grundläggande krav på behandlingen av personuppgifter

9 § Den persondataansvarige skall **se till**

a) att personuppgifter behandlas bara när det är lagligt, särskilt att samtycke inhämtas när så krävs,
b) att personuppgifter alltid behandlas på **ett korrekt** sätt,
c) att personuppgifter samlas in bara för särskilda, uttryckligt angivna och berättigade ändamål,
d) att personuppgifter inte behandlas för något ändamål **som** är **oförenligt** med det för vilket uppgifterna samlades in,
e) att de personuppgifter som behandlas är adekvata och relevanta **i** förhållande till ändamålen med behandlingen,
f) att inte fler personuppgifter behandlas än som är nödvändigt med hänsyn till ändamålen med behandlingen,
g) att de personuppgifter som behandlas är riktiga och, om det är nödvändigt, aktuella,

h) att alla rimliga åtgärder vidtas för att rätta, blockera eller utplåna sådana personuppgifter som är felaktiga, missvisande eller ofullständiga med hänsyn till ändamålen med behandlingen, och
i) att personuppgifter inte bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen.

Beträffande första stycket d) gäller att en behandling av personuppgifter för historiska, statistiska eller vetenskapliga ändamål inte skall anses som oförenlig med de ändamål för vilka uppgifterna samlades in. I fråga om första stycket i) gäller att personuppgifter far bevaras under längre tid än som sagts där för historiska, statistiska eller vetenskapliga ändamål.

Personuppgifter som behandlas för historiska, statistiska eller vetenskapliga ändamål far användas för att vidta åtgärder beträffande den registrerade bara om den registrerade har lämnat sitt samtycke eller det finns synnerliga skäl med hänsyn till den registrerades eller någon annans vitala intressen.

När **behandling av personuppgifter är tillåten**

Allmänt

10 § Personuppgifter far behandlas bara om den registrerade har lämnat sitt samtycke till behandlingen eller när behandlingen är nödvändig
a) för att fullgöra ett avtal med den registrerade,
b) för att på den registrerades begäran vidta åtgärder innan ett avtal träffas,
c) för att den persondataansvarige skall kunna fullgöra en rättslig skyldighet,
d) för att skydda vitala intressen för den registrerade,
e) för att utföra en arbetsuppgift av allmänt intresse,
f) för att den persondataansvarige eller en tredje man till vilken personuppgifter lämnas ut skall kunna utföra en arbetsuppgift i samband med myndighetsutövning, eller
g) för ändamål som rör ett berättigat intresse hos den persondataansvarige eller hos sådana tredje män till vilka personuppgifterna lämnas ut när detta intresse väger tyngre än den registrerades intresse.

Direkt marknadsföring

11 § Personuppgifter får inte behandlas för ändamål som rör direkt marknadsföring, om den registrerade hos den personansvarige skriftligen har anmält att han eller hon motsätter sig sådan behandling.

Samtycke återkallas

12 § I de fall där behandling av personuppgifter bara är tillåten när den registrerade har lämnat sitt samtycke enligt 10, 15 eller 34 § har den registrerade rätt att när som helst återkalla ett lämnat samtycke. Ytterligare personuppgifter om den registrerade får därefter inte behandlas.

En registrerad har utöver vad som följer av första stycket och 11 § inte rätt att motsätta sig sådan behandling av personuppgifter som är tillåten enligt denna lag.

Förbud mot behandling av känsliga personuppgifter

13 § Det är förbjudet att behandla personuppgifter som avslöjar
a) ras eller etniskt ursprung,
b) politiska åsikter,
c) religiös eller filosofisk övertygelse, eller
d) medlemskap i fackförening.

Det är också förbjudet att behandla sådana personuppgifter som rör hälsa eller sexualliv.

Undantag från förbudet mot behandling av känsliga personuppgifter

Allmänt

14 § Utan hinder av 13 § är det tillåtet att behandla känsliga personuppgifter i de fall som anges i 15-19 §§.

I 10 § finns det bestämmelser om i vilka fall behandling av personuppgifter över huvud taget är tillåten.

Samtycke eller offentliggörande

15 § Känsliga personuppgifter får behandlas, om den registrerade har samtyckt till behandlingen eller på ett tydligt sätt offentliggjort uppgifterna.

Behandlingen är nödvändig i vissa fall

16 § Känsliga personuppgifter får behandlas när behandlingen är nödvändig för att

a) den personadataansvarige skall kunna fullgöra sina skyldigheter eller utöva sina rättigheter inom arbetsrätten,
b) skydda vitala intressen för den registrerade eller någon annan och den registrerade inte kan lämna samtycke, eller
c) rättsliga anspråk skall kunna fastställas, göras gällande eller försvaras.

Uppgifter som behandlas med stöd av första stycket a) får lämnas ut till tredje man bara om det inom arbetsrätten finns en uttrycklig skyldighet för den persondataansvarige att göra det eller den registrerade har samtyckt till utlämnandet.

Ideella organisationer

17 § Ideella organisationer med politiskt, filosofiskt, religiöst eller fackligt syfte får inom ramen för sin verksamhet behandla känsliga personuppgifter om organisationens medlemmar och sådana andra personer som på grund av organisationens syfte har regelbunden kontakt med denna. Känsliga personuppgifter får dock lämnas ut till tredje man bara om den registrerade har samtyckt till det.

Hälso- och sjukvård

18 § Känsliga personuppgifter får behandlas, om behandlingen är nödvändig för

a) förebyggande hälso- och sjukvård,
b) medicinska diagnoser,
c) vård eller behandling, eller
d) administration av hälso- och sjukvård.

Den som är yrkesmässigt verksam inom hälso- och sjukvårdsområdet och har tystnadsplikt får alltid behandla känsliga personuppgifter som omfattas av tystnadsplikten.

Forskning och statistik

19 § Känsliga personuppgifter far behandlas för forsknings- och statistikändamål, om behandlingen är nödvändig och om samhällsintresset av det forsknings- eller statistikprojekt vari behandlingen ingår klart väger över den risk för otillbörligt intrång i enskildas personliga integritet som behandlingen kan innebära.

Har projektet godkänts av en forskningsetisk kommitté, skall förutsättningarna enligt första stycket anses uppfyllda. Med forskningsetisk kommitté avses ett sådant särskilt organ för prövning av forskningsetiska frågor som har företrädare för såväl det allmänna som forskningen och som är knutet till ett universitet eller en högskola eller till någon annan instans som i mera betydande omfattning finansierar forskning.

Personuppgifter far lämnas ut för att användas i sådana projekt som avses i första stycket, om inte något annat följer av sekretesslagen (1980:100).

Bemyndigande att föreskriva ytterligare undantag

20 § Regeringen eller den myndighet som regeringen bestämmer far föreskriva ytterligare undantag från förbudet i 13 §, om det behövs med hänsyn till ett viktigt allmänt intresse.

Uppgifter om lagöverträdelser

21 § Det är förbjudet för andra än myndigheter att behandla personuppgifter om lagöverträdelser eller om domar och säkerhetsåtgärder i brottmål.

Regeringen eller den myndighet som regeringen bestämmer får föreskriva undantag från förbudet i första stycket.

Användning av personnummer

22 § Uppgift om personnummer far behandlas bara när det är klart motiverat med hänsyn till

a) ändamålet med behandlingen,
b) vikten av en säker identifiering, eller
c) något annat beaktansvärt skäl.

Information till den registrerade

Information skall lämnas självmant när uppgifterna samlas in

23 § När uppgifter om en person samlas in från denne själv, skall den persondataansvarige självmant lämna den registrerade information rörande behandlingen.

24 § Om personuppgifterna har samlats in från annan källa än den registrerade, skall den persondataansvarige självmant lämna den registrerade information rörande behandlingen när uppgifterna noteras. Är uppgifterna avsedda att lämnas ut till tredje man, behöver informationen dock lämnas först när uppgifterna lämnas ut för första gången.

Information enligt första stycket behöver inte lämnas, om det finns bestämmelser om registrerandet eller utlämnandet av personuppgifterna i en lag eller någon annan författning.

Information behöver inte heller lämnas enligt första stycket, om detta visar sig vara omöjligt eller skulle innebära en oproportionerligt stor arbetsinsats. Om uppgifterna används för att vidta åtgärder beträffande den registrerade, skall dock information alltid lämnas senast i samband med att så sker.

Vilken information skall lämnas självmant

25 § Information enligt 23 § eller 24 § första stycket skall omfatta

a) uppgift om den persondataansvariges identitet,
b) uppgift om ändamålen med behandlingen, och
c) all övrig information som behövs för att den registrerade skall kunna ta till vara sina rättigheter, såsom information om mottagarna av uppgifterna, skyldighet att lämna uppgifter och rätten att ansöka om information.

Uppgifter behöver dock inte lämnas om sådant som den registrerade redan känner till.

Information skall också lämnas efter ansökan

26 § Den persondataansvarige är skyldig att till var och en som ansöker om det en gång per kalenderår gratis lämna information, om personuppgifter som rör sökanden behandlas eller inte. Behandlas sådana uppgifter skall skriftlig information lämnas också om

a) vilka uppgifter om sökanden som behandlas,
b) varifrån dessa uppgifter har hämtats,
c) ändamålen med behandlingen, och
d) till vilka mottagare eller kategorier av mottagare som uppgifterna lämnas ut.

En ansökan enligt första stycket skall göras skriftligen hos den persondataansvarige och vara undertecknad av den sökande själv. Information enligt första stycket skall lämnas inom en månad från det att ansökan gjordes. Det är dock tillåtet att lämna information bara vid tre över året jämnt fördelade tillfällen, om det finns särskilda skäl för det.

Information enligt första stycket behöver inte lämnas beträffande personuppgifter i löpande text som inte fatt sin slutliga utformning när ansökan gjordes eller som utgör minnesanteckning eller liknande. Vad som nu sagts gäller dock inte om uppgifterna har lämnats ut till tredje man, om uppgifterna behandlas bara för historiska, statistiska eller vetenskapliga ändamål eller, såvitt gäller löpande text som inte fått sin slutliga utformning, om uppgifterna har behandlats under längre tid än ett år.

Undantag från informationsskyldigheten vid sekretess och tystnadsplikt

27 § I den utsträckning det är särskilt föreskrivet i lag eller annan författning eller i beslut som har meddelats med stöd av författning att uppgifter inte får lämnas ut till den registrerade gäller inte bestämmelserna i 23-26 §§.

Regeringen eller den myndighet som regeringen bestämmer får medge undantag från bestämmelserna i 23-26 §§, om det behövs för att skydda grundläggande intressen för enskilda eller för att förebygga, undersöka eller avslöja brott.

Rättelse

28 § Den persondataansvarige är skyldig att på begäran av den registrerade rätta, blockera eller utplåna sådana personuppgifter som inte har behandlats i enlighet med denna lag eller föreskrifter som har utfärdats med stöd av lagen. Den persondataansvarige skall också underrätta de tredje män till vilka uppgifterna har lämnats ut om åtgärden, om den registrerade begär det eller om en underrättelse skulle kunna undvika mera betydande skada eller olägenhet för den registrerade. Någon sådan underrättelse behöver dock inte lämnas om detta visar sig vara omöjligt eller skulle innebära en oproportionerligt stor arbetsinsats.

Automatiserade beslut

29 § Ett beslut som har rättsliga följder för en fysisk person eller annars har märkbara verkningar för denne far grundas enbart på automatisk behandling av personuppgifter, vilka är avsedda att bedöma egenskaper hos den berörda personen, bara om den som berörs av beslutet har möjlighet att på begäran fa beslutet omprövat på manuell väg.

Var och en som varit föremål för ett sådant beslut som avses i första stycket har rätt att på ansökan fa information från den persondataansvarige om vilka regler som har styrt den automatiska behandling som har lett fram till beslutet. I fråga om ansökan och lämnandet av information gäller i tillämpliga delar bestämmelserna i 26 §.

Säkerheten vid behandling

De personer som arbetar med personuppgifter

30 § Ett persondatabiträde och den eller de personer som arbetar under dennes eller den persondataansvariges ledning får behandla personuppgifter bara i enlighet med instruktioner från den persondataansvarige. I fråga om sekretess och tystnadsplikt i det allmännas verksamhet tillämpas i stället bestämmelserna i sekretesslagen (1980:100).

Det skall finnas ett skriftligt avtal om persondatabiträdets behandling av personuppgifter för den persondataansvariges räkning. I det avtalet skall det särskilt föreskrivas att persondatabiträdet får behandla personuppgifterna bara i enlighet med instruktioner från den persondataansvarige och

att persondatabiträdet är skyldigt att vidta de åtgärder som avses i 31 § första stycket.

Skyddsåtgärder

31 § Den persondataansvarige skall vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna skall åstadkomma en säkerhetsnivå som är lämplig med beaktande av

a) de tekniska möjligheter som finns,
b) vad det skulle kosta att genomföra åtgärderna,
c) de särskilda risker som finns med behandlingen av personuppgifterna, och
d) hur pass känsliga de behandlade personuppgifterna är.

När den persondataansvarige anlitar ett persondatabiträde, skall den persondataansvarige förvissa sig om att persondatabiträdet kan genomföra de säkerhetsåtgärder som måste vidtas och se till att persondatabiträdet verkligen vidtar åtgärderna.

Tillsynsmyndigheten får besluta om skyddsåtgärder

32 § Tillsynsmyndigheten får besluta om vilka skyddsåtgärder som den persondataansvarige skall vidta enligt 31 §.

I 47 § finns det bestämmelser om tillsynsmyndighetens möjligheter att förena beslutet med vite.

Överföring av personuppgifter till tredje land

Förbud mot överföring

33 § Det är förbjudet att till tredje land föra över personuppgifter som behandlas. Förbudet gäller också överföring av personuppgifter för behandling i tredje land.

Undantag från förbudet

34 § Utan hinder av 33 § är det tillåtet att föra över personuppgifter till tredje land, om den registrerade har samtyckt till överföringen eller när överföringen är nödvändig för att

a) fullgöra ett avtal mellan den registrerade och den personansvarige,
b) på den registrerades begäran vidta åtgärder innan ett avtal träffas,
c) ingå eller fullgöra ett sådant avtal mellan den personansvarige och tredje man som är i den registrerades intresse,
d) rättsliga anspråk skall kunna fastställas, göras gällande eller försvaras, eller
e) skydda vitala intressen för den registrerade.

Det är också tillåtet att föra över personuppgifter för användning enbart i en stat som har anslutit sig till Europarådets konvention om skydd för enskilda vid automatisk databehandling av personuppgifter.

35 § Regeringen far för överföring av personuppgifter till vissa stater föreskriva undantag från förbudet i 33 §. Regeringen far också föreskriva att överföring av personuppgifter till tredje land är tillåten, om överföringen regleras av ett avtal som innehåller vissa bestämmelser till skydd för de registrerades rättigheter.

Regeringen eller den myndighet som regeringen bestämmer får vidare medge undantag från förbudet i 33 §, om det behövs med hänsyn till ett viktigt allmänt intresse eller om det finns tillräckliga garantier till skydd för de registrerades rättigheter.

Anmälan till tillsynsmyndigheten

Anmälningsskyldighet

36 § Behandling av personuppgifter som är helt eller delvis automatisk omfattas av anmälningsskyldighet. Den personansvarige skall innan en sådan behandling eller en serie av sådana behandlingar, som har samma eller liknande ändamål, genomförs göra en skriftlig anmälan till tillsynsmyndigheten.

Regeringen eller den myndighet som regeringen bestämmer tar föreskriva undantag från anmälningsskyldigheten för sådana typer av behandlingar som sannolikt inte kommer att leda till otillbörligt intrång i den personliga integriteten.

Anmälan behöver inte göras om det finns ett persondataombud

37 § När den personuppgiftsansvarige har offentliggjort en uppgift om att ett persondataombud utsetts och vem det är, behöver anmälan enligt 36 § inte göras.

Persondataombudets uppgifter

38 § Persondataombudet skall ha till uppgift att självständigt se till att den personuppgiftsansvarige behandlar personuppgifter på ett korrekt och lagligt sätt och påpeka eventuella brister för denne.

Har persondataombudet anledning att misstänka att den personuppgiftsansvarige bryter mot de bestämmelser som gäller för behandlingen av personuppgifter och vidtas inte rättelse så snart det kan ske efter påpekande, skall persondataombudet anmäla förhållandet till tillsynsmyndigheten.

Persondataombudet skall även i övrigt samråda med tillsynsmyndigheten vid tveksamhet om hur de bestämmelser som gäller för behandlingen av personuppgifter skall tillämpas.

39 § Persondataombudet skall föra en förteckning över de behandlingar som den personuppgiftsansvarige genomför och som skulle ha omfattats av anmälningsskyldighet om ombudet inte hade funnits. Förteckningen skall omfatta åtminstone de uppgifter som en anmälan enligt 36 § skulle ha innehållit.

40 § Persondataombudet skall hjälpa registrerade att fa rättelse när det finns anledning att misstänka att behandlade personuppgifter är felaktiga, missvisande eller ofullständiga.

Obligatorisk anmälan för särskilt integritetskänsliga behandlingar

41 § Regeringen far föreskriva att vissa behandlingar av personuppgifter som kan innebära särskilda risker för otillbörligt intrång i den personliga integriteten skall för förhandskontroll anmälas till tillsynsmyndigheten enligt 36 § tre veckor i förväg. Om regeringen har meddelat sådana föreskrifter, gäller inte undantaget från anmälningsskyldigheten enligt 37 §.

Upplysningar till allmänheten om behandlingar som inte anmälts

42 § Den persondataansvarige skall till var och en som begär det skyndsamt och på lämpligt sätt lämna upplysningar om sådana automatiska eller andra behandlingar av personuppgifter som inte har anmälts till tillsynsmyndigheten. Upplysningarna skall omfatta det som en anmälan enligt 36 § skulle ha omfattat. Den persondataansvarige är dock inte skyldig att lämna ut uppgifter om vilka säkerhetsåtgärder som har vidtagits.

Skadestånd

43 § Den persondataansvarige skall ersätta den registrerade för den skada som en behandling av personuppgifter i strid med denna lag eller föreskrifter som har meddelats med stöd av lagen har fört med sig. Ersättning skall också betalas för ren förmögenhetsskada och för den kränkning av den personliga integriteten som behandlingen har inneburit.

Ersättningsskyldigheten enligt första stycket kan i den utsträckning det är skäligt sättas ned eller helt falla bort, om den persondataansvarige visar att felet inte berodde på honom eller henne.

Straff för osanna uppgifter

44 § Till böter eller fängelse högst sex månader eller, om brottet är grovt, till fängelse i högst två år döms den som uppsåtligen eller av oaktsamhet lämnar osann uppgift

a) i information till registrerade som föreskrivs i denna lag,
b) i anmälan till tillsynsmyndigheten enligt 36 §, eller
c) till tillsynsmyndigheten när myndigheten begär information enligt 45 §.

Tillsynsmyndighetens befogenheter

45 § Tillsynsmyndigheten har rätt att för sin tillsyn på begäran fa

a) tillgång till de personuppgifter som behandlas,
b) upplysningar och dokumentation rörande behandlingen av personuppgifter och säkerheten vid denna, och
c) tillträde till sådana lokaler som har anknytning till behandlingen av personuppgifter.

46 § Om tillsynsmyndigheten inte efter begäran enligt 45 § kan fa tillräckligt underlag för att konstatera att behandlingen av personuppgifter är laglig, får myndigheten vid vite förbjuda den persondataansvarige att behandla personuppgifter på annat sätt än genom att lagra dem.

47 § Om tillsynsmyndigheten konstaterar att personuppgifter behandlas eller kan komma att behandlas på ett olagligt sätt, skall myndigheten genom påpekanden eller liknande förfaranden försöka åstadkomma rättelse. Går det inte att få rättelse på annat sätt eller är det riskfyllt att vänta, får myndigheten vid vite förbjuda den persondataansvarige att fortsätta att behandla personuppgifterna på annat sätt än genom att lagra dem.

Om den persondataansvarige inte frivilligt följer ett beslut om skyddsåtgärder enligt 32 §, som vunnit laga kraft, får tillsynsmyndigheten föreskriva vite för att beslutet skall genomföras.

48 § Innan tillsynsmyndigheten beslutar om vite enligt 46 eller 47 §, skall den persondataansvarige ha fatt tillfälle att yttra sig. Om det är riskfyllt att vänta, får myndigheten dock i avvaktan på yttrandet meddela ett tillfälligt beslut om vite. Det tillfälliga beslutet skall prövas om, när yttrandetiden har gått ut.

Ett vitesföreläggande skall delges den persondataansvarige. Delgivning enligt 12 § delgivningslagen (1970:428) får dock användas bara om det finns skäl att anta att den persondataansvarige har avvikit eller håller sig undan på något annat sätt.

49 § Tillsynsmyndigheten får hos länsrätten i det län där myndigheten är belägen ansöka om att sådana personuppgifter som har behandlats på ett olagligt sätt skall utplånas.

Beslut om utplånande får inte meddelas om det är oskäligt.

Överklagande

50 § Tillsynsmyndighetens beslut enligt denna lag om annat än generella föreskrifter får överklagas hos allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Tillsynsmyndigheten får bestämma att dess beslut skall gälla även om det överklagas.

Närmare föreskrifter

51 § Regeringen eller den myndighet som regeringen bestämmer får meddela närmare föreskrifter om

a) i vilka fall behandling av personuppgifter är tillåten,
b) vilka krav som ställs på den persondataansvarige vid behandling av personuppgifter,
c) i vilka fall användning av personnummer är tillåten,
d) innehållet i en anmälan eller ansökan till en persondataansvarig,
e) vilken information som skall lämnas till registrerade och hur lämnandet av information skall gå till, och
f) anmälan till tillsynsmyndigheten och förfarandet när anmälda uppgifter har ändrats.

Övergångsbestämmelser

1. Denna lag träder i kraft den 1 januari 1999, då datalagen (1973:289) skall upphöra att gälla. Den äldre lagen gäller dock fortfarande i fråga om överklagande av beslut som har meddelats före den 1 januari 1999.
2. Beträffande sådan behandling av personuppgifter som pågår vid ikraftträdandet skall till utgången av september månad 2001 den äldre lagen tillämpas i stället för den nya. Detta gäller även bestämmelserna i den äldre lagen om överklagande.
3. Bestämmelserna i 9, 10, 13 och 21 §§ i den nya lagen skall inte börja tillämpas förrän den 1 oktober 2007 beträffande sådan manuell behandling av personuppgifter som pågår vid ikraftträdandet.
4. Beträffande personuppgifter som vid ikraftträdandet lagras för historisk forskning skall bestämmelserna i 9, 10, 13 och 21 §§ i den nya lagen börja tillämpas först när uppgifterna behandlas på något annat sätt. Dessförinnan skall motsvarande bestämmelser i den äldre lagen tillämpas. De angivna bestämmelserna i den nya lagen skall dock inte till följd av vad som nu sagts börja tillämpas tidigare än vad som följer av punkt 2 eller 3 ovan.
5. Anmälan enligt 36 § i den nya lagen får göras före ikraftträdandet.
6. Ett samtycke som har lämnats före ikraftträdandet skall gälla även efter ikraftträdandet om samtycket uppfyller kraven i den nya lagen.
7. Har en begäran om registerutdrag enligt 10 § i den äldre lagen kommit in före ikraftträdandet men har utdraget inte expedierats före ikraftträ-

dandet skall framställningen anses som en ansökan enligt 26 § i den nya lagen.

8. Den nya lagens bestämmelser om skadestånd skall bara tillämpas om den omständighet som yrkandet hänför sig till har inträffat efter ikraftträdandet. I annat fall tillämpas de äldre bestämmelserna.

OPINION NU

September 1996

Borgerne er langt mere trygge ved at give CPR-nummer til offentlige myndigheder end til private virksomheder

Men kun meget få har været ude for, at personlige oplysninger er blevet brugt til andet formål

Blev vi spurgt, ville kun de færreste give tilladelse til, at en virksomhed gav købsoplysninger videre til andre

Næsten tre ud af fire danskere (74%) ville altid eller som oftest være trygge ved at oplyse CPR-nummer til offentlige myndigheder, mens det kun drejer sig om fire ud af ti (39%), når det gælder private virksomheder.

Kun 8% mener, at oplysninger givet til en privat virksomhed er blevet brugt til andet "irriterende" end det oprindelige formål. Når det gælder offentlige myndigheder har 3% denne oplevelse.

Otte ud af ti danskere (81%) ville *ikke* give en privat virksomhed tilladelse til at videregive købsoplysninger, hvis de blev spurgt. Og rabatter eller gaver giver ikke mere sympati for tanken.

Det viser en undersøgelse gennemført af Aim Nielsen i august måned baseret på telefoninterviews med en repræsentativ stikprøve med ca 1.000 danskere på 13 år og derover.

Aim Nielsen

Kun få er utrygge ved at give CPR-nummer til offentlige myndigheder - mange flere, hvis det er en privat virksomhed

Registrering af oplysninger om borgere er i disse måneder et emne, der er højt på dagsordenen hos både medierne og forbrugerne. På den ene side er det offentlige kontorers behov for udveksling af oplysninger med andre myndigheder, og på den anden side private virksomheder, der i stigende grad tager direkte markedsføring med på kommunikationsplanen. Målrettede henvendelser baseret på kundeoplysninger.

Til belysning af borgernes mening om disse emner har Aim Nielsen stillet følgende spørgsmål til et repræsentativt udsnit af den voksne danske befolkning (13 år og derover):

"Man bliver i dag i mange situationer bedt om at oplyse sit CPR-nummer til såvel det offentlige som til private virksomheder. Hvor tryg eller utryg foler De Dem, når De oplyser Deres CPR-nummer til henholdsvis private virksomheder og offentlige myndigheder?"

	Private virksomheder	**Offentlige virksomheder**
Helt utryg ved det	17%	6%
Som oftest utryg ved det	19%	8%
Nogle gange tryg - andre gange utryg ved det	16%	9%
Som oftest tryg ved det	18%	26%
Helt tryg ved det	21%	48%
Ved ikke	9%	3%
Antal interviews	1015	1015

Tabellen viser, at der næsten er lige mange, der er utrygge henholdsvis trygge ved at oplyse CPR-nummer til en privat virksomhed, nemlig 36% og 39%. Og hver sjette, nemlig 17%, er endda *"helt utryg"* v *eu* det. Det drejer sig om ca. 30.000 mennesker.

Derimod er der klart mere tryghed over for offentlige myndigheder. Hele 74% er altid eller som oftest trygge, og kun 14% utrygge. Betegnelsen "kun" er måske ikke helt velvalgt. Det drejer sig om ca. **250.000 borgere,** der er helt utrygge ved at give CPR-nummer til offentlige myndigheder.

Undersøgelsen viser i øvrigt klart stigende utryghed med alderen, når det gælder CPR-numre og private virksomheder. Kun 6% af de 13-24 årige er helt utrygge, mens det gælder 24% af de på 55 år og derover.

Signifikant færre kvinder end mænd er *helt* trygge ved at give CPR-numre. Det gælder både private virksomheder og offentlige myndigheder. Kun 15% kvinder er helt trygge ved et at give CPR-nummer til en virksomhed mod næsten dobbelt så mange, nemlig 27% af mændene. Når det gælder en offentlig virksomhed er 42% af kvinderne helt trygge mod 56% af mændene.

Aim Nielsen

Mere end ni ud af ti oplever ikke "misbrug" af oplysninger

En del af diskussionen om registrering af borgerne går på, at oplysninger "misbruges", d.v.s. bruges til andet formål end det oprindelige. For at belyse udbredelsen af *oplevet* "misbrug", stillede Aim Nielsen følgende spørgsmål:

"Har De været ude for, at oplysninger, De har givet om Dem selv, er blevet brugt til noget andet end det oprindelige formål. Enten noget godt eller noget irriterende ?"

	Private virksomheder	Offentlige virksomheder
Ja, noget andet godt	1%	
Ja, noget andet irriterende	8%	3%
Nej, ikke brugt til noget andet	90%	96%
Ved ikke	2%	V%
Antal interviews	1015	1015

Langt flere oplever, at private virksomheder har brugt personlige oplysninger til noget andet "irriterende" end det oprindelige formål, nemlig 8% mod kun 3%, når det gælder offentlige myndigheder. Det er meget sjældent, at oplysningerne efter forbrugernes opfattelse er blevet brugt positivt, d.v.s. til noget andet "godt", nemlig 1%. I øvrigt er det bemærkelsesværdigt, at næsten alle har svaret "ja" eller "nej" på spørgsmålet, mens kun 1-2% siger "ved ikke". Meget få er altså usikre på, om oplysninger bruges til andet eller ej.

De mest markante forskelle mellem befolkningsgrupper er med hensyn til *private virksomheders* brug af oplysninger til noget "andet irriterende". Det er klart de "mest velstillede", der har denne oplevelse, nemlig de midterste aldersgrupper, funktionærer og de med de højeste husstandsindkomster:

*Har oplevet noget "andet irriterende" - **private virksomheder***

Alle	**8%**
Alder: 35-44 år	14%
Funktionærer	14%
Husstandsindkomst 500.000 kr.+	14%

Når det gælder *offentlige myndigheder,* er "misbrugs-tallene" relativt små for alle grupper, men enkelte skiller sig klart ud med større hyppighed. Tabellen viser en helt anden person-profil end for oplevet "misbrug" af private virksomheder: Det er mænd i hovedstadsområdet, pensionister og arbejdsløse.

*Har oplevet noget "andet irriterende" - **offentlige myndigheder***

Alle	**3%**
Mænd	5%
Hovedstadsområdet	5%
Ude af erhverv (pensionist o.a.)	5%
Arbejdsløs	7%

Aim Nielsen

80% vil ikke tillade, at oplysninger gives til anden virksomhed

Der er udbredt skepsis til at lade oplysninger om navn, adresse og køb af bestemte varer blive videregivet til andre virksomheder. Det fremgår af besvarelsen af dette spørgsmål:

"Jeg vil bede Dem forestille Dem, at en virksomhed har Deres navn og adresse samt oplysninger om Deres køb - f.eks. fordi De har købt en vare gennem et postordrefirma, eller fordi De har et medlemskort til en benzinstation, supermarked eller lignende. Hvis virksomheden ønskede at videregive disse oplysninger til en anden virksomhed, ville De så give tilladelse til dette?"

	Alle	Mænd	Kvinder
Ja, helt sikkert	5%	6%	4%
Ja, sandsynligvis	11%	12%	10%
Nej, sandsynligvis ikke	17%	18%	16%
Nej, helt sikkert ikke	64%	61%	66%
Ved ikke	4%	4%	4%
Antal interviews	1015	498	517

Undersøgelsen viser, at et stort flertal "helt sikkkert" ikke ville give en sådan tilladelse (64%), hvortil kommer 17%, der "sandsynligvis" ikke ville, d.v.s. i alt 81%. Kun 5% ville "ubetinget" give tilladelse til at give oplysninger videre, mens 11% er positivt indstillet, men forbeholdne. Strukturen i svarene findes både hos mænd og kvinder med kvinderne som de lidt mere forsigtige/ skeptiske.

De yngre er klart mest imødekommende over for spørgsmålet. Godt hver fjerde af de 13-24 årige ville "helt sikkert eller sandsynligvis" tillade at give oplysninger videre til en anden virksomhed (27%) mod 16% for hele befolkningen. Ikke overraskende er *de ældste (55 år og derover) mest negative.* Kun 10% ville give tilladelse, mens tre ud af fire (76%) helt bestemt *ikke* ville.

' 'ndersøgelsen viser også, at der *ikke* vindes mange sympatisører for at give oplysninger videre ved at tilbyde "en mindre rabat eller gave" som modydelse:

"Ville De give tilladelse til, at virksomheden videregav disse oplysninger til en anden virksomhed, hvis De fik en mindre rabat eller gave?"

	***Uden* mindre gave/rabat**	**Medmindre rabat/gave**
Ja, helt sikkert	5%	5%
Ja, sandsynligvis	11%	15%

En sådan modydelse får ikke flere personer til at være "sikre" på at give tilladelse, men får "ekstra" 4% til at sige, at de "sandsynligvis" vil give tilladelse til at videregive oplysninger. De, der kan vindes for ideen, findes helt klart oftest blandt de 13-24 årige og blandt lærlinge/elever/studerende.

A.C. Nielsen

Undersøgelsens gennemførelse

Landsdækkende repræsentativ stikprøve med 1.015 personer på 13 år og derover.

Dataindsamlingen har fundet sted med telefoniske interviews i perioden 22.-28. august 1996.

COPYRIGHT: Aim Nielsen A/S.
Gengivelse af resultaterne må kun finde sted med angivelse af Aim Nielsen som kilde.

OPINION NU ! fra Aim Nielsen A/S er resultater fra landsdækkende interviews med en simpel, tilfældig stikprøve af telefonabonnenter på Aim Nielsens TeleBus*Plus. Interviewene er gennemført af interviewere fra Aim Nielsen ved hjælp af CATI-teknik (Computer Assisted Telephone Interviewing).

Udarbejdet for Aim Nielsen af: Cand.scient.soc. Ole E. Andersen,
tlf. 45 85 23 43.

02.09.96 OEA/pø

Aim Nielsen

Datacentralen a/s -ui~ POST

BILAG 1 5

Danskernes holdninger til informationsteknologi

Forkortet udgave

Instituttet for Fremtidsforskning
for
Post Danmark og Datacentralen

Januar 1996

Indholdsfortegnelse

Undersøgelsens baggrund og metodik . . . . . side 1
Danskernes tidssyn . . . . . side 1
Rapportens hovedkonklusioner . . . . . side 4
Holdninger til den informationsteknologiske udvikling . . . . . side 7
Holdninger til registrering . . . . . side 13
Holdninger til reklamer, direct mail og registrering . . . . . side 21

Undersøgelsens baggrund og metodik

Danmark er et af de lande, som har mest informationsteknologi på arbejdspladserne. Næst efter USA har vi flest computere i hjemmet. Men hvad mener danskerne egentlig om den nye teknologi, som i de sidste år allerede har forandret deres arbejdsliv og fritidsliv på mange måder? Hvad tænker de om de mange nye mulige anvendelser, som teknologien stadig udfordrer med?

Hvad mener danskerne egentlig om at blive registreret i offentlige registre, og hvad mener de om samkøring af disse registre?

Og hvad er danskernes holdning til reklamer og direct mail? Vil danskerne aflevere personlige oplysninger, så de kun får reklamer og direct mail om de emner, der interesserer dem?

For Post Danmark og Datacentralen har Instituttet for Fremtidsforskning foretaget denne undersøgelse, der belyser disse forhold.

Rapporten er gennemført som en holdningsundersøgelse, der består af såvel en kvantitativ som en kvalitativ del. Den kvantitative omfatter 1500 interviews og den kvalitative fire gruppeinterviews

Danskernes tidssyn

Indgangsvinklen for undersøgelsen var antagelsen af, at danskerne har forskellige *tidssyn*, d.v.s. forskellige syn på udvikling og ændringer, og dermed også på nye tiltag i samfundet og på nye produkter. Også denne hypotese blev bekræftet af såvel den kvantitative undersøgelse som af de kvalitative interviews.

Ud fra denne indfaldsvinkel har Instituttet for Fremtidsforskning inddelt befolkningen i tre grupper:

- De fremtidsorienterede
- De nutidsorienterede
- De fortidsorienterede

Tidssynet fungerer som en usynlig kontaktlinse, som vi fortolker vores tilværelse igennem, men som vi ikke selv kan se. Vi ved bare, hvordan tilværelsen og fremtiden skal være, for at vi kan have et godt liv. Det tidssyn, vi selv har, sætter vi ikke mange ord på, mens de anderledes tidssyn opfattes som forkert, bagstræberisk, uigennemtænkt, overfladisk - betegnelserne er mange.

Når informationer om nye tiltag inden for informationsteknologien udformes af mennesker med eet tidssyn, men modtages af personer med et modsatrettet tidssyn, opstår der en forståelseskløft, som gør, at debatten risikerer at køre i skyttegravsstillinger. Man forstår sjældent hinanden.

De tre tidssyns-grupper er defineret således:

De fremtidsorienterede

Denne gruppe tror på, at fremtiden bliver bedre end nutiden. Tingene vil udvikle sig i den rigtige retning. De ser muligheder i "det nye" og mener, at man ved at bære sig fornuftigt ad kan begrænse eller helt undgå problemerne ved forandring.

De fortidsorienterede

Denne gruppe synes, at forandringerne i samfundet går for hurtigt med tab af grundlæggende værdier til følge. Tabet af "det gamle" kompenseres ikke af gevinsten ved "det nye". De er meget opmærksomme på farer og trusler ved det nye og føler ofte, at det udkonkurrerer afprøvede og mere "fornuftige" måder at gøre tingene på.

De nutidsorienterede

Denne gruppe ser ingen grund til at interessere sig for hypotetiske forandringer, før de er indtruffet. De er ikke overbeviste om, at tingene nødvendigvis vil forandre sig ret meget og føler i hvert fald ikke, at de selv vil kunne få den store indflydelse. De forholder sig nødigt til "det nye", før de har mulighed for at "afprøve" det eller "tænke det ind" i deres hverdag.

Lige store grupper

De tre tidssyns-grupper er omtrent lige store. Desuden er der en stor restgruppe, der ikke kan rubriceres.

Inddelingen af danskerne i tidssyn er et redskab, der kan skabe et overblik over og give et indblik i holdninger til forandring, holdninger til "det nye" - det kunne være informationsteknologi, Storebæltsbroen eller EU, men det kunne også være et nyt produkt.

Informationsteknologien ændrer sig i et stadigt hastigere tempo. Og dens konsekvenser føles mere og mere i såvel samfundet, som i arbejdslivet og i fritiden. Vi håber, at undersøgelsens resultater vil blive brugt som baggrund til bedre at kunne informere og debattere de mange aspekter, som har konsekvenser for os alle.

Spørgeskemaundersøgelserne er foretaget i september-oktober 1995, og rapporten er færdiggjort i januar 1996.

Februar 1996

Instituttet for Fremtidsforskning.

Rapportens hovedkonklusioner

Holdninger til informationsteknologi

Danskerne har virkelig taget informationsteknologien til sig og er ikke, delt op i to informationsteknologiske lejre: en venlig og en fjendtlig.

Samtidig med. at udviklingen betragtes som spændende og naturlig, er der en vis bekymring og et onske om mere styring.

Mulighederne i den nye teknologi relateres gerne til ens egen konkrete tilværelse, mens bekymringerne relateres til et mere generelt, samfundsmæssigt niveau ude i fremtiden.

Denne tendens, at det kendte og konkrete generelt afføder en positiv respons og det ukendte og abstrakte generelt en negativ respons, går som en rød tråd igennem hele undersøgelsen.

Udviklingen anses for så naturlig, at den slet ikke kan diskuteres. Ønsket om mere styring er helt abstrakt. Få har gjort sig tanker om hvem, der skal styre, eller hvad, der skal styres. Ønsket kan mere ses som et udtryk for usikkerhed over for det ukendte.

Et mindretal af danskerne mener, at de måske vil blive gjort overflødige af den informationsteknologiske udvikling - undtagen den yngste aldersgruppe, hvor flertallet mener dette. I næsten alle spørgsmål om informationsteknologien skiller den yngste gruppe sig ud med mere negative forventninger og mindre positive holdninger.

Danskerne har allerede oplevet, hvordan informationsteknologien har ændret deres arbejdsliv og deres tilværelse, og det opleves af de allerfleste som positivt.

Holdninger til registrering

Det er vanskeligt at generalisere om danskernes holdning til registrering. For som med så mange andre ting, findes der ikke én men mange forskellige holdninger. Desuden er holdningerne hos den enkelte - såvel som hos "det statistiske flertal" - i nogen grad præget af modsætninger og paradokser.

Der er imidlertid nogle træk, som går igen hos de fleste: På det overordnede og abstrakte plan opfattes registrering som noget ubehageligt, der kan krænke privatlivets fred. Men så snart registrering bliver et middel til at opfylde nogle konkrete formål stiger tilslutningen. Det store flertal mener således, at man skal kunne samkøre registre for at bekæmpe socialt bedrageri.

Samtidig med bekymringen for registrering som abstrakt begreb og som fremtidstendens, er flertallet af danskerne ikke bekymrede for registrering på det konkrete plan og som nutidsfænomen. Der er dog et stort mindretal, som udtrykker bekymring.

Generelt mener danskerne ikke, at det offentlige skal have flere oplysninger. Men der skal være bedre mulighed for at udnytte dem, man har, bl.a. gennem samkøring af registre. Igen er der et ston mindretal, som ser afslappet på at afgive flere oplysninger, og omvendt er der en lille gruppe, der er helt imod samkøring.

Forskellige holdninger til registrering udmønter sig først og fremmest i, hvordan folk bedømmer forholdet mellem den opfattede ulempe ved registrering og de mål, som registrering er et middel til at opnå.

Personer med et fremtidsorienteret tidssyn er meget bevidste om fordelene og mener, at ulemper og farer kan minimeres ved klart at definere formålet og grænserne for registrering. Ved at registrere "fornuftigt" kan man undgå de negative konsekvenser.

Personer med et fortidsorienteret tidssyn er sig nok fordelene bevidst, men lægger vægt på ulemperne. De mener ikke, at det vil være muligt at sætte effektive grænser, der forhindrer overdreven registrering.

Personer med et nutidsorienteret tidssyn interesserer sig ikke videre for teoretiske og abstrakte diskussioner, men er meget påvirkelige for argumenter fra de to øvrige grupper og bliver let skræmte over nye tiltag.

På det overordnede, abstrakte plan er der stor forskel på holdningerne hos de respektive tidssyn. Når det drejer sig om mere konkrete emner, f.eks. samkøring af registre, snævrer forskellene ind.

Der er en ret klar kønsforskel i holdningen til registrering: Kvinder er konsekvent mere skeptiske end mænd. Dette gælder i alle aldersgrupper. Til gengæld er der ikke noget mønster i, hvordan forskellige aldersgrupper ser på registrering; det varierer fra spørgsmål til spørgsmål, hvilke grupper der "scorer" højest, hhv. lavest.

Holdninger til reklamer, direct mail og registrering

Når det gælder reklamer, har danskerne flere forskellige holdninger samtidigt og med rimeligt vandtætte skodder imellem. Det mere generelle abstrakte begreb "reklamer" giver tydelige associationer til noget negativt, specielt ressourcespild. Men samtidig går man med tydeligt velbehag i gang med at tale om de fordele, man på det konkrete personlige plan får ud af specifikke reklamer. Reklamer bliver ikke smidt ulæste ud, så snart de ryger ind ad brevsprækken.

Der er bred enighed om, at reklamemængden er for stor - altså den, man ikke selv har brug for. De negative aspekter ved reklamerne opfattes ens af både kvinder og mænd. Når det derimod drejer sig om de positive aspekter, adskiller kvinderne sig noget fra mændene.

Flere kvinder end mænd læser reklamebladene. De bruger dem dels som information om tilbud, men en vigtig funktion er det hyggelige. At sidde med reklamebladene en søndag eftermiddag med en kop kaffe.

Mændene indrømmer kun nødtvungent, at de kigger i reklameblade - men de gør det!

Det nuværende direct mail system afføder en kraftig, negativ respons hos et flertal. Man finder det stødende, at det personlige aspekt er falsk.

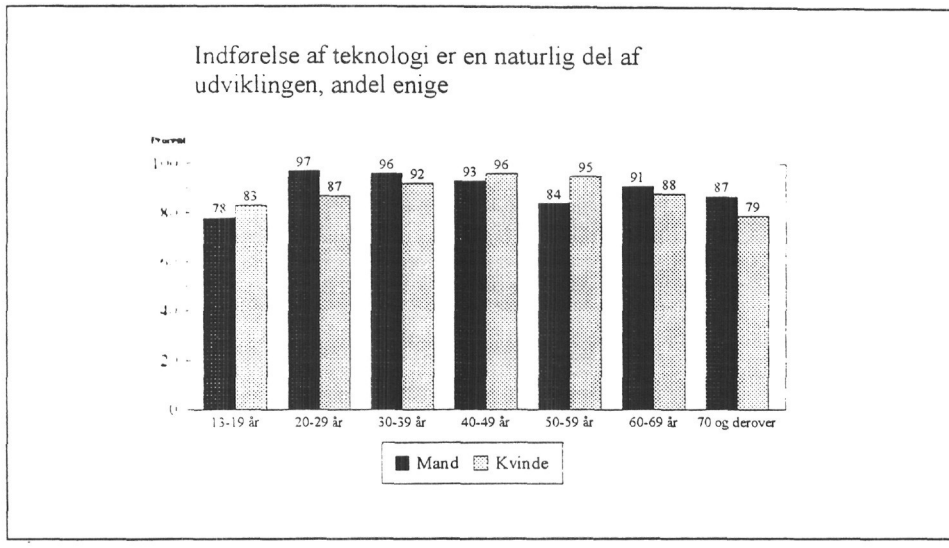
Interessen for at kunne vælge at være med i en interessedatabase, hvor man kunne få selektive reklamer inden for sine egne interesseområder er tydeligvis stor. Aspektet, at man selv kan vælge - individualismen - spiller en stor rolle.

Bekymringen for at blive registreret i en database overskygges helt tydeligt af fordelen ved at være med i en interessedatabase. Et klart eksempel på, hvorledes den abstrakte ængstelse forsvinder, når det drejer sig om ens konkrete interesser.

Holdninger til den informationsteknologiske udvikling

Der er generel enighed om (90%), at den informationsteknologiske udvikling er spændende. Denne enighed går stort set på tværs af aldersgrupper, køn og tidssynsgrupper.

90% mener også, at der er tale om en naturlig udvikling, men der er forskel på meningerne efter alder og køn.



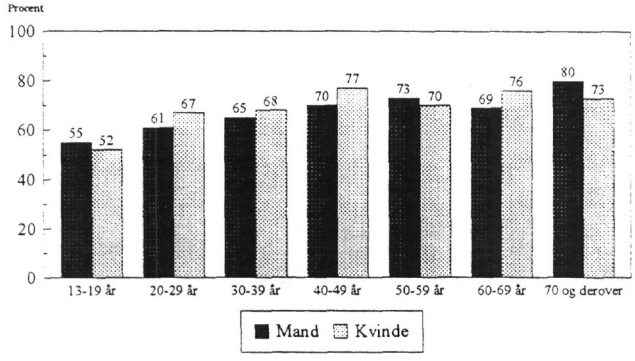
Den gruppe, der **mindst** er enige, er de unge under 20, her er det 22% af drengene og 17% af pigerne, som ikke er enige i udsagnet. Først derefter kommer de over 70 årige. Man kan undre sig over. hvad årsagen til de unges holding er, men måske er der en sammenhæng imellem denne holdning og deres udprægede frygt for, at teknologien vil overflødiggøre dem.

Bør der være mere styring?

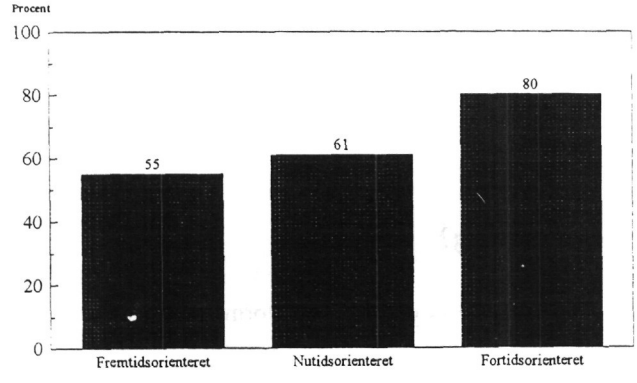
På spørgsmålet om der bør være mere styring af den informationsteknologiske udvikling, siger 69% ja. Aldersmæssigt er der stigende tilslutning til synspunktet dog således, at tilslutningen falder lidt hos de 50-59 årige for så at stige igen.

I den yngste aldersgruppe mener kun 53%, at der skal mere styring - måske p.g.a. den mindre autoritetstro, som er karakteristisk for gruppen.

Mere styring af den teknologiske udvikling,
andel enige



Mere styring af den teknologiske udvikling,
andel enige

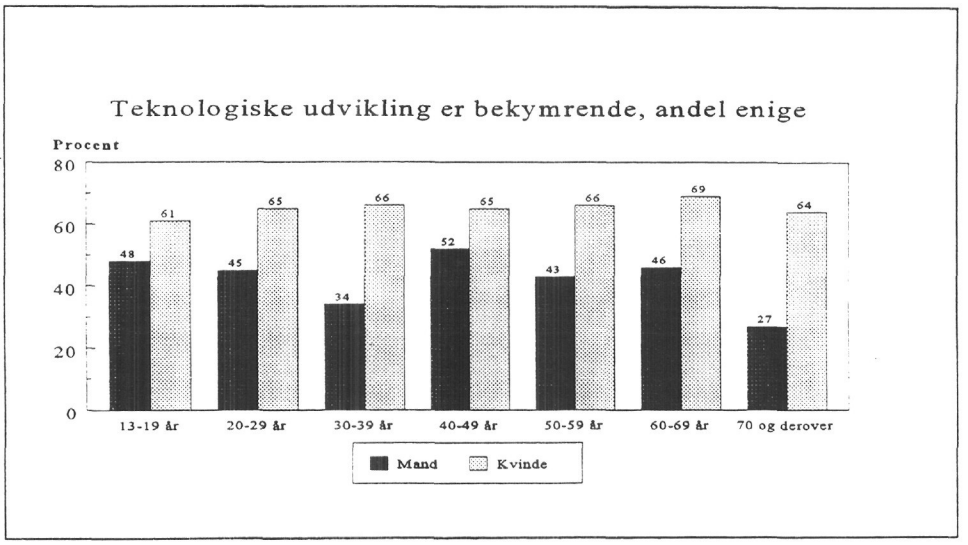


Med hensyn til tidssyn er der stor forskel. Denne graf fremviser den næststørste forskel mellem grupperne af fremtidsorienterede og fortidsorienterede af samtlige grafer fordelt på tidssyn. Det kan tolkes i retning af, at området er meget kontroversielt.

De fire gruppeinterviews afslører imidlertid, at alle har meget vage forestillinger om, hvem der skal styre udviklingen og hvordan.

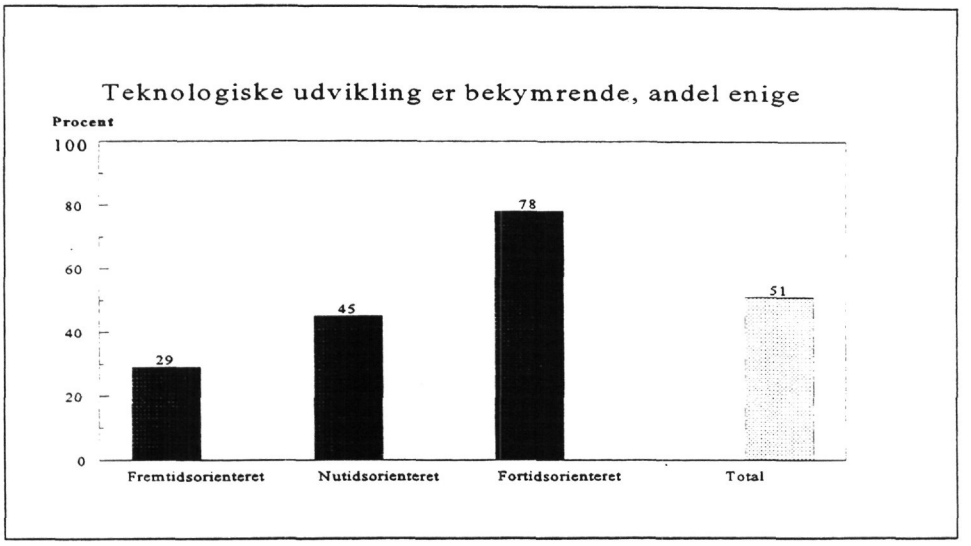
Teknologi og bekymring

Ca. halvdelen af danskerne mener, at den informationsteknologiske udvikling er bekymrende. Men dette gennemsnit dækker over store forskelle. Først og fremmest på køn, og kvinderne bekymrer sig langt mere end mændene. Det gælder dog ikke alene i relation til den informationsteknologiske udvikling. Kvinder bekymrer sig generelt mere for fremtiden end mænd.



Kvinderne bekymrer sig mest om tab af kontakt og menneskelighed.

Mændene udviser derimod et meget mere varieret billede af hvem, der bekymrer sig. Det strækker sig fra 27% til 52 % i de forskellige aldersgrupper. De mindst bekymrede er mænd over 70. De mest bekymrede er mænd mellem 40 og 49 år, lige fulgt af de unge mænd mellem 13 og 19 år.



Tidssynene viser virkelig store forskelle. Dette udsagn giver simpelthen rekord i forskel, hvis man sammenligner grafer på tidssyn i rapporten. Mellem de fortidsorienterede og de fremtidsorienterede er der her en procentforskel på hele 49%. Området er med andre ord ekstremt kontroversielt, og det er da også dette emne, som i den offentlige debat afføder ren skyttegravskrig.

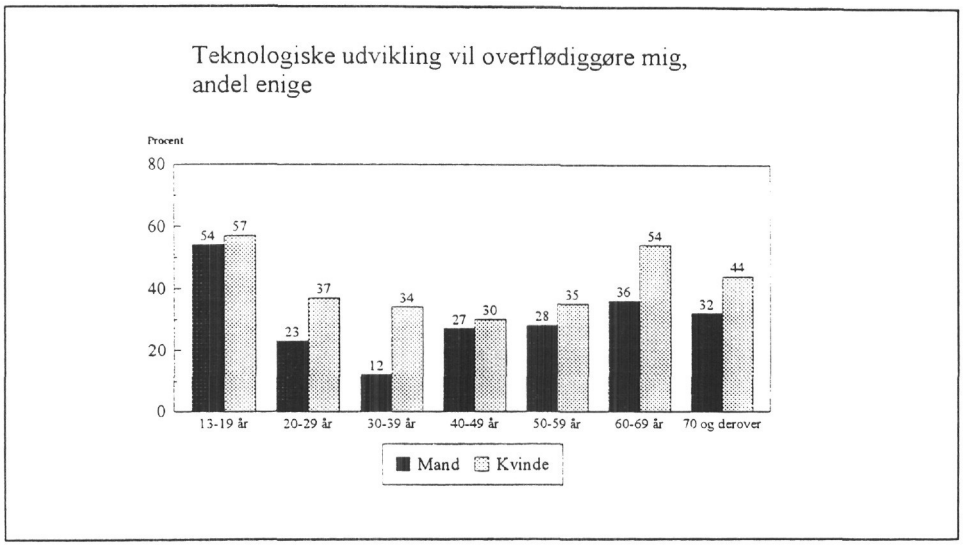
Hvad bekymrer ?

Det overordnede generelle tema i bekymringerne for den informationsteknologiske udvikling er "Big brother is watching you" syndromet samt registrering.

Det er imidlertid vigtigt at slå fast, at der samtidig med bekymringerne generelt er en positiv nysgerrighed over for de spændende muligheder. Disse muligheder refererer gerne til ens egen konkrete tilværelse, mens bekymringerne relateres til et mere generelt, samfundsmæssigt niveau.

Teknologien og arbejdsløshed

Gennemsnitligt mener 34%, at de måske vil blive gjort overflødige på grund af den teknologiske udvikling, men her er der meget store variationer:



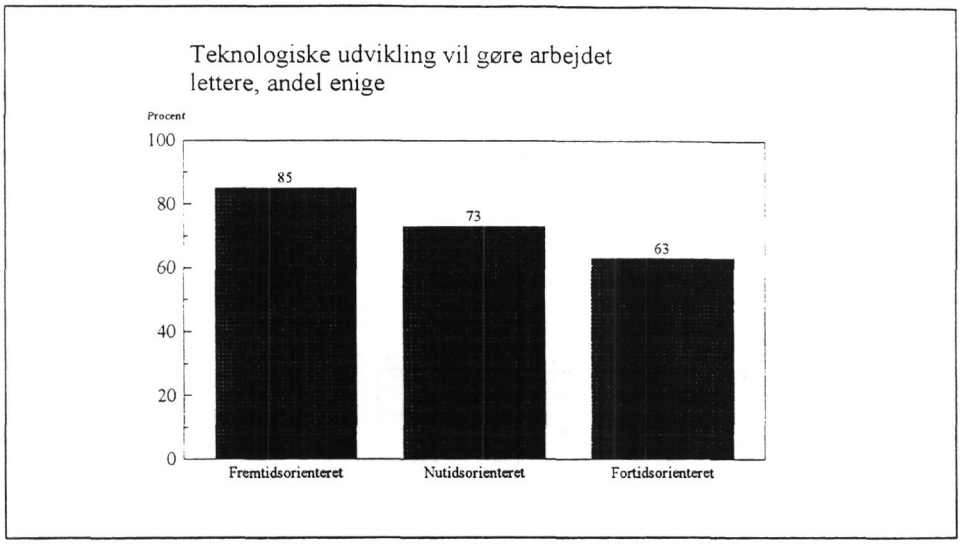
Det er et overraskende resultat, at 56% af den yngste aldersgruppe svarer ja til dette spørgsmål. Det er mere end 20% over gennemsnittet. Det må antages, at det kan få alvorlige konsekvenser for samfundets fremtid, at over halvdelen af de unge har disse forventninger, som slet ikke deles i samme omfang af deres forældre.

Det er også værd at bemærke, at de unges forventninger til fremtiden generelt ikke er negativ. Det er kun med hensyn til teknologiens konsekvenser for arbejdet, de bekymrer sig mere end andre aldersgrupper.

Arbejdet bliver lettere

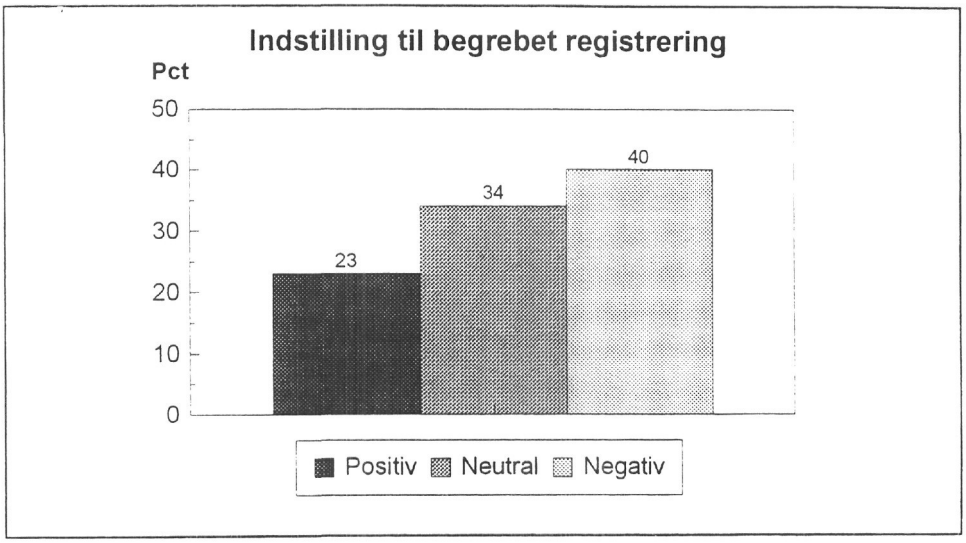
71 % er enige i dette udsagn. Men det dækker over, at 85% af gruppen med et fremtidsorienteret tidssyn og kun 63% af de med et fortidsorienteret tidssyn mener dette. Spændvidden mellem tidssynene er ikke så stor, som tilfældet er på spørgsmålene om bekymring og styring. Emnet er med andre ord ikke så kontroversielt.

Den kvalitative del af undersøgelsen viser, at mange allerede har oplevet, at den informationsteknologiske udvikling har givet lettelser i dagligdagen.



Danskernes holdning til registrering

Danskerne synes overvejende ikke om registrering. I hvert fald ikke, når man spørger dem direkte:



40% er altså negativt indstillet over for registrering, kun 23% er positive, mens 34% erklærer sig neutrale. Af den række af begreber og fænomener, som folk i undersøgelsen blev bedt om at forholde sig positivt, neutralt eller negativt til, er det kun direct mail, solarier og home-shopping, som folk er mere negative over for end registrering.

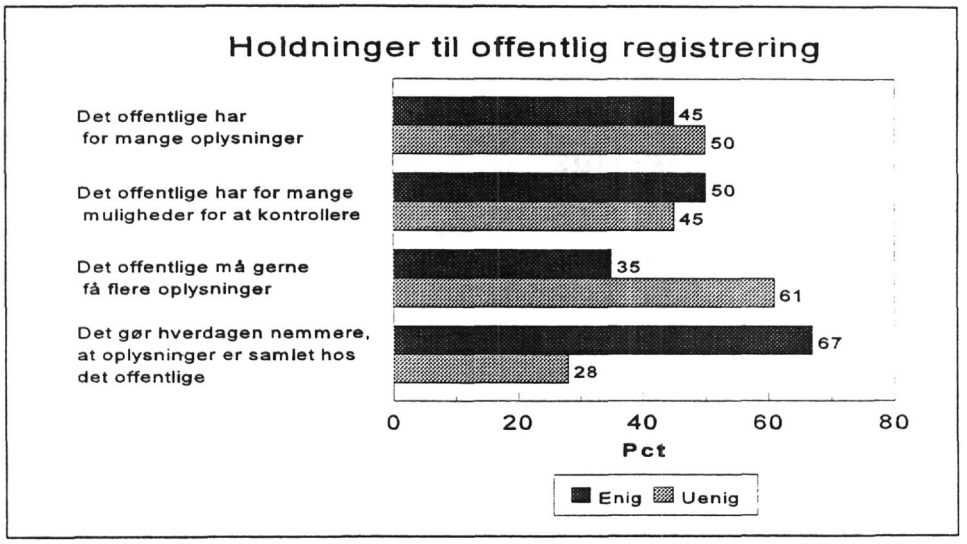
Ser man på mere konkrete begreber, der indeholder et **element** af registrering, ser det anderledes ud. Man er overvejende negativt indstillet over for borgerkortet (22% positive, 32% negative), som til gengæld er et forholdsvis ukendt begreb - det eksisterer jo heller ikke endnu. Men hele 66% er positive over for Dankortet.

Spørger man endelig om holdningen til databaser, er den helt overvejende positiv. 48% er positivt indstillet og - hvad der er exceptionelt - kun 13% er negative (hvor hele 22% er negativt indstillet over for Dankortet). Begrebet database har tilsyneladende en klart positiv klang, mens begrebet registrering er negativt ladet. Man kan mene, at dette er selvmodsigende; man kan jo ikke have en database, hvis man ikke har registreret nogen eller noget? Men undersøgelsen viser altså tydeligt, at begreberne ikke opfattes som synonymer.

At stemningen over for begrebet registrering er negativ kan måske forklares med, at registrering ikke har nogen værdi i sig selv. Det kan højst være et middel til at få opfyldt andre formål, som er noget værd for mennesker.

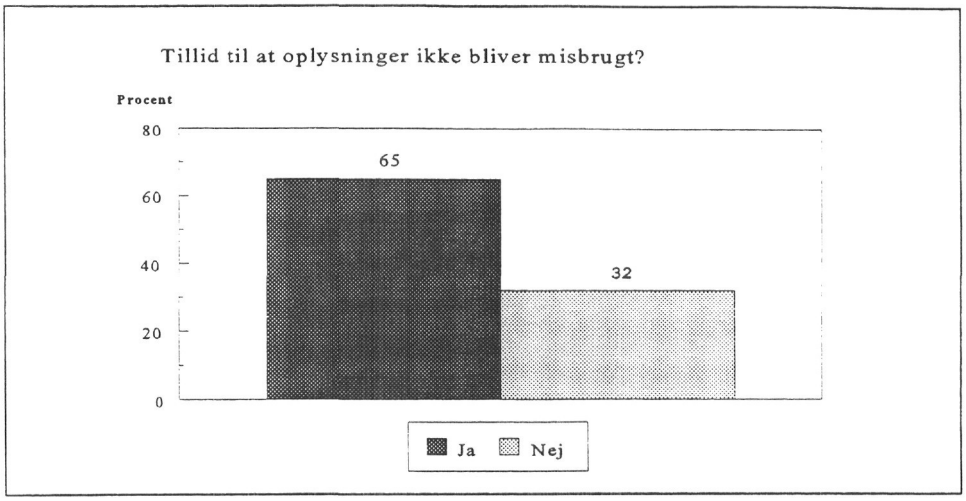
Holdninger til det offentliges registrering

I international sammenligning er danskerne gennemregistreret af myndighederne. Men det er et mindretal, der mener, at det offentlige har for *mange* oplysninger - selv om dette mindretal er ret stort, nemlig på 45% mod 50%, der ikke synes det.



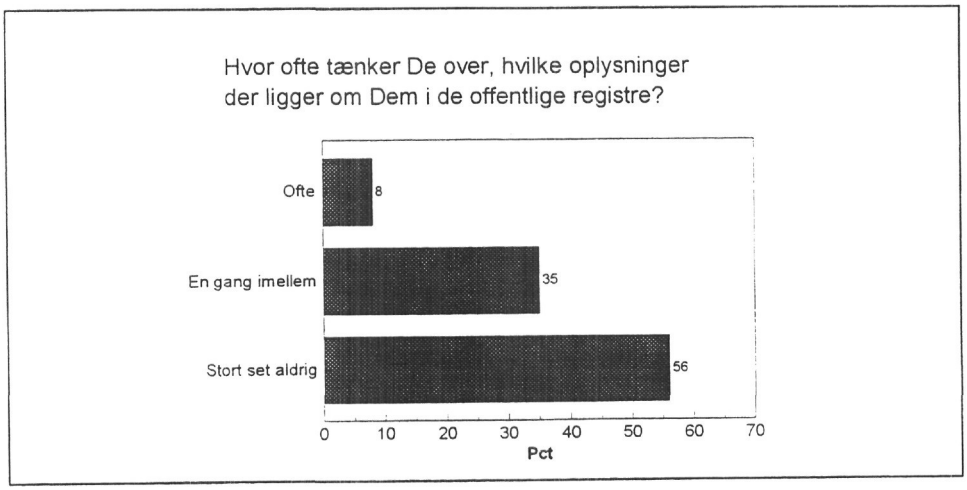
Spørger man, om det offentlige har for mange muligheder for at kontrollere danskerne, er fordelingen den omvendte: 50% er enige, 45% uenige. Men spørger man, om det offentlige gerne må få *flere* oplysninger, er der meget stor overvægt af uenige: 61% mod 35%. Til gengæld er der udbredt enighed om, at det gør hverdagen nemmere, at oplysningerne er samlet hos det offentlige. Det er 67% enige i, mens kun 28% er uenige. Det har altså praktiske fordele, at det offentlige har mange oplysninger, men der er ikke behov for, at det får flere.

Der er ikke den store frygt for, at det offentlige misbruger oplysninger:



65% har tillid til, at de oplysninger, som det offentlige har registreret om dem, ikke bliver misbrugt, og næsten lige så mange - 61% - føler sig tryg ved et system, hvor man kan få indblik i, hvilke oplysninger det offentlige har registreret om ens person (hvilket man faktisk kan i dag).

Dette afspejler sig også i, at de fleste stort set aldrig tænker over, hvilke oplysninger det offentlige har registreret om dem.

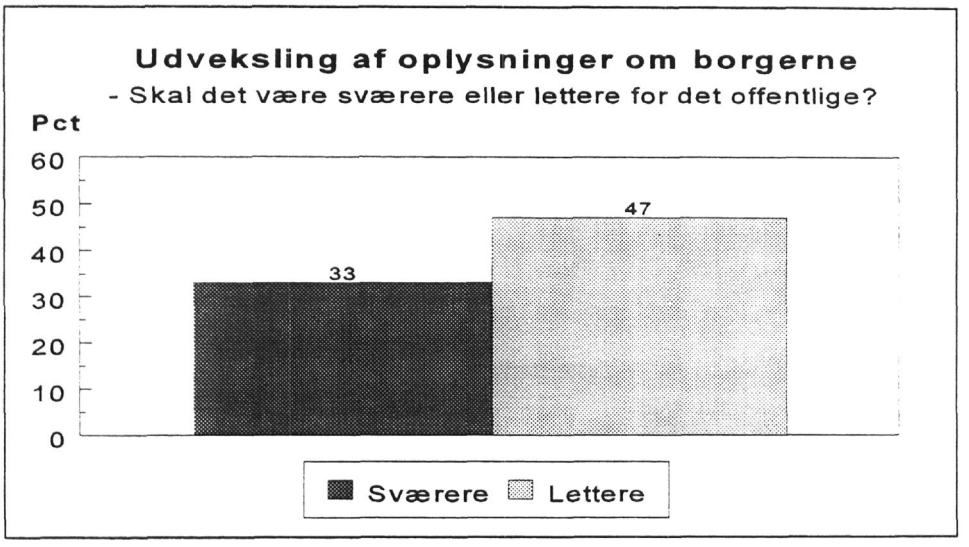


Trods den generelt negative reaktion over for begrebet registrering, er folks oplevelse af det offentliges registrering i dag altså ikke noget, der indeholder det 'helt store sprængstof.

Dette billede blev bekræftet i gruppesamtalerne. De fleste udtrykte bekymring for registrering som abstrakt begreb, men mente samtidig ikke, at der konkret - sådan som forholdene er i dag - er behov for bekymring.

Anvendelse af registre

Generelt mener de adspurgte, at det skal være muligt for de offentlige myndigheder at samkøre registre:



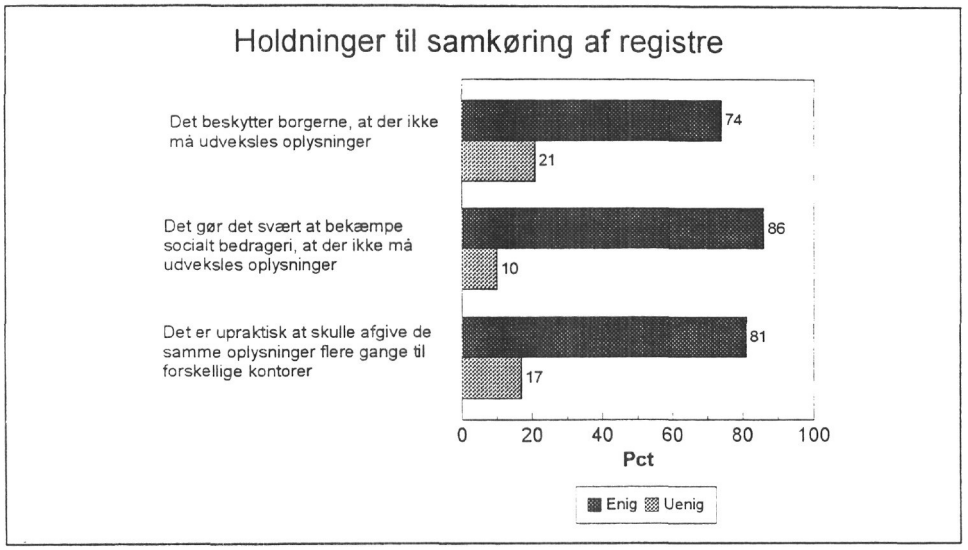
47% mener, at det skal gøres lettere for offentlige instanser at udveksle oplysninger om borgerne, og kun 33% at det skal gøres sværere. Her er der i øvrigt en ganske markant kønsforskel, idet kvinderne overvejende mener, at det skal gøres sværere - 38% mod 37%. Modsat er mændene meget klart for at gøre det lettere: Her er tallene 57% mod 28%. Denne kønsforskel i holdningerne til det offentliges registrering går igen i flere af spørgsmålene.

Danskerne angiver to væsentlige grunde til at give det offentlige bedre muligheder for at samkøre registre.

1. Det er praktisk, fordi borgerne kun behøver at afgive oplysninger til en enkelt offentlig instans, så vil alle andre instanser have adgang til de samme oplysninger, når det er nødvendigt for at betjene borgeren.

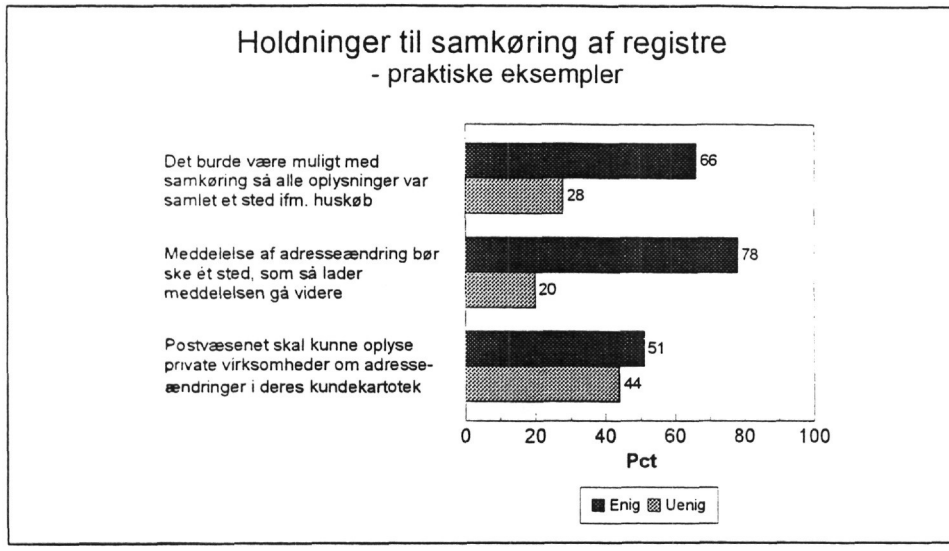
2. Det giver forbedrede muligheder for at afsløre diverse former for socialt bedrageri.

Over for disse samkøringsfordele står hensynet til borgernes sikkerhed for, at oplysningerne ikke bliver misbrugt. Og det er præcis, hvad folk svarer, når de bliver spurgt direkte:



74% er enige i, at det beskytter borgerne, at forskellige kommunale kontorer ikke må udveksle oplysninger. Det gør det på den anden side svært at bekæmpe socialt bedrageri, svarer hele 86%, og 81 % mener, at det er upraktisk at skulle afgive de samme oplysninger flere gange til forskellige kontorer.

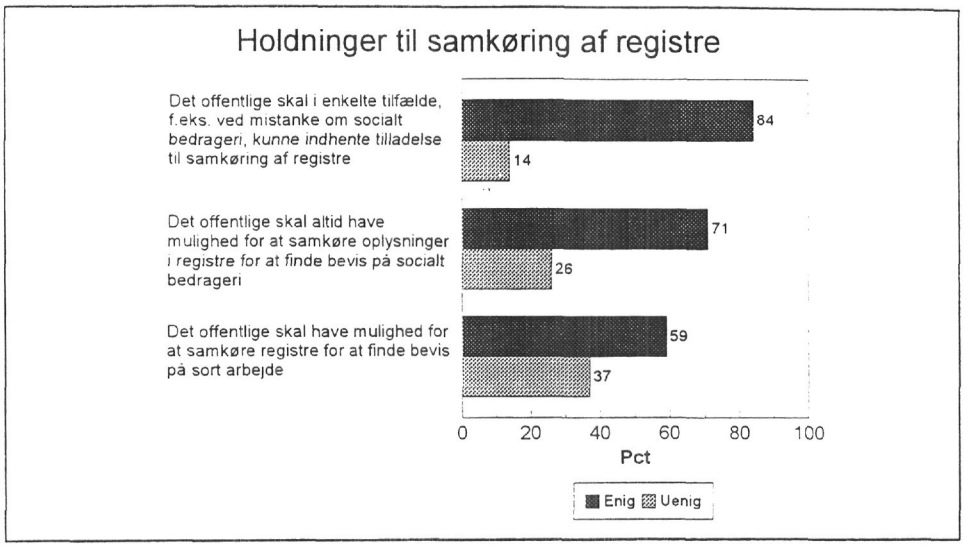
Hvordan er så afvejningen mellem fordele og ulemper ved samkøring af registre? De adspurgte er i undersøgelsen blevet bedt om at tage stilling til nogle konkrete eksempler:



Hvis vi tager de *praktisk orienterede* eksempler først, så er 66% enige i, at det ville være bedre, hvis man kunne samkøre registre i forbindelse med hushandler, så man undgår at skulle møde personligt frem hos flere forskellige myndigheder. Kun 28% er uenige i det. Endnu flere, nemlig 78%, er enige i, at det burde være muligt at kunne nøjes med at meddele adresseændring ét sted, som så kan lade meddelelsen gå videre.

Hvis man går et skridt længere og spørger om postvæsenet skal kunne oplyse private virksomheder om adresseændringer hos kunder, som disse har registreret, falder tilslutningen drastisk. 51 % er enige i, at dette er en god idé, mens 44% er uenige, men det er altså stadig en overvægt til fordel for en mindre restriktiv holdning til brug af registeroplysninger.

Når talen er om at samkøre registre med det formål at afsløre *socialt bedrageri,* er folk meget positive:



Det gælder især, når man spørger, om hvorvidt det offentlige "i enkelte tilfælde" ved mistanke om socialt bedrageri skal kunne indhente tilladelse til registersamkøring. Det er der 84%, der er enige i. Spørger man mere kategorisk, om det offentlige *altid* skal have mulighed for samkøring, er det stadig 71 %, der er enige i dette. Og selv når det konkretiseres til at dreje sig om sort arbejde (der ofte antages at nyde udbredt accept i befolkningen), mener et solidt flertal på 59%, at det offentlige skal have mulighed for registersamkøring.

Disse resultater underbygges af gruppesamtalerne. På den ene side blev der i alle grupperne på det generelle plan udtrykt bekymring for, hvad registrering kunne medføre af misbrug og krænkelser over for den enkelte borger - for nogles vedkommende resulterede det i meget kraftig afstandtagen. På den anden side var de fleste positivt stemt over for registrering og samkøring af registre i konkrete situationer.

Samlet kan det konstateres, at befolkningen overvejende er villig til at afgive noget af den beskyttelse, der ligger i en restriktiv registerlovgivning og -praksis for at opnå fordele i form af praktiske lettelser og en forbedret indsats over for socialt bedrageri.

Tidssyn og holdninger til registrering

Når man ser på kategorierne fortidsorienterede, nutidsorienterede og fremtidsorienterede, er holdningerne til registrering ensartet på grænsen til det kedelige.

Når det drejer sig om de overordnede, abstrakte og principielle spørgsmål, er uenigheden mellem de tre grupper stor, mens den er relativt lille på det konkrete plan.

På det mere specifikke plan, er personer med det fremtidsorienterede tidssyn mindst restriktive mht. samkøringsmuligheder og er herunder mest villig til at bruge dette til at fange sociale bedragere og sort arbejde. De tror på, at man kan adskille positive og negative konsekvenser og ved at bruge de nye muligheder fornuftigt, kan man undgå de negative konsekvenser.

Gruppen med det fortidsorienterede tidssyn delte generelt set ikke denne optimisme mht. mulighederne for at isolere de positive konsekvenser af udviklingen og undgå de negative, og efter at have nævnt det positive i at kunne bekæmpe socialt bedrageri spurgte gruppen: "Men hvor skal man stoppe?".

I gruppen med det nutidsorienterede tidssyn var der meget lidt debat af de overordnede, abstrakte problemstillinger. I stedet diskuterede man ud fra en række konkrete eksempler - ofte baseret på personlig erfaring.

Som ulemper ved registrering fremhævede alle grupperne risikoen for, at arbejdsgivere fik fat i følsomme oplysninger, f.eks. vedrørende sygdomme.

En anden ting, som ofte blev fremhævet som negativ, var risikoen for årelang registrering som dårlig betaler. Det anses f.eks. for uretfærdigt, at man stadig kan blive "mindet om" 5-10 år gamle forseelser i den henseende. Dummer man sig bør det tilgives efter en (ikke for lang) årrække, synes holdningen at være.

Desuden nævntes risikoen for registrering af politiske modstandere, uønsket manipulation med menneskets gener eller abort på grundlag af DNA-analyser.

Holdninger til reklamer, direct mail og privat registrering

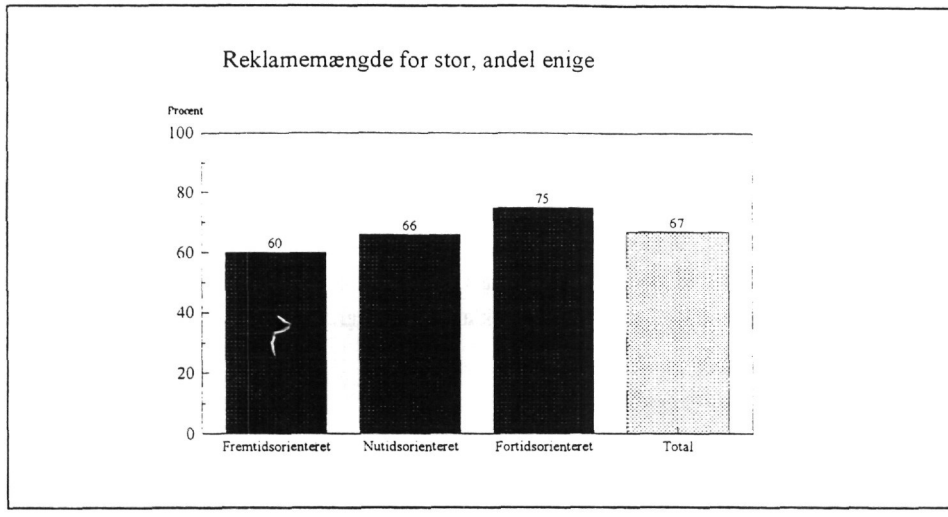
Danskernes holdning til reklamer er hverken rationelle eller konsistente.
De kvalitative interviews viste således på den ene side, at det generelle abstrakte begreb "reklamer" giver tydelige associationer til noget negativt, specielt ressourcespild, mens man samtidig gar hurtigt og med tydeligt velbehag i gang med at tale om de fordele, man på det konkrete personlige plan får ud af specifikke reklamer. Ens egne interesseområder er noget helt andet.

Negative aspekter ved reklamer

Der er bred enighed om, at reklamemængden er for stor - altså den, man ikke selv har brug for. I undersogelsen blev stillet to spørgsmål, som belyser dette på hver sin måde. Ud fra en mere abstrakt opfattelse: "Reklamemængden er for stor" og ud fra en mere konkret, personlig opfattelse: "Alt det papir irriterer mig". Der var flertal for begge synspunkter, men mere tilslutning til det abstrakte (70%) end det konkrete (60%), hvilket er helt i overensstemmelse med de tendenser, der kan iagttages i de generelle holdninger til registrering. Det ukendte og uvisse fremkalder stærkere reaktion end det kendte og identificerbare.

1 den kvalitative undersøgelse gav både mænd og kvinder udtryk for, at de var irriterede over mængden og dermed også over ressourcespildet.
Tilslutningen til, at reklamemængden er for stor stiger med alderen - undtagen for den ældste generation over 70 år. I gruppen mellem 60 og 69 er 80% enige i, at mængden er for stor, mens kun ca 50% af de 13-19 årige har den holdning.

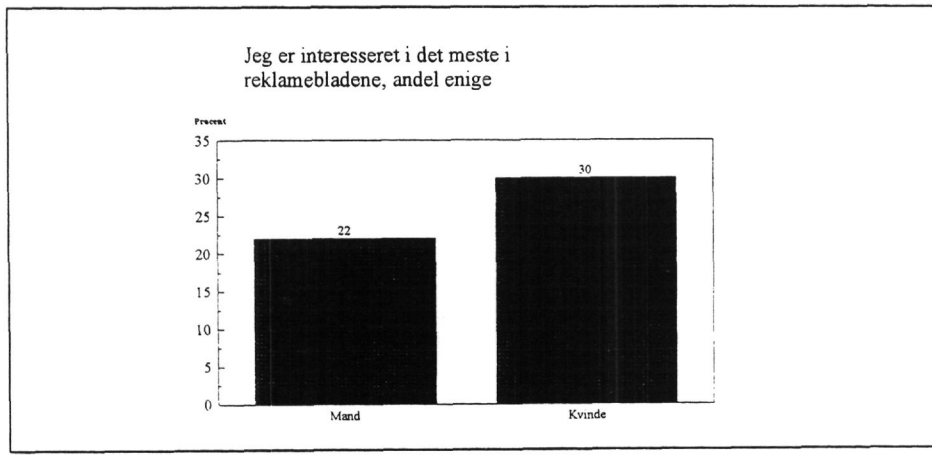
Ser vi på tidssyn, viser det klassiske mønster sig:



Positive aspekter ved reklamer

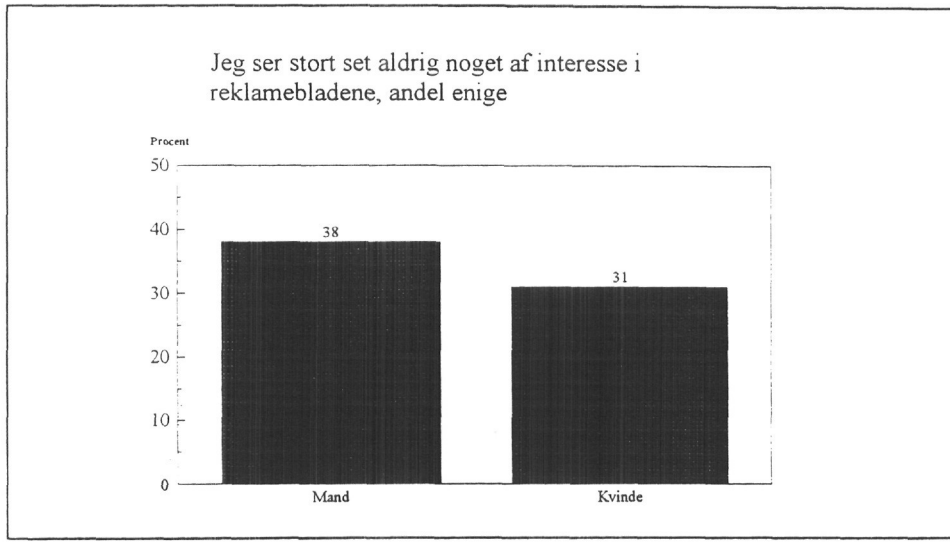
Ovenstående tal og holdninger kunne måske lede til den konklusion, at reklamer blev smidt ulæste ud, så snart de røg ind ad brevsprækken. Det er ikke tilfældet. I princippet er man imod de abstrakte, negative aspekter ved reklamer, men når det gælder det konkrete, ens egne interesser, så er man interesseret.

De negative aspekter ved reklamerne opfattes ens af både kvinder og mænd. Når det derimod drejer sig om de positive aspekter, adskiller kvinderne sig noget fra mændene.



En gængs hypotese er, at kvinder er mere interesserede i reklameblade end mænd. Den må siges at holde stik i undersøgelsen, også i den kvalitative del. Selvom kvinderne er lige så irriterede over reklamerne som mændene, så var de ikke bange for at "indrømme", at de faktisk læste dem.

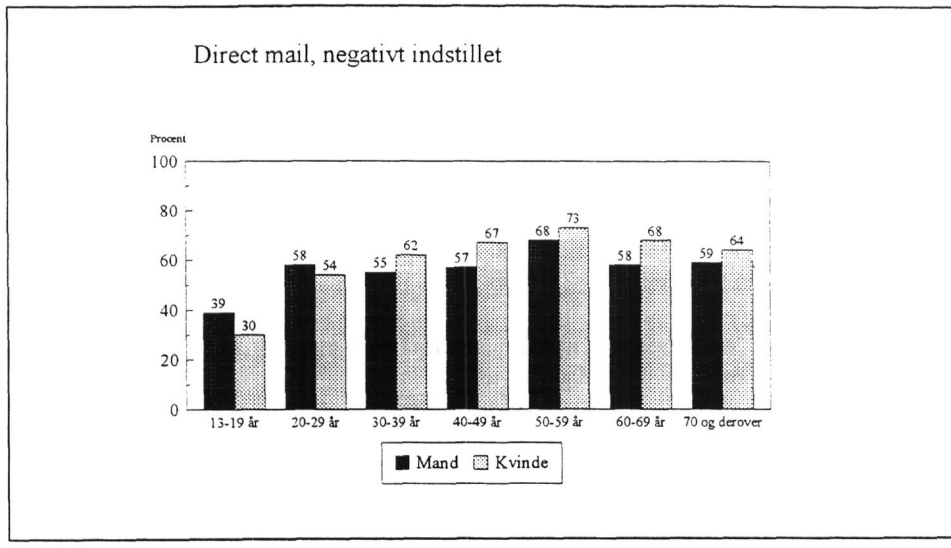
Mændene indrømmer kun nødtvungent, at de kigger i reklameblade - men de gør det!
Og som nedenstående graf viser, er der 62% af mændene, som er uenige i udsagnet "jeg ser stort set aldrig noget af interesse i reklameblade" og hele 69% af kvinderne.



Direct mail

Det nuværende, direct mail system afføder en negativ respons hos et flertal. I undersøgelsens generelle spørgsmål om man var positiv, neutral eller negativ indstillet over for forskellige produkter og begreber, er direct mail det fænomen, som afføder den største negative respons: 59% ! Kun 18% mener, at begrebet er positivt og andre 18%, at de er neutralt indstillede over for fænomenet.

Sådan fordeler de negative sig på alder og køn:



Interessedatabase

79 % af de adspurgte ville fravælge nogle af de reklametryksager, de får tilsendt i dag, hvis det var muligt.

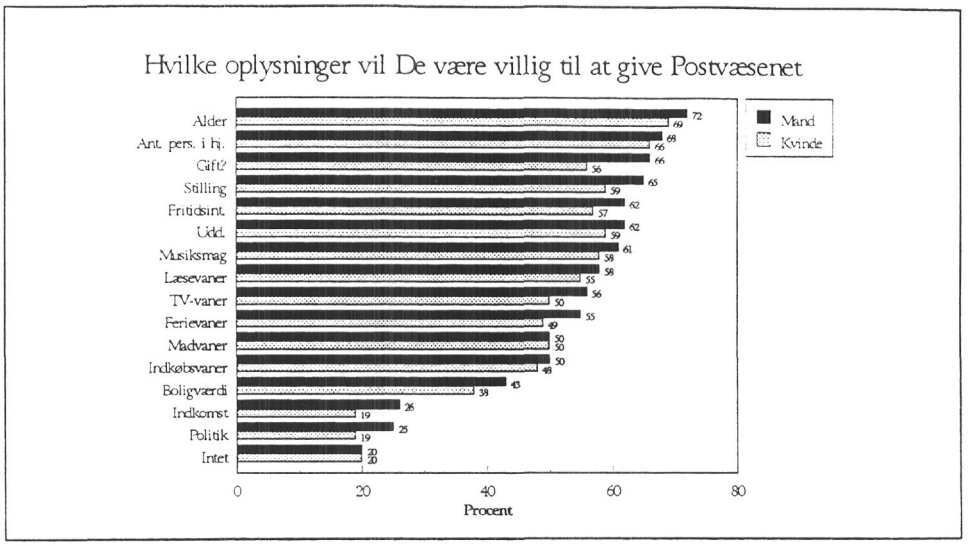
Tanken om, at man selv kunne vælge at være med i en interessedatabase, hvor man kunne få selektive reklamer inden for sine egne interesseområder, vakte også i de kvalitative interviews generelt en positiv respons.

Bekymringen for at blive registreret overskygges helt tydeligt af fordelene ved at være med i en interessedatabase. Her ses et klart eksempel på, hvorledes den abstrakte ængstelse forsvinder, når det drejer sig om ens egne interesser.

Holdninger til registrering hos postvæsenet

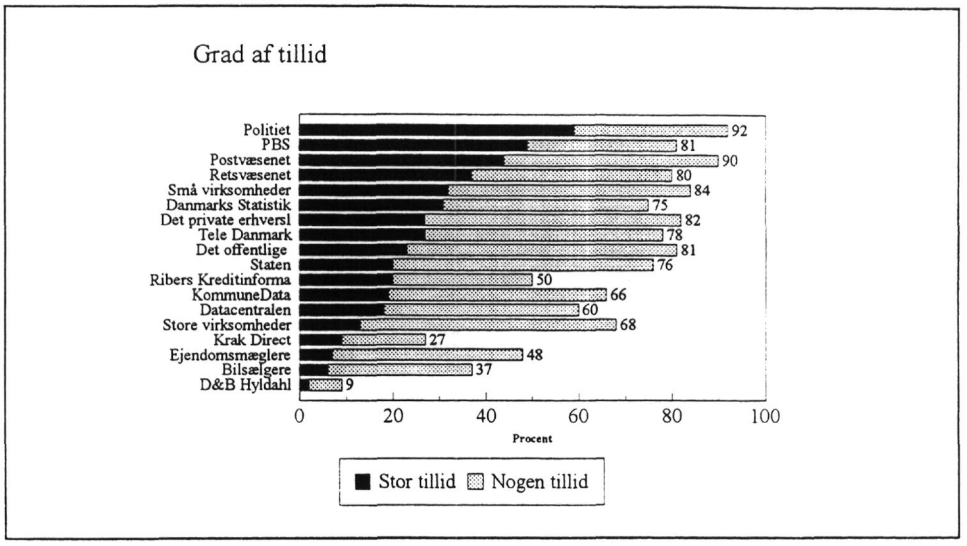
Der er således meget, der tyder på, at der er et potentiale for et koncept, der kan tilvejebringe en bedre overensstemmelse mellem på den ene side afsenderne af reklametryksager og direct mail-markedsføring og på den anden side de interesser, som modtagerne har. Men er folk så

villige til at afgive oplysninger til postvæsenet for at opnå en sådan bedre overensstemmelse? Her er man i undersøgelsen blevet stillet over for 15 forskellige typer af personoplysninger, og der viser sig en stor villighed til at afgive oplysninger om ganske mange personlige forhold.



Som det ses, er det kun 20% af de adspurgte, som siger, at de ikke vil give nogen oplysninger overhovedet. Af de øvrige oplistede muligheder, er der kun fire, hvor der ikke er et flertal, der er villige til at afgive oplysninger til postvæsenet. Politisk stemmeafgivning og personlig indkomst skiller sig her klart ud som oplysninger, man er mindst villig til at afgive til postvæsenet. Kun hhv. 22% og 23% vil oplyse dette. Langt flere (41 %) er villige til at oplyse værdien af deres bolig - som kunne opfattes som en indikator for indkomstniveau. Det sidste gælder i nogen grad også stilling og uddannelse, som er nogle af topscorerne mht. villigheden til at oplyse om dem. Den resterende kategori, som folk ikke overvejende er villig til at oplyse om, er indkøbsvaner, som en stor minoritet på 49% siger, de er villige til at oplyse om. Hvis man ser bort fra de 20%, der principielt ikke vil afgive nogle oplysninger, er der i øvrigt en overvægt af resten, der er villige til at oplyse om såvel værdien af deres bolig som om deres indkøbsvaner.

Den pæne villighed til at give personlige oplysninger til postvæsenet hænger naturligvis sammen med, at postvæsenet generelt nyder en ret stor grad af tillid i befolkningen. Det er faktisk kun politiet og PBS, der opnår en højere grad af tillid af de institutioner, som undersøgelsen har medtaget.



Konklusionen er, at undersøgelsen ikke peger på nogen udbredt folkelig modvilje mod at lade personlige oplysninger registrere af postvæsenet. Tværtimod er man i høj grad villig til dette, hvis det kan føre til, at de reklametryksager og direct mail-forsendelser, man modtager, i højere grad svarer til det, der interesserer en.

BILAG 16

JUSTITSMINISTERIET
Lovafdelingen

NHC00145
J.nr. 1996-793-0033
Den 10. september 1996

N O T I T S

om udformningen af lovbestemmelser i tilknytning til gennemførelse af direktiver i dansk ret.

1. EU-retten indeholder ikke regler om, hvilken form gennemførelsen af et direktiv til national ret skal have. Efter EF-traktatens art. 189 er et direktiv med hensyn til det tilsigtede mål bindende for enhver medlemsstat, som det rettes til, men overlader det til de nationale myndigheder at bestemme form og midler for gennemførelsen. Efter bestemmelsen har medlemsstaterne således et skøn med hensyn til formen og midlerne for gennemførelsen.

Indledningsvis bemærkes, at direktiver skal gennemføres ved bindende regler, således at det ikke er nok, at myndighederne **kan** overholde direktivet i medfør af en bemyndigelse til at udøve et skøn, jf. f.eks. sag C-334/94, Kommissionen mod Frankrig, dom af 7. marts 1996 (endnu utrykt). Dette indebærer imidlertid ikke, at direktiver nødvendigvis skal gennemføres ved lov eller bekendtgørelse. Såfremt den nationale retstilstand allerede er i overensstemmelse med direktivets regler, er ny lovgivning selvsagt overflødig (konstatering af normharmoni).

Ved gennemførelsen af et direktiv til national ret kan medlemsstaterne principielt vælge enten at omskrive direktivet eller at inkorporere det ved i en lov eller bekendtgørelse at henvise til direktivet.

Fordelen ved omskrivningsmetoden er, at den giver mulighed for at opretholde den sædvanlige lovgivningssystematik og det lovsprog, som myndighederne og borgerne er vant til.

Samtidigt er det muligt at udelade bestemmelser, som ikke skal gennemføres i national ret. Derudover kan eventuelle uklarheder fjernes ved at præcisere direktivets bestemmelser. Ud fra en EU-lovteknisk synsvinkel er den åbenbare ulempe ved omskrivningsmetoden, at den skaber risiko for, at der opstår en konflikt mellem national ret og direktivets bestemmelser.

Inkorporering ved henvisning er derimod en enkel metode, der giver sikkerhed for, at direktivet gennemføres korrekt til national ret. Den åbenbare ulempe er imidlertid, at et inkorporeret direktiv kan virke uoverskueligt og systemfremmed og dermed vanskeligt at benytte af de retsanvendende myndigheder. Hertil kommer, at uklarheder i direktivteksten ikke præciseres eller afhjælpes i den nationale lov.

2. Efter EF-domstolens praksis er udgangspunktet ved omskrivning af et direktiv til nationale retsforskrifter, at gennemførelsen efter EU-retten ikke nødvendigvis forudsætter, "at direktivets bestemmelser formeligt og ordret gengives i udtrykkelige, særlige lovbestemmelser, men at det alt efter direktivets indhold er tilstrækkeligt, at der foreligger et generelt retligt grundlag, der giver sikkerhed for, at direktivet efterleves fuldt ud og med bestemthed og klarhed, således at den af direktivet omfattede personkreds i det omfang det ved direktivet tilsigtes at skabe rettigheder for private, sættes i stand til at få fuldt kendskab til deres rettigheder- og i givet fald til at håndhæve disse rettigheder ved nationale domstole", jf. sag 363/85, Kommissionen mod Italien, Saml. 1987, side 1733.

I tilknytning hertil skal man dog være opmærksom på, at mange direktivbestemmelser har direkte virkning, hvilket påvirker medlemsstaternes mulighed for at omskrive disse bestemmelser, jf. nedenfor under pkt. 3.

3. På trods af ordlyden af art. 189 har EF-domstolen fastslået, at et direktivs bestemmelser kan have direkte virkning, når de er tilstrækkeligt præcise og ubetingede, og direktivets gennemførelsesfrist er udløbet, se f.eks. sag C-91/92, Dori, Saml. 1994, side 3325. Dette indebærer, at i

sådanne tilfælde skal en national ret anvende direktivets bestemmelser og tilsidesætte eventuelt modstridende nationale gennemførelsesbestemmelser.

Det forhold, at et direktiv kan indeholde - og oftest indeholder - bestemmelser, der har direkte virkning, taler med styrke for, at såfremt man gennemfører et direktiv ved omskrivning, holder man sig så tæt op ad direktivets formuleringer som overhovedet muligt. Herved undgås, at man utilsigtet fastsætter regler, der er i strid med direktivet, og som i givet fald må vige for dettes bestemmelser.

Ud fra en EU-lovteknisk synsvinkel skal man således ved gennemførelsen af et direktiv i videst muligt omfang undgå at anvende andre begreber, afgrænsninger, formuleringer o. lign. for derved at undgå at skabe en potentiel konfliktmulighed i forhold til EU-retten.

Disse synspunkter gælder også selv i de tilfælde, hvor direktivets bestemmelser ikke indeholder tilstrækkeligt præcise og ubetingede bestemmelser, og således ikke har direkte virkning. Baggrunden herfor er, at EF-domstolen i en række domme har udtalt, at direktivteksten kan styre fortolkningen af en national lovbestemmelse, selv om direktivbestemmelsen ikke opfylder betingelserne for at have direkte virkning. Der kan bl.a. henvises til sag C-334/92, Miret, dom af 16. december 1993 (endnu utrykt), hvor Domstolen udtalte, at ved anvendelsen af nationale retsforskrifter, hvad enten de er yngre eller ældre end direktivet, er den nationale domstol forpligtet til i videst muligt omfang at fortolke de nationale retsforskrifter i lyset af direktivets ordlyd og formål og at fremkalde det med direktivet tilsigtede mål.

Muligheden for, at et direktiv kan styre fortolkningen af en national lovbestemmelse, selv om direktivet ikke har direkte virkning, sammenholdt med at sådanne fortolkningsspørgsmål kan forelægges EF-domstolen i medfør af EF-traktatens art. 177, og at EF-domstolen kan give den nationale lovbestemmelse en fortolkning, der afviger fra den, der er valgt ved omskrivningen, medfører således, at man i videst muligt omfang bør gengive direktivets bestemmelser ordret eller i hvert

fald anvende direktivets begreber og afgræsninger uden at omskrive dem.

4. Ved en omskrivning af et direktiv kan der rejses spørgsmål om, hvorvidt medlemsstaten har mulighed for at udelade visse af direktivets bestemmelser og i stedet angive disse i lovforslagets almindelige bemærkninger.

Dette var spørgsmålet i den danske såkaldte Ligelønssag. Danmark havde gennemført ligelønsdirektiv 75/117 dels ved kollektive overenskomster og dels ved lov, der fandt anvendelse i det omfang en arbejdsgiver ikke var omfattet af de kollektive overenskomster. Efter loven blev arbejdsgiveren forpligtet til at yde ligeløn for samme arbejde. I lovforslagets bemærkninger var det præciseret, at udtrykket "samme løn for samme arbejde" havde samme rækkevidde som direktivets "samme løn for samme arbejde, der tillægges samme værdi".

Under en traktatkrænkelsessag, som Kommissionen havde anlagt i medfør af EF-traktatens art. 169 mod Danmark, udtalte EF-domstolen bl.a., at medlemsstaterne ved gennemførelsen af direktivet har pligt til at sikre, at alle arbejdstagere i fuld udstrækning kan nyde godt af direktivets beskyttelse. Under hensyn til, at loven særlig gjaldt arbejdstagere, der ikke er fagligt organiserede og er beskæftiget i små eller mellemstore virksomheder, var der efter Domstolens opfattelse anledning til særligt og omhyggeligt at tilsikre dem de rettigheder, de kan udlede af direktivet. Domstolen fandt, at den nævnte bemærkning i lovforarbejderne ikke var tilstrækkelig til at sikre en hensigtsmæssig information af de berørte arbejdstagere, og Danmark tabte sagen, jf. sag 143/83, Kommissionen mod Danmark, Saml. 1985, side 427.

Hensynet til retsbeskyttelsen og retssikkerheden krævede således en utvetydig formulering, der satte de berørte arbejdstagere i stand til på tilstrækkelig klar og tydelig måde at kende deres rettigheder og forpligtelser, og de nationale domstole i stand til at sikre iagttagelsen heraf. Uanset at lovgivning i motiverne er en anvendt lovteknik i Danmark, kan den, som Ligelønssagen viser, være utilstrækkelig.

5. For god ordens skyld tilføjes, at EF-domstolen har fastslået i en nyligt afsagt dom, at en medlemsstat er erstatningsansvarlig i henhold til EU-retten, når der vedtages eller opretholdes en bekendtgørelse, der må anses for en ukorrekt gennemførelse af et direktiv. Det er dog en betingelse for retten til erstatning, at den overtrådte direktivbestemmelse tillægger borgeren eller virksomheden rettigheder, at overtrædelsen er tilstrækkelig kvalificeret, og at der er årsagsforbindelse mellem overtrædelsen af direktivbestemmelsen og borgerens og virksomhedens lidte tab, jf. sag C-392/93, British Telecommunications, dom af 26. marts 1996 (endnu utrykt). Selv om sagen vedrørte en bekendtgørelse og ikke en lov, og således ikke angår erstatningsansvaret ved udstedelse af love, er der grund til at tro, at erstatningsbetingelserne i sagen uden videre kan overføres til statens erstatningsansvar, når lovgiver gennemfører et direktiv ved lov.

BILAG 1 7

JUSTITSMINISTERIET
Lovafdelingen

JFK00239
J.nr. 1997-610/3-0216
Den 9. juni 1997

N O T A T

om

direktiv 95/46/EF og kreditoplysningsbureauers behandling af personoplysninger.

1. Baggrunden for det rejste spørgsmål.

Udvalget om Registerlovgivningen har overfor Justitsministeriet rejst spørgsmål om fortolkning af direktiv 95/46/EF i forhold til reglerne i lov om private registre kapitel 3 om kreditoplysningsbureauer.

Udvalget har således oplyst, at udvalget - ligesom det er tilfældet efter lov om private registre § 9, stk. 2, - overvejer at foreslå en ordning, hvorefter kreditoplysningsbureauer ikke må behandle visse kategorier af personoplysninger.

Udvalget ønsker i den forbindelse oplyst, om et generelt forbud svarende til det foreslåede vil være foreneligt med registerdirektivet, jf. navnlig artikel 7 og 8.

Udvalget har endvidere oplyst, at udvalget - i tråd med den nugældende regel i lov om private registre § 10, stk. 1, - overvejer at foreslå en ordning, hvorefter kreditoplysningsbureauer inden en vis frist skal meddele visse oplysninger til den registrerede.

Udvalget ønsker i den forbindelse oplyst, om et krav om obligatorisk underretning svarende til det foreslåede vil være i overensstemmelse med registerdirektivet, jf. navnlig artikel 10 og 11.

Det bemærkes indledningsvist, at det uden videre må lægges til grund, at kreditoplysningsbureauers behandling af personoplysninger som led i deres virksomhed vil være omfattet af direktivets anvendelsesområde, jf. således artikel 3.

2. Forbud mod kreditoplysningsbureauers behandling af visse former for personoplysninger.

Udvalget har foreslået en bestemmelse med følgende ordlyd:

"[§ **20]**(*). Kreditoplysningsbureauer må kun behandle oplysninger, som efter deres art er af betydning for bedømmelse af økonomisk soliditet og kreditværdighed.

Stk. 2. Oplysninger som nævnt i § 7, stk. 1, og § 8, stk. 2, samt oplysninger om væsentlige sociale problemer, må ikke behandles." (stk. 3 er udeladt her)

De foreslåede bestemmelser i § 7, stk. 1, og § 8, hvortil der henvises, har følgende ordlyd:

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

"§ 8. Offentlige myndigheder må behandle oplysninger om strafbare forhold under de i § 6 angivne betingelser.

Stk. 2. Private må behandle oplysninger om strafbare forhold, hvis det er nødvendig til varetagelse af en berettiget interesse, og denne interesse klart overstiger hensynet til den registrerede. [.....**]** (*).

Stk. 3. Et fuldstændigt register over straffedomme må kun føres for en offentlig myndighed."

Det vil være en følge af de foreslåede bestemmelser, at kreditoplysningsbureauer ikke lovligt vil kunne behandle følgende type personoplysninger:

- Oplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold og oplysninger om helbredsmæssige og seksuelle forhold.

- Oplysninger om strafbare forhold.

- Oplysninger om væsentlige sociale problemer.

Der er derfor grund til at overveje, hvorvidt direktivets bestemmelser vil være til hinder for en ordning, hvorved der gøres visse begrænsninger i kreditoplysningsbureauernes muligheder for at behandle personoplysninger.

Det følger af direktivet, at medlemsstaterne kan fastsætte regler for, hvornår behandling af personoplysninger må finde sted, jf. artikel 7.

Det fremgår navnlig af artikel 7, litra f, at medlemsstaterne fastsætter bestemmelser om, at behandling af personoplysninger kun må finde sted, hvis behandlingen er nødvendig, for at den registeransvarlige eller den tredjemand eller de tredjemænd, til hvem oplysningerne videregives, kan forfølge en legitim interesse, medmindre den registreredes interesser eller de grundlæggende rettigheder og frihedsrettigheder, der skal beskyttes i henhold til direktivets artikel 1, stk. 1, går forud herfor. Bestemmelsen skal sammenholdes med 30. indledende betragtning til direktivet.

Ved afgørelsen af, om en behandling af personoplysninger skal være lovlig, må medlemsstaten således vurdere nødvendigheden for den registeransvarlige, ligesom det må vurderes, om denne varetager en legitim interesse ved behandlingen. Denne interesse skal imidlertid afvejes overfor den registreredes interesser.

Det følger af bestemmelsen, at medlemsstaterne er overladt en skønsmargin ved vurderingen af, hvornår en behandling af personoplysninger skal være lovlig.

Dette bør sammenholdes med direktivets artikel 5, hvorefter medlemsstaterne i henhold til bestemmelserne i direktivet præciserer, på hvilke betingelser behandling af personoplysninger er lovlig.

Direktivet indeholder endvidere bestemmelser for særlige kategorier af oplysninger, jf. således artikel 8. Denne bestemmelse må formentlig forstås som en specialbestemmelse således at oplysninger, der er omfattet af artikel 8, stk. 1, ikke samtidig er omfattet af artikel 7.

Direktivets artikel 8, stk. 1, indeholder et generelt forbud mod behandling af visse kategorier af personoplysninger, mens artikel 8, stk. 2, indeholder mulighed for at gøre undtagelse herfra.

Efter artikel 8, stk. 1, forbyder medlemsstaterne behandling af personoplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssigt tilhørsforhold og oplysninger om helbredsforhold og seksuelle forhold.

Efter artikel 8, stk. 2, finder forbudet i stk. 1, ikke anvendelse i nærmere opregnede tilfælde. Der er tale om en udtømmende opregning af undtagelsestilfælde. Da der er tale om en undtagelsesbestemmelse, taler dette for en indskrænkende fortolkning.

Der synes at være grundlag for at antage, at undtagelsen i stk. 2 giver medlemsstaterne en fakultativ mulighed for at gøre undtagelse for at imødekomme visse behov, jf. således 33. indledede betragtning, og at der derfor næppe kan gøres krav på at behandle oplysninger omfattet af stk. 1 i tilfælde, der falder ind under en af de kategorier, der er nævnt i stk. 2.

Hertil kommer, at medlemsstaterne er overladt en manøvremargin, jf. således 9. indledende betragtning, og at et generelt forbud mod kreditoplysningsbureauers behandling af sådanne oplysninger må antages at være begrundet i hensynet til de registrerede, og at dette vil være i overensstemmelse med direktivets formål, jf. således artikel 1, stk. 1, og 10. indledende betragtning.

Det bemærkes endelig, at medlemsstaterne som nævnt kan fastsætte generelle betingelser for, hvornår behandling af personoplysninger er lovlig, og at medlemsstaterne i denne forbindelse kan fastsætte særlige betingelser på specifikke områder, jf. 22. indledende betragtning.

Det må lægges til grund, at de personoplysninger, der er omfattet af § 7, stk. 1, i udvalgets forslag, falder ind under den særlige bestemmelse i artikel 8, mens de øvrige personoplysninger, der er nævnt i [§ 20, stk. 2](*), vil være omfattet af artikel 7, litra f.

For så vidt angår de oplysninger, der ikke er omfattet af lovudkastets § 7, stk. 1, må det kunne lægges til grund, at forbudet mod behandling af disse oplysningstyper er udtryk for lovgivers afvejning af, hvad artikel 7, litra f, fører til inden for kreditoplysningsområdet.

Det må endvidere kunne lægges til grund, at artikel 8 ikke kan antages at give kreditoplysningsbureauer et egentligt krav på at behandle de i lovudkastets § 7, stk. 1, nævnte oplysningstyper, jf. herved artikel 8, stk. 2.

På denne baggrund må det antages, at bestemmelsen i den foreslåede [§ 20, stk. 2](*), er forenelig med direktivets artikel 7 og 8.

3. Kreditoplysningsbureauers obligatoriske underretning til registrerede personer.

Udvalget har foreslået en bestemmelse, der har følgende ordlyd:

" [§ 21] (*) . Kreditoplysningsbureauer skal inden 4 uger efter behandlingens iværksættelse give meddelelse til den, der behandles oplysninger om. Meddelelsen skal indeholde de i [§ 28, stk. 1, nr. 1-3, eller § 29, stk. 1, nr. 1-3](*), nævnte oplysninger."

Bestemmelsen pålægger kreditoplysningsbureauer en oplysningspligt i forhold til den registrerede.

Af bestemmelsen følger, at et kreditoplysningsbureau inden 4 uger efter behandlingens iværksættelse skal give meddelelse til den, der behandles oplysninger om. Meddelelsen skal indeholde de oplysninger, der er nævnt i [§ 28, stk. 1, nr. 1-3, eller § 29, stk. 1, nr. 1-3] (*) .

Som det fremgår af bestemmelsens ordlyd, er oplysningspligten ikke alene obligatorisk, men der er endvidere ikke mulighed for at gøre undtagelse herfra.

Dette giver derfor anledning til at overveje, om det vil være i overensstemmelse med direktivet, at kreditoplysningsbureauer pålægges en pligt til at give underretning til den registrerede, uden mulighed for at gøre undtagelse i visse tilfælde.

Det bemærkes i denne forbindelse, at der ikke herved vil blive taget stilling til oplysningspligtens omfang eller tidspunktet for meddelelsen til den registrerede, men alene spørgsmålet om, hvorvidt det er i overensstemmelse med direktivet, at der ikke gøres undtagelse fra oplysningspligten for så vidt angår visse oplysningstyper, der efter deres karakter og indhold falder ind under anvendelsesområdet for artikel 10 og 11.

Efter direktivet har den registeransvarlige en oplysningspligt overfor den registerede. Direktivet sondrer mellem tilfælde, hvor oplysningerne er indsamlet hos den registrerede, og tilfælde, hvor oplysningerne ikke er indsamlet hos den registrerede, jf. således henholdsvis artikel 10 og 11.

Efter artikel 10 fastsætter medlemsstaterne bestemmelser om, at den registeransvarlige eller dennes repræsentant mindst skal give den person hos og om hvem der indsamles oplysninger, visse oplysninger, der er nævnt i litra a til c. Dette gælder for så vidt som disse yderligere informationer, under

hensyn til de særlige omstændigheder hvorunder oplysningerne indsamles, er nødvendige for at sikre den registrerede en rimelig behandling af oplysningerne.

Efter bestemmelsen gælder dette, medmindre den pågældende er bekendt med oplysningerne.

Efter artikel 11 fastsætter medlemsstaterne bestemmelser om, at den registeransvarlige eller dennes repræsentant allerede ved registreringen af oplysningerne, eller senest når oplysningerne første gang videregives til tredjemand, mindst skal give den person hos og om hvem der indsamles oplysninger, visse oplysninger, der er nævnt i litra a til c. Bestemmelsen vedrører tilfælde, hvor oplysningerne ikke er indsamlet hos den registrerede. Dette gælder for så vidt som disse yderligere informationer, under hensyn til de særlige omstændigheder hvorunder oplysningerne indsamles, er nødvendige for at sikre den registrerede en rimelig behandling af oplysningerne.

Efter bestemmelsen gælder dette, medmindre den pågældende allerede er bekendt med oplysningerne.

Det følger af artikel 11, stk. 2, at bestemmelserne i stk. 1, ikke finder anvendelse, navnlig ikke når behandlingen foretages i statistisk øjemed eller til historiske eller videnskabelige forskningsformål, hvis underretning af den registrerede viser sig umulig eller uforholdsmæssig vanskelig, eller registreringen eller videregivelsen af oplysningerne er udtrykkeligt fastsat ved lov. I sådanne tilfælde fastsætter medlemsstaterne de fornødne garantier.

Fælles for de to bestemmelser er, at oplysningspligten gælder, medmindre den registrerede er bekendt hermed. Artikel 11, stk. 2, indeholder her ud over visse yderligere undtagelser fra oplysningspligten.

For så vidt angår tilfælde, hvor den registrerede er bekendt med oplysningerne, jf. artikel 10, stk. 1, og artikel 11,

stk. 1, synes bestemmelserne at pålægge medlemsstaterne at fastsætte regler, hvorefter den registeransvarlige pålægges en oplysningspligt. Bestemmelserne gør som nævnt undtagelse herfra i tilfælde, hvor de registrerede allerede er bekendt med oplysningerne. Dette synes at måtte forstås således, at medlemsstaterne i disse tilfælde ikke er forpligtet til at fastsætte regler om oplysningspligt. Der synes imidlertid ikke i bestemmelsernes ordlyd at være grundlag for at antage, at dette skulle udelukke medlemsstaterne fra at fastsætte sådanne regler. Bestemmelserne kan derfor næppe fortolkes således, at der er en egentlig ret for den registeransvarlige til ikke at meddele visse oplysninger til den registrerede, når denne er bekendt hermed. En undtagelsesfri oplysningspligt vil endvidere være i harmoni med direktivets formål, nemlig beskyttelse af individet. Hertil kommer, at 38., 39. og navnlig 40. indledende betragtning, synes at tale for, at medlemsstaterne i de nævnte tilfælde ikke er forpligtet til at fastsætte en oplysningspligt, men at de på den anden side ikke er forhindrede i at fastsætte sådanne regler. Det følger således heraf, at det i visse situationer ikke er nødvendigt at pålægge en pligt til at underrette.

Det ovenfor anførte synes at gælde tilsvarende for de tilfælde, der er omfattet af artikel 11, stk. 2.

Såfremt det ovenfor anførte lægges til grund, er der i de nævnte situationer ikke nogen pligt for medlemsstaterne til at fastsætte en oplysningspligt overfor den registrerede, men bestemmelserne synes ikke at udelukke, at medlemsstaterne af hensyn til den registrerede vælger af fastsætte en sådan underretningsforpligtelse.

Det bemærkes, at det endvidere synes at have støtte i direktivets forarbejder at lægge til grund, at artikel 11, stk. 2, må fortolkes som en bemyndigelse til medlemsstaterne, der ikke samtidig indeholder en udtrykkelig ret for de registeransvarlige, jf. således artikel 10 i det oprindelige direktivforslag, jf. KOM(90) endelig udg. - SYN 287, jf. EF-tidende nr. C 277 af 5. november 1990, side 3, og KOM(90)

314 endelig udg. - SYN 287 og 288, side 19f, og KOM(92) 422 endelig udg. - SYN 287, side 22.

4. Sammenfatning.

Sammenfattende kan det konkluderes, at der ikke synes at være grundlag for at antage, at de af registerudvalget foreslåede bestemmelser, jf. [§ 20, stk. 2, og § 21](*), vil være uforenelige med direktiv 95/46/EF, jf. navnlig artikel 7 og 8, og artikel 10 og 11.

*: I det af Justitsministeriet afgivne notat er der henvist til bestemmelser i et af udvalget tidligere udarbejdet lovudkast. For at gøre notatet mere læsevenligt i forhold til udvalgets endelige lovudkast, jf. herved betænkningens kapitel 6, er der fra sekretariatets side foretaget en tilpasning hertil.

REGISTERTILSYNET **ABP**
29. sept. 1997

Notits
om
anmeldelsesordningen*

På baggrund af den debat, som har udspillet sig i udvalget vedrørende anmeldelsesordningen - navnlig i relation til, hvorvidt lovudkastet i tilstrækkelig grad indebærer en afbureaukratisering - har Registertilsynet fundet det formålstjenligt at udarbejde denne oversigtlige notits vedrørende den foreslåede ordning.

1. Oplysningstyper, som skal fremgå af anmeldelsen
Af artikel 19 fremgår, hvilke oplysningstyper, der mindst skal indgå. I lovudkastets § 43, stk. 2, er tilføjet
1) navn og adresse på en evt. databehandler,
2) behandlingens betegnelse (m.h.p. identifikation af behandlingen),
3) en generel beskrivelse af behandlingen,
4) tidspunktet for påbegyndelsen af behandlingen, samt
5) tidspunktet for sletning af oplysningerne.

Især pkt. 3 har været diskuteret. Indsættelsen af punktet skyldes, at en anmeldelse typisk vil omfatte flere enkelte behandlinger - se nærmere nedenfor under pkt. 2 - da det vil være unødigt bureaukratisk af kræve anmeldelse af hver enkelt behandling. Disse behandlinger er imidlertid alle hver for sig undergivet direktivets materielle behandlingsregler. Det vil ikke være muligt for en tilsynsmyndighed at foretage en efterfølgende eller forudgående kontrol af de enkelte behandlinger, hvis ikke myndigheden er bekendt med disse. Navnlig vil det som oftest ikke kunne ses ud af anmeldelsen, at der finder en indsamling sted på en bestemt måde, at der sker en samkøring i kontroløjemed eller lignende. Tilsynets kontrol vil derfor i bedste fald være mangelfuld, hvis der ikke indhentes nærmere oplysninger om disse enkelte behandlinger, som ikke kan læses ud af formålsbeskrivelsen i anmeldelsen.

Beskrivelsen skal holdes på et helt overordnet plan, idet der blot skal gives tilstrækkelige oplysninger til, at tilsynet kan vurdere, om der er grund til at foretage en nærmere vurdering af behandlingerne. Der er vedlagt et eksempel på, hvordan en anmeldelse *eventuelt* kan udformes.

Det bemærkes i øvrigt, at en borger, som læser en anmeldelse, hvori der ikke indgår en sådan beskrivelse, næppe vil kunne forstå, hvad behandlingen nærmere går ud på (hvor kommer oplysningerne fra og hvad sker der med dem i myndigheden?), hvilket kan medføre en følelse af uoverskuelighed og utryghed. Et af formålene med anmeldelsen er netop at skabe gennemsigtighed (transparens) for borgerne. Der erindres i denne forbindelse om, at Datatilsynet skal føre en offentligt tilgængelig fortegnelse over anmeldte behandlinger, jf. lovudkastets § 54, stk. 1.

2. Genstanden for en anmeldelse
Genstanden for en anmeldelse kan efter artikel 18, stk. 1, være *en enkelt behandling* eller *en række behandlinger,* hvis formål er identiske eller indbyrdes relaterede. Det må forventes, at der i praksis vil ske anmeldelse af *rækker af behandlinger.* Der skal blot kunne formuleres et logisk, sammenhængende formål med en sådan række af behandlinger. Affattelsen af lovudkastets bestemmelser om anmeldelse, § 43, stk. 1, og § 48, stk. 1, udelukker ikke, at der sker anmeldelse af *rækker ai* behandlinger, da bestemmelserne alene fastslår, at der skal ske anmeldelse inden iværksættelsen af en behandling.

I et vist omfang vil formålsangivelserne svare til de formålsangivelser, som i dag fremgår af forskrifterne for offentlige registre (se f.eks. Registertilsynets fortegnelse over offentlige registre, 1996).

Hidtil er mulighederne for at formulere brede formålsbestemmelser for offentlige registre dog ikke altid blevet udnyttet fuldt ud af myndighederne. I praksis vil der derfor for mange myndigheder være mulighed for i forbindelse med anmeldelse efter den nye lov at revurdere formålsangivelserne for de registre/behandlinger, som føres for myndigheden. Hertil kommer, at der fremover vil kunne ske anmeldelse af behandlinger, som omfatter *dels* tidligere egne registre og *dels* tidligere fælleskommunale registre. Et eksempel skulle kunne illustrere dette:

En kommune har hidtil benyttet sig af følgende registre i forbindelse med administrationen af bistandslovens kap. II og III (kontanthjælp samt råd og vejledning):

FORMAL: ADM. AF BISTANDSLOVENS KAP. II OG III.	**ANDRE FORMAL**
Eget statistiksystem vedr. bistandsydelser	
Det fælleskommunale debitorsystem (Bl.a. adm. af opkrævning og indbetaling af tilbagebetalingskrav)	
Register for oplysninger om udbetalte ydelser (Kontrol med evt. uberettigede udbetalinger)	
Register vedr. udbetaling af bistandsydelser (Anvisninger til PBS)	
Eget bistandssystem (Sagsbehandling)	
Edb-journalsystem (Nuværende journalsystem)	
Manuelle journalkort (Tidligere journalsystem)	

Der har hidtil været fastsat forskrifter for alle disse registre, undtagen for samlingen af manuelle journalkort. Fremover vil der kunne ske anmeldelse af alle de behandlinger, som foretages i registrene, og som vedrører bistand, under følgende formålsbestemmelse:

"Administration af bistandslovens afsnit II (rådgivning og tilsyn) og afsnit III (kontanthjælp) samt førelse af statistik i forbindelse hermed." Se det vedlagte eksempel på en anmeldelse.

3. Antallet af anmeldelser

Den offentlige forvaltning
Tidligere var **samtlige** offentlige registre enten undergivet et krav om *anmeldelse* eller om *forskriftsfastsættelse.*

Systemet efter lov om offentlige myndigheders registre:	**Systemet efter lovudkastet:**
Registre, som anmeldes på blå blanket (Ikke-fortrolige registre, lovens § 8 a og § 8 b) Ca. 8.100 registre fra 1991 til nu	Ingen anmeldelse, jf. § 44, stk. 1
Registre, som anmeldes på grøn blanket (Visse fortrolige registre, lovens § 8 e og bekendtgørelse nr. 872 af 17. december 1991) Ca. 1.450 registre fra 1991 til nu	Ingen anmeldelse, da undtagelse efter § 44, stk. 4, er forudsat.
Registre, som der er fastsat gruppe 2-forskrifter for (Fortrolige oplysninger, dog ikke følsomme)	Anmeldelse, dog mulighed for undtagelse, jf. § 44, stk. 4.
Registre, som der er fastsat gruppe 3-forskrifter for (Følsomme oplysninger) Ca. 4.050 gruppe 2 og 3-registre fra 1979 til nu	Anmeldelse og forudgående kontrol (udtalelse), jf. § 45.

Fælleskommunale registre, som der er fastsat forskrifter for	I vidt omfang dækket af anmeldelser jf. ovenfor eller evt. ikke anmeldelsespligtige.
79 registre Ca. 7.300 tilslutningsmeddelelser	Resten: Der kan indgives fælles anmeldelse, jf. udkastets § 43, stk. 1.

Den private sektor

I udkastets regler vedrørende anmeldelse/tilladelse af behandlinger, som foretages for private dataansvarlige, skal de behandlinger, som i dag skal anmeldes eller tillades, fremover tillades. Desuden er det tilstræbt, at behandlinger, der er undtaget fra anmeldelse/tilladelse i dag, fortsat vil være undtaget, jf. § 49, stk. 1. Det kan ikke udelukkes, at der vil være behandlinger af mere banal karakter, som ikke er medtaget i § 49, stk. 1. Der er imidlertid indsat en hjemmel for justitsministeren til at fastsætte yderligere undtagelser i § 49, stk. 3.

Endvidere er manuelle, følsomme registre fremover anmeldelsespligtige i modsætning til tidligere. Disse vil dog, jf. det ovenfor anførte, i vid udstrækning kunne anmeldes sammen med edb-baserede behandlinger. Endvidere må det antages, at der i takt med den teknologiske udvikling vil blive færre og færre manuelle registre.

4. Konklusion

På baggrund af ovennævnte må det konkluderes, at den ordning, som fremgår af lovudkastet, indebærer, at der i anmeldelsen skal anføres ganske få yderligere oplysningstyper, som er velbegrundede af hensyn til Datatilsynet og borgerne, og som kun udgør en meget begrænset arbejdsbyrde. Desuden medfører ordningen en meget betydelig afbureaukratisering i den offentlige sektor og en i hovedsagen uændret ordning i den private sektor.

*: Registertilsynet har siden notitsens udarbejdelse foretaget en ajourføring af de angivne tal, således at disse er opgjort pr. 1. november 1997. Der er endvidere foretaget en opdatering af paragrafhenvisningerne, så disse er i overensstemmelse med lovudkastet i betænkningen.

REGISTERTILSYNET

ABP
28. okt. 1997

Notits
om

visse særlige spørgsmål i forbindelse med behandling af personoplysninger på Internettet

1. Indledning

Intemettet - i det følgende kaldet nettet - er et elektronisk medie af en hidtil uset størrelse for udbredelse af oplysninger, billeder, lyd, programmer, services m.v. Udbredelsen er ikke kendt præcist, men i slutningen af 1996 blev det antaget, at der var adgang til nettet fra mere end 140 lande, at nettet bestod af mere end fire millioner websteder, samt at mere end 40 millioner brugere havde adgang til nettet. Det forventes, at der i 1999 vil være ca. 200 mill, brugere.

Nedenfor redegøres for nettet som et informationsmedie samt for (nogle af) de særlige problemer, som behandlingen af personoplysninger via nettet rejser i relation til databeskyttelsesdirektivet. Det bemærkes, at brugen af nettet også rejser andre spørgsmål end rent databeskyttelsesretlige, f.eks. vedrørende udbredelsen af racistiske budskaber, børnepornografi eller lignende, men disse emner er ikke berørt nedenfor. Det bemærkes endvidere, at mulighederne for anonymitet på nettet for tiden debatteres i flere forskellige sammenhænge og fora. Debatten fokuserer navnlig på spørgsmålet om afvejningen af hensynet til brugeren, som gerne vil fremstå anonym, og hensynet til muligheden for at opspore bestemte brugere af nettet i tilfælde af sikkerhedsbrud eller andre ulovlige handlinger. Denne diskussion er heller ikke berørt nedenfor. Det skal dog nævnes, at i det omfang der opnås en fuldstændig anonymitet ved brug af nettet, er der ikke længere tale om oplysninger om brugeren (dvs. personoplysninger), og flere af nedenstående problemstillinger vil dermed miste sin relevans. I det omfang der benyttes pseudoidentiteter eller lignende, som kan føres tilbage til en bestemt person, vil der stadig være tale om personoplysninger.

Det er i det følgende alene hensigten at gøre opmærksom på diverse problemstillinger, ikke at komme med endelige svar på de rejste spørgsmål, eller lægge op til bestemte løsninger, bortset fra i de få tilfælde, hvor det forekommer helt uproblematisk.

2. Nettet som informationsmedie

2.1. Nettets infrastruktur

Som nettet fungerer i dag, er der tale om et netværk bestående af et meget stort antal datanet, der er indbyrdes forbundet i en kompliceret og kaotisk struktur, hvor de kommunikerer med hinanden på grundlag af standardiserede kommunikationsprotokoller.

Kommunikationen sendes via teleforbindelser og computere, som udgør henholdsvis forbindelseslinier og knudepunkter på nettet. Knudepunkterne er henholdsvis routere og servere. En router er en computer, der modtager og afsender data uden at gøre noget ved indholdet af de meddelelser, som udgøres af disse data. En server er en computer, der lagrer programmer og data, og hvor data bliver til, ændres eller forarbejdes på anden vis.

Adgang til nettet opnås ved en aftale med en internetleverandør, som etablerer forbindelse mellem abonnentens egen computer (pc eller server) og resten af nettet. Endvidere skal der på en brugers computer installeres det programmel (en browser), som gør det muligt for en bruger at kalde netudbydernes servere/routere op og oversætte de data, som indhentes via nettet, til forståelig tekst og billeder.

Hver computer, som er forbundet til nettet, har en unik adresse (IP-adresse). Kommunikationen via nettet foregår herefter ved, at brugeren fra den tilsluttede computer via telefonnettet "ringer" internetleverandøren op, hvorefter der rent teknisk sker en omstilling hos denne til den IP-adresse (e-postadresse eller websted), som brugeren ønsker at kontakte. Det er ikke muligt at forudsige, hvilke routere og teleforbindelser, de sendte data konkret vil passere igennem. Det afhænger bl.a. af belastningen af routere og forbindelser, samt af om nogle routere eller forbindelser eventuelt er ude afdrift.

Der er ingen central styring af nettet, men der eksisterer et vist samarbejde omkring koordineringen og udviklingen af kommunikationsprotokoller.

2.2. Aktørerne

Der er forskellige aktører i forbindelse med kommunikation via nettet. Overordnet set er der:

- Teleoperatører, der stiller de telenetværk til rådighed, som oplysningerne passerer igennem.

- Internetleverandører, som udbyder service i form af lagring, transmission og præsentation. Disse er ansvarlige for kanaliseringen af oplysningerne til de relevante routere/servere.

- Informationsudbydere, som tilbyder oplysninger på websteder.

- Serviceudbydere, der udbyder deres services via websteder, f.eks. booking af hoteller, bankydelser og lignende.

- Abonnenter, som har truffet aftale med en internetleverandør om at få adgang til nettet.

- Brugere, som får adgang til nettet og benytter sig af de forskellige tilbud.

Mange aktører har imidlertid flere af de ovennævnte roller.

2.3. Anvendelser af nettet

Nettet kan bruges til at stille oplysninger og services til rådighed for brugerne på websteder. Websteder oprettes af informations- og serviceudbydere. Brugerne vil kunne kalde de pågældende websteder op ("surfe") og se de oplysninger, som er gjort almindeligt tilgængelige på disse websteder. I nogle tilfælde vil brugeren endvidere kunne sende oplysninger - meddelelser - til webstedet (interaktive hjemmesider).

Brugeren vil endvidere kunne sende elektronisk post til e-postadresser og kan selv modtage e-post.

Endelig kan en bruger aflæse eller overføre egne indlæg til fælles "opslagstavler" eller diskussionsfora, i det følgende kaldet nyhedsgrupper. Indholdet i en sådan nyhedsgruppe stammer således fra brugerne, men det er kendetegnende, at brugerne ikke længere efter overførslen af et indlæg er i stand til at rette eller slette oplysninger i dette. Den videre behandling af indlæggene - herunder sletningen i disse - forestås af en administrator af nyhedsgruppen.

2.4. Typer af personoplysninger

Der behandles grundlæggende set flere forskellige typer af personoplysninger via nettet.

Dels behandles personoplysninger, som er indeholdt i de meddelelser, der sendes via nettet.

Dels behandles elektroniske spor (trafikdata), som er oplysninger om de meddelelser, som sendes via nettet, men ikke om indholdet, jf. ovenfor. Disse oplysninger består af en række numre, som gør det muligt for brugeren at nå frem til den ønskede e-postadresse eller webstedet - enten med en meddelelse eller blot for at se oplysningerne på webstedet - og for meddelelser herfra at nå frem til brugeren. De elektroniske spor indeholder f.eks. afsender og modtagers IP-adresser, dato og tidspunkt, men kan også indeholde mere detaljerede oplysninger om, hvilke konkrete dele af et websted, der er hentet oplysninger fra. Oplysningerne bruges endvidere til afregning i forbindelse med transmissionen af meddelelserne.

Endelig bør det nævnes, at det ikke kan udelukkes, at der ved brugen af cookies - se nedenfor - kan genereres personoplysninger, f.eks. hvis cookien samler tilstrækkelig mange og detaljerede oplysninger om brugeren.

2.5. Typer af overførsler

Via nettet foregår såvel aktive som passive overførsler af personoplysninger.

Aktive overførsler er overførsler, som faktisk finder sted ved en aktiv handling, og som sker til en bestemt (kreds af) modtager(e).

Overførslerne kan være bevidste, dvs. de foretages på initiativ af brugeren eller den, som er dataansvarlig for oplysningerne.

Aktive overførsler kan imidlertid også være skjulte. En informations- eller serviceudbyder kan programmere sin server således, at den placerer "cookies" hos brugerne. En cookie er en

fil indeholdende linier af tekst, som et websted ved henvendelse fra en bruger placerer på brugerens harddisk, som udgangspunkt uden brugeren bemærker det. I den information, der er lagret i cookien, indgår bl.a. en entydig nummerering af den anvendte browser. Når brugeren derefter på ny sender til webstedet, medsendes en kopi af den lagrede cookie, således at webstedet kan se, at det er den samme browser, transmissionen kommer fra. Der er herved hverken lagret en direkte identifikation af den person, som har anvendt browseren, eller oplysning om browserens fysiske placering (adresse). Ved svar fra webstedet medsendes og geniagres cookien, eventuelt ajourført med yderligere oplysninger, som brugeren har givet ved sin seneste henvendelse til webstedet.

En cookie er ikke tilgængelig fra andre websteder end det, som har placeret den i den pågældende computer.

Det oprindelige formål med anvendelsen af cookies angives at være en effektivisering af kommunikationen brugeren og webstedet imellem. Ved en session, som indebærer et antal sammenhængende transmissioner frem og tilbage mellem bruger og websted, vil passende information i cookien kunne gøre den samlede session hurtigere. Særlige detaljer vedrørende transmissionen, f.eks. at brugeren ønsker svaret på sin forespørgsel fremsendt uden grafik, således at transmissionen vil gå hurtigere, kan lagres i cookien, hvorved brugeren ved fornyet henvendelse får sit foretrukne format uden at skulle specificere det igen. Det er endvidere muligt på webstedet at opnå et overblik over, hvorledes en bruger "bevæger sig" rundt mellem de tilgængelige informationer, om den samme type informationer søges gang på gang, om den givne brugervejledning fungerer, om der er information som ikke har brugerens interesse, etc. Cookies kan også anvendes i forbindelse med de reklamer, som mange websteder lader indgå i de sendte skærmbilleder. Baseret på en brugers opsøgte typer af information på et websted kan der dannes en interesseprofil og på grundlag heraf indsættes de relevante reklamer.

Jo mere information brugeren afgiver til et websted, desto større er muligheden for, at en egentlige personlig identifikation kan finde sted.

Den ovennævnte type cookies indeholder kun tekst og ikke programmer, som kunne tænkes at starte udførelse på brugerens computer. Den omtalte type af cookies kan således ikke indsamle oplysninger hos brugeren, men vil kun indeholde de oplysninger, som webstedet placerer i dem. Det bemærkes i den forbindelse, at der fremover - og måske allerede på nuværende tidspunkt - kan tænkes cookies, som indeholder programmer, hvilket rejser en række andre problemer.

Passive overførsler består i, at en informations- eller serviceudbyder på et websted gør oplysninger tilgængelige via nettet, uden der nødvendigvis nogensinde sker en overførsel til andre.

3. Spørgsmål i forhold til direktivets bestemmelser

Der er ikke ved nedenstående opregning tilstræbt en udtømmende beskrivelse af de særlige spørgsmål, som kan opstå i relation til anvendelsen af direktivet på de behandlinger af personoplysninger, som finder sted i tilknytning til nettet.

3.1. Definitioner, artikel 2

Personoplysninger

Navnlig i forbindelse med elektroniske spor og oplysninger, som stammer fra cookies, kan man stille det spørgsmål, om disse er personoplysninger i direktivets forstand. Dette synes særlig tvivlsomt, når oplysningerne vedrører en IP-adresse eller browser på en computer, som anvendes af mange brugere.

Behandling

Al transmission af personoplysninger via nettet må betragtes som behandling i direktivets forstand. Det samme gælder den indsamling af oplysninger, indtastning og eventuelle lagring og systematisering af oplysningerne, som går forud for transmissionen, samt en eventuel efterfølgende decentral lagring (downloading) og brug af oplysningerne, som foretages af brugeren. Mere tvivlsomt synes det, om selve den søgning og visning, som brugeren iværksætter, skal betragtes som en behandling i direktivets forstand.

Registeransvarlig *(i det følgende kaldet dataansvarlig)*

I relation til nettet får betragtning 47 en særlig betydning, idet det fremgår af denne, at når en meddelelse fremsendes via en telekommunikations- eller elektronisk posttjeneste, hvis eneste formål er at sende meddelelser af denne type, er det den person, som er ophavsmand til meddelelsen, og ikke den person, der tilbyder tjenesten, der normalt vil blive betragtet som ansvarlig for behandlingen af de personoplysninger, der er indeholdt i meddelelsen. De personer, som udbyder disse tjenester, vil dog normalt blive betragtet som ansvarlige for behandlingen af de supplerende personoplysninger, der er nødvendige for tjenestens udførelse.

I almindelighed vil teleoperatører og internetleverandører med andre ord ikke være dataansvarlige for meddelelserne, men eventuelt registerførere (databehandlere). Det vil typisk være informations- eller serviceudbyderen eller eventuelt en bruger, som er dataansvarlig for indholdet af de meddelelser, som hidrører fra denne. Hvis en bruger eller en informations- eller serviceudbyder imidlertid lagrer oplysninger fra nettet til brug for deres egne formål og med den effekt, at de fremover afgør, med hvilke hjælpemidler en senere behandling kan foretages, må disse formentlig anses for dataansvarlige.

Det synes mere tvivlsomt, hvem der er dataansvarlig for oplysninger, som indlægges af brugere i diskussionsfora og lignende.

Man kan endvidere rejse det spørgsmål, hvorvidt teleoperatører og internetleverandører kan betragtes som dataansvarlige for de elektroniske spor, der generes under en transmission til brug for den ydelse, som operatørerne/leverandørerne tilbyder. Dette er imidlertid kun relevant, i det omfang oplysningerne kan betragtes som personoplysninger.

Samtykke
Et samtykke skal være en frivillig, specifik og informeret viljestilkendegivelse. Kravet om. at samtykket skal være informeret, har til formål at sikre, at den registrerede er klar over de fordele og ulemper, som er forbundet med dennes samtykke. Spørgsmålet er, om selve det faktum, at oplysningerne skal transmitteres via nettet, eller måske ligefrem skal stilles til rådighed for enhver bruger på nettet, udløser en særlig pligt til at informere herom i forbindelse med indhentningen af et samtykke.

Omvendt giver nettet mulighed for afgivelse af et mere differentieret samtykke. En interaktiv hjemmeside kan opbygges således, at brugeren ledes etapevis gennem en menu, hvor brugeren hele tiden kan vælge, om denne ønsker at afgive de oplysninger, som der anmodes om. eller ej. Undervejs kan brugeren i de enkelte menubilleder oplyses om, hvad afgivelsen af oplysningerne vil indebære.

3.2. Gældende national lovgivning, artikel 4

Et vanskeligt problem opstår i relation til direktivets regler om lovvalg, jf. artikel 4, stk. 1. Det er en følge af artikel 4, stk. 1, litra c, at dansk lovgivning finder anvendelse på behandlinger, som foretages af en dataansvarlig, der ikke er etableret på Fællesskabets område, og som med henblik på behandling af personoplysninger anvender midler, som befinder sig på Danmarks område, medmindre disse midler kun benyttes med henblik på forsendelse gennem Det Europæiske Fællesskabs område. Se i øvrigt betænkningens kapitel 5, pkt. 3.4.3.

Det synes ikke oplagt, hvilken lovgivning der skal finde anvendelse, såfremt en bruger i Danmark sender oplysninger via nettet til en dataansvarlig, som er etableret i et tredjeland. Spørgsmålet er, om man kan betragte situationen således, at der finder en behandling sted (en indsamling) ved hjælp af midler, som befinder sig i Danmark (den registreredes egen computer, teleselskabets kabler og netudbyderens faciliteter). Tilsvarende kunne det overvejes, om dansk lovgivning finder anvendelse, hvis en dataansvarlig i et tredjeland indsamler oplysninger om danske brugere ved hjælp af cookies.

3.3. Behandlingsregime

Oplysningerne skal behandles rimeligt og lovligt, artikel 6, stk. 1, litra a
Det kan herunder bl.a. diskuteres, hvorvidt det er rimeligt at indsamle oplysninger ved hjælp af cookies. Dette er dog kun relevant i det omfang, der er tale om personoplysninger.

Formålsbestemthedsprincippet, artikel 6, stk. 1, litra b
Man kan rejse det spørgsmål, om selve den handling, som består i at gøre oplysninger tilgængelige på nettet, skal betragtes som en selvstændig, særlig behandling, som ikke fuldt ud kan ligestilles med en videregivelse. I så fald må behandlingen - dvs. offentliggørelsen via nettet - kun finde sted, hvis det ikke er uforeneligt med det formål, til hvilket oplysningerne er indsamlet.

Kendetegnende for passive overførsler via nettet er i øvrigt, at det ikke er muligt at forudse eller begrænse de formål, som brugere af nettet senere kan benytte oplysningerne til. Dette adskiller sig naturligvis ikke principielt fra brugen af oplysninger, som er blevet offentlig-

gjort på anden måde end via nettet, men det vil være langt lettere at finde og kopiere oplysninger, forarbejde og benytte dem, fordi de foreligger i standardiseret, elektronisk form, og fordi brugeren forholdsvis let kan indhente oplysningerne fra sin egen computer.

Benytter en bruger oplysningerne til et formål, som er uforeneligt med det, som oplysningerne oprindeligt blev indsamlet til, vil der i princippet være tale om en ny behandling, som efter omstændighederne kan udløse en pligt til at informere den registrerede, jf. artikel 11. Det kan imidlertid være vanskeligt eller umuligt at finde frem til disse registrerede.

Behandlingsbetingelser, artikel 7 og 8
Hvis selve den passive overførsel (offentliggørelse) via nettet skal betragtes som en selvstændig behandling, skal behandlingsbetingelserne være opfyldt i relation til denne særlige behandling. Det vil i så fald ikke være tilstrækkeligt at konstatere, at betingelserne er opfyldt i relation til en traditionel videregivelse eller en aktiv, bevidst videregivelse via nettet med en kendt modtagerkreds, idet der så skal foretages en selvstændig vurdering af offentliggørelsen via nettet.

Særligt i forbindelse med fortegnelser over e-postadresser kunne det overvejes, om - og i givet fald under hvilke omstændigheder - en registreret skal kunne hindre, at dennes e-postadresse indgår i offentligt tilgængelige fortegnelser over sådanne adresser.

3.4. Den registreredes rettigheder
Underretningspligten, artikel 10-11
Hvis en interaktiv hjemmeside opfordrer brugere til at sende personlige data, vil oplysningspligten kunne opfyldes ved, at webstedet redegør for de oplysninger, som er pligtige efter artikel 10. Dette kan f.eks. være tilfældet, hvis der er tale om en serviceudbyder, men også hvis oplysningerne indgår i et diskussionsforum.

Oplysningspligten er mere problematisk i relation til indsamling af oplysninger, som ikke sker hos den registrerede, jf. artikel 11, navnlig hvis oplysningerne stammer fra en ikke-navngiven kilde på nettet, og der ikke er anført adresseoplysninger eller lignende.

Efter artikel 10-11 skal den dataansvarlige give en række nærmere opregnede informationer, herunder formålene med behandlingen. Det kan imidlertid, som nævnt ovenfor, ikke garanteres, at oplysningerne ikke vil blive anvendt til andre formål af de brugere, som eventuelt måtte have adgang til oplysningerne. Endvidere skal gives alle yderligere informationer, for så vidt som disse informationer under hensyn til de særlige omstændigheder hvorunder oplysningerne er indsamlet, er nødvendige for at sikre den registrerede en rimelig behandling af oplysningerne. Det kunne overvejes, om denne bestemmelse giver den dataansvarlige en særlig pligt til at informere om det, hvis oplysningerne vil blive stillet til rådighed for principielt enhver, herunder enhver i tredjelande. Tilsvarende vil den dataansvarlige måske have en pligt til at informere om de særlige sikkerhedsrisici ved transmission via nettet.

I relation til cookies har bestemmelserne om oplysningspligt en særlig relevans (hvis der er tale om personoplysninger), idet den registrerede som hovedregel ikke er bekendt med indsamlingen af oplysningerne.

Retten til indsigt, artikel 12, litra a
På grund af det store antal aktører i forbindelse med brugen af nettet, kan det være svært for en registreret at gennemskue, hvem der behandler oplysninger om vedkommende, navnlig hvis aktørerne ikke har oplyst vedkommende om det, jf. ovenfor.

Efter artikel 12, litra a, 2. pind, skal en registreret have meddelt letforståelig information om, hvilke oplysninger der er omfattet af behandlingerne, samt enhver tilgængelig information om, hvorfra disse oplysninger stammer. Det sidste vil formentlig i mange situationer være vanskeligt, såfremt oplysningerne stammer fra en ukendt kilde på nettet.

Retten til at få berigtiget oplysninger, artikel 12, litra c
Der kan opstå særlige vanskeligheder i relation til efterlevelsen af denne bestemmelse, hvis de pågældende oplysninger, som viser sig ufuldstændige eller urigtige, har været almindeligt tilgængelige på nettet, idet den dataansvarlige ikke kan vide, hvem der rent faktisk har modtaget oplysningerne.

Retten til at gøre indsigelse imod brugen af oplysninger i mårkedsføringsøjemed, artikel 15, litra b
Elektroniske spor og cookies kan danne grundlag for meget detaljerede profiler over brugere, som giver mulighed for markedsføringstiltag på et mere individuelt niveau end behandlinger, der finder sted i andre medier.

3.5. Sikkerhed, artikel 17

Sikkerhedsreglerne rejser spørgsmål i flere forskellige sammenhænge.

For det første skal der være den fornødne sikkerhed i relation til oplysninger, som overføres aktivt og bevidst til bestemte modtagere. Her må det tages i betragtning, at mange personer har adgang til nettet, hvilket i sig selv indebærer en større risiko for, at oplysninger udbredes ubeføjet, end hvis der tale om et lukket system. Af artikel 17, stk. 1, fremgår det direkte, at den dataansvarlige skal iværksætte de fornødne foranstaltninger til hindring af bl.a. ubeføjet udbredelse eller ikke-autoriseret adgang, navnlig hvis behandlingen omfatter fremsendelser af oplysninger i et net. Endvidere bør erindres, at en dataansvarlig ikke kan vide, hvilke linier/servere oplysningerne passerer og dermed ikke vurdere en eventuel særlig risiko for hændelig eller ulovlig tilintetgørelse, hændeligt tab eller forringelse. Hertil kommer, at oplysningerne kan passere gennem linier og servere, som befinder sig i tredjelande uden et sikkerhedsniveau, som svarer til direktivets.

For det andet vil den omstændighed, at en abonnent har en forbindelse mellem sin computer, fra hvilken der er etableret netadgang, og resten af dennes interne net, indebærer en sikkerhedsrisiko i sig selv. Risikoen for, at en hacker får adgang til det interne net, er langt større,

når der er tale om et så omfattende net som Internettet, allerede på grund af det meget store antal brugere. Dette problem kan reduceres ved brug af "fire walls".

For det tredje vil der være en risiko forbundet med at downloade (lagring decentralt på egen computer) oplysninger og programmer fra nettet i og med, at der kan være indeholdt virus i filer på nettet. En sådan virus kan selvsagt både medføre tilintetgørelse og forringelse af oplysninger på en abonnents interne net.

For det fjerde henledes opmærksomheden på den særlige misbrugsmulighed, som består i, at det er langt lettere at manipulere oplysninger, som foreligger i en standardiseret, elektronisk form, end på anden vis. Det vil f.eks. være muligt at manipulere med billeder af personer eller tekst fra myndigheder eller andre officielle kilder og gøre de ændrede oplysninger tilgængelige på nettet i en form, som giver indtryk af, at oplysningerne fortsat stammer fra de officielle kilder.

Artikel 17, stk. 2 og 3, om valg af registerfører (databehandler) og indgåelse af kontrakt med denne, rejser det særlige problem, at den dataansvarlige typisk ikke ved, hvilke virksomheder m.v., der kommer til at behandle oplysningerne, der er indeholdt i de meddelelser, som den dataansvarlige sender via nettet.

En række af de sikkerhedsrisici, som kan tænkes i relation til nettet, vil kunne afhjælpes gennem kryptering, efter omstændighederne suppleret af en (sikker) digital signatur.

3.6. Ansvar, artikel 23

På grund af det store antal aktører, som er involveret i transmissioner over nettet, kan det være vanskeligt at afgøre, hvem der er ansvarlig for et eventuelt misbrug, uautoriseret adgang, datatab, manipulation af oplysninger eller lignende.

3.7. Overførsel til tredjelande, artikel 25-26

Som nævnt ovenfor er det kendetegnende for passive overførsler via nettet, at den dataansvarlige ikke kan vide, hvem der modtager oplysningerne. Hvem som helst vil kunne se oplysningerne, herunder brugere, som befinder sig i et tredjeland. Det vil således være tvivlsomt, hvorvidt der vil kunne ske passive overførsler efter artikel 25, da der i så fald principielt må ske en vurdering af beskyttelsesniveauet i alle de tredjelande, fra hvilke der kan opnås adgang til oplysningerne.

Med hensyn til aktive, bevidste overførsler vil den endelige modtagers elektroniske adresse være kendt. Hvis det også er kendt, hvor denne er etableret, vil den dataansvarlige kunne foretage en vurdering af beskyttelsesniveauet i det tredjeland, som modtageren er etableret i. Det er imidlertid ikke altid muligt at se ud fra en elektronisk adresse, hvilket land modtageren er etableret i. Endvidere vil den dataansvarlige ikke kunne vide, hvilke tredjelande oplysningerne eventuelt overføres til undervejs i transmissionen, da det langt fra er sikkert, at transmissionen sker i en "lige linje".