KOM(90) 314

DE EUROPÆISKE FÆLLESSKABER
RÅDET

Bruxelles, den 20. september 1990
(03.10)
(OR. f)

8460/90	
	RESTREINT

ECO 158

OVERSÆTTELSE AF SKRIVELSE

ORIGINAL

af 27. juli 1990

fra Kommissionen for De Europæiske Fællesskaber, underskrevet af Jean DONDELINGER, medlem

til Gianni DE MICHELIS, formand for Rådet for De Europæiske Fællesskaber

Vedr.: Beskyttelse af personer i forbindelse med behandling af personoplysninger og informationssystemers sikkerhed

Hr. formand,

Hermed følger en meddelelse fra Kommissionen om beskyttelse af personer i forbindelse med behandling af personoplysninger og om informationssystemers sikkerhed, som ledsages af følgende dokumenter:

a) et forslag til Rådets direktiv om indbyrdes tilnærmelse af visse af medlemsstaternes love og administrative bestemmelser vedrørende beskyttelse af personer i forbindelse med behandling af personoplysninger SYB 287

b) et udkast til resolution vedtaget af repræsentanterne for regeringerne for De Europæiske Fællesskabers medlemsstater, forsamlet i Rådet, om anvendelse på den offentlige sektor af principper i direktivet, som ikke henhører under fællesskabsrettens anvendelsesområde

c) en erklæring fra Kommissionen om anvendelse på De Europæiske Fællesskabers institutioner og organer af principperne i Rådets direktiv om indbyrdes tilnærmelse af visse af medlemsstaternes love og administrative bestemmelser om beskyttelse af personer i forbindelse med behandling af personoplysninger

.../...

KOMMISSIONEN FOR DE EUROPÆISKE FÆLLESSKABER

KOM(90) 314 endelig udg. - SYN 287 og 288

Bruxelles, den 24. september 1990

MEDDELELSE FRA KOMMISSIONEN

om beskyttelse af personer
i forbindelse med behandling af personoplysninger i Fællesskabet
og om informationssystemers sikkerhed

Forslag til SYN 287

RÅDETS DIREKTIV

om beskyttelse af personer
i forbindelse med behandling af personoplysninger

Udkast til

RESOLUTION VEDTAGET AF REPRÆSENTANTERNE FOR REGERINGERNE

FOR DE EUROPÆISKE FÆLLESSKABERS MEDLEMSSTATER, FORSAMLET I RÅDET

ERKLÆRING FRA KOMMISSIONEN

om anvendelse på De Europæiske Fællesskabers institutioner og organer
af principperne i Rådets direktiv om beskyttelse af personer
i forbindelse med behandling af personoplysninger

Forslag til SYN 288

RÅDETS DIREKTIV

om beskyttelse af personoplysninger og kommunikationshemmeligheden
i forbindelse med offentlige digitale telenet, herunder det
tjenesteintegrerede digitalnet (ISDN) og
offentlige digitale mobilnet

Henstilling med henblik på

RÅDETS AFGØRELSE

om åbning af forhandlinger med henblik på
De Europæiske Fællesskabers tiltrædelse af Europarådets konvention
om beskyttelse af individet i forbindelse med
automatisk behandling af personlige data

Forslag til

RÅDETS AFGØRELSE

om informationssikkerhed

---

d) et forslag til Rådets direktiv om beskyttelse af personoplysninger og kommunikationshemmeligheden i forbindelse med offentlige digitale telenet, herunder det tjenesteintegrerede digitalnet (ISDN) og offentlige digitale mobilnet. SYN 288

e) en henstilling med henblik på Rådets afgørelse om åbning af forhandlinger med henblik på De Europæiske Fællesskabers tiltrædelse af Europarådets konvention om beskyttelse af individet i forbindelse med automatisk behandling af personlige data.

f) et forslag til Rådets afgørelse om informationssikkerhed.

En indsats fra Fællesskabets side er nødvendig for at beskytte personer i forbindelse med behandling af personoplysninger med henblik på gennemførelsen af det indre marked og for at sikre dataindustriens og de nye telekommunikationstjenesters udvikling.

Kommissionen foreslår derfor sektorspecifikke foranstaltninger for telekommunikation, foruden et rammedirektiv, der er det centrale element i beskyttelsessystemet i det indre marked, og som ledsages af foranstaltninger, der udvider de samme beskyttelsesprincipper til Fællesskabets institutioner og organer og til aktiviteter, der ikke henhører under fællesskabsrettens anvendelsesområde.

Da forslagene i a) og d) bygger på artikel 100A i Traktaten om Oprettelse af Det Europæiske Økonomiske Fællesskab, skal samarbejdsproceduren med Europa-Parlamentet finde anvendelse, og Det Økonomiske og Sociale Udvalg skal høres.

Da forslaget i f) bygger på artikel 235 i Traktaten om Oprettelse af Det Europæiske Økonomiske Fællesskab, skal Europa-Parlamentet høres. Henset til det behandlede spørgsmål foreslår Kommissionen, at også Det Økonomiske og Sociale Udvalg høres.

Rådet skal fastlægge sin fælles holdning til forslagene i a) og d) og tage stilling til forslaget i f) i marts 1991. På denne baggrund ses det gerne, at Europa-Parlamentet og Det Økonomiske og Sociale Udvalg afgiver udtalelse inden årets udgang.

(Høflighedsformel).

(sign.) Jean DONDELINGER

Bilag: KOM(90) 314 endelig udg. SYN 287-288

d) et forslag til Rådets direktiv om beskyttelse af personoplysninger og kommunikationshemmeligheden i forbindelse med offentlige digitale telenet, herunder det tjenesteintegrerede digitalnet (ISDN) og offentlige digitale mobilnet. SYN 288

e) en henstilling med henblik på Rådets afgørelse om åbning af forhandlinger med henblik på De Europæiske Fællesskabers tiltrædelse af Europarådets konvention om beskyttelse af individet i forbindelse med automatisk behandling af personlige data.

f) et forslag til Rådets afgørelse om informationssikkerhed.

En indsats fra Fællesskabets side er nødvendig for at beskytte personer i forbindelse med behandling af personoplysninger med henblik på gennemførelsen af det indre marked og for at sikre dataindustriens og de nye telekommunikationstjenesters udvikling.

Kommissionen foreslår derfor sektorspecifikke foranstaltninger for telekommunikation, foruden et rammedirektiv, der er det centrale element i beskyttelsessystemet i det indre marked, og som ledsages af foranstaltninger, der udvider de samme beskyttelsesprincipper til Fællesskabets institutioner og organer og til aktiviteter, der ikke henhører under fællesskabsrettens anvendelsesområde.

Da forslagene i a) og d) bygger på artikel 100A i Traktaten om Oprettelse af Det Europæiske Økonomiske Fællesskab, skal samarbejdsproceduren med Europa-Parlamentet finde anvendelse, og Det Økonomiske og Sociale Udvalg skal høres.

Da forslaget i f) bygger på artikel 235 i Traktaten om Oprettelse af Det Europæiske Økonomiske Fællesskab, skal Europa-Parlamentet høres. Henset til det behandlede spørgsmål foreslår Kommissionen, at også Det Økonomiske og Sociale Udvalg høres.

Rådet skal fastlægge sin fælles holdning til forslagene i a) og d) og tage stilling til forslaget i f) i marts 1991. På denne baggrund ses det gerne, at Europa-Parlamentet og Det Økonomiske og Sociale Udvalg afgiver udtalelse inden årets udgang.

(Høflighedsformel).

(sign.) Jean DONDELINGER

Bilag: KOM(90) 314 endelig udg. SYN 287-288

MEDDELELSE FRA KOMMISSIONEN

om beskyttelse af personer
i forbindelse med behandling af personoplysninger i Fællesskabet
og om informationssystemers sikkerhed

I. INDLEDNING

1. Den stigende hyppighed, hvormed personoplysninger gøres til genstand for behandling i alle facetter af det økonomiske liv og samfundslivet, og det voksende behov for informationsudveksling i tilknytning til Fællesskabets videreudbygning gør det bydende nødvendigt, at Fællesskabet iværksætter foranstaltninger til at beskytte personer i forbindelse med behandling af personoplysninger og højne sikkerheden ved sådan behandling, ikke mindst i forbindelse med udbygningen af åbne telenet.

2. I en tidsalder, hvor den informationsteknologiske udvikling gør behandling og udveksling af data af enhver art betydeligt lettere, er den der store forskelle i EF-medlemsstaternes måde at gribe beskyttelsen af personer i forbindelse med sådan behandling an på. I 1970'erne medførte bekymring vedrørende beskyttelsen af personer i forbindelse med behandling af personoplysninger, at adskillige medlemsstater tog lovgivningsinitiativer for at begrænse behandlingen af denne type oplysninger og fastsætte lovrammer for den. Alligevel er der på nuværende tidspunkt kun syv medlemsstater, der har specifik lovgivning på området. Selv om sigtet med de forskellige lovgivninger er det samme, udviser de i nogle henseender store forskelle, f.eks. med hensyn til anvendelsesområde (om manuelle registre er omfattet eller ej, om juridiske personer er beskyttet eller ej) og med hensyn til de betingelser, der skal opfyldes, forinden behandling kan finde sted (omfanget af anmeldelsespligten, oplysningspligten ved indsamling af oplysninger, behandlingen af følsomme data).

3. Bortset fra den nationale lovgivning og henstillingen fra OECD's Råd om fastlæggelse af retningslinjer for beskyttelsen af privatlivets fred og strømmen af personoplysninger på tværs af grænserne af 23. september 1980 er Europarådets konvention af 28. januar 1981 om beskyttelse af personer i forbindelse med automatiseret behandling af persondata den eneste internationale retsforskrift, der findes på området. Den lader dog en lang række valgmuligheder stå åbne for at gennemføre de grundprincipper, den opstiller, og den er kun blevet ratificeret af syv medlemsstater, hvoraf én endnu ikke har nogen intern lovgivning.

4. Der er også blevet udtrykt bekymring i Fællesskabet vedrørende denne situation. Europa-Parlamentet har således siden 1976 følt sig foranlediget til at vedtage en række beslutninger(1), hvori det tilkendegiver betænkelighed ved udviklingen på området og opfordrer Kommissionen til at udarbejde et forslag til direktiv om harmonisering af medlemsstaternes lovgivning om beskyttelse af personoplysninger.

5. I en henstilling af 29. juli 1981 understregede Kommissionen, at en sådan beskyttelse har karakter af en grundlæggende rettighed, og at det er ønskeligt, at der sker en indbyrdes tilnærmelse af alle medlemsstaternes retsforskrifter på dette område. Den henstillede ligeledes til medlemsstaterne, at de inden udgangen af 1982 ratificerede Europarådets konvention af 28. januar 1981 om beskyttelse af personer i forbindelse med automatiseret behandling af persondata. Samtidig blev det præciseret, at hvis alle medlemsstaterne ikke inden for et rimeligt tidsrum undertegnede og ratificerede konventionen, forbeholdt Kommissionen sig ret til at foreslå Rådet at vedtage en retsakt på grundlag af EØF-Traktaten.

6. Forskellene i medlemsstaternes lovgivning og mangelen på et beskyttelsessystem på fællesskabsplan udgør en hindring for virkeliggørelsen af det indre marked. Hvis de registrerede personers grundlæggende rettigheder, specielt retten til privatlivets fred, ikke er beskyttet på EF-plan, vil informationsstrømmen på tværs af landegrænserne reelt blive hindret, og dette i en situation, hvor denne informationsstrøm har afgørende betydning for virksomhedernes og forskningsinstitutionernes aktiviteter og det samarbejde mellem medlemsstaternes offentlige administrationer, der etableres som følge af oprettelsen af et område uden indre grænser i henhold til Traktatens artikel 8 A. I forbindelse med foranstaltningerne til fremme af personers frie bevægelighed og Borgernes Europa påpegede Det Europæiske Råd derfor på mødet i Strasbourg den 8. og 9. december 1989, at det var nødvendigt at sørge for, at der ved fastlæggelse af samarbejdsformerne mellem administrationerne på forhånd garanteres borgerne beskyttelse i forbindelse med brugen af databaser med personoplysninger.

7. En samlet fællesskabsstrategi inden for beskyttelse af personer i forbindelse med behandling af personoplysninger er ligeledes en afgørende forudsætning for at udbygge informationsindustrien og tillægstjenesterne på telekommunikationsområdet. For at virkeliggøre det indre marked for teletjenester og -udstyr er det bydende nødvendigt, at der snarest muligt indføres harmoniserede bestemmelser om beskyttelse af personoplysninger og privatlivets fred i forbindelse med brug af digitale telenet.

8. Endvidere udgør datamatiseringens indtrængen i alle dele af det økonomiske liv og samfundslivet sammenholdt med fremkomsten af globale kommunikationssystemer, der gør det lettere at integrere forskelligartede aktiviteter, en ny udfordring, der nødvendiggør en "beskyttelse", der er tilpasset de risici, der kan opstå som følge af tekniske eller menneskelige fejl, hvad enten disse er hændelige eller forsætlige. At informationssystemer er effektivt sikrede har afgørende betydning for effektivt at beskytte privatlivets fred og bevare integriteten i den informationsrigdom,

(1) EFT nr. C 100 af 3.5.1976, s. 27; EFT nr. C 140 af 5.6.1979, s. 34; EFT nr. C 87 af 5.4.1982, s. 39.

som edb-registrerede og edb-overførte data udgør. Fællesskabet politik og program for udbygning af informations- og telekommunikationsindustrien og oprettelsen af det indre marked risikerer at støde på alvorlige hindringer, hvis der ikke vedtages en aktiv politik for udarbejdelse, udvikling og fremme af sikkerhedsstandarder for informationssystemer. Dagens telekommunikationssystemer giver mulighed for at overføre data fra den ene ende af Jorden til den anden, og denne politik må tage højde for denne kendsgerning. Det er endvidere uhyre vigtigt, at medlemsstaternes politik inden for edb-sikkerhed ikke udvikler til at blive en hindring for, at Fællesskabet og dets forbindelser med tredjelande kan udvikle sig harmonisk.

II. DEN VALGTE FREMGANGSMÅDE

9. Den fremgangsmåde, der foreslås benyttet, tilsigter at sikre et højt beskyttelsesniveau ved indførelse af et beskyttelsessystem på fællesskabsplan, der bygger på en række indbyrdes supplerende foranstaltninger.

A. Et højt beskyttelsesniveau

10. Eftersom den nationale lovgivning har til formål at garantere individets grundlæggende rettigheder, ikke mindst retten til privatlivets fred, og eftersom Fællesskabet selv har givet udtryk for sin tro på de grundlæggende rettigheder, nærmere bestemt i tredje afsnit i præamblen til Den Europæiske Fælles Akt, må Fællesskabets aktion ikke medføre en forringelse af beskyttelsen, men skal tværtimod sikre et højt beskyttelsesniveau overalt i Fællesskabet. Gennem en fællesskabsaktion er det muligt at garantere et ensartet, højt beskyttelsesniveau i alle EF's medlemsstater og samtidig fjerne hindringerne for virkeliggørelsen af det indre marked i overensstemmelse med artikel 100 A.

11. Som et supplement til en indbyrdes tilnærmelse af individets anerkendte rettigheder på et højt niveau er en aktiv politik inden for informationssystemers sikkerhed af afgørende betydning. At skabe sikre informationssystemer har afgørende betydning for såvel individet som for handelen, industrien og det offentlige. Det afgørende i denne forbindelse er at tilvejebringe en effektiv og praktisk anvendelig sikkerhed for oplysninger, der er registreret i edb-registre, og samtidig undgå, at der skabes nye tekniske handelshindringer mellem medlemsstaterne og over for tredjelande. Dette krav forudsætter, at de forskellige behov og muligheder undersøges på fællesskabsplan i nært samarbejde med de berørte erhvervskredse og medlemsstaterne.

B. En samlet strategi

12. For at indføre et system til beskyttelse af personer i forbindelse med behandling af personoplysninger i Fællesskabet er det nødvendigt at iværksætte en række foranstaltninger, der dækker de forskellige aspekter af området.

13. Internt foreslås der ud over et rammedirektiv om indbyrdes tilnærmelse af medlemsstaternes love og administrative bestemmelser om beskyt-

telse af personer i forbindelse med behandling af personoplysninger (generelt direktiv), som er kernen i beskyttelsessystemet, en pakke af supplerende foranstaltninger med henblik på at sikre en så omfattende beskyttelse som mulig. Selv om hver enkelt af de foreslåede foranstaltninger tager sigte på en specifik situation, tager de alle udgangspunkt i de samme beskyttelsesprincipper, som er opstillet i det generelle direktiv. Formålet med en resolution til vedtagelse af repræsentanterne for medlemsstaternes regeringer, forsamlet i Rådet, og en erklæring fra Kommissionen er således at lade direktivets principper finde anvendelse på registre, der ikke er omfattet af dette. Ligeledes er det nødvendigt med et sektorafgrænset direktiv for offentlige digitaltelenets vedkommende. Endelig kræver informationssystemers sikkerhed en handlingsplan på fællesskabsplan.

14. Eksternt må Det Europæiske Fællesskab over for sine handelspartnere søge at tilskynde til, at de indfører passende beskyttelsesforanstaltninger, og støtte Europarådets indsats på området. Det er i denne forbindelse specielt ønskeligt, at Fællesskabet indleder forhandlinger med henblik på tiltrædelse af Europarådets konvention 108.

Disse forslag må ses under ét for ikke at bringe ensartetheden og sammenhængen i det foreslåede beskyttelsessystem i fare.

C. Gennemgang af de enkelte forslag

15. Sigtet med forslaget til et generelt direktiv er at sikre en ensartet beskyttelse på højt niveau i alle EF's medlemsstater og derved fjerne hindringerne for den informationsudveksling, der er en afgørende forudsætning for det indre markeds funktion. For at opnå dette skal de principper, der opstilles i udkastet til direktivforslag, garanteres af alle medlemsstaterne. Principperne vedrører specielt spørgsmålet om, på hvilke betingelser det er legitimt at behandle personoplysninger, den registrerede persons rettigheder (oplysningsret, ret til aktindsigt, ret til berigtigelse, ret til at tage til genmæle osv.), oplysningernes pålidelighed (de skal være korrekte, indsamles loyalt, registreres til nøje definerede og legitime formål, osv.) og nedsættelse af en Gruppe til Beskyttelse af Personoplysninger, som skal rådgive Kommissionen om spørgsmål vedrørende beskyttelsen af personoplysninger. Udkastet til direktivforslag omfatter den private sektor samt de grene af den offentlige sektor, hvis aktiviteter falder ind under fællesskabsrettens anvendelsesområde. Eftersom enhver vil blive ydet en ensartet, høj beskyttelse i forbindelse med behandling af personoplysninger i alle medlemsstater, vil medlemsstaterne ikke længere under henvisning til den registrerede persons beskyttelse kunne begrænse den frie udveksling af personoplysninger i Fællesskabet.

16. Udkastet til resolution til vedtagelse af repræsentanterne for De Europæiske Fællesskabers medlemsstater, forsamlet i Rådet, tager sigte på at udvide anvendelsesområdet for principperne i det generelle direktiv til at omfatte offentlige registre, som ikke er omfattet af direktivet, dvs. registre, der føres af offentlige forvaltninger, hvis aktiviteter ikke falder ind under fællesskabsrettens anvendelsesområde. Ud fra ønsket om at skabe ensartethed ville det egentlig være ønskeligt, at alle offentlige registre, selv dem, der ikke er omfattet af det generelle direktiv, under-

lægges de samme beskyttelsesprincipper. Med henblik herpå bør medlemsstaterne forpligtes til at indlede de nødvendige nationale lovgivningsprocedurer.

17. Erklæringen fra Kommissionen om anvendelse af bestemmelserne i det generelle direktiv på Fællesskabets institutioner og organer afspejler Kommissionen ønske om, at direktivets principper finder anvendelse på Fællesskabets institutioner og organer. I erklæringen tilkendegiver Kommissionen sin hensigt om, at den vil træffe og foreslå de nødvendige foranstaltninger i denne forbindelse, og at den, indtil dette sker, vil lade direktivets bestemmelser finde anvendelse på sine egne registre.

18. Forslaget til Rådets direktiv om beskyttelse af personoplysninger og privatlivets fred i forbindelse med brug af offentlige digitaltelenet, navnlig det tjenesteintegrerede digitalnet (ISDN) og de offentlige digitalnet for mobilkommunikation supplerer det generelle direktiv derved, at det lader de generelle principper for beskyttelse af personoplysninger finde anvendelse på de nye telenet. Direktivet tager sigte på at garantere brugerne af telenet i alle medlemsstater en grundlæggende beskyttelse gennem foranstaltninger, som skal integreres i de tjenester, der udbydes via de nye net. Rådet og Europa-Parlamentet har ved flere lejligheder understreget vigtigheden af, at der træffes passende foranstaltninger til at beskytte personoplysninger og privatlivets fred i lyset af den fremtidige udvikling på telekommunikationsområdet og specielt inden for ISDN(1). Denne bekymring kom kraftigt til udtryk på det årlige møde af medlemsstaternes kommitterede inden for beskyttelse af personoplysninger i Berlin i august 1989.

19. Henstillingen om, at Rådet træffer beslutning om, at Det Europæiske Fællesskab tiltræder Europarådets konvention om beskyttelse af personer i forbindelse med automatiseret behandling af persondata, er et af elementerne i den eksterne del af Fællesskabets strategi inden for beskyttelse af personoplysninger. Ved tiltrædelse af konventionen sikres det, at de registrerede personer beskyttes, og at personoplysninger kan udveksles frit i forbindelserne mellem Fællesskabet og de tredjelande, der tiltræder den.

20. Forslaget til Rådets afgørelse om vedtagelse af en toårig handlingsplan inden for informationssystemers sikkerhed er et supplement til de retsforskrifter, der tilsigter at styrke individets rettigheder i forbindelse med behandling af personoplysninger. At tilvejebringe sikkerhed for edb-registrerede og edb-overførte oplysninger, dvs. at beskytte de registrerede data, mod trusler af enhver art (hændelige eller forsætlige) er af afgørende betydning for, at personer får mulighed for effektivt at udøve deres rettigheder i forbindelse med behandling af personoplysninger. Mere generelt er dette et altafgørende krav for beskyttelse af ejendom og personer, som i forbindelse med den større og

---

(1) EFT nr. C 257 af 4.10.1988, s. 1; EFT nr. C 196 af 1.8.1989, s. 4; EFT nr. C 7 af 12.1.1987, s. 334; EFT nr. C 12 af 16.1.1989, s. 66; EFT nr. C 12 af 16.1.1989, s. 69.

større udbredelse af åbne telenet forudsætter, at der udarbejdes en samlet strategi og samordnede aktioner på fælleskabsplan inden for teknologier, standarder og procedurer for godkendelse og prøvning samt inden for teknologiudvikling af den type, der indebærer et samarbejde inden for prækonkurrencemæssig forskning og udvikling.

21. Den foreslåede handlingsplan indeholder krav om, at der udarbejdes strategiske rammer for informationssystemers sikkerhed, at sikkerhedsbehovet analyseres, at der udarbejdes løsninger for en række prioriterede problemer, at der udarbejdes valideringsspecifikationer, -standarder og -prøver, at teknologiske og driftsmæssige videreudviklinger inden for informationssystemers sikkerhed integreres i generelle strategiske rammer, og at en række sikkerhedsfunktioner integreres i informationssystemer.

Forslag til

RÅDETS DIREKTIV

SYN 287

om beskyttelse af personer
i forbindelse med behandling af personoplysninger

INDHOLDSFORTEGNELSE

Resumé

Sigtet med dette direktivforslag er at sikre en ensartet beskyttelse på højt niveau i alle EF's medlemsstater og derved fjerne hindringerne for den informationsudveksling, der er en forudsætning for det indre markeds funktion. For at opnå dette skal de principper, der opstilles i udkastet til direktivforslag, garanteres af alle medlemsstaterne. Principperne vedrører specielt spørgsmålet om, på hvilke betingelser det er legitimt at behandle personoplysninger, den registrerede persons rettigheder (oplysningsret, ret til aktindsigt, ret til berigtigelse, ret til at tage til genmæle osv.), oplysningernes pålidelighed (de skal være korrekte, indsamles loyalt, registreres til nøje definerede og legitime formål osv.) og nedsættelse af en Gruppe til Beskyttelse af Personoplysninger, som skal rådgive Kommissionen om spørgsmål vedrørende beskyttelsen af personoplysninger. Udkastet til direktivforslag omfatter den private sektor samt de grene af den offentlige sektor, hvis aktiviteter falder ind under fællesskabsrettens anvendelsesområde. Eftersom enhver vil blive ydet en ensartet, høj beskyttelse i forbindelse med behandling af personoplysninger i alle medlemsstater, vil medlemsstaterne ikke længere under henvisning til den registrerede persons beskyttelse kunne begrænse den frie udveksling af personoplysninger i Fællesskabet.

Begrundelse

I. INDLEDNING

Den bekymring vedrørende beskyttelsen af personer i forbindelse med behandling af personoplysninger, der i stigende grad er kommet til udtryk gennem de seneste femten år, skyldes dels de muligheder, som den hastige informationsteknologiske udvikling har banet vejen for, og dels den stadigt hyppigere behandling af personoplysninger inden for en lang række områder. Bekymringen er kommet til udtryk i forskellige sammenhænge og har affødt lovgivningsinitiativer i adskillige medlemsstater. Bortset fra den nationale lovgivning er Europarådets konvention af 28. januar 1981 om beskyttelse af personer i forbindelse med automatiseret behandling af persondata for øjeblikket den eneste internationale retsakt, der findes på dette område. OECD har udarbejdet retningslinjer for beskyttelsen af privatlivets fred og strømmen af personoplysninger på tværs af grænserne i en henstilling af 23. september 1980, og De Forenede Nationer er ligeledes i gang hermed.

Bekymringen er også kommet til udtryk inden for Fællesskabets rammer. Europa-Parlamentet har således siden 1976 følt sig foranlediget til at vedtage en række beslutninger[1], hvori det tilkendegiver betænkelighed ved udviklingen på dette område og opfordrer Kommissionen til at udarbejde et forslag til et direktiv om harmonisering af medlemsstaternes lovgivning om beskyttelse af personoplysninger.

I en henstilling af 29. juli 1981 understregede Kommissionen, at denne beskyttelse har karakter af en grundlæggende rettighed, og at det er ønskeligt, at der sker en indbyrdes tilnærmelse af alle medlemsstaternes retsforskrifter på dette område. Den henstillede endvidere til medlemsstaterne, at de inden udgangen af 1982 ratificerede Europarådets konvention af 28. januar 1981 om beskyttelse af personer i forbindelse med automatiseret behandling af persondata. Samtidig blev det præciseret, at hvis alle medlemsstaterne ikke inden for et rimeligt tidsrum undertegnede og ratificerede konventionen, forbeholdt Kommissionen sig ret til at foreslå Rådet at vedtage en retsakt på grundlag af EØF-Traktaten.

I forbindelse med foranstaltningerne til fremme af personers frie bevægelighed og Borgernes Europa påpegede Det Europæiske Råd på mødet i Strasbourg den 8. og 9. december 1989, at det var nødvendigt at sørge for, at der ved fastlæggelse af samarbejdsformerne mellem administrationerne på forhånd garanteres borgerne beskyttelse i forbindelse med brugen af databaser med personoplysninger.

Ud over disse tilkendegivelser af behovet for beskyttelse i generel forstand skal det bemærkes, at bekymringen også er kommet til udtryk inden for rammerne af specifikke eller sektorafgrænsede EF-aktioner, navnlig inden for de nye informationsteknologier.

Som forholdene er nu med hensyn til behandling af personoplysninger, og på

---

1) EFT nr. C 100 af 3.5.1976, s. 27; EFT nr. C 140 af 5.6.1979, s. 34; EFT nr. C 87 af 5.4.1982, s. 39.

baggrund af de krav, der udspringer af opbygningen af en fællesskabsenhed, er det blevet absolut nødvendigt med et direktiv til at sikre beskyttelsen af personer i forbindelse med denne form for behandling.

II. NØDVENDIGHEDEN AF BESKYTTELSE INDEN FOR FÆLLESSKABET

Forskellene i de nationale love og mangelen på ensartet beskyttelse i Fællesskabet

Beskyttelsen af personer med hensyn til personoplysninger behandles vidt forskelligt i medlemsstaterne. Forskellen kommer af, at der i nogle medlemsstater ikke findes nogen specifik lovgivning på området, og af, at når der findes sådan lovgivning, har den forskelligt indhold.

For øjeblikket finder der specifik lovgivning i syv medlemsstater (Tyskland, Danmark, Frankrig, Irland, Luxembourg, Nederlandene og Det Forenede Kongerige). I visse andre medlemsstater arbejdes der med at udarbejde sådan lovgivning.

Selv om sigtet med den nationale lovgivning er det samme, nemlig at beskytte den registrerede person, er de løsninger, der vælges til at sikre dette, vidt forskellige, fordi der findes en lang række mulige måder at garantere denne beskyttelse på. Således er f.eks. spørgsmålet om, hvorvidt manuelle registre er omfattet, beskyttelsen af juridiske personer, de procedurer, der skal følges forud for oprettelse af et register, omfanget af anmeldelsespligten, oplysningspligten ved indsamling af data, behandlingen af følsomme oplysninger og videregivelse af oplysninger til andre lande blot nogle af de spørgsmål, der behandles vidt forskelligt. Desuden får den teknologiske udvikling medlemsstaterne til at reagere forskelligt, hvilket blot øger forskellene.

Europarådets konvention af 28. januar 1981 om beskyttelse af personer i forbindelse med automatiseret behandling af persondata har ikke medført en vis form for udjævning af disse forskelle, dels fordi den lader en lang række valgmuligheder stå åbne for at gennemføre de grundprincipper, den opstiller, og dels fordi den kun er blevet ratificeret af syv medlemsstater (Tyskland, Danmark, Spanien, Frankrig, Irland, Luxembourg og Det Forenede Kongerige), hvoraf én medlemsstat (Spanien) stadig ikke har nogen national lovgivning. Kommissionens henstilling af 29. juli 1981, hvori EF-medlemsstaterne blev opfordret til at ratificere Europarådets konvention, har ikke ændret ved denne situation.

På grund af den vidt forskellige måde, hvorpå dette problemområde er blevet behandlet i medlemsstaterne, er beskyttelsen af personer i forbindelse med behandling af personoplysninger ikke ensartet i alle medlemsstaterne, og beskyttelsesniveauet kan være forskelligt fra én medlemsstat til en anden.

Konsekvenserne af denne situation for Fællesskabet

For Fællesskabet rejser denne situation tre vanskeligheder:

- Mangelen på specifik lovgivning i visse medlemsstater eller lakunerne i de lovgivninger, der findes, stemmer ikke overens med Fællesskabets tro på respekten for de grundlæggende rettigheder, som denne blev understreget i fælleserklæringen fra Europa-Parlamentet, Rådet og Kommissionen af 5. april 1977 om de grundlæggende rettigheder og i stk. 3 i præamblen

til Den Europæiske Fælles Akt. Bortset herfra er respekten for de grundlæggende rettigheder en integreret del af de generelle principper i fællesskabsretten, som det påhviler EF-Domstolen at håndhæve.

- Det synes at være nødvendigt for det indre markeds oprettelse og funktion, at der kan udveksles personoplysninger, forudsat at dette sker uden at krænke den registrerede persons rettigheder. Med den tekniske udvikling, der har fundet sted inden for informationsbehandling, ikke mindst med etableringen af digitale telekommunikationsnet i Fællesskabet, viser informationsstrømmens grænseoverskridende dimension sig på tre niveauer:

  . Personoplysninger bruges på flere forskellige stadier af økonomiske aktiviteter. En forudsætning for at sikre fri bevægelighed for varer, personer, tjenesteydelser og kapital er, at økonomiske aktører med grænseoverskridende aktiviteter kan udveksle personoplysninger.
  . Integrationsprocessen inden for Fællesskabet, ikke mindst afskaffelsen af grænsekontrollen, medfører nødvendigvis et mere intensivt samarbejde mellem medlemsstaternes offentlige administrationer. En national administration pålægges derved at udføre opgaver, som hører under en anden medlemsstats administration. Derved bliver informationsudveksling er nødvendig forudsætning for samarbejdet. Derfor kræver den forpligtelse til at samarbejde eller udveksle oplysninger, som fællesskabsretten pålægger de nationale administrationer, at der sideløbende må tilvejebringes fuld personbeskyttelse for de involverede personer.
  . Udveksling af oplysninger er ligeledes nødvendig i forbindelse med det videnskabelige samarbejde.

  Behovet for udveksling af oplysninger mellem medlemsstaterne støder for øjeblikket på det problem, at beskyttelsen af personer i forbindelse med behandlingen af personoplysninger er så uensartet i de forskellige medlemsstater. Denne forskel i beskyttelsen kan føre til, at en medlemsstat opstiller hindringer for udvekslingen af oplysninger uder påberåbelse af, at beskyttelsen i den stat, hvor oplysningerne stammer fra, eller som oplysningerne er bestemt til, er utilstrækkelig eller helt mangler.

- Denne forskel i beskyttelsen vil endvidere i visse tilfælde kunne fordreje konkurrencen mellem de private virksomheder alt efter, hvor strenge restriktioner de er underlagt i deres land.

III. DEN VALGTE FREMGANGSMÅDE

<u>En ensartet beskyttelse i Fællesskabet</u>

For at beskytte enhver, der er bosiddende i Fællesskabet, i forbindelse med behandlingen af personoplysninger og give mulighed for udveksling af denne type oplysninger mellem medlemsstater må der etableres et ensartet beskyttelsesniveau i hele Fællesskabet. Med henblik herpå er det nødvendigt at tilvejebringe en indbyrdes tilnærmelse af medlemsstaternes lovgivning. I Kommissionens arbejdsprogram for 1990 er databeskyttelse endvidere nævnt som en prioriteret opgave i forbindelse med oprettelsen af det indre marked[1].

1) EF-Bull. supplement 1/90, s. 18, 26 og 28.

Artikel 100 A i Traktaten udgør i denne forbindelse det rette retsgrundlag i det omfang, et ensartet, højt beskyttelsesniveau er en nødvendig forudsætning for at oprette det indre marked. For at det indre marked, defineret i artikel 8 A som "et område uden indre grænser med fri bevægelighed for varer, personer, tjenesteydelser og kapital i overensstemmelse med bestemmelserne i denne Traktat", kan oprettes og fungere, kræves af de ovenfor anførte grunde, at der sker en indbyrdes tilnærmelse af medlemsstaternes lovgivning på dette område.

Ved udarbejdelsen af dette forslag har Kommissionen taget hensyn til kravene i artikel 8 C i EØF-Traktaten og har draget den konklusion, at særbestemmelser eller undtagelser ikke synes hensigtsmæssige eller begrundede på dette stadium. Kommissionen har endvidere undersøgt problemet med det høje sundheds-, sikkerheds-, miljø- og forbrugerbeskyttelsesniveau, der kræves i EØF-Traktatens artikel 100 A, stk. 3.

Et højt beskyttelsesniveau

Eftersom sigtet med medlemsstaternes lovgivning på dette område er at beskytte de grundlæggende rettigheder, navnlig retten til privatlivets fred, må formålet med en indbyrdes tilnærmelse af lovgivningen være at garantere et højt beskyttelsesniveau. Bortset fra de tilpasninger, der er en uundgåelig følge af enhver indbyrdes tilnærmelse af lovgivning, må tilnærmelsen ikke medføre en forringelse af den allerede sikrede beskyttelse i medlemsstaterne.

De generelle principper, der er opstillet i Europarådets konvention, bør tjene som reference, fordi de i forvejen udgør det fælles grundlag for lovgivningen i de lande, der har ratificeret den. Derfor har man i direktivet valgt løsninger, der stemmer overens med konventionen, og samtidig suppleret dens generelle principper med yderligere bestemmelser for at sikre et ensartet, højt beskyttelsesniveau.

For at sikre et højt beskyttelsesniveau kræves, at den beskyttelse, der garanteres ved direktivet, spænder vidt, og at alle situationer, hvor behandlingen af personoplysninger kan indebære en risiko for at krænke den registrerede person, er omfattet. Dette er baggrunden for, at direktivet dækker såvel manuelle registre som edb-registre samt såvel offentlige som private registre.

Direktivets principper, navnlig dem, der opstilles for behandlingens legitimitet, videregivelse af oplysninger til tredjemand, anmeldelsesprocedurerne, den registrerede persons rettigheder og oplysningernes pålidelighed, tager sigte på at sikre et højt beskyttelsesniveau, hvori de forskellige løsninger, man har valgt i medlemsstaternes lovgivning, har tjent som reference. Man har ligeledes gjort sig særlige anstrengelser ved valget af de midler - ud over de sædvanlige mekanismer til kontrol af fællesskabsrettens gennemførelse - der skal benyttes for at sikre en effektiv gennemførelse af direktivets bestemmelser. De bestemmelser, hvorved der nedsættes en Gruppe til Beskyttelse af Personoplysninger og redegøres for dets ansvarsområde, er en afspejling heraf.

Direktivets principper vil efter behov kunne suppleres med andre. Med henblik herpå fastsættes det i adskillige af direktivets bestemmelser, at medlemsstaterne kan afsætte nærmere regler for registre, der er underlagt deres lovgivning. Det kan ligeledes være nødvendigt at iværksætte supplerende foranstaltninger for at bringe nogle af de generelle principper i anvendelse i sektorer, hvor der gælder særlige forhold.

IV. GENNEMGANG AF DE ENKELTE BESTEMMELSER

KAPITEL I

Almindelige bestemmelser

Artikel 1

Direktivets sigte

Denne artikel indeholder bestemmelse om, at medlemsstaterne har pligt til at beskytte personer i forbindelse med behandlingen af personoplysninger i henhold til direktivets bestemmelser. Eftersom der i kraft af direktivet sikres en beskyttelse, der følger de samme principper i alle medlemsstater og således er ensartet, må medlemsstaterne ikke længere på de af direktivet omfattede områder indskrænke den frie udveksling af oplysninger under henvisning til beskyttelsen af den registrerede person. Beskyttelsen af personer og den frie udveksling af oplysninger er ved direktivet imidlertid kun garanteret på de af dette omfattede områder. Derfor er registre, der føres til private formål, eller registre, der føres af almennyttige foreninger, ikke omfattet af bestemmelserne i denne artikel, eftersom de ved artikel 3, stk. 2, udelukkes fra direktivets anvendelsesområde.

Artikel 2

Definitioner

Denne artikel har til formål at definere de vigtigste begreber i direktivet. Definitionerne svarer til dem, der benyttes i konvention 108 fra Europarådet, men er dog tilpasset og præciseret i det omfang, dette er nødvendigt for at sikre et ensartet, højt beskyttelsesniveau i Fællesskabet.

a) "Personoplysninger". Som i konvention 108 benyttes en bred definition for at dække alle former for oplysninger, der kan knyttes til en person. Faktisk kan enhver oplysning om en person, selv en tilsyneladende harmløs oplysning (f.eks. en simpel postadresse), være af følsom karakter alt efter, hvilken brug der gøres af den. For at forhindre, at man med indirekte identifikationsmetoder kan omgå definitionen, præciseres det, at en person, der kan identificeres ved henvisning til et nummer eller en oplysning af lignende art, betragtes som identificerbar.

b) "Anonymisere". Dette begreb har til formål at gøre det muligt at undtage oplysninger, der ikke længere kan knyttes til en identificerbar person, fra at falde ind under visse af direktivets bestemmelser. En oplysning kan betragtes som anonymiseret, selv om den i teorien på ny ville kunne knyttes til en person, men kun ved en uforholdsmæssig stor indsats i teknisk henseende eller i form af penge.

c) "Register over personoplysninger". Kriteriet for definitionen er muligheden for adgang til personoplysninger, enten manuelt gennem indsamling af strukturerede oplysninger eller ved hjælp af edb på en sådan måde, at oplysninger, der forekommer spredt, kan samles på ny, eller at oplysninger kan uddrages af en tekstmelhed gennem en konsultation, der svarer til den, der giver adgang til registret.
Definitionen omfatter således strukturerede hulkortregistre og manuelle registre. Individuelle sagsakter, herunder bl.a. administrative sagsakter, der ikke indeholder en struktureret samling af personoplysninger, er ikke omfattet på grund af den særlige og indbyrdes forskellige lovgivning, der gælder for disse i medlemsstaterne.

d) "Behandling". Ved i denne definition at opregne de vigtigste behandlingsmåder tilpasses definitionen i konventionen til det bredere anvendelsesområde, som begrebet register omfatter. Samkøring af data er omfattet, fordi det derved er muligt at frembringe nye data (f.eks. elektroniske personprofiler). Ved "blokering" forstås det forhold, at adgangen til data er blokeret på anden måde end gennem de normale sikkerhedsforanstaltninger, uden at dataene derved er slettet.

e) "Den registeransvarlige". Begrebet "registerfører" ("maître du fichier") fra konventionen er blevet tilpasset på to måder: for det første ved at henvise til fællesskabsretten med henblik på de tilfælde, hvor særdirektiver indeholder materielle bestemmelser om beskyttelse af personoplysninger, og for det andet ved at præcisere, at den, der giver tilladelse til, at et register kan konsulteres, navnlig ved on-line konsultation, er den registeransvarlige.

f) "Tilsynsmyndighed". I denne definition understreges det, at myndigheden skal være uafhængig, og der henvises til artikel 26, hvori tilsynsmyndighedens opgaver er beskrevet nærmere.

g) og h) "Den offentlige sektor" og "den private sektor". Den omstændighed, at begreberne den offentlige sektor og den private sektor er defineret i direktivet, er begrundet i, at nogle af dets bestemmelser kun gælder for den ene af disse sektorer (kapitel II og III om legitimiteten af behandlingen af personoplysninger i henholdsvis den offentlige sektor og den private sektor). Definitionen tager udgangspunkt i arten af den tjenesteydelse, der leveres af det pågældende organ, og tager ikke hensyn til, om organet har privatretlig eller offentligretlig status. Organet skal alt efter, om det driver handelsvirksomhed eller varetager offentlige myndighedsopgaver, opfylde de specifikke regler, der gælder for henholdsvis den private sektor eller den offentlige sektor.

Artikel 3

Anvendelsesområde

Direktivet gælder for alle registre, hvor den ansvarlige hører til den private sektor eller den offentlige sektor. For sidstnævntes vedkommende indebærer varetagelsen af en lang række administrative opgaver, ikke mindst i kraft af fællesskabsretten, at der etableres et samarbejde mellem medlemsstaternes administrationer. Offentlige registre, der vedrører forhold, der ikke henhører under fællesskabsrettens anvendelsesområde, er dog ikke omfattet. Dette gælder for registre, der udelukkende føres med henblik på aktiviteter, der ikke falder ind under fællesskabsrettens anvendelsesområde (f.eks. efterretningstjenesterne).

Stk. 2 omtaler to undtagelser, der er begrundet i det forhold, at det er lidet sandsynligt, at der her forekommer krænkelser af privatlivets fred, dels fordi det drejer sig om en fuldstændig privat brug af data, f.eks. personlige elektroniske kalendere, dels fordi det drejer sig om registre over medlemmer af foreninger, som ved selve deres indmeldelse i foreningen må formodes at meddele deres samtykke til at stå registreret i registret, og hvis oplysninger ikke videregives til tredjemand.

Artikel 4

Gældende ret

I denne artikel fastsættes de tilknytningskriterier, der er bestemmende for, om direktivets bestemmelser finder anvendelse i en medlemsstat. Baggrunden for at vælge de kriterier, der er anført i stk. 1, er, at man har ønsket at undgå, at en registreret person kan unddrages beskyttelse, specielt ved omgåelse af lovgivningen. Derfor har man lagt sig fast på det kriterium, at det sted, hvor registret reelt er placeret, er afgørende. Med henblik herpå betragtes hver enkelt del af et register, der er placeret flere forskellige steder enten inden for et lands grænser eller i flere forskellige medlemsstater, som et selvstændigt register.

Det samme ønske om at beskytte den registrerede person i tilfælde af en permanent flytning af et register er forklaringen på bestemmelsen om, at en bruger, der konsulterer et register, der er placeret i et tredjeland, fra en terminal, der befinder sig i en medlemsstat, skal opfylde direktivets bestemmelser om behandlingens legitimitet, om oplysningspligt over for den registrerede person ved videregivelse af oplysninger, om følsomme oplysninger, om datasikkerhed og om ansvar. Dette gælder dog ikke, hvis brugen kun forekommer lejlighedsvis.

I betragtning af, at registre nemt kan flyttes, udgør en midlertidig flytning af et register ikke en ændring af dets placering. Flytning af det hjælpeudstyr, hvori oplysningerne er registreret, må ikke give anledning til, at nye formaliteter kræves opfyldt i forhold til dem, der allerede er opfyldt i den stat, hvor registret er placeret permanent.

Formålet med bestemmelserne i denne artikel er også at undgå kumulativ anvendelse af flere forskellige lovgivninger.

KAPITEL II

Legitim behandling af personoplysning i den offentlige sektor

Behandling af personoplysninger må kun finde sted, hvis denne er legitim. I dette kapitel samt i kapitel III fastsættes de betingelser, hvorunder en behandling anses for legitim. Legitimiteten kan afhængigt af det konkrete tilfælde bero på den registrerede persons samtykke, på en bestemmelse i direktivet eller fællesskabsretten eller på en national retsakt.

Artikel 5

Principper

I denne artikel bestemmes det, at oprettelse af et offentligt register og

enhver anden behandling af personoplysninger kun er legitim, hvis dette er nødvendigt af hensyn til en registeransvarlig offentlig myndigheds varetagelse af sine opgaver.

Der er anført fire tilfælde, hvor behandling af personoplysninger kan finde sted til andre formål end det, med henblik på hvilket registret er oprettet: hvis den registrerede person meddeler sit samtykke hertil, hvis behandlingen sker med hjemmel i en retsforskrift, hvis den registrede persons legitime interesser efter en afvejning af de involverede interesser tilsyneladende ikke taler herimod, og endelig hvis der består en overhængende trussel mod den offentlige orden eller en grov krænkelse af andres rettigheder.

Disse principper vedrører ikke det specifikke tilfælde, hvor oplysninger videregives til tredjemand, i hvilket tilfælde bestemmelserne i artikel 6 finder anvendelse.

Artikel 6

Behandling af personoplysninger i den offentlige sektor med henblik på videregivelse af sådanne oplysninger

Det er nødvendigt med en særlig bestemmelse om videregivelse af oplysninger til tredjemand, fordi denne form for behandling indebærer den største risiko for den registrerede person. I bestemmelsen anføres to tilfælde, hvor personoplysninger kan videregives til tredjemand alt efter, om modtageren hører til den offentlige sektor eller den private sektor. I førstnævnte tilfælde skal videregivelse være nødvendig af hensyn til de opgaver, den forvaltning, der videregiver eller anmoder om videregivelse af oplysningerne, varetager; i sidstnævnte tilfælde skal der foretages en afvejning af de involverede interesser med henblik på at afgøre, om den, der anmoder om oplysningerne, har en begrundet legitim interesse, eller om den registrerede persons interesser går forud herfor.

Medlemsstaterne kan i deres lovgivning fastsætte de nærmere vilkår, hvorunder videregivelse er legitim inden for grænserne af de to ovenfor anførte principper. Dette kan f.eks. bestå i at præcisere, på hvilke områder og i hvilke tilfælde den registrerede persons interesser går forud.

For at sikre, at muligheden for videregivelse af personoplysninger fra private registre ikke er til skade for den registrerede persons interesser, er der fastsat en pligt til at underrette denne. Der er dog mulighed for at fravige denne oplysningspligt, hvis tilsynsmyndigheden giver tilladelse hertil. Denne kan knytte betingelser til tilladelsen eller beslutte selv at underrette den registrerede person.

Artikel 7

Anmeldelsespligt over for tilsynsmyndigheden

Den i denne artikel fastsatte pligt til at foretage anmeldelse til et register, der føres af tilsynsmyndigheden, gælder kun for offentlige registre, hvis personoplysninger vil kunne videregives. Dette tager sigte på at tilvejebringe det mindstemål af gennemsigtighed, der er nødvendigt af hensyn til den registrerede persons udøvelse af sine rettigheder, samtidig med at de forudgående formaliteter begrænses mest muligt, idet disse ville påføre tilsynsmyndigheden en betydelig arbejdsbyrde, ikke mindst i betragtning af den brede definition af et register. Medlemsstaterne har dog mulighed for at udvide anmeldelsespligten til at gælde andre offentlige registre.

KAPITEL III

Legitim behandling af personoplysninger i den private sektor

Artikel 8

Principper

Legitimiteten af behandling af personoplysninger i den private sektor kan bero på den registrerede persons samtykke. Samtykke skal meddeles i overensstemmelse med bestemmelserne i artikel 12 om samtykke på et velinformeret grundlag og i artikel 13 om oplysningspligt ved indsamling af oplysninger.

Foreligger der ikke samtykke fra den registrerede person, kan behandlingens legitimitet bero på et kontraktlignende forhold mellem den registeransvarlige og den registrerede person i det omfang, behandlingen er nødvendig af hensyn til kontraktens fuldbyrdelse (f.eks. behandling af ordrer eller fakturering).

Behandlingens legitimitet kan ligeledes bero på den omstændighed, at oplysningerne stammer fra offentligt tilgængelige kilder (offentligt tilgængelige fortegnelser) i det omfang, behandlingen udelukkende sker med henblik på korrespondance.

Endelig kan behandlingens legitimitet bero på en interesseafvejning, som viser, at den registeransvarlige har en legitim interesse, og at den registrerede person ikke har en interesse, der går forud herfor.

Videregivelse af oplysninger er kun legitim, hvis den sker i overensstemmelse med registrets anvendelsesformål, således som dette er blevet anmeldt (artikel 11, stk. 2) og opfyldt i forbindelse med registreringen af oplysninger (artikel 16, stk. 1, litra b)). I tilfælde af videregivelse er den registeransvarlige endvidere underlagt en forpligtelse til at underrette den registrerede person, jf. artikel 9 og 10. Medlemsstaterne kan i deres lovgivning fastsætte nærmere betingelser for legitimiteten inden for rammerne af de principper, der er anført ovenfor. Dette kan f.eks. bestå i at præcisere, på hvilke områder og i hvilke tilfælde den registrerede persons interesser går forud.

Artikel 9

Oplysningspligt over for den registrerede person

For at give den registrerede person mulighed for at udøve sine rettigheder skal den registeransvarlige ifølge stk. 1 underrette den registrerede person, når der videregives oplysninger vedrørende ham. Den registrerede person kan endvidere gøre krav på aktindsigt og modsætte sig den pågældende behandling. Oplysningspligten over for den registrerede person gælder ikke, når oplysningerne stammer fra offentligt tilgængelige kilder, og behandlingen alene sker med henblik på korrespondance.

Artikel 10

Fravigelse af oplysningspligten over for den registrerede person i særlige tilfælde

Ved denne artikel gives der medlemsstaterne mulighed for at fastsætte

bestemmelser i deres lovgivning om, at tilsynsmyndigheden, når opfyldelse af oplysningspligten over for den registrerede person er forbundet med betydelige praktiske problemer eller strider mod tungtvejende legitime interesser hos den registeransvarlige eller lignende interesser hos tredjemand, på den registeransvarliges anmodning kan give tilladelse til at fravige oplysningspligten over for den registrerede person. Tilsynsmyndigheden kan inden for rammerne af den lovgivning, hvorved den bemyndiges hertil, præcisere, på hvilke betingelser fravigelsen indrømmes, og beslutte selv at underrette den registrerede person.
Ved betydelige praktiske problemer forstås f.eks. oplysninger om personer, hvis private adresse ikke er kendt.

Artikel 11

Anmeldelsespligt over for tilsynsmyndigheden

Af de samme årsager som dem, der ligger til grund for anmeldelsespligten i den offentlige sektor (artikel 7), gælder anmeldelsespligten i den private sektor ikke for registre, hvis oplysninger ikke skal videregives eller stammer fra offentligt tilgængelige kilder. Anmeldelsen skal foretages på ny, hvis registret skifter anvendelsesformål.

Ved anmeldelse skal der afgives alle oplysninger, der er nødvendige for at påse, at bestemmelserne i dette direktiv er overholdt (dvs. i hvert fald den registeransvarliges navn og adresse, registrets anvendelsesformål, en beskrivelse af, hvilken type oplysninger det indeholder, hvilke tredjemænd oplysningerne vil kunne videregives til, og en beskrivelse af sikkerhedsforanstaltningerne). Medlemsstaterne kan udvide anvendelsesområdet for anmeldelsespligten.

KAPITEL IV

Den registrerede persons rettigheder

Artikel 12

Den registrerede persons samtykke

I denne bestemmelse fastsættes det, under hvilke forhold en registreret persons samtykke til behandling af oplysninger vedrørende ham selv i såvel den offentlige som den private sektor har retsgyldighed.

Den registrerede persons samtykke til, at oplysninger vedrørende ham selv behandles, er afgørende som legitimation for, at den registeransvarlige behandler personoplysninger. Ved "samtykke" i artikel 12's forstand forstås "samtykke på et velinformeret grundlag". For at sætte den registrerede person i stand til at foretage en afvejning af risici og fordele ved den påtænkte behandling af oplysninger vedrørende ham selv og at udøve sine rettigheder i henhold til artikel 14 i direktivet (berigtigelse, sletteise, blokering), skal den registeransvarlige meddele den registrerede person alle oplysninger, der er relevante for den pågældende beslutning, herunder bl.a. den registeransvarliges navn og adresse, registrets anvendelsesformål, hvilke oplysninger der er indholdt i registret osv.

Hvad angår den form, hvori samtykket skal meddeles, stilles der i direktivet af praktiske grunde ikke krav om, at den registrerede person meddeler samtykke skriftligt. Samtykke skal dog være udtrykkeligt. Samtykke fra den registrerede person skal desuden være specifikt i den forstand, at det skal vedrøre behanding af oplysninger vedrørende den registrerede person gennem en ganske bestemt registeransvarlig og til et eller flere ganske bestemte formål. Endvidere skal samtykket nøje angive, hvilke typer oplysninger der

må gøres til genstand for behandling, hvilken type behandling, der accepteres, og hvilke potentielle modtagere oplysningerne må videregives til.

I henhold til artikel 12, litra c), har den registrerede person ret til til enhver tid at tilbagekalde samtykke. Tilbagekaldelsen har dog ingen tilbagevirkende kraft, idet en tidligere ellers lovlig behandling af personoplysninger derved ville blive gjort ulovlig.

Artikel 13

Oplysningspligt over for den registrerede person
ved indsamling af oplysninger

For at sikre en effektiv databeskyttelse må den registrerede person være fuldt informeret om, hvilken behandling oplysninger vedrørende ham selv gøres til genstand for, ikke blot når disse oplysninger allerede er registreret og behandlet i en datafil, men allerede i stadiet forud for behandlingen af oplysninger, nemlig ved indsamlingen af personoplysninger.

I henhold til artikel 16, stk. 1, litra a), skal indsamling af oplysninger udføres loyalt og på lovlig vis. I artikel 13 er fastsat de krav, der gælder for den situation, hvor der indsamles oplysninger hos den registrerede person selv.
En loyal og lovlig indsamling af personoplysninger forudsætter, at den registrerede person træffer sin beslutning om, hvorvidt han skal afgive oplysninger om sig selv ved indsamlingen, på et pålideligt faktuelt grundlag med hensyn til behandlingens formål, den registeransvarliges identitet og spørgsmålet om, hvorvidt han er forpligtet ved lov til at afgive oplysningerne, eller om afgivelse af oplysninger er frivillig. For at udøve de rettigheder, der er indrømmet den registrerede person i henhold til direktivets artikel 14, og føre en effektiv kontrol med, hvilken brug der gøres af oplysninger vedrørende ham selv, skal han ligeledes underrettes om sin ret til aktindsigt og til berigtigelse samt om, hvem modtagerne er i forbindelse med videregivelse af oplysninger. Ved artikel 13, stk. 1, i direktivet forpligtes medlemsstaterne til at fastsætte bestemmelser i deres nationale databeskyttelseslovgivning om, at den registrerede person får disse oplysninger.
De personer, der indsamler oplysninger, vil hyppigt ikke være de samme som dem, der er ansvarlige for det register, hvori oplysningerne i sidste ende registreres og behandles. For at kunne udøve sine rettigheder over for disse personer er det vigtigt, at den registrerede person oplyses om disses navn og adresse på dataindsamlingstidspunktet.

Ved artikel 13, stk. 2, bemyndiges medlemsstaterne til at begrænse oplysningspligten over for den registrerede person i forbindelse med indsamling af oplysninger, når der er tale om afgørende hensyn til offentlige interesser. Ifølge denne bestemmelse finder pligten til at afgive de i artikel 13, stk. 1, anførte oplysninger til den registrerede person ikke anvendelse, hvis oplysningspligten forhindrer en offentlig myndighed i at varetage dens tilsyns- og kontrolopgaver eller opretholde den offentlige orden.

Artikel 14

Supplerende rettigheder indrømmet den registrerede person

Artikel 14 i direktivet indeholder bestemmelser om den registrerede persons rettigheder og krav over for den registeransvarlige. Databeskyttelse har til formål at beskytte den registrerede persons ret til privatlivets fred. Derfor udgør dennes rettigheder og krav over for den registeransvarlige et fundamentalt element i databeskyttelsen.

Artikel 14, stk. 1, giver den registrerede person ret til af legitime grunde at modsætte sig, at personoplysninger vedrørende ham selv gøres til genstand for behandling.
Ved legitime grunde forstås i denne bestemmelse manglende lovhjemmel til at foretage en bestemt behandling af personoplysninger, f.eks. fordi kravene i kapitel II og III i direktivet vedrørende behandlingens legitimitet ikke er opfyldt i forbindelse med en bestemt behandling af personoplysninger.

Artikel 14, stk. 2, beskytter den registrerede person mod at underlægges afgørelser truffet af et organ henhørende under den offentlige eller den private sektor, der indebærer en vurdering af hans adfærd, der alene er begrundet i, at personoplysninger vedrørende ham selv med en beskrivelse af hans karakteregenskaber eller personlighed skal behandles elektronisk. Sigtet med bestemmelsen er at beskytte den registrerede persons interesser ved at lade ham deltage i beslutninger, der er af betydning for ham. Magtfulde offentlige og private organers omfattende brug af dataprofiler om enkeltpersoner berøver den enkelte mulighed for at påvirke beslutningsprocesserne inden for disse organisationer, hvis sådanne beslutninger alene træffes på grundlag af den pågældendes "data shadow".

For effektivt at kunne udøve sin ret til berigtigelse, sletteIse eller blokering af oplysninger over for den registeransvarlige er det afgørende for den registrerede person, at han har adgang til registeroplysningerne, hvilket indrømmes ham ved artikel 14, stk. 3 og 4. Ved artikel 14, stk. 3, indrømmes den registrerede person ret til at blive informeret af den registeransvarlige om relevante forhold vedrørende behandlingen af personoplysninger vedrørende ham selv, så han bliver i stand til at fremsætte krav om berigtigelse, sletteIse og blokering og at øve effektiv kontrol med, hvilken behandling personoplysninger vedrørende ham selv gøres til genstand for. Ved artikel 14, stk. 4, indrømmes den registrerede person ret til med rimelige mellemrum og uden større ventetid eller udgifter at få bekræftet, hvorvidt der er registreret personoplysninger vedrørende ham selv i et register, samt, hvis dette er tilfældet, at blive gjort bekendt med disse oplysninger i letforståelig form. Bestemmelserne i artikel 14, stk. 3 og 4, overlader det til medlemsstaterne at afgøre, hvordan disse oplysninger bringes til den registrerede persons kendskab.
Hvad der skal forstås ved "rimelige mellemrum" fastlægges ligeledes i medlemsstaternes nationale lovgivning. Ved en afvejning af den registrerede persons og den registeransvarliges interesser kan medlemsstaternes lovgivning bestemme, at den registeransvarlige over for den registrerede person kun må kræve betaling for de med dennes udøvelse af retten til aktindsigt forbundne udgifter, som ikke må være uforholdsmæssigt store.

Ved artikel 14, stk. 4, gives medlemsstaterne hjemmel til ved en særbestemmelse at fastsætte, at den registrerede persons ret til aktindsigt ikke finder anvendelse, når det drejer sig om helbredsoplysninger. For at beskytte den registrerede person mod psykiske chok, der i ekstreme tilfælde kan føre til selvmordsforsøg, kan oplysninger af denne art kun udleveres til ham gennem en læge.

Ved artikel 14, stk. 5, i direktivet indrømmes der den registrerede person ret til berigtigelse, sletteIse og blokering af oplysninger, hvis behandlingen af dem er uforenelig med direktivets bestemmelser.
Den registrerede person kan fremsætte krav om berigtigelse, hvis oplysninger vedrørende ham selv er urigtige, ufuldstændige, unøjagtige, vildledende eller forældede. Den registrerede persons ret til at få oplysninger slettet eller blokeret forudsætter, at oplysningerne er gjort til genstand for en behandling, der er i strid med direktivets bestemmelser. Med henblik herpå henviser artikel 14, stk. 5, til alle de bestemmelser i direktivet, der vedrører indsamling, opbevaring, behandling og brug af personoplysninger.

Begrebet blokering stammer fra den tyske databeskyttelseslov (§§ 14, 27 og 35 i BDSG: "Sperrung"). Ved blokering af data - fordi de er blevet indsamlet, opbevaret, behandlet eller brugt i strid med direktivets bestemmelser - er det fortsat tilladt den registeransvarlige at opbevare dem i sit register, men det er forbudt at behandle eller bruge dem og navnlig at videregive dem til trejdemand. Data, der er blokeret, skal være mærket i registret på en sådan måde, at en bruger af registret informeres om blokeringen.

Ved at bruge udtrykket "i givet fald" i direktivet overlades det til medlemsstaterne at fastsætte specifikke regler i deres databeskyttelseslovgivning for den registrerede persons ret til sletteise, blokering eller berigtigelse i de forskellige situationer, hvor personoplysninger behandles og bruges i strid med direktivets bestemmelser.

Ofte behandles oplysninger ikke blot af den registeransvarlige, men videregives til tredjemand. Hvis det pålægges den registeransvarlige at berigtige, slette eller blokere oplysninger, fordi de er urigtige eller er blevet underkastet ulovlig behandling eller brug, er det i den registrerede persons interesse, at tredjemænd, til hvem sådanne oplysninger er videregivet, underrettes om sådan berigtigelse, sletteise eller blokering, således at vedkommende tredjemænd ligeledes kan berigtige, slette eller blokere oplysningerne. Denne interesse hos den registrerede person er beskyttet ved artikel 14, stk. 7.

Artikel 14, stk. 6, giver den registrerede person ret til at få oplysninger vedrørende ham selv slettet i registre, der benyttes til markedsføringsformål og i reklameøjemed med henblik på f.eks. postordreforretninger. Derved kan den registrerede person beskytte sig mod at få tilsendt uønsket reklamemateriale.

Endelig forpligtes medlemsstaterne ved artikel 14, stk. 8, til at give den registrerede person en effektiv klageadgang i tilfælde, hvor den registeransvarlige eller en anden person krænker den registrerede persons rettigheder og krav i henhold til artikel 14 i direktivet.

Artikel 15

Begrænsninger i den registrerede persons adgang til offentlige registre

Ved artikel 15 bemyndiges medlemsstaterne til at begrænse den registrerede persons adgang til registre, når dette sker for at beskytte tungtvejende hensyn til offentlige interesser eller enkeltpersoners interesser, der svarer til den registrerede persons ret til privatlivets fred, forudsat at det drejer sig om offentlige registre. Det er op til medlemsstaterne at afgøre, i hvor stort omfang de - på grundlag af artikel 15 - ønsker at indføre begrænsninger i deres nationale databeskyttelseslovgivning. De begrænsninger, der er anført i denne bestemmelse, omfatter kun dem, der er nødvendige for at beskytte afgørende demokratiske værdier, og skal vedtages ved en formel retsakt. Opregningen af de interesser, der kan begrunde en begrænsning af retten til aktindsigt i medfør af artikel 15 i direktivet, er udtømmende.
Udtrykket "den nationale sikkerhed" skal forstås som beskyttelse af den nationale suverænitet mod indre og ydre trusler.
"Strafferetlig forfølgning" omfatter retsforfølgning af kriminelle handlinger, som allerede er begået, medens begrebet "den offentlige sikkerhed" omfatter statslige organers politimæssige funktioner, herunder kriminalpræventive foranstaltninger.
Udtrykket "en tungtvejende økonomisk eller finansiel interesse hos en medlemsstat eller Det Europæiske Fællesskab" omfatter alle politisk-økonomiske virkemidler og midler til finansiering af en medlemsstats eller Fællesskabets politik, f.eks. valutakontrol, udenrigshandelskontrol,

skatteopkrævning. Det er dog kun en tungtvejende interesse af denne art, der kan begrunde en begrænsning af retten til aktindsigt.
Endelig kan en tredjemands interesser, der svarer til den registrerede persons ret til aktindsigt, eller andres rettigheder og friheder påberåbes som gyldig begrundelse for at begrænse retten til aktindsigt. Det, der særlig tænkes på her, er interesser såsom andres forretningshemmeligheder eller pressefriheden.

Nægtes den registrerede person adgang til oplysninger vedrørende ham selv i et register, fordi det drejer sig om en af de i artikel 15, stk. 1, anførte interesser, er tilsynsmyndigheden på hans forlangende forpligtet til at foretage den nødvendige inspektion og kontrol af det register, hvori disse oplysninger opbevares.
Artikel 15, stk. 3, bemyndiger medlemsstaterne til at begrænse retten til aktindsigt vedrørende oplysninger, der kun opbevares midlertidigt til statistiske formål, idet sådanne operationer kun frembyder en ubetydelig risiko for den registrerede person.

KAPITEL V

Oplysningernes pålidelighed m.v.

De i dette kapitel opstillede principper for databeskyttelse går videre end titlen, idet de ikke blot omfatter oplysningernes pålidelighed (artikel 16), men også behandling af bestemte typer oplysninger, som betragtes som særligt følsomme i forhold til den registrerede persons interesser (artikel 17) og de fornødne datasikkerhedsforanstaltninger (artikel 18).

Artikel 16

Principper

Ved artikel 16 i direktivet forpligtes medlemsstaterne til i deres nationale databeskyttelseslovgivning at indføre de grundlæggende principper vedrørende personoplysningers pålidelighed. Sigtet med disse principper er at sikre den registrerede persons ret til privatlivets fred ved at opstille visse begrænsninger ikke alene for indsamlingen og behandlingen af personoplysninger, men også for, hvad registre over personoplysninger må indeholde.

Artikel 16, stk. 1, litra a), kræver, at indsamling og behandling af personoplysninger skal udføres loyalt og på lovlig vis.
Bestemmelsen dækker behandling af personoplysninger som defineret i artikel 2, litra d), samt indsamling heraf.
Bestemmelsen i artikel 16, stk. 1, litra a), udelukker f.eks. brug af tekniske indretninger, der er skjult for den registrerede person, til hemmeligt og uden dennes vidende at indsamle oplysninger, f.eks. telefonaflytning, anden form for aflytning og lignende metoder. Bestemmelsen forhindrer ligeledes registeransvarlige i at oprette og bruge hemmelige registre indeholdende personoplysninger.

I artikel 16, stk. 1, litra b), fastsættes princippet om formålsspecificering. Ifølge dette princip må personoplysninger kun registreres til nøje definerede, udtrykkeligt angivne og legitime formål.
Formålet med registrering af personoplysninger skal være defineret i den forstand, at formålet med registreringen og brugen af oplysningerne er defineret og specificeret så snævert som muligt. En generel eller vag definition eller beskrivelse af et registers anvendelsesområde (f.eks. "til forretningsformål") er ikke tilstrækkelig til at opfylde princippet om formålsspecificering som fastsat i artikel 16, stk. 1, litra b).
Formålet skal specificeres, forinden der sker registrering. Indsamles oplysningerne hos den registrerede person, stiller artikel 13 krav om, at

formålet skal være fastlagt på det tidspunkt, hvor indsamlingen af oplysninger finder sted. Senere ændring af et registers formål er kun tilladt, hvis ændringen ikke er uforenelig med det oprindelige formål.
Artikel 16, stk. 1, litra b), kræver også, at den registeransvarlige udtrykkeligt angiver formålet med registreringen og brugen af oplysningerne. Kravet om eksplicitering tager sigte på at forhindre, at personoplysninger registreres og bruges til skjulte formål.
Kravet om, at formålet med registrering og brug af personoplysninger skal være legitimt, begrænser de potentielle formål, et register kan tjene; et register kan således kun oprettes og bruges til formål, der er forenelige med bestemmelserne i dette direktiv og medlemsstaternes nationale lovgivning. Endvidere er sådanne formål kun legitime, hvis de er relevante i forhold til de administrative opgaver, en registeransvarlig i den offentlige sektor varetager, eller i forhold til den type erhvervsvirksomhed, en registeransvarlig i den private sektor udøver. Artikel 16, stk. 1, litra b), fastslår klart og tydeligt, at princippet om formålsspecificering ikke kun finder anvendelse ved behandlingen af personoplysninger, men også ved brugen af sådanne oplysninger, som skal være forenelig med registrets anvendelsesformål.

Artikel 16, stk. 1, litra c), bestemmer, at oplysninger i et register skal være fyldestgørende, relevante og nødvendige i forhold til registeringsformålet. Dette princip skal således sikre, at et registers indhold svarer til dets formål.

Kravene i artikel 16, stk. 1, litra b) og c), har nær forbindelse med bestemmelsen i artikel 16, stk. 1, litra d). Personoplysninger i et register skal være korrekte og om nødvendigt ajourføres. Er oplysningerne urigtige eller ufuldstændige i forhold til registrets anvendelsesformål, kræver artikel 16, stk. 1, litra d), at de slettes eller berigtiges.

Artikel 16, stk. 1, litra e), behandler spørgsmålet om, hvor længe personoplysninger må være registreret. Ifølge denne bestemmelse må oplysninger, der giver mulighed for at identificere den registrerede person, kun opbevares så længe, som dette synes at være nødvendigt af hensyn til registreringsformålet.
Der kan forekomme situationer, hvor det f.eks. af statistiske grunde er nødvendigt at opbevare oplysninger længere end dette tidsrum. I så tilfælde er det af afgørende betydning for beskyttelsen af den registrerede person, at enhver forbindelse mellem hans navn og de øvrige oplysninger fjernes.

Artikel 16, stk. 2, forpligter den registeransvarlige til at påse, at bestemmelserne om oplysningernes pålidelighed i artikel 16, stk. 1, overholdes.

Artikel 17

Særlige kategorier af oplysninger

Det er et almindeligt anerkendt synspunkt, at retten til privatlivets fred ikke krænkes ved personoplysningers art, men snarere ved den sammenhæng, hvori personoplysningerne gøres til genstand for behandling. Der er dog bred enighed blandt medlemsstaterne om, at visse kategorier af oplysninger ved deres art - og uanset den sammenhæng, hvori de gøres til genstand for behandling - indebærer en risiko for at krænke den registrerede persons ret til privatlivets fred. Derfor fastsættes der i artikel 17 i direktivet snævre grænser for elektronisk behandling og udnyttelse af følsomme oplysninger i registre over personoplysninger.

Følgende kategorier af oplysninger anføres i artikel 17 som følsomme: oplysninger om race (herunder oplysning om hudfarve), oplysninger om politisk, religiøs og filosofisk overbevisning (herunder oplysning om, at en person ikke har nogen religiøs overbevisning, samt oplysninger om den registrerede persons aktiviteter i tilknytning til hans politiske, religiøse eller filosofiske overbevisning), oplysninger om medlemskab af fagforeninger, helbredsoplysninger om den registrerede person (herunder oplysninger om dennes fortidige, nuværende og fremtidige fysiske og psykiske helbredstilstand og oplysninger om narkotika- og alkoholmisbrug) samt oplysninger om seksuelle forhold.

Som hovedregel forbyder artikel 17, stk. 1, edb-behandling af følsomme oplysninger. Undtagelser fra denne regel kan tillades, hvis den registrerede person meddeler sit samtykke, som skal afgives frit, udtrykkeligt og skriftligt, og når det drejer sig om den i artikel 17, stk. 2, anførte undtagelse.
Ifølge denne bestemmelse kan medlemsstaterne tillade edb-behandling af følsomme oplysninger under henvisning til afgørende hensyn til samfundsmæssige interesser. En forudsætning for at bringe denne undtagelse i anvendelse er imidlertid, at der som retsgrundlag vedtages en formel lov, hvori det anføres, hvilke typer følsomme oplysninger der må edb-behandles, hvilke personer der har adgang til oplysningerne, samt hvilke sikkerhedsforanstaltninger der er truffet mod misbrug og uberettiget indtrængen.
Artikel 17, stk. 3, er en særbestemmelse om registrering af oplysninger om strafbare forhold. Registrering af sådanne oplysninger i edb-registre er kun tilladt, når det drejer sig om offentlige registre.

Artikel 17's anvendelsesområde er begrænset; den omfatter kun oplysninger, der behandles elektronisk.
Artikel 17 omfatter endvidere ikke edb-registrering og edb-behandling af oplysninger om politisk, religiøs og filosofisk overbevisning og fagforeningsmæssigt tilhørsforhold, når sådanne oplysninger behandles af almennyttige foreninger i henhold til bestemmelserne i artikel 3, stk. 2, litra b).

Artikel 18

Datasikkerhed

Krænkelser af den registrerede persons ret til privatlivets fred kan ikke kun forekomme ved, at den registeransvarlige indsamler, opbevarer, behandler og videregiver oplysninger om den pågældende til egne formål.
Hans ret til privatlivets fred bringes ligeledes i fare, hvis oplysninger vedrørende ham selv misbruges af tredjemand gennem uberettiget adgang til eller brug af oplysningerne.

Bestemmelsen i første punktum i artikel 18, stk. 1, pålægger medlemsstaterne at forpligte den registeransvarlige til at træffe passende organisatoriske og tekniske foranstaltninger til at beskytte oplysningerne i et register mod uberettiget indtrængen fra tredjemands side i registret eller mod hændeligt tab af oplysninger. Dette omfatter tilintetgørelse af oplysninger, hvad enten dette er hændeligt eller sker som følge af uberettiget indtrængen, hændeligt tab samt uberettiget ændring af og adgang til oplysninger og enhver anden uberettiget behandling af oplysninger.
Tekniske datasikkerhedsforanstaltninger omfatter: sikkerhedsforanstaltninger med hensyn til adgang til databehandling og til lagre, identifikationskoder til personer, der har adgang hertil, edb-sikkerhedsforanstaltninger som f.eks. brug af password for at få adgang til edb-registre, omsættelse af data til kode og kontrol med hacking og andre usædvanlige aktiviteter i edb-registret.
Gennem organisatoriske foranstaltninger tager den registeransvarlige proceduremæssige skridt inden for hans offentlige myndigheds eller erhvervsvirk-

somheds hierarki, f.eks. ved at etablere forskellige autorisationsniveauer for adgangen til registret.
Bestemmelsen i andet punktum i artikel 18, stk. 1, specificerer, hvad der betragtes som passende datasikkerhedsforanstaltninger med hensyn til edb-registre. For sådanne registres vedkommende skal foranstaltningerne sikre en passende sikkerhedsstandard, der på den ene side tager hensyn til den bedste disponible teknik inden for datasikkerhed og de med dennes anvendelse forbundne udgifter og på den anden arten af de oplysninger, der er registreret, og en vurdering af de potentielle sikkerhedsrisici. Ved afgørelsen af, om datasikkerhedsforanstaltningerne er passende, skal den registeransvarlige tage hensyn til de henstillinger om edb-sikkerhed og indbyrdes netkompatibilitet, der måtte blive udarbejdet af Fællesskabet i henhold til artikel 29 i direktivet.

Forpligtelsen til at træffe de fornødne sikkerhedsforanstaltninger er ikke begrænset til det sted, hvor behandlingen af oplysninger finder sted, eller til det maskinel og programmel, der benyttes til behandlingen. Sker der en overførsel af data fra én datamat til en anden eller fra en datamat til en terminal via et telenet, skal sikkerhedsforanstaltningerne desuden i henhold til artikel 18, stk. 2, omfatte nettet, så der garanteres en sikker og uafbrudt dataoverførsel.

Artikel 18, stk. 3, vedrører spørgsmålet om en ekstern brugers direkte adgang til et register ved on-line konsultation. Brugerens tilladelse til at indsamle oplysninger fra registret er specificeret i og begrænset ved hans kontrakt med den registeransvarlige. Direktivet pålægger den registeransvarlige at udforme maskinel og programmel, der benyttes til on-line konsultation, på en sådan måde, at brugerens adgang holder sig inden for de grænser, der er fastsat i den registeransvarliges autorisation til brugeren.

I artikel 18, stk. 4, fastsættes det, hvem der er ansvarlig for at påse overholdelse af de ved artikel 18, stk. 1-3, fastsatte forpligtelser. Personer, som faktisk eller i henhold til kontrakt fører tilsyn med registeroperationer, er ligeledes ansvarlige for overholdelse af datasikkerhedskravene. Disse kan alt efter omstændighederne være den registeransvarlige, den bruger, der har adgang til registret ved on-line konsultation, og edb-servicebureauer, der udfører databehandlingsoperationer på den registeransvarliges vegne.

Endelig indeholder artikel 18, stk. 5, en bestemmelse om, at den registeransvarlige ansatte og andre personer, der i embeds medfør har adgang til personoplysninger i et register, er underkastet tavshedspligt. Disse personer må ikke videregive oplysninger, de har adgang til, til tredjemand uden den registeransvarliges samtykke.

KAPITEL VI

Særbestemmelser for visse sektorer

Artikel 19

Medlemsstaterne kan for organer inden for pressen og den audiovisuelle sektor fastsætte bestemmelser, der afviger fra dette direktivs bestemmelser i det omfang, disse er nødvendige for at forene personers grundlæggende

rettigheder, f.eks. retten til privatlivets fred, med informations- og pressefriheden. Der er faktisk konfliktmuligheder mellem de to kategorier af grundlæggende rettigheder. Den løsning, der er valgt, lægger vægt på, at der foretages en afvejning af de involverede interesser i tilfælde af fravigelse. Ved denne afvejning af interesser vil der bl.a. kunne tages hensyn til, om der foreligger klagemuligheder for den registrerede person eller eventuelt ret til at tage til genmæle, om der findes etiske regler, hvilke grænser der er fastat i den europæiske menneskerettighedskonvention og de almindelige retsprincipper.

Artikel 20

Ifølge denne artikel skal medlemsstaterne opfordre de berørte erhvervskredse til at udarbejde en europæisk adfærdskodeks, som kan gøre det lettere at anvende principperne i dette direktiv i visse sektorer.
Kommissionen støtter et sådant initiativ og vil i givet fald tage hensyn til en sådan kodeks i forbindelse med udøvelsen af sine gennemførelsesbeføjelser og udarbejdelsen af nye forslag.

KAPITEL VII

Ansvar og straffebestemmelser

Artikel 21

Ansvar

I tilfælde af krænkelse som følge af overtrædelse af bestemmelserne i dette direktiv påhviler ansvaret herfor, jf. denne artikel, den registeransvarlige, over for hvem den registrerede person kan kræve skadeserstatning. Begrebet krænkelse omfatter både materiel og immateriel skade. Der gælder dog en bestemmelse om, at i tilfælde af tab, tilintetgørelse eller uberettiget indtrængen er den registeransvarlige ansvarsfri, forudsat at han kan bevise, at sikkerhedsforanstaltningerne er overholdt.

Artikel 22

Behandling af oplysninger på den registeransvarliges vegne

Sigtet med denne artikel er at forhindre, at behandling af oplysninger af en tredjemand på den registeransvarliges vegne medfører en forringelse af den registrerede persons beskyttelse. Med henblik herpå pålægges der såvel den registeransvarlige som den tredjemand, der udfører behandlingen, forpligtelser.

Artikel 23

Straffebestemmelser

For at sikre overholdelse af de bestemmelser, der vedtages i medfør af dette direktiv, forpligtes medlemsstaterne til at fastsætte effektive sanktioner, f.eks. straffeforanstaltninger, under særlig hensyntagen til den kendsgerning, at overtrædelse af principperne om beskyttelse af den registrerede person udgør en krænkelse af en grundlæggende rettighed.

KAPITEL VIII

Videregivelse af personoplysninger til tredjelande

Artikel 24

Principper

Ved denne artikel fastsættes det princip, at videregivelse af personoplysninger fra en medlemsstat til et tredjeland ikke må finde sted, medmindre dette land sikrer et passende beskyttelsesniveau. Det påhviler medlemsstaterne og eventuelt Kommissionen at afgøre, om et land sikrer et passende beskyttelsesniveau. Medlemsstaterne skal underrette Kommissionen, hvis et modtagende tredjeland ikke sikrer et passende beskyttelsesniveau. I så tilfælde kan der indledes en forhandlingsprocedure mellem Kommissionen og det pågældende tredjeland.
Kommissionen kan i medfør af de gennemførelsesbeføjelser, der tillægges den ved artikel 29, træffe beslutning om, at et land sikrer et passende beskyttelsesniveau på grundlag af dets nationale lovgivning eller internationale forpligtelser, som dette land har indgået. Europarådets konvention af 28. januar 1981 om beskyttelse af personer i forbindelse med behandling af persondata hører blandt de forpligtelser, som Kommissionen vil tage i betragtning. Den vil i denne forbindelse ligeledes kunne høre de sagkyndige medlemmer af Gruppen til Beskyttelse af Personoplysninger.

Artikel 25

Fravigelse

Selv om et tredjeland ikke sikrer et passende beskyttelsesniveau, er der mulighed for at indrømme en fravigelse for en specifik videregivelse af oplysninger til dette land. Den medlemsstat, hvor registret befinder sig, kan give tilladelse til en sådan videregivelse af oplysninger, hvis den registeransvarlige kan garantere et passende beskyttelsesniveau for den pågældende videregivelses vedkommende, og hvis de øvrige medlemsstater eller Kommissionen ikke modsætter sig dette. Med henblik herpå er der fastsat bestemmelser om en informationsprocedure med en indsigelsesfrist på ti dage. I tilfælde af indsigelse kan Kommissionen træffe passende foranstaltninger, herunder bl.a. træffe beslutning om at forbyde videregivelsen af oplysninger.

KAPITEL IX

Tilsynsmyndighed og Gruppen til Beskyttelse af Personoplysninger

Artikel 26

Tilsynsmyndighed

Ved denne artikel oprettes en tilsynsmyndighed, der er kendetegnet ved at være uafhængig og besidde undersøgelses- og interventionsbeføjelser, der er tilpasset de tilsynsopgaver, der tillægges. Disse to kendetegn skal være garanteret ved national lov. Udtrykket "tilsynsmyndighed" udelukker ikke på forhånd muligheden for, at de enkelte medlemsstater alt efter deres forfatningsmæssige opbygning overlader disse opgaver til et flerstrenget internt organ.

Artikel 27

Gruppen til Beskyttelse af Personoplysninger

På grund af den specifikke karakter af hele problematikken omkring beskyttelse af personer med hensyn til personoplysninger nedsættes der ved denne artikel en rådgivende gruppe benævnt Gruppen til Beskyttelse af Personoplysninger. Denne Gruppe til Beskyttelse af Personoplysninger er kendetegnet ved at være uafhængig og består af repræsentanter for de nationale tilsynsmyndigheder. En repræsentant for Kommissionen er formand for gruppen.

Artikel 28

Gruppens opgaver

I denne artikel fastsættes de opgaver, som Gruppen til Beskyttelse af Personoplysninger skal varetage. Gruppen stiller sin viden og sagkundskab inden for området beskyttelse af personer i forbindelse med behandling af personoplysninger til rådighed for Kommissionen. Derved bidrager den til, at de nationale regler, der vedtages til gennemførelse af dette direktiv, fortolkes ensartet. Den vurderer beskyttelsesniveauet i Fællesskabet og i tredjelande og underretter Kommissionen herom. Endelig kan den rådgive Kommissionen om, hvilke supplerende foranstaltninger der bør træffes. Gruppen til Beskyttelse af Personoplysninger kan udarbejde henstillinger, som, hvis den ønsker det, kan forelægges for det rådgivende udvalg, som kommer ind i billedet i forbindelse med Kommissionens gennemførelsesbeføjelser.
Gruppen til Beskyttelse af Personoplysninger udarbejder en årlig rapport om situationen inden for beskyttelse af personoplysninger i Fællesskabet og tredjelande. Denne rapport forelægges Kommissionen.

KAPITEL X

Kommissionens gennemførelsesbeføjelser

Artikel 29 og 30

Udøvelse af gennemførelsesbeføjelserne
Rådgivende udvalg

Ved artikel 29 tillægges Kommissionen gennemførelsesbeføjelser med hensyn til den tekniske tilpasning, der er nødvendig som følge af, at området behandling af personoplysninger spænder vidt og har teknisk karakter.

Eftersom direktivet har til formål at bidrage til det indre markeds oprettelse, er der i artikel 30 fastsat bestemmelser om medvirken fra et udvalg af rådgivende karakter, som har til opgave at bistå Kommissionen i forbindelse med udøvelsen af dens beføjelser, og hvori der anvendes de procedurer, der er fastsat i Rådets afgørelse af 13. juli 1987 om fastsættelse af de nærmere vilkår for udøvelsen af de gennemførelsesbeføjelser, der tillægges Kommissionen.

Forslag til SYN 287

RADETS DIREKTIV

om beskyttelse af personer
i forbindelse med behandling af personoplysninger

RADET FOR DE EUROPÆISKE FÆLLESSKABER HAR -

under henvisning til Traktaten om Oprettelse af Det Europæiske Økonomiske Fællesskab, særlig artikel 100 A og 113,

under henvisning til forslag fra Kommissionen(1),

i samarbejde med Europa-Parlamentet(2),

under henvisning til udtalelse fra Det Økonomiske og Sociale Udvalg(3), og

ud fra følgende betragtninger:

(1) Fællesskabets målsætninger, således som disse er nedfældet i Traktaten, som ændret ved Den Europæiske Fælles Akt, er at gennemføre en stadig snævrere sammenslutning mellem de europæiske folk, at skabe snævrere forbindelser mellem de stater, som Fællesskabet 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 ved medlemsstaternes forfatninger og love samt ved den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder;

(2) det indre markeds oprettelse og funktion, som i henhold til Traktatens artikel 8 A indebærer fri bevægelighed for varer, personer, tjenesteydelser og kapital, forudsætter ikke blot, at personoplysninger kan cirkulere frit, uanset i hvilken medlemsstat de gøres til genstand for behandling, eller fra hvilken medlemsstat de anmodes udleveret, men også, at de grundlæggende rettigheder beskyttes i betragtning af den stadigt hyppigere behandling af personoplysninger inden for de forskellige økonomiske og samfundsmæssige aktivitetsområder i Fællesskabet;

(3) det indre marked indebærer et område uden indre grænser; dette medfører, at det i kraft af anvendelsen af fællesskabsretten stadigt hyppigere er nødvendigt for de forskellige medlemsstaters administrative myndigheder at samarbejde og indbyrdes udveksle personoplysninger for at varetage deres opgaver eller udføre hverv for en administrativ myndighed fra en anden medlemsstat;

(4) udbygningen af det teknisk-videnskabelige samarbejde og den koordinerede etablering af nye telekommunikationsnet i Fællesskabet nødvendiggør og letter personoplysningers frie bevægelighed på tværs af landegrænserne;

(5) forskellen i den beskyttelse af privatlivets fred, medlemsstaterne yder i forbindelse med behandlingen af personoplysninger, kan hindre transmission af oplysninger af denne art fra en medlemsstats område til en anden medlemsstats område; denne forskel kan derfor udgøre en hindring for udøvelsen af en række økonomiske aktiviteter på fællesskabsplan, virke konkurrencefordrejende og hindre de nationale administrationer i at udføre opgaver, der falder ind under fællesskabsrettens anvendelsesområde; denne forskel i beskyttelsesniveauet hidrører fra forskellene i de nationale love og administrative bestemmelser;

(6) for at fjerne hindringerne for den frie udveksling af personoplysninger bør beskyttelsen af privatlivets fred i forbindelse med behandlingen af sådanne oplysninger være ensartet i alle medlemsstater; med henblik herpå er det nødvendigt, at der sker en indbyrdes tilnærmelse af de gældende lovbestemmelser på området;

(7) sigtet med de nationale love om behandling af personoplysninger er at sikre respekt for de grundlæggende rettigheder, navnlig retten til privatlivets fred, som også er anerkendt ved artikel 8 i konventionen til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder og ved fællesskabsrettens generelle principper; af denne grund må en indbyrdes tilnærmelse af disse lovbestemmelser ikke medføre en forringelse af den beskyttelse, de yder, men skal tværtimod have til sigte at garantere et højt beskyttelsesniveau overalt i Fællesskabet;

(8) de principper for beskyttelse af privatlivets fred i forbindelse med behandling af personoplysninger, som dette direktiv foreskriver, vil for visse sektorers vedkommende kunne suppleres med eller præciseres i særregler, der skal være i overensstemmelse med disse principper;

(9) principperne for beskyttelse finder anvendelse på alle registre, hvor den registeransvarliges aktiviteter falder ind under fællesskabsrettens anvendelsesområde; offentlige registre, som ikke falder ind under fællesskabsrettens anvendelsesområde, bør være underlagt de samme principper for beskyttelse, nedfældet i medlemsstaternes lovgivning, som fastsat ved resolutionen vedtaget af repræsentanterne for regeringerne for De Europæiske Fællesskabers medlemsstater, forsamlet i Rådet, den ....; registre, der udelukkende henhører under en fysisk persons udøvelse af retten til privatlivets fred, som f.eks. private adressekartoteker, bør dog være undtaget;

(10) enhver behandling af personoplysninger i Fællesskabet skal ske under overholdelse af lovgivningen i den medlemsstat, hvor registret befinder sig for derved at sikre, at ingen person kan unddrages den beskyttelse, der skal garanteres ham ved dette direktiv; med henblik herpå betragtes hver enkelt del af et register, der er placeret i flere forskellige medlemsstater, som et selvstændigt register, og placering af en del af et register i et tredjeland må ikke medføre bortfald af beskyttelsen;

(11) enhver behandling af personoplysninger skal være legitim; denne legitimitet skal bygge på den registrerede persons samtykke eller på fællesskabsretten eller på nationale love;

(12) I den nationale lovgivning kan der på de i direktivet fastlagte betingelser fastsættes nærmere regler for behandlingens legitimitet; denne mulighed må dog ikke benyttes som begrundelse for, at en anden medlemsstat end den stat, hvori registret befinder sig, foretager kontrol, idet sidstnævnte stats pligt til i henhold til dette direktiv at beskytte privatlivets fred i forbindelse med behandlingen af personoplysninger er tilstrækkelig set i forhold til fællesskabsretten til at sikre fri udveksling af oplysning er;

(13) de anmeldelsesprocedurer, der gælder for offentlige og private registre, og den oplysningspligt ved første videregivelse, der gælder for private registre, har til formål at tilvejebringe den gennemsigtighed, der er absolut nødvendig for sikre en registreret person adgang til oplysninger om ham selv;

(14) for at en registreret persons samtykke kan betragtes som gyldigt, og når en registreret person anmodes om at afgive oplysninger om sig selv, skal den pågældende gives reel og fuld oplysning;

(15) en registreret person skal kunne udøve sin ret til aktindsigt for at forvisse sig om legitimiteten af behandlingen af oplysninger om ham selv og disses pålidelighed;

(16) for at oplysninger kan gøres til genstand for behandling, skal de opfylde visse krav; behandling af oplysninger, som ifølge selve deres art kan krænke retten til privatlivets fred, bør være forbudt uden den registrerede persons udtrykkelige samtykke; dog kan der til varetagelse af afgørende hensyn til samfundsmæssige interesser, navnlig for lægestandens vedkommende, fastsættes undtagelser ved en lov, hvori der fastsættes præcise og strenge betingelser for og indskrænkninger i behandlingen af oplysninger af denne art;

(17) for at forhindre enhver form for uberettiget behandling må der af hensyn til beskyttelsen af privatlivets fred i forbindelse med behandlingen af personoplysninger træffes de fornødne sikkerhedsforanstaltninger, såvel med hensyn til behandlingens form som med hensyn til den teknologi, der benyttes;

(18) på medieområdet kan medlemsstaterne fastsætte undtagelser fra bestemmelserne i dette direktiv i det omfang, disse tager sigte på at forene retten til privatlivets fred med informationsfriheden og retten til at modtage og give meddelelser som garanteret ved bl.a. artikel 10 i konventionen til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder;

(19) medlemsstaterne bør opfordre de berørte erhvervskredse til at udarbejde en europæisk adfærdskodeks for visse nærmere bestemte sektorer; Kommissionen vil støtte sådanne initiativer og vil tage hensyn til en sådan kodeks ved vurderingen af, om der bør træffes nye specifikke foranstaltninger for visse sektorer;

(20) i tilfælde af overtrædelse af bestemmelserne i dette direktiv bør den registeransvarlige betragtes som ansvarlig i forbindelse med en erstatningssag; der bør fastsættes passende sanktioner for at sikre en effektiv beskyttelse;

(21) det er ligeledes nødvendigt, at der kan videregives personoplysninger til et tredjeland, der sikrer et passende beskyttelsesniveau; for det tilfælde, at beskyttelsesniveauet i et tredjeland er utilstrækkeligt, indeholder dette direktiv procedurer for forhandling med det pågældende land;

(22) principperne i dette direktiv er en konkretisering og videreudbygning af principperne i Europarådets konvention af 28. januar 1981 om beskyttelse af personer i forbindelse med automatiseret behandling af persondata;

(23) det forhold, at hver medlemsstat skal råde over en uafhængig tilsynsmyndighed, har afgørende betydning for beskyttelsen af personer i forbindelse med behandling af personoplysninger; på fællesskabsplan bør der nedsættes en Gruppe til Beskyttelse af Personoplysninger, der bør være fuldstændig uafhængig i udøvelsen af sine funktioner; som følge af dens specifikke karakter bør den have til opgave at rådgive Kommissionen og bidrage til at sikre en ensartet anvendelse af de nationale regler, der vedtages til gennemførelse af dette direktiv;

(24) med henblik på at vedtage de supplerende foranstaltninger, der er nødvendige for at anvende principperne i dette direktiv, er det nødvendigt at tildele Kommissionen gennemførelsesbeføjelser og nedsætte et rådgivende udvalg i henhold til de nærmere vilkår, der er fastsat i Rådets afgørelse 87/373/EØF[1] -

UDSTEDT FØLGENDE DIREKTIV:

KAPITEL I

ALMINDELIGE BESTEMMELSER

Artikel 1

Direktivets sigte

1. Medlemsstaterne drager i overensstemmelse med bestemmelserne i dette direktiv omsorg for at beskytte personers privatliv i forbindelse med behandlingen af personoplysninger, der er indeholdt i registre.

2. Medlemsstaterne kan ikke af grunde, der har forbindelse med den i henhold til 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 person"); ved identificerbar person forstås bl.a. en person, der kan identificeres ved et identifikationsnummer eller lignende oplysning;

(1) EFT nr. L 197 af 18.7.1987, s. 33.

b) "anonymisere" en sådan ændring af personoplysninger, at de pågældende oplysninger ikke længere kan knyttes til en bestemt eller identificerbar fysisk person eller kun ved en uforholdsmæssig stor indsats i henseende til personale, udgifter og tid;

c) "register over personoplysninger" (register) enhver samling af personoplysninger, der er placeret samlet eller flere forskellige steder, og som gøres til genstand for edb-behandling, eller som er strukturerede og tilgængelige i en samling, der er opbygget efter bestemte kriterier med henblik på at lette brug eller samkøring af de pågældende oplysninger, selv om dette reelt ikke sker;

d) "behandling" følgende operationer, hvad enten disse udføres ved brug af elektronisk databehandling eller ej: registrering, opbevaring, samkøring samt ændring, brug og videregivelse af data, herunder transmission, formidling og udtrækning samt blokering og sletteIse;

e) "den registeransvarlige" den fysiske eller juridiske person, offentlige myndighed, forvaltningsgren eller ethvert andet organ, der i henhold til fællesskabsretten eller en medlemsstats lovgivning er beføjet til at afgøre, hvad et register må bruges til, hvilke typer personoplysninger der må registreres i det, hvilke operationer de må underkastes, og hvilke tredjemænd der må få adgang hertil;

f) "tilsynsmyndighed" den uafhængige offentlige myndighed eller ethvert andet uafhængigt organ, der udpeges af hver enkelt medlemsstat i henhold til bestemmelserne i artikel 26 i dette direktiv;

g) "den offentlige sektor" samtlige en medlemsstats offentligretlige administrationer, organer og forvaltninger med undtagelse af dem, der driver industri- eller handelsvirksomhed, samt privatretlige organer og enheder, når de deltager i udøvelse af offentlig myndighed;

h) "den private sektor" enhver fysisk eller juridisk person eller sammenslutning, herunder offentligretlige administrationer, organer og forvaltninger, når de udøver en industri- eller handelsvirksomhed.

Artikel 3

Anvendelsesområde

1. Medlemsstaterne anvender dette direktivs bestemmelser på alle private og offentlige registre med undtagelse af offentlige registre, hvis aktiviteter ikke falder ind under fællesskabsrettens anvendelsesområde.

2. Dette direktivs bestemmelser finder ikke anvendelse på registre:

   a) der føres af en fysisk person til rent private og personlige formål, eller

   b) der føres af almennyttige foreninger af bl.a. politisk, filosofisk, religiøs, kulturel, fagforeningsmæssig, sportslig eller fritidsmæssig art med henblik på disses legitime formål

forudsat, at registreringen alene vedrører den pågældende forenings medlemmer og tilknyttede, og disse har meddelt deres samtykke til registreringen, samt at denne ikke videregives til tredjemand.

Artikel 4

Gældende ret

1. Medlemsstaterne anvender dette direktivs bestemmelser på:

   a) alle registre, der befinder sig på deres område;

   b) registeransvarlige, der har bopæl på deres område og herfra udnytter et register, der befinder sig i et tredjeland, hvis lovgivning ikke sikrer et passende beskyttelsesniveau, medmindre denne brug kun forekommer lejlighedsvis.

2. Medlemsstaterne anvender bestemmelserne i artikel 5, 6, 8, 9, 10, 17, 18 og 21 på brugere, der konsulterer et register, der befinder sig i et tredjeland, fra en terminal, der befinder sig på en medlemsstats område, medmindre denne brug kun forekommer lejlighedsvis.

3. Når et register midlertidigt flyttes fra én medlemsstat til en anden, må sidstnævnte ikke stille hindringer for eller kræve yderligere formaliteter opfyldt i forhold til gældende regler i den medlemsstat, hvor registret er placeret permanent.

KAPITEL II

LEGITIM BEHANDLING AF PERSONOPLYSNINGER I DEN OFFENTLIGE SEKTOR

Artikel 5

Principper

1. Med forbehold af bestemmelserne i artikel 6 fastsætter medlemsstaterne følgende retsforskrifter vedrørende offentlige registre:

a) oprettelse af et register og enhver anden behandling af personoplysninger er legitim i det omfang, dette er nødvendigt af hensyn til en registeransvarlig offentlig myndigheds varetagelse af sine opgaver;

b) behandling af oplysninger til andre formål end det, med henblik på hvilket registret er oprettet, er legitim, såfremt:

- den registrerede person meddeler sit samtykke hertil, eller
- behandlingen sker med hjemmel i fællesskabsretten eller med hjemmel i en lov - eller en retsakt, der udstedes med hjemmel i en lov - udstedt i overensstemmelse med dette direktiv af en medlemsstat, som giver sin tilladelse hertil og fastsætter grænserne herfor, eller
- den registrerede persons legitime interesser ikke taler imod en sådan ændring i anvendelsesformålet, eller
- dette er nødvendigt for at afværge en overhængende trussel mod den offentlige orden eller en grov krænkelse af andres rettigheder.

Artikel 6

Behandling af personoplysninger i den offentlige sektor med henblik på videregivelse af sådanne oplysninger

1. Medlemsstaterne fastsætter bestemmelser i deres lovgivning om, at videregivelse af personoplysninger fra registre, der føres af en offentlig forvaltning, kun er legitim:

   a) såfremt dette er nødvendigt af hensyn til de opgaver, den pågældende offentlige forvaltning, som videregiver eller anmoder om videregivelse af disse oplysninger, varetager, eller

   b) såfremt det sker efter anmodning fra en fysisk eller juridisk person i den private sektor, der påberåber sig en legitim interesse, der går forud for den registrerede persons interesser.

2. Uden at dette i øvrigt berører bestemmelserne i stk. 1, kan medlemsstaterne fastsætte de nærmere vilkår, hvorunder videregivelse af personoplysninger er legitim.

3. Medlemsstaterne fastsætter bestemmelser i deres lovgivning om, at den registeransvarlige i de i stk. 1, litra b), omhandlede tilfælde skal underrette de registrerede personer, når personoplysninger vedrørende dem videregives. Medlemsstaterne kan bestemme, at denne underretning erstattes af en forudgående tilladelse fra tilsynsmyndigheden.

Artikel 7

Anmeldelsespligt over for tilsynsmyndigheden

1. Medlemsstaterne fastsætter bestemmelser i deres lovgivning om, at der ved oprettelse af et offentligt register, hvis personoplysninger vil kunne videregives, på forhånd skal foretages anmeldelse til tilsynsmyndigheden, der indfører anmeldelsen i et register. Dette register skal være offentligt tilgængeligt.

2. Medlemsstaterne fastsætter, hvilke oplysninger der skal anmeldes til tilsynsmyndigheden. Disse oplysninger skal mindst omfatte den registeransvarliges navn og adresse, registrets anvendelsesformål, en beskrivelse af, hvilke typer oplysninger det indeholder, hvilke tredjemænd oplysningerne kan videregives til, samt en beskrivelse af, hvilke foranstaltninger der er truffet i henhold til artikel 18.

3. Medlemsstaterne kan bestemme, at bestemmelserne i stk. 1 og 2 finder anvendelse på andre offentlige registre, samt at konsultation af registret kan begrænses under henvisning til de i artikel 15, stk. 1, anførte grunde.

KAPITEL III

LEGITIM BEHANDLING AF PERSONOPLYSNINGER I DEN PRIVATE SEKTOR

Artikel 8

Principper

1. Medlemsstaterne fastsætter bestemmelser i deres lovgivning om, at registrering af personoplysninger i et register og enhver anden behandling heraf uden den registrerede persons samtykke kun er legitim, dersom dette sker i overensstemmelse med bestemmelserne i dette direktiv, og såfremt:

a) behandlingen sker i forbindelse med en kontrakt, eller et kontraktlignende tillidsforhold, med den registrerede person og er nødvendiggjort heraf, eller

b) oplysningerne stammer fra offentligt tilgængelige kilder, og behandlingen heraf alene sker med henblik på korrespondance, eller

c) den registeransvarlige forfølger en legitim interesse, der går forud for den registrerede persons interesser.

2. Medlemsstaterne fastsætter bestemmelser i deres lovgivning om, at det påhviler den registeransvarlige at forhindre, at der sker videregivelse af oplysninger, der er uforenelig med registrets anvendelsesformål, eller som er til skade for den offentlige orden. Ved on-line konsultation påhviler de samme forpligteiser brugeren.

3. Uden at det i øvrigt berører bestemmelserne i stk. 1, kan medlemsstaterne fastsætte de nærmere vilkår, hvorunder behandling af personoplysninger er legitim.

Artikel 9

Oplysningspligt over for den registrerede person

1. Medlemsstaterne fastsætter bestemmelser i deres lovgivning for den private sektor om, at den registeransvarlige ved første videregivelse af oplysninger fra et register eller ved etablering af mulighed for on-line konsultation af et register underretter den registrerede person herom med angivelse af registrets anvendelsesformål, hvilke typer oplysninger der er registreret heri samt registrets navn og adresse.

2. Den i stk. 1 omhandlede oplysningspligt er ikke obligatorisk i det i artikel 8, stk. 1, litra b), omhandlede tilfælde. Der består ingen oplysningspligt, når videregivelse af oplysninger er påbudt ved lov.

3. Såfremt den registrerede person gør indsigelse mod videregivelse af oplysninger eller enhver anden behandling, er den registeransvarlige forpligtet til at bringe den pågældende behandling til ophør, medmindre den er tilladt ved lov.

Artikel 10

Fravigelse af oplysningspligten over for den registrerede person i særlige tilfælde

Såfremt opfyldelsen af den i artikel 9, stk. 1, omhandlede oplysningspligt over for den registrerede person viser sig umulig eller indebærer en uforholdsmæssig stor indsats eller strider mod fortrinsberettigede legitime interesser hos den registeransvarlige eller lignende interesser hos tredjemand, kan medlemsstaterne fastsætte bestemmelser i deres lovgivning om, at tilsynsmyndigheden kan give tilladelse til at fravige oplysningspligten.

Artikel 11

Anmeldelsespligt over for tilsynsmyndigheden

1. Medlemsstaterne fastsætter bestemmelser i deres lovgivning om, at den registeransvarlige skal foretage anmeldelse af oprettelsen af et register over personoplysninger, når oplysningerne føres med henblik på videregivelse og ikke stammer fra offentligt tilgængelige kilder. Anmeldelse foretages til tilsynsmyndigheden i den medlemsstat, hvor registret befinder sig, eller, hvis det ikke befinder sig i en medlemsstat, til tilsynsmyndigheden i den medlemsstat, hvor den registeransvarlige har bopæl. Den registeransvarlige skal give de kompetente nationale myndigheder meddelelse om enhver ændring i registrets anvendelsesformål samt om ændringer af sin adresse.

2. Medlemsstaterne fastsætter, hvilke oplysninger der skal anmeldes til tilsynsmyndigheden. Disse oplysninger skal mindst omfatte den registeransvarliges navn og adresse, registrets anvendelsesformål, en beskrivelse af, hvilke typer oplysninger det indeholder, hvilke tredjemænd oplysningerne kan videregives til, samt en beskrivelse af, hvilke foranstaltninger der er truffet i henhold til artikel 18.

3. Medlemsstaterne kan bestemme, at bestemmelserne i stk. 1 og 2 finder anvendelse på andre private registre, samt at de i stk. 2 omhandlede oplysninger skal være offentligt tilgængelige.

KAPITEL IV

DEN REGISTREREDE PERSONS RETTIGHEDER

Artikel 12

Samtykke på et velinformeret grundlag

En registreret persons samtykke til, at personoplysninger, der vedrører ham selv efter dette direktiv, gøres til genstand for behandling, er kun gyldigt, såfremt:

a) den registrerede råder over følgende oplysninger:

- registrets anvendelsesformål og de typer oplysninger, der er registreret heri;
- hvilken brug der gøres af personoplysningerne i registret, og i givet fald hvem de er bestemt til;
- den registeransvarliges navn og adresse;

b) samtykke meddeles specifikt og udtrykkeligt og angiver, hvilke typer oplysninger, hvilken type behandling samt evt. hvilke modtagere det gælder for;

c) samtykke til enhver tid kan tilbagekaldes af den registrerede person uden tilbagevirkende kraft.

Artikel 13

Oplysningspligt ved indsamling af oplysninger

1. Medlemsstaterne garanterer personer, hos hvem der indsamles personoplysninger, ret til at få mindst følgende oplyst:

   a) anvendelsesformålet for det register, som oplysningerne skal registreres i, og
   b) hvorvidt der består pligt til at besvare de spørgsmål, indsamlingen af oplysninger drejer sig om, og
   c) hvilke konsekvenser det har for de pågældende at undlade at besvare de stillede spørgsmål, og
   d) hvem oplysningerne er bestemt til, og
   e) hvorvidt de pågældende har adgang til og ret til berigtigelse af oplysninger, der vedrører dem selv, og
   f) den registeransvarliges navn og adresse.

2. Bestemmelserne i stk. 1 finder ikke anvendelse ved indsamling af oplysninger i tilfælde, hvor oplysningspligten over for den registrerede person ville forhindre en offentlig myndighed i at varetage sine tilsyns- og kontrolopgaver eller opretholdelse af den offentlige orden.

Artikel 14

Supplerende rettigheder for den registrerede person

Medlemsstaterne indrømmer den registrerede person følgende rettigheder:

1. ret til af legitime grunde at modsætte sig, at personoplysninger vedrørende ham selv gøres til genstand for behandling;

2. ret til ikke at være undergivet administrative eller privatretlige afgørelser, der indebærer en vurdering af hans adfærd, der alene er begrundet i, at personoplysninger vedrørende ham selv med en beskrivelse af hans karakteregenskaber eller personlighed behandles elektronisk;

3. ret til at kende et registers eksistens og vigtigste anvendelsesformål samt den registeransvarliges identitet, faste bopæl, hovedsæde eller forretningssted;

4. ret til med rimelige mellemrum og uden større ventetid eller omkostninger at få bekræftet, hvorvidt der er registreret personoplysninger vedrørende ham selv i et register, samt at få meddelt disse oplysninger i letforståelig form.

   Medlemsstaterne kan bestemme, at helbredsoplysninger kun udleveres gennem en læge;

5. ret til i givet fald at få registrerede oplysninger berigtiget, slettet eller blokeret, såfremt behandlingen af dem ikke er i overensstemmelse med bestemmelserne i dette direktiv;

6. ret til efter anmodning og uden omkostninger at få slettet oplysninger vedrørende ham selv i registre, der har handelsmæssige eller reklamemæssige øjemed;

7. ret til i tilfælde af anvendelse af stk. 5 at få udvirket, at tredjemand, hvortil oplysninger er blevet videregivet, underrettes om berigtigelse, sletteise eller blokering af oplysninger;

8. ret til at indbringe krænkelser af de ved denne artikel garanterede rettigheder for en domstol.

Artikel 15

Begrænsninger i den registrerede persons adgang til offentlige registre

1. Medlemsstaterne kan ved lov begrænse de i artikel 14, stk. 3 og 4, omhandlede rettigheder af grunde, der vedrører:

   a) den nationale sikkerhed eller
   b) det nationale forsvar eller
   c) strafferetlig forfølgning eller
   d) den offentlige sikkerhed eller
   e) en vital og behørigt begrundet økonomisk eller finansiel interesse hos en medlemsstat eller Fællesskabet eller
   f) hensynet til en offentlig myndigheds varetagelse af sine tilsyns- eller kontrolopgaver eller
   g) en tilsvarende rettighed for en anden person og andres rettigheder og friheder.

2. I de i stk. 1 anførte tilfælde skal tilsynsmyndigheden efter anmodning fra den registrerede person kunne foretage den fornødne kontrol af registret.

3. Medlemsstaterne kan begrænse den registrerede persons adgang til registre, hvori der midlertidigt er registreret oplysninger med henblik på at foretage statistiske uddrag.

KAPITEL V

OPLYSNINGERNES PÅLIDELIGHED M.V.

Artikel 16

Principper

1. Medlemsstaterne fastsætter bestemmelser om, at:

a) indsamling og behandling af personoplysninger skal udføres loyalt og på lovlig vis;

b) oplysningerne skal registreres til nøje definerede, udtrykkeligt angivne og legitime formål og udnyttes på en måde, der er forenelig med disse formål;

c) oplysningerne skal være fyldestgørende, relevante og nødvendige i forhold til registreringsformålet;

d) oplysningerne skal være korrekte og om nødvendigt ajourføres; urigtige eller ufuldstændige oplysninger skal slettes eller berigtiges;

e) oplysningerne ikke må opbevares på en måde, der giver mulighed for at identificere de registrerede personer i et tidsrum, der er længere end det, der er nødvendigt af hensyn til registreringsformålet.

2. Det påhviler den registeransvarlige at sikre overholdelse af bestemmelserne i stk. 1.

Artikel 17

Særlige kategorier af oplysninger

1. Medlemsstaterne skal, medmindre den registrerede person frit, udtrykkeligt og skriftligt meddeler sit samtykke hertil, forbyde edb-behandling af oplysninger om racemæssig og etnisk baggrund, politisk, religiøs eller filosofisk overbevisning og fagforeningsmæssigt tilhørsforhold samt af oplysninger om helbredsforhold og seksuelle forhold.

2. Medlemsstaterne kan af grunde, der vedrører afgørende hensyn til samfundsmæssige interesser, ved lov fastsætte undtagelser fra bestemmelserne i stk. 1, forudsat at det i loven nøje præciseres, hvilke typer oplysninger der må registreres, og hvilke personer der har adgang til registret, samt at der ved loven fastsættes passende garantier mod misbrug og uberettiget indtrængen.

3. Oplysninger om strafbare forhold må kun opbevares i offentlige registre.

Artikel 18

Datasikkerhed

1. Medlemsstaterne fastsætter bestemmelser i deres lovgivning om, at den registeransvarlige har pligt til at træffe passende tekniske og organisatoriske foranstaltninger til at beskytte registret mod tilintetgørelse, hvad enten denne er hændelig eller sker som følge af uberettiget indtrængen, mod hændeligt tab af oplysninger samt mod uberettiget ændring af eller adgang til og enhver anden uberettiget behandling af personoplysninger.

   For edb-registres vedkommende skal disse foranstaltninger tilvejebringe et passende sikkerhedsniveau under hensyntagen til på den ene side den bedste disponible teknologi og de med foranstaltningernes iværksættelse forbundne udgifter og på den anden arten af de oplysninger, der ønskes beskyttet, og en vurdering af de potentielle sikkerhedsrisici. Med henblik herpå skal den registeransvarlige tage hensyn til de henstillinger om edb-sikkerhed og indbyrdes netkompatibilitet, der udarbejdes af Kommissionen i henhold til artikel 29.

2. Ved transmission af personoplysninger via et net skal der træffes foranstaltninger, der garanterer en tilstrækkelig sikkerhed.

3. Ved on-line konsultation skal dataanlægget og programmellet være udformet således, at konsultationen holder sig inden for grænserne af den af den registeransvarlige tildelte autorisation.

4. De i stk. 1-3 omhandlede forpligtelser påhviler ligeledes personer, som faktisk eller i henhold til kontrakt fører tilsyn med register-operationer.

5. Det er forbudt enhver, der i embeds medfør får adgang til oplysninger i et register, at videregive disse til tredjemand uden den registeransvarliges samtykke.

KAPITEL VI

SÆRBESTEMMELSER FOR VISSE SEKTORER

Artikel 19

Medlemsstaterne kan for organer inden for pressen og den audiovisuelle sektor tillade undtagelser fra dette direktivs bestemmelser i det omfang, disse er nødvendige for at forene retten til privatlivets fred med reglerne for informations- og pressefrihed.

Artikel 20

Medlemsstaterne opfordrer de berørte erhvervskredse til at medvirke ved udarbejdelsen af en europæisk adfærdskodeks for visse sektorer på grundlag af de i dette direktiv opstillede principper.

KAPITEL VII

ANSVAR OG SANKTIONER

Artikel 21

Ansvar

1. Medlemsstaterne fastsætter bestemmelser i deres lovgivning om, at enhver, hvis personoplysninger er registreret i et register, og som lider skade som følge af behandlingen af disse oplysninger eller enhver anden handling, der er uforenelig med bestemmelserne i dette direktiv, har ret til at kræve skadeserstatning over for den registeransvarlige.

2. Medlemsstaterne kan bestemme, at den registeransvarlige, såfremt denne godtgør, at han har truffet passende foranstaltninger til at opfylde de i artikel 18-22 anførte krav, ikke kan holdes ansvarlig for skade, der forvoldes som følge af tab eller tilintetgørelse af data eller uberettiget indtrængen.

Artikel 22

Behandling af oplysninger på den registeransvarliges vegne

1. Medlemsstaterne fastsætter bestemmelser i deres lovgivning om, at den registeransvarlige, når oplysninger behandles på hans vegne, skal sikre sig, at de krævede sikkerhedsmæssige og organisatoriske foranstaltninger overholdes og udpege en person eller virksomhed, som frembyder fornøden garanti herfor.

2. Enhver, der indsamler eller behandler personoplysninger på den registeransvarliges vegne, skal overholde de ved artikel 16 og 18 fastsatte forpligtelser.

3. En kontrakt herom skal være skriftlig og skal specifikt anføre, at personoplysninger kun må videregives af tjenesteleverandøren eller dennes ansatte med den registeransvarliges samtykke.

Artikel 23

Sanktioner

Medlemsstaterne fastsætter i deres lovgivning passende sanktioner med henblik på at sikre overholdelse af de bestemmelser, der vedtages til gennemførelse af dette direktiv.

KAPITEL VIII

VIDEREGIVELSE AF PERSONOPLYSNINGER TIL TREDJELANDE

Artikel 24

Principper

1. Medlemsstaterne fastsætter bestemmelser i deres lovgivning om, at videregivelse, hvad enten denne er midlertidig eller definitiv, til et tredjeland af personoplysninger, der gøres til genstand for behandling eller indsamles med henblik på at gøres til genstand for behandling, kun må finde sted, hvis det pågældende land sikrer et passende beskyttelsesniveau.

2. Medlemsstaterne underretter Kommissionen, såfremt et modtagende tredjeland ikke sikrer et passende beskyttelsesniveau.

3. Konstaterer Kommissionen på grundlag af oplysninger fra medlemsstaterne eller fra anden kilde, at et tredjeland ikke sikrer et passende beskyttelsesniveau, og at den deraf opståede situation er til skade for Fællesskabets eller en medlemsstats interesser, kan den indlede forhandlinger med henblik på at afhjælpe denne situation.

4. Kommissionen kan efter den procedure, der er fastsat i artikel 30, stk. 2, fastslå, at et tredjeland sikrer et passende beskyttelsesniveau som følge af internationale forpligtelser indgået af det pågældende land eller på grundlag af dets nationale lovgivning.

5. De i medfør af denne artikel trufne foranstaltninger skal være i overensstemmelse med de forpligtelser, der påhviler Fællesskabet i henhold til såvel bilaterale som multilaterale internationale aftaler om beskyttelse af personer i forbindelse med edb-behandling af personoplysninger.

Artikel 25

Fravigelse

1. En medlemsstat kan for en given videregivelse af oplysninger til et tredjeland fravige bestemmelserne i artikel 24, stk. 1, såfremt den registeransvarlige fremlægger tilstrækkelige beviser for, at der sikres et passende beskyttelsesniveau. Medlemsstaten kan først indrømme en fravigelse, når den har underrettet Kommissionen og medlemsstaterne herom, og såfremt der ikke er rejst indsigelse herimod fra en medlemsstat eller Kommissionen inden for en frist på ti dage.

2. Foreligger der en sådan indsigelse, vedtager Kommissionen passende foranstaltninger efter den procedure, der er fastsat i artikel 30, stk. 2.

KAPITEL IX

TILSYNSMYNDIGHED OG GRUPPE TIL BESKYTTELSE AF PERSONOPLYSNINGER

Artikel 26

Tilsynsmyndighed

1. Medlemsstaterne sørger for, at en kompetent uafhængig myndighed fører

tilsyn med beskyttelsen af personoplysninger. Myndigheden har til opgave at påse overholdelse af de nationale bestemmelser, der vedtages i medfør af dette direktiv, samt at udøve alle de funktioner, der tillægges den ved dette direktiv.

2. Myndigheden skal kunne iværksætte undersøgelser og skal besidde de fornødne beføjelser til at gribe ind over for oprettelse og udnyttelse af registre i strid med bestemmelserne i dette direktiv. Med henblik herpå har den bl.a. adgang til registre, der er omfattet af dette direktiv, og skal kunne indsamle alle oplysninger, der er nødvendige for at varetage dens tilsynsopgaver.

3. Enhver kan for denne myndighed forelægge klager vedrørende beskyttelsen af personer med hensyn til personoplysninger.

Artikel 27

Gruppen til Beskyttelse af Personoplysninger

1. Der nedsættes en Gruppe til Beskyttelse af Personoplysninger. Denne rådgivende og uafhængige gruppe består af repræsentanter for den i artikel 26 omhandlede tilsynsmyndighed i alle medlemsstater og har Kommissionens repræsentant som formand.

2. Sekretariatsopgaverne for Gruppen til Beskyttelse af Personoplysninger varetages af Kommissionens tjenestegrene.

3. Gruppen til Beskyttelse af Personoplysninger fastsætter selv sin forretningsorden.

4. Gruppen til Beskyttelse af Personoplysninger behandler de spørgsmål, der sættes på dagsordenen af dens formand, enten på dennes initiativ eller efter begrundet anmodning fra en repræsentant for en af tilsynsmyndighederne, og som vedrører anvendelsen af bestemmelserne i fællesskabsretten om beskyttelse af personoplysninger.

Artikel 28

Gruppens opgaver

1. Gruppen til Beskyttelse af Personoplysninger har til opgave:

   a) at bidrage til en ensartet anvendelse af de nationale bestemmelser, der vedtages til gennemførelse af dette direktiv;

   b) at afgive udtalelser om beskyttelsesniveauet i Fællesskabet og i tredjelande;

   c) at rådgive Kommissionen om, hvilke supplerende eller specifikke foranstaltninger der bør træffes for at sikre beskyttelsen af privatlivets fred.

2. Såfremt Gruppen til Beskyttelse af Personoplysninger konstaterer alvorlige forskelle mellem medlemsstaternes lovgivning eller praksis vedrørende beskyttelse af personoplysninger, der kan være til fare for den ensartede beskyttelse i Fællesskabet, underretter den Kommissionen herom.

3. Gruppen til Beskyttelse af Personoplysninger kan fremsætte henstillinger om ethvert spørgsmål vedrørende beskyttelsen af personer i forbindelse med personoplysninger i Fællesskabet. Henstillingerne optages i mødeprotokollen og kan forelægges for det i artikel 30 omhandlede rådgivende udvalg. Kommissionen underretter Gruppen til Beskyttelse af Personoplysninger om, hvorledes den har taget hensyn til dens henstillinger.

4. Gruppen til Beskyttelse af Personoplysninger udarbejder en årlig rapport om situationen vedrørende beskyttelsen af personer i forbindelse med behandling af personoplysninger i Fællesskabet og i tredjelande, som den forelægger for Kommissionen.

KAPITEL X

KOMMISSIONENS GENNEMFØRELSESBEFØJELSER

Artikel 29

Udøvelse af gennemførelsesbeføjelserne

1. Kommissionen vedtager efter den procedure, der er fastsat i artikel 30, stk. 2, de tekniske bestemmelser, der er nødvendige for, at dette direktiv kan finde anvendelse på de særlige forhold, der gør sig gældende i visse sektorer, under hensyntagen til den bedste disponible teknologi og gældende adfærdskodeks.

Artikel 30

Rådgivende udvalg

1. Kommissionen bistås af et udvalg af rådgivende karakter, der består af repræsentanter for medlemsstaterne, 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 hensyntagen til det pågældende spørgsmåls hastende karakter, i givet fald ved afstemning. Udtalelsen optages i mødeprotokollen; derudover har hver medlemsstat ret til at anmode om, at dens holdning indføres i mødeprotokollen. Kommissionen tager størst muligt hensyn til udvalgets udtalelse. Den underretter udvalget om, hvorledes den har taget hensyn til dets udtalelse.

AFSLUTTENDE BESTEMMELSER

Artikel 31

1. Medlemsstaterne sætter de nødvendige love og administrative bestemmelser i kraft for at efterkomme dette direktiv senest den 1. januar 1993.

   De i henhold til første afsnit vedtagne bestemmelser skal indeholde en udtrykkelig henvisning til dette direktiv.

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

Artikel 32

Kommissionen forelægger regelmæssigt en rapport for Rådet og Europa-Parlamentet om anvendelsen af dette direktiv, i givet fald ledsaget af passende ændringsforslag.

Artikel 33

Dette direktiv er rettet til medlemsstaterne.

Udfærdiget i Bruxelles, den

På Rådets vegne

Formand

Fiche Financière

PROJET DE PROPOSITION DE DIRECTIVE DU CONSEIL VISANT AU RAPPROCHEMENT DE CERTAINES DISPOSITIONS LEGISLATIVES, REGLEMENTAIRES ET ADMINISTRATIVES DES ETATS MEMBRES RELATIVES A LA PROTECTION DES PERSONNES A L'EGARD DU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL

1. Ligne budgétaire concernée (éventuellement à créer) :

   A 2511 : Frais de réunions de comités dont la consultation n'est pas un élément obligatoire de la procédure de formation d'actes communautaires.

2. Base légale (ou autre) :

   Article 100 A

3. Proposition de classification en dépense obligatoire/non obligatoire

   (avec justification succincte en vertu de la déclaration commune du 30 juin 1982) :
   non-obligatoire

4. Description et justification de l'action :

   4.1. Objectifs : - assurer la protection des personnes à l'égard des données à caractère personnel,
   - permettre la circulation transfrontière de données à caractère personnel dans la Communauté,
   - permettre le bon fonctionnement du marché intérieur.

   4.2. Création de 2 comités compétents en matière de protection des personnes à l'égard des données à caractère personnel (Art. 27,30)

   personnes concernées : 1. Pour le Comité de protection des données à caractère personnel (Art. 27) : représentants de l'autorité de contrôle de tous les Etats membres (groupe 4)

   2. Pour le Comité consultatif (Art.30) : représentants des Etats membres (groupe 3)

   4.3. Un représentant de la Commission préside le Comité de protection des données à caractère personnel et le Comité consultatif. Le secrétariat du Comité de protection des données à caractère personnel est assuré par les services de la Commission.

5. Nature de la dépense et mode de calcul :

5.1. Nature : réunions
(frais de participation des membres des 2 Comités)

5.2. Calcul : - Comité de protection des données :
24 membres (non-gouvernementals) x 3 réunions
a 2 jours x 1180 ECU (590 ECU/jour) = 84.960 ECU*
- Comité consultatif :
24 membres (gouvernemental) x 1 réunion a 2 jours x
780 ECU (390 ECU/jour) = 18.720 ECU*

6. Incidence financière de l'action sur les crédits d'intervention :

6.1. Echéancier des crédits d'engagement et de paiement

	CE-CP
1993 :	103.680 ECU
1994 :	" "
1995 :	" "
1996 :	" "
1997 :	" "

6.2. Part du financement communautaire dans le coût total : 100%

7. Observations :

1. Le Comité de protection des données à caractère personnel (Art. 27) :

Il est institué ce Comité à caractère consultatif et indépendant et est composé de représentants de l'autorité de contrôle de tout les Etats membres, présidé par un représentant de la Commission.

Ce Comité établit son règlement intérieur. Le secrétariat du Comité est assuré par les services de la Commission.

Missions de ce Comité : voir Art.28.

2. Le Comité consultatif (Art.30) :

Il est institué un Comité consultatif composé des représentants des Etats membres, présidé par le représentant de la Commission.

La Commission est assistée par ce Comité afin de prendre les éventuelles mesures complémentaires nécessaires pour adapter les dispositions de la directive aux spécificités de cèrtaines secteurs.

---

* estimation

FICHE D'IMPACT SUR LA COMPETITIVITE ET L'EMPLOI

I. Quelle est la justification principale de la mesure ?

- Assurer la protection des personnes à l'égard des données à caractère personnel.

- Permettre la circulation transfrontière de données à caractère personnel dans la Communauté.

- Permettre le bon fonctionnement du marché intérieur.

II. Caractéristiques des entreprises concernées.

La proposition concerne toutes les entreprises qui utilisent des fichiers de données à caractère personnel quel que soit leur taille ou leur secteur d'activité.

III. Quelles sont les obligations imposées directement aux entreprises ?

Se conformer aux dispositions applicables aux traitements de données à caractère personnel, notamment celles relatives à la légitimité de ces traitements dans le secteur privé.

IV. Quelles sont les obligations susceptibles d'être imposées indirectement aux entreprises via les autorités locales ?

Aucune.

V. Y a-t-il des mesures spéciales pour les PME ?

Non.

VI. Quel est l'effet prévisible ?

a) sur la compétitivité des entreprises ?

Les règles de protection s'appliquent à toutes les entreprises et élimineront les distorsions de concurrence dûes à l'actuelle disparité des législations nationales. En ce qui concerne leur compétitivité internationale, la directive prévoit des négociations avec les pays tiers qui n'assurent pas encore un niveau de protection adéquat.

b) sur l'emploi ?

La directive prévoit la création d'instances de contrôle nationales.

VII. Les partenaires sociaux ont-ils été consultés sur cette proposition ?

Non.

Udkast til

RESOLUTION VEDTAGET AF REPRÆSENTANTERNE FOR REGERINGERNE FOR DE EUROPÆISKE FÆLLESSKABERS MEDLEMSSTATER, FORSAMLET I RÅDET

Repræsentanterne for regeringerne for De Europæiske Fællesskabers medlemsstater, forsamlet i Rådet,

som tager i betragtning, at Rådets direktiv om beskyttelse af personer i forbindelse med behandling af personoplysninger beskytter privatlivets fred i forbindelse med behandling af personoplysninger, der er indeholdt i private og offentlige registre med undtagelse af offentlige registre, hvis aktiviteter ikke falder ind under fællesskabsrettens anvendelsesområde,

som ønsker at lette samarbejdet mellem medlemsstaternes administrationer inden for de områder, der ikke falder ind under fællesskabsrettens anvendelsesområde, samtidig med der sikres et højt beskyttelsesniveau med hensyn til de berørte personers privatliv,

som tager i betragtning, at principperne i direktivet udgør en konkretisering og videreudbygning af principperne i Europarådets konvention af 28. januar 1981 om beskyttelse af personer i forbindelse med automatiseret behandling af persondata,

vedtager følgende resolution:

Medlemsstaternes regeringer forpligter sig til at anvende principperne i Rådets direktiv om beskyttelse af personer i forbindelse med behandling af personoplysninger på de grene af den offentlige sektor, der ikke falder ind under fællesskabsrettens anvendelsesområde, og at indlede de nødvendige lovgivningsprocedurer med henblik herpå.

ERKLÆRING FRA KOMMISSIONEN
om anvendelse på De Europæiske Fællesskabers institutioner og organer af principperne i Rådets direktiv om beskyttelse af personer i forbindelse med behandling af personoplysninger

1. Kommissionen finder, at principperne i direktivet om beskyttelse af personer i forbindelse med behandling af personoplysninger ("direktivet") bør finde anvendelse på De Europæiske Fællesskabers institutioner og organer.

2. Med henblik herpå agter Kommissionen snarest muligt at træffe og foreslå de nødvendige foranstaltninger.

3. Indtil sådanne foranstaltninger træffes, forpligter Kommissionen sig til at anvende principperne i direktivet på enhver behandling af personoplysninger, der henhører under dens kompetence.

4. Kommissionen finder, at Fællesskabernes øvrige institutioner ligeledes bør forpligte sig til at anvende principperne i direktivet på enhver behandling af personoplysninger, der henhører under deres kompetence.

FORSLAG TIL

SYN 288

RÅDETS DIREKTIV

OM

BESKYTTELSE AF PERSONOPLYSNINGER OG KOMMUNIKATIONSHEMMELIGHEDEN I FORBINDELSE MED OFFENTLIGE DIGITALE TELENET, HERUNDER DET TJENESTEINTEGREREDE DIGITALNET (ISDN) OG OFFENTLIGE DIGITALE MOBILNET

INDHOLDSFORTEGNELSE

A. RESUMÉ

Digitaliseringen af de offentlige telenet er nu godt i gang i Fællesskabet. I begyndelsen af 90'erne vil mere end 70% af langdistancetrafikken, mere end 50% af langdistancecentralerne og mere end 30% af al lokalcentralerne blive digitaliseret.

Den større udbredelse af offentlige digitale telenet i Fællesskabet - og specielt indførelsen af det tjenesteintegrede digitalnet og nye digitale mobiltjenester - vil give offentligheden adgang til en lang række nye telekommunikationsfunktioner. Dette forudsætter dog, at der fra EF's side lægges en fælles kurs for, hvorledes privatlivets fred, herunder kommunikationshemmeligheden, personoplysninger og datasikkerheden, skal beskyttes under de forhold, der vil blive resultatet af dette nye digitale telekommunikationsmiljø.

Både Rådet og Europa-Parlamentet har allerede flere gange udtalt, at de for at imødekomme den fremtidige udvikling af telekommunikationen i EF finder det overordentligt vigtigt at få fastsat passende foranstaltninger til beskyttelse af data og privatlivets fred. Europa-Parlamentet har således i de beslutninger, som det vedtog den 14. december 1988 vedrørende telekommunikation, opfordret til at træffe specifikke foranstaltninger med henblik på at sikre beskyttelse af private og fortrolige oplysninger, og det har henvist til det politiske ansvar, der påhviler Kommissionen med hensyn til at sikre, at de forskellige lovgivningsforslag om liberalisering af af telekommunikationsmarkedet følges op af handling på EF-niveau i form af foranstaltninger til beskyttelse af oplysninger af personlig art.

I Fællesskabet bliver man nu mere og mere opmærksom på de konsekvenser, som de digitale net vil få med hensyn til beskyttelsen af personoplysninger og privatlivets fred. I en resolution, der blev vedtaget i Berlin i august 1989, opfordrede medlemsstaternes kommitterede for databeskyttelse til at udvise særlig opmærksomhed med hensyn til beskyttelse af personoplysninger og privatlivets fred inden for ISDN.

Det vedlagte forslag tager specifikt sigte på at tilgodese det behov for beskyttelse af personoplysninger og privatlivets fred, der vil opstå i forbindelse de nye offentlige digitale telenet. Forslaget skal ses på baggrund af de forslag, som Kommissionen har fremsat med henblik på etablering af generelle rammer for databeskyttelse i EF, og betragtes som et supplement til disse.

En effektiv beskyttelse af personoplysninger og privatlivets fred er efterhånden en forudsætning for samfundets accept af de nye digitale net og tjenester. En sådan beskyttelse må nødvendigvis udgøre en integrerende del af EF's telekommunikationspolitik, idet dennes sigte netop er at give Europas borgere mulighed for fuldt ud at udnytte de fordele, som er forbundet med sådanne avancerede teletjenester og EF's udvikling til et endnu mere informationsrigt samfund.

Det vedlagte forslag til rådsdirektiv er udformet med denne globale målsætning for øje.

B. FORKLARENDE BEMÆRKNINGER

I. INDLEDNING

Den stadig større udbredelse af offentlige digitale telenet i Fællesskabet - og specielt indførelsen af det tjenesteintegrede digitalnet (ISDN)[1] og nye digitale mobiltjenester[2] - vil give offentligheden adgang til en lang række nye telekommunikationsfunktioner. Dette forudsætter dog, at der på fælleseuropæisk grundlag fastlægges en fælles kurs for, hvorledes privatlivets fred, herunder kommunikationshemmeligheden, person-oplysninger og datasikkerheden, skal beskyttes under de vilkår, som dette nye digitale telekommunikationsmiljø bringer med sig.

I en beslutning om koordineret indførelse af det tjenesteintegrerede digitalnet i Det Europæiske Fællesskab af 12. december[3] udtalte Europa-Parlamentet, at det kommende tjenesteintegrerede digitalnet (ISDN), dvs. udbygningen af telefonnettet, vil give både erhvervslivet og private adgang til mange nye tjenester. Parlamentet opfordrede dog samtidig Kommissionen til at forelægge forslag til, hvorledes sagerne i praksis kan gribes an, for at der inden for det ISDN-system, som begynder at blive en realitet i hele Europa, kan etableres en ensartet beskyttelse af data- og kommunikationssikkerheden, således at misbrug af de nye tekniske faciliteter i dette net kan forhindres. Europa-Parlamentet understregede igen dette synspunkt i en mere generel sammenhæng i en beslutning vedtaget den 14. december 1988[4], hvori det hedder, at der bør fastlægges specifikke bestemmelser for brugen af telenet, således at private og fortrolige data sikres den fornødne beskyttelse. Parlamentet gjorde i denne forbindelse igen opmærksom på det politiske ansvar, der påhviler Kommissionen med hensyn til at sikre, at de forskellige lovgivningsforslag om liberalisering af af telekommunikationsmarkedet følges op af handling på EF-niveau med foranstaltninger til beskyttelse af oplysninger af personlig art.

---

1) Rådets henstilling af 22. december 1986 om samordnet indførelse af et tjenesteintegreret digitalnet (ISDN) i Det Europæiske Fællesskab (86/659/EØF)
ISDN kan betragtes som en naturlig videreudvikling af telefonnettet. Systemet giver via en enkelt tilslutning, der udnytter den allerede eksisterende abonnentlinje, mulighed for transmission af tale (telefoni), tekst, data samt billeder via en lang række udbyggede og nye tjenester (for nærmere oplysninger henvises der til Rådets henstilling 86/659/EØF og kapitel II).
Kommissionen har indtil nu - efter Rådets henstilling - forelagt to rapporter over udviklingen af ISDN, (KOM(88)589 og KOM(90)123).

2) Rådets henstilling af 25. juni 1987 om samordnet indførelse af offentlig fælleseuropæisk digital celleopbygget landmobilradiokommunikation i Fællesskabet (87/371/EØF - EFT nr. L 196 af 17.7.87, s. 81) og Rådets direktiv af 25. juni 1987 om de frekvensbånd, der skal stilles til rådighed for samordnet indførelse af offentlig fælleseuropæisk digital celleopbygget landmobilradiokommunikation i Fællesskabet (87/372/EØF - EFT nr. 196 af 17.7.87, s. 85), samt senere forslag fra Kommissionen vedrørende offentlig digital mobilkommunikation.

3) Beslutning om Rådets henstilling 86/659/EØF, EFT nr. C 7 af 12. januar 1987, s. 344.

4) Beslutning om post og telekommunikation, EFT nr. C 12 af 16. januar 1989, s. 69, beslutning om nødvendigheden af at standse spredningen inden for telekommunikationssektoren EFT nr. C 12 af 16. januar 1989, s. 66.

I en resolution af 30. juni 1988[5], hvori Rådet fastslog principperne i Grønbogen om Etablering af et Fælles Marked for Teletjenester og -Udstyr[6], gav det udtryk for sin generelle støtte til målsætningerne i det handlingsprogram, der var genstand for meddelelsen af 9. februar 1988[7], idet det fastslog, at én af de politiske hovedmålsætninger var at beskytte personoplysninger og samtidig sørge for, at de enkelte borgere via kommunikationsmedierne får adgang til et væsentligt mere informationsrigt miljø end tidligere.

I en resolution om en større samordning i forbindelse med indførelsen af det tjenesteintegrerede digitalnet (ISDN) i Det Europæiske Fællesskab inden 1992[8] understregede Rådet igen, hvor stor betydning det tillægger ISDN, og fremhævede, at det var påkrævet at gennemføre yderligere drøftelser på europæisk niveau af behovet for beskyttelse af kommunikationshemmeligheden og -sikkerheden på baggrund af de nye tjenesters forskellige funktioner, jf. Europa-Parlamentets beslutning af 12. december 1986 om henstilling 86/659/EØF.

Repræsentanter for databeskyttelsesmyndighederne vedtog på deres 11. internationale konference, der blev afholdt den 28.-31. august 1989 i Berlin, en resolution med opfordring til at være særlig opmærksom med hensyn til databeskyttelsen og kommunikationshemmelighed inden for ISDN.

Vedlagte forslag er at betragte som Kommissionen respons på nødvendigheden af at træffe sådanne foranstaltninger, at personoplysninger og kommunikationshemmeligheden beskyttes i hele EF i forbindelse med implementeringen af nye offentlige digitale telenet, herunder det tjenesteintegrerede digitalnet og det offentlige digitale mobilnet. Der tages i forslaget hensyn til, at der hersker en dyb - og ikke uberettiget - bekymring med hensyn til den virkning, digitale net umiddelbart vil kunne få på beskyttelsen af personoplysninger og kommunikationshemmeligheden. Kommissionen opfatter ligeledes beskyttelsen af data og kommunikationshemmeligheden som et ufravigeligt hensyn i forbindelse med den fremtidige etablering af et åbent netmiljø[9] i EF.

---

5) Rådets resolution af 30. juni 1988 om etablering af et fælles marked for teletjenester og -udstyr (EFT nr. C 257, s.1).
6) KOM(87)290.
7) Etablering af et mere konkurrencebaseret telekommunikationsmarked for hele EF inden 1992: Virkeliggørelse af målene i Grønbogen om etablering af et fælles marked for teletjenester og -udstyr. Diskussionernes nuværende stade og Kommissionens forslag (KOM(88) 48).
8) EFT nr. C 196 af 1.8.1989, s. 4.
9) Fællesholdning om Rådets direktiv om oprettelse af et indre marked for teletjenester gennem indførelse af ONP (Open Network Provision - Tilrådighedsstillelse af åbne net), KOM(88)825 (EFT nr. .....).

Forslaget afspejler de forskellige drøftelser samt de generelle principper, der er blevet fastsat i Europa for beskyttelse af personlige oplysninger på basis af Europarådets konvention af 1981 om beskyttelse af personer i forbindelse med automatiseret behandling af persondata. Denne konvention er nu ratificeret af syv af EF's medlemslande. Forslaget skal ses som et supplement til og et led i de forslag, som Kommissionen sideløbende fremsætter med henblik på etablering af generelle rammer for databeskyttelse, hvoriblandt kan nævnes udkast til forslag til rådsdirektiv om indbyrdes tilnærmelse af medlemsstaternes love og administrative bestemmelser om beskyttelse af personer i forbindelse med behandling af personoplysninger; udkast til rådsbeslutning om indledning af forhandlinger - inden for Fællesskabets kompetenceområde - med henblik på Det Europæiske Økonomiske Fællesskabs tiltrædelse af Europarådets konvention af 1981 om beskyttelse af personer i forbindelse med automatiseret behandling af persondata, samt udkast til rådsbeslutning om informationssystemers sikkerhed. Ydermere agter Kommissionen at fastlægge interne regler med henblik på at sikre de berørte personer samme beskyttelsesniveau som i ovennævnte rådsdirektiv.

Inden for disse generelle rammer tager det vedlagte direktiv sigte på fastlæggelse af de specifikke bestemmelser, der kræves for en indbyrdes tilnærmelse af medlemsstaternes love og administrative bestemmelser vedrørende beskyttelse af personoplysninger og kommunikationshemmeligheden, med henblik på de offentlige faste og mobile digitale telenet og de nye "intelligente" funktioner, disse åbner mulighed for.

II. DE NYE SPECIFIKKE BEHOV FOR BESKYTTELSE AF PERSONOPLYSNINGER OG KOMMUNIKATIONSHEMMELIGHEDEN I TELESEKTOREN

Digitaliseringen af de offentlige telenet er nu godt i gang i Fællesskabet. I begyndelsen af 90'erne vil mere end 70% af langdistancetrafikken, mere end 50% af transitcentralerne og mere end 30% af al lokalcentralerne blive digitaliseret.

Digitalisering indebærer, at centralerne styres ved hjælp af datamater, og at behandling og transmission af al information - tale, data og billeder - via telenettene sker i form af binære tal[10]. Datamater kan foretage en intelligent behandling af disse strømme af bits, både i selve nettet og i abonnentens terminal. Dette giver langt bedre servicemuligheder end hvad der kan opnås ved hjælp af den traditionelle analoge teknik, hvilket betyder, at der via telenettene kan skabes adgang til et stort antal intelligente funktioner og dermed til en lang række nye aktiviteter. Det nye ISDN-system, der er under udvikling, og det nye offentlige digitale mobilkommunikationssystem[11] giver begge mulighed for fuldt digitaliseret kommunikation end-to-end (dvs. fra abonnent til abonnent).

Indførelsen af offentlige digitale net får to væsentlige konsekvenser med hensyn til databeskyttelse.

På den ene side vil den datamatbaserede teknik, der nu bliver mulighed for, kunne give en betydeligt større datasikkerhed med hensyn til specifikke individuelle behov, blandt andet ved hjælp af en sofistikeret krypteringsteknik.

På den anden side bliver det nu muligt - hvis der ikke træffes passende beskyttelses-foranstaltninger - systematisk at lade apparatet vise og lagre specifikke opkaldsdata, blandt andet det nummer, opkaldet foretages fra, som følge af at både driftsdata og samtaledata nu behandles på edb og at der anvendes edb-styrede centraler. Noget sådant var ikke nogen reel mulighed i de traditionelle analoge uintelligente net uden et større teknisk arbejde og forekom derfor kun under helt exceptionelle omstændigheder.

Samtidig hermed skal det fremhæves, at de nye intelligente telekommunikations-funktioner - f.eks. de ekstratjenester[12], der kan indføres i forbindelse med ISDN - vil give abonnenten adgang til flere nye servicefaciliteter,som f.eks. udspecificerede regninger, hvorved både serviceniveauet og forbrugerbeskyttelsen forbedres. Disse nye funktioner betyder imidlertid, at der må gennemføres nye specifikke foranstaltninger og bestemmelser, hvis kommunikationshemmeligheden skal sikres i det nye miljø.

Før der kan indføres digitale telenet, må man således afklare forskellige væsentlige

---

10) Datamater behandler al information som binære tal (dvs. bits), idet al information opsplittes i to grundelementer, der kan antage værdien 1 eller 0.

11) Se Rådets henstilling 86/659/EØF og 87/371/EØF, ovenstående fodnote 1 og 2.

12) Se Rådets henstilling 86/659/EØF, fodnote 1.

spørgsmål i forbindelse med beskyttelsen af personoplysninger, idet der blandt andet må tages stilling til, hvordan man skal behandle:

- abonnentinformation, som stadig hyppigere lagres i form af edb-filer
- trafikdata og andre driftsdata
- specificerede debiteringsdata
- identificering af kaldende terminal (dvs. hvor opkaldet foretages fra)
- automatisk viderestilling til tredjepart
- uopfordrede henvendelser
- specifikke tekniske faciliteter i terminal og andet udstyr, som kræves, hvis der skal opnås en passende beskyttelse

De generelle bestemmelser om beskyttelse af personoplysninger, jf. blandt andet Europarådets konvention og de bestemmelser, der skal fastlægges for EF med ovennævnte kommissionsinitiativer, repræsenterer blot de bredere rammer omkring forholdet, og der er ikke heri taget stilling til mere specifikke detaljer, der må afklares i forbindelse med disse spørgsmål.

Generelle bestemmelser om beskyttelse af personoplysninger har imidlertid ikke været nok til at sikre, at medlemsstaterne ikke gennemfører indbyrdes divergerende lovgivninger, bestemmelser og administrative tiltag for driften af det kommende digitalnet. Dette kan meget hurtigt blive en fare for det fælles marked for teletjenester og teleudstyr.

For eksempel med hensyn til identificering af den kaldende terminal planlægges det i visse medlemsstater, at den kaldende abonnent skal kunne blokere denne funktion ved hvert opkald. Hvis denne blokering hos det ene teleselskab sker ved hjælp af en knap på telefonapparatet, mens den hos en anden sker ved hjælp af en kode, der skal indtastes inden nummeret, vil dette skabe problemer for en fri omsætning af terminaludstyr i EF.

En sammenligning af de forskellige medlemsstaters bestemmelser viser, at der er store forskelle med hensyn til indhold og art. Det kan således konstateres, at der i EF er ved at opstå en situation, hvor der hersker usikkerhed med hensyn til telenet og teletjenester, og at dette truer med at blive en hindring for tjenesteudbuddet på tværs af grænserne.

Det vil være umuligt at hindre, at der opstår forskelle mellem medlemsstaterne, medmindre der vedtages et direktiv, der indeholder specifikke bestemmelser for, hvorledes de generelle principper for beskyttelse af data og kommunikationshemmeligheden skal finde anvendelse inden for offentlige faste og mobile digitalnet.

Samtidig er det ved at blive en forudsætning for samfundets accept af de nye digitale net og tjenester, at der indføres en EF-dækkende effektiv beskyttelse af personoplysninger og kommunikationshemmeligheden. Dette blev også bekræftet på Rådets møde den 7.

november 1989, hvor det med hensyn til telekommunikations samfundsmæssige aspekter konkluderedes, at det var fornødent at sikre beskyttelsen af kommunikationshemmeligheden og personoplysninger i europæisk regi.

Vedlagte forslag til rådsdirektiv tager sigte på at tilgodese disse specifikke behov.

III. FORSLAG TIL FREMGANGSMÅDE: BESTEMMELSERNE I DIREKTIV-UDKASTET

Den overordnede målsætning i direktivforslaget er at sikre, at borgerne overalt i EF nyder samme grundlæggende beskyttelse hvad angår sikring af personoplysninger og kommunikationshemmeligheden, og at denne beskyttelse indgår som en integrerende del af det generelle nye digitale teletjenesteudbud. Ønsker om større datasikkerhed i specifikke individuelle tilfælde og applikationer skal tilgodeses i de specifkke foranstaltninger, der skal gennemføres som led i den arbejdsplan, der er fastlagt i det ovennævnte forslag fra Kommissionen til et rådsdirektiv om informationssystemers sikkerhed.

Direktivforslaget tager sigte på at sikre en vis minimumsbeskyttelse af den almindelige abonnent i det nye digitale miljø og bygger på to grundlæggende principper:

- risikoen for misbrug skal minimeres ved, at mængden af data, der må behandles og lagres som led i driften af den offentlige telekommunikation, begrænses til det strengt nødvendige, dvs. data, der er nødvendige for at varetage drift, service-kvalitet og abonnentfaciliteter

- abonnentens ret til selv at bestemme over informationen skal beskyttes fuldt ud, både i forholdet til det teleselskab, der stiller tjenesten til rådighed, og i forholdet til den anden part i et opkald, samt en eventuel tredjepart, der ønsker at få adgang til data, der transmitteres eller stilles til rådighed i forbindelse med en transaktion via et offentligt telenet

Direktivforslaget tager i første omgang sigte på taletelefoni, da det er inden for dette område, at de almindelige abonnenter kommer til at opleve de største forandringer. Direktivet indeholder imidlertid også bestemmelser om, hvordan bestemmelserne for taletelefoni i givet fald finder anvendelse på andre offentlige digitale teletjenester, herunder offentlige datatransmissionstjenester inden for ISDN, samt offentlige pakke- og kredsløbskoblede datanet og andre offentlige teletjenester, der er knyttet hertil.

I betragtning af, at de offentlige telenet i EF befinder sig i en overgangsfase, og specielt at visse datamatstyrede centraler (de såkalde SPC-centraler - *Stored Program Controlled*) allerede nu stiller en række af de pågældende intelligente funktioner til rådighed, på trods af at de endnu ikke er fuldt ud digitaliserede, tages der i direktivforslaget ydermere højde for de tilfælde, hvor en medlemsstat endnu ikke fuldt ud har implementeret ISDN eller offentlige digitale mobilnet, idet det fastlægges, at bestemmelser i direktivet i så fald skal implementeres i det omfang, de også kan finde anvendelse på analoge nettjenester.

Ud fra disse generelle principper tager direktivforslag navnlig sigte på følgende:

indsamling, opbevaring og behandling af personoplysninger i abonnentfilen; opbevaring og behandling af trafik- og debiteringsdata, specielt med henblik på specificerede opgørelser over samtaler; problemerne i forbindelse med identificeringen af den kaldende terminal; tredjeparts adgang; uopfordrede henvendelser; samt de procedurer, der skal vedtages for udarbejdelse af de fornødne tekniske standarder.

I det følgende gives en kort forklaring på de enkelte artikler i direktivet:

Artikel 1 og 2 vedrører direktivets overordnede målsætninger og anvendelsen af direktivet med henblik på beskyttelse af data og kommunikationshemmeligheden i offentlige teletjenester formidlet via offentlige digitale telenet i EF.

Artikel 3 indeholder definitioner af de vigtigste udtryk svarende til ovennævnte forslag til rådsdirektiv om implementering af åbne net (ONP)[13].

Det i artikel 4 fastlagte generelle princip om, at teleselskabet kun må indsamle, lagre og behandle personoplysninger i den udstrækning, dette er nødvendigt for at kunne stille den pågældende tjeneste, og at personoplysninger ikke uden lovhjemmel eller uden abonnentens forudgående samtykke må anvendes til nogen som helst andre formål, finder i artikel 5 anvendelse i forbindelse med oprettelse af abonnentfiler. Som det fremhæves i begrundelsen til direktivet, gælder det specielt, at indsamling, opbevaring og behandling af personoplysninger ikke må udnyttes på en sådan måde, at teleselskabet herved opnår uretmæssige konkurrencefordele i forhold til andre tjenesteleverandører.

I artikel 6 opregnes abonnentens rettigheder for så vidt angår de personoplysninger, som teleselskabet opbevarer vedrørende ham. I artikel 7 fastslås det som et princip, at sådanne oplysninger ikke må videregives til tredjepart uden abonnentens samtykke eller en retskendelse.

Artikel 8 tager sigte på at sørge for en passende sikkerhed for, at uvedkommende ikke får adgang til data.

Artikel 9 og 10 fastlægges det, at indsamling, opbevaring og behandling af data principielt kun må finde sted i den udstrækning, dette er nødvendigt af hensyn til telekommunikationen, dvs. debiterings- og trafikdata. Artikel 11 tager sigte på at beskytte kommunikationshemmeligheden i forbindelse med specificerede opgørelser over samtaler, idet det fastlægges, at den kaldte abonnent skal holdes anonym.

I artikel 12 og 13 fastlægges der detaljerede bestemmelser for identificeringen af den kaldende terminal. Det skal være muligt at blokere identificeringsfunktionen blandt andet af hensyn til personer, der foretager opkald til og fra behandlingscentre for alkohol- og

13) Se fodnote 9.

stofmisbrugere, tilflugtscentre for voldsramte og psykiatriske behandlingscentre, således at disse personer ikke behøver frygte for deres anonymitet. Det samme gælder andre nødhjælpstjenester (selvmord, AIDS, mm.).

Den kaldte abonnent kan imidlertid have en legitim interesse i kun at acceptere de opkald, hvor den kaldende identificerer sig. For at sikre både den kaldendes og den kaldtes rettigheder, må den kaldte abonnent have mulighed for kun at acceptere de indgående opkald, hvoraf den kaldende abonnents nummer fremgår.

Teleselskaberne må imidlertid have adgang til en funktion, der giver mulighed for at suspendere eller ophæve denne blokering af identificeringen, blandt andet hvor der er tale om chicane-opkald. Denne funktion må også kunne bruges blandt andet af politiet med henblik på at opklare kriminalitet og af forskellige nødhjælpstjenester, blandt andet brandvæsenet, med henblik på at forhindre misbrug.

Artikel 14 sikrer, at både den kaldende og den kaldte abonnents kommunikations-hemmelighed er beskyttet ved viderestilling af opkald.

Artikel 15's formål er at hindre ad teknisk vej, at indholdet af telefonsamtaler lagres og/eller videregives til tredjepart uden den kaldende abonnents vidende.

Artikel 16 og 17 har til formål at forhindre, at leverandører af teleindkøbs- og teledatatjenester uden autorisation får adgang til personoplysninger om abonnenten. Tanken hermed er både at undgå, at der opstilles forbrugerprofiler, og at beskytte abonnenten mod uopfordrede henvendelser, f.eks. uønsket reklame via telenettet.

Artikel 18 skal forebygge, at der ved indførelse af tekniske funktioner for at tilgodese behovet for databeskyttelse skabes hindringer for den frie omsætning af teleudstyr og -tjenester i EF. Det fastlægges i denne artikel, at der i givet fald skal udarbejdes fælles europæiske standarder for, hvorledes specifikke tekniske funktioner skal implementeres. Som fastlagt i Rådets direktiv om indbyrdes tilnærmelse af medlemsstaternes lovgivning om teleterminaludstyr samt gensidig anerkendelse af udstyrets overensstemmelse[14] og Rådets beslutning 87/95/EØF af 22. december 1986 om standardisering inden for informationsteknologi og telekommunikation[15] skal det tekniske arbejde overdrages de europæiske standardiseringsorganisationer, blandt andet Det Europæiske Institut for Telestandarder (ETSI) og CEN/CENELEC.

De afsluttende bestemmelser i artikel 19-25 vedrører anvendelsesrådet, procedurer for ændring af direktivet med henblik på tilpasning til den tekniske udvikling, samt konsultationsprocedurer. Det planlægges, at Kommissionen ved direktivets

14) KOM(89)289 - SYN 204 af 27.7.1989.
15) EFT nr. L 36 af 7.2.1987, s. 31.

gennemførelse skal bistås af et udvalg bestående af repræsentanter for de myndigheder, der har ansvar for databeskyttelse i medlemsstaterne, og et udvalg bestående af repræsentanter for medlemsstaterne. Det foreslås, at disse udvalg skal være de samme som de udvalg, der er nedsat med henblik herpå i det udkast til rådsdirektiv om indbyrdes tilnærmelse af medlemsstaternes love og administrative bestemmelser om beskyttelse af personer i forbindelse med behandling af personoplysninger, der forelægges sideløbende med nærværende direktiv, dog således at disse udvalg specifikt konstitueres med sigte på nærværende direktiv.

IV. KONKLUSION

En effektiv beskyttelse i hele EF af personoplysninger og kommunikationshemmeligheden er ved at blive en væsentlig forudsætning for samfundets accept af de nye digitale net og tjenester

Det vil være umuligt at hindre en divergerende udvikling medlemsstaterne imellem, hvis ikke der vedtages et direktiv, hvori der fastlægges specifikke bestemmelser for, hvorledes de generelle principper for beskyttelse af data og kommunikationshemmeligheden skal gennemføres inden for offentlige faste og mobile digitalnet. En divergerende udvikling kan meget hurtigt blive en fare for det fælles marked for teletjenester og teleudstyr.

Vedlagte direktivudkast tager sigte på fastlæggelse af sådanne specifikke bestemmelser.

Det henstilles derfor, at Rådet vedtager vedlagte direktivforslag.

Forslag til

RÅDETS DIREKTIV SYN 288

om beskyttelse af personoplysninger og kommunikationshemmeligheden i forbindelse med offentlige digitale telenet, herunder det tjenesteintegrerede digitalnet (ISDN) og offentlige digitale mobilnet

---

RÅDET FOR DE EUROPÆISKE FÆLLESSKABER HAR -

under henvisning til Traktaten om Oprettelse af Det Europæiske Økonomiske Fællesskab, særlig artikel 100 A;

under henvisning til forslag fra Kommissionen[1],

i samarbejde med Europa-Parlamentet[2],

under henvisning til udtalelse fra Det Økonomiske og Sociale Udvalg[3], og

ud fra følgende betragtninger:

1. Det er fastlagt i Rådets direktiv om beskyttelse af personer i forbindelse med behandling af personoplysninger, at medlemsstaterne skal sikre beskyttelsen af kommunikationshemmeligheden;

2. Nye avancerede digitale offentlige telefonnet er i færd med at vinde indpas i Det Europæiske Fællesskab, og dette resulterer i et specifikt behov for beskyttelse af personoplysninger og kommunikationshemmeligheden;

3. dette gælder i særlig grad i forbindelse med indførelsen af det tjenesteintegrerede digitalnet (ISDN) samt offentlige digitale mobilnet;

---

1) ...
2) ...
3) ...

4. Rådet har i en resolution af 30. juni 1988 om etablering af et fælles marked for teletjenester og –udstyr inden 1992[4] opfordret til, at der tages skridt til at beskytte oplysninger af personlig art, således at den fremtidige udvikling af telekommunikation i Fællesskabet kan foregå under betryggende forhold; Rådet har endvidere lagt vægt på beskyttelsen af personoplysninger og kommunikationshemmeligheden i en resolution af 18. juli 1989 om forstærket samordning i forbindelse med indførelsen af et tjenesteintegreret digitalnet (ISDN) i Det Europæiske Fællesskab inden 1992[5] ;

5. Europa-Parlamentet har understreget vigtigheden af at beskytte personoplysninger og kommunikationshemmeligheden i telenet, navnlig i forbindelse med indførelsen af det tjenesteintegrerede digitalnet (ISDN)[6][7][8];

6. I Kommissionens henstilling 81/679/EØF opfordres medlemsstaterne til at godkende og ratificere Europarådets konvention om beskyttelse af personer i forbindelse med automatiseret behandling af persondata, hvori der er fastlagt generelle principper for beskyttelse af personoplysninger;

7. en række medlemsstater har godkendt og ratificeret denne konvention;

8. i henhold til Rådets afgørelse ... skal der indledes forhandlinger - på de områder, som henhører under Det Europæiske Fællesskabs kompetence - med henblik på Det Europæiske Fællesskabs tiltrædelse af Europarådets konvention om beskyttelse af personer i forbindelse med automatiseret behandling af persondata[9];

---

4) EFT nr. C 257 af 4.10.1988, s. 1.
5) EFT nr. C 196 af 1.8.1989, s. 4.
6) EFT nr. C 7 af 12.1.1987, s. 334.
7) EFT nr. C 12 af 16.1.1989, s. 69.
8) EFT nr. C 12 af 16.1.1989, s. 66.
9) ...

9. ved Rådets direktiv [om beskyttelse af personer i forbindelse med behandling af personoplysninger] bringes disse generelle principper i anvendelse i Fællesskabet;

10. med hensyn til offentlige digitale net bør der træffes specifikke foranstaltninger af lovgivningsmæssig, administrativ og teknisk art for at beskytte personoplysninger og kommunikationshemmeligheden mod den voksende risiko, der gør sig gældende i forbindelse med opbevaring og behandling på edb af personoplysninger i sådanne net;

11. de bestemmelser, som medlemsstaterne er i færd med at udarbejde på dette område, afviger fra hinanden;

12. sådanne indbyrdes afvigende love og administrative og tekniske bestemmelser til beskyttelse af personoplysninger og kommunikationshemmeligheden i forbindelse med implementeringen i Fællesskabet af offentlige digitale telenet, herunder tjenesteintegrerede digitalnet og offentlige digitale mobilnet, vil resultere i handelshindringer, hvorfor det er påkrævet, at der hurtigt indføres harmoniserede bestemmelser, således at der kan etableres et EF-dækkende marked for teletjenester og -udstyr

13. i nærværende direktiv fastlægges, i hvilket omfang personoplysninger må indsamles, lagres og behandles i forbindelse med tilrådighedsstillelsen af teletjenester;

14. et teleselskab må kun indsamle, lagre og behandle personoplysninger, hvor dette er nødvendigt for at kunne stille den pågældende tjeneste til rådighed; oplysningerne må ikke benyttes til andre formål uden særlig lovhjemmel eller uden abonnentens forudgående udtrykkelige samtykke; indsamling, opbevaring og behandling af personoplysninger må således ikke udnyttes af teleselskabet til at opnå uretmæssige konkurrencefordele i forhold til andre tjenesteleverandører;

15. ved nærværende direktiv fastslås det som et generelt princip, for så vidt angår telekommunikationssektoren, at abonnenten har ret til at få kendskab til lagrede personoplysninger vedrørende ham og til i givet fald at kræve sådanne oplysninger rettet eller slettet, samt at personoplysninger ikke må videregives uden abonnentens tilladelse;

16. nærværende direktiv tager sigte på en harmonisering af medlemsstaternes bestemmelser om beskyttelse af kommunikationshemmeligheden i forbindelse med specificerede opgørelser over samtaler;

17. for så vidt angår identificeringen af den kaldende terminal er det nødvendigt at beskytte såvel den kaldende abonnents ret til at forblive anonym, som den kaldte abonnents ret til ikke at acceptere uidentificerede opkald;

18. personer, der gør brug af teleindkøb og teledata, må sikres mod uautoriseret brug af personlige oplysninger vedrørende dem, ligesom som abonnenterne generelt må sikres mod forstyrrelser af privatlivets fred i form af uopfordrede henvendelser;

19. skal der indføres nye tekniske funktioner i telekommunikationsudstyr med henblik på beskyttelse af data, bør det sikres, at dette sker på et harmoniseret grundlag, således at realiseringen af det indre marked i 1992 ikke bringes i fare;

20. i forbindelse med anvendelse af dette direktiv over for tredjelande må der tages hensyn til, hvor omfattende en beskyttelse personoplysninger og kommunikationshemmeligheden er genstand for i de pågældende lande, jf. Rådets direktiv [om beskyttelse af personer i forbindelse med behandling af personoplysninger];

21. for så vidt angår alle spørgsmål vedrørende beskyttelse af data og kommunikationshemmeligheden i forbindelse med offentlige digitale telenet, der ikke omfattes af bestemmelserne i nærværende særdirektiv, bør ovennævnte rådsdirektiv finde anvendelse;

22. dette direktiv vedrører ikke beskyttelse af personoplysninger og kommunikationshemmeligheden i forbindelse med den nationale sikkerhed;

23. i forbindelse med fastlæggelsen af foranstaltninger til gennemførelse og ændring af dette direktiv vil det være det formålstjenligt at udnytte erfaringen i den gruppe, hvori medlemsstaternes myndigheder for tilsyn med beskyttelse af personoplysninger er repræsenteret, og som er nedsat ved artikel 27 i Rådets direktiv ..... om beskyttelse af personer i forbindelse med behandling af personoplysninger;

24. sådanne foranstaltninger bør udarbejdes med bistand af det udvalg, der er sammensat af repræsentanter for medlemsstaterne, og som er nedsat ved artikel 30 i Rådets direktiv ..... [om beskyttelse af personer i forbindelse med behandling af personoplysninger] -

UDSTEDT FØLGENDE DIREKTIV:

Artikel 1

1. Dette direktiv tager sigte på en harmonisering af de bestemmelser, der er nødvendige for at sikre et ensartet niveau med hensyn til beskyttelse af kommunikationshemmeligheden i Fællesskabet, og på at sikre fri omsætning af teleudstyr og -tjenester i medlemsstaterne og mellem disse.

2. Medlemsstaterne vedtager i overensstemmelse med dette direktiv de særlige bestemmelser, der er nødvendige for at sikre beskyttelse af personoplysninger og kommunikationshemmeligheden inden for telesektoren.

Artikel 2

1. Dette direktiv finder specifikt anvendelse på indsamling, opbevaring og behandling af personoplysninger, som teleselskaber foretager i forbindelse med tilrådighedsstillelse af offentlige teletjenester via offentlige digitale telenet i Fællesskabet, herunder det tjenesteintegrerede digitalnet (ISDN) og offentlige digitale mobilnet, jf. i øvrigt de generelle bestemmelser i Rådets direktiv ....[om beskyttelse af personer i forbindelse med behandling af personoplysninger].

2. For så vidt angår medlemsstater, hvori der endnu ikke er implementeret et tjenesteintegreret digitalnet (ISDN) eller offentlige digitale mobilnet, gennemføres direktivets bestemmelser i den udstrækning, hvor de kan finde anvendelse på tjenester formidlet via analoge net.

Artikel 3

I dette direktiv forstås ved:

1. "personoplysninger" enhver form for information, der vedrører en identificeret eller identificerbar person.

2. "teleselskab" en offentlig eller privat virksomhed, som af en medlemsstat har fået tildelt særlige eller eksklusive rettigheder med henblik på tilrådighedsstillelse af offentlige telenet, og i givet fald offentlige teletjenester.

3. "offentligt telenet" en offentlig telekommunikationsinfrastruktur, der giver mulighed for at formidle signaler mellem bestemte nettermineringspunkter ved hjælp af trådforbindelse, radiobølger, optiske medier eller andre elektromagnetiske medier.

4. "offentlig teletjeneste" en teletjeneste, hvis tilrådighedsstillelse medlemsstaterne specifikt har overdraget til f.eks. ét eller flere teleselskaber.

Artikel 4

1. Teleselskaber må kun foretage indsamling, opbevaring og behandling af personoplysninger, hvor dette sker med henblik på telekommunikation, navnlig med henblik på opsættelse af kald til transmission af tale, data og billeder, udskrift af regninger, eller andre legitime formål, der er nødvendige af hensyn til driften, herunder fejlretning, sikring af teleselskabets udstyr mod forkert brug samt registrering af indkommende opkald, jf. artikel 13, stk. 1.

2. Teleselskabet må ikke bruge disse oplysninger til at udarbejde elektroniske profiler over abonnenterne eller klassificere individuelle abonnenter i kategorier.

Artikel 5

1. Det er tilladt at opsamle og opbevare personlige oplysninger om abonnenten i det omfang, noget sådant er nødvendigt for at indgå, ændre eller ophæve en kontrakt med teleselskabet. Ved kontraktens ophævelse skal oplysningerne slettes, medmindre - og da kun så længe - de er nødvendige af hensyn til behandling af klager, inddrivelse af skyldige beløb eller overholdelse af andre forpligtelser, der følger af medlemsstatens lovgivning, i overensstemmelse med fællesskabsretten.

2. Indholdet af information, der transmitteres, må ikke opbevares af teleselskabet efter transmissionens afslutning, medmindre dette er nødvendigt for at kunne overholde forpligtelser, der følger af medlemsstatens lovgivning, i overensstemmelse med fællesskabsretten.

Artikel 6

1. Abonnenten har ret til

   - med rimelige mellerum, inden for et rimeligt tidsrum og mod en rimelig betaling at få oplyst, om der lagres personoplysninger vedrørende ham, og til at få disse oplysninger meddelt i en umiddelbart forståelig form

   - alt efter tilfældet at få disse oplysninger korrigeret eller slettet, hvis deres behandling har været i strid med de bestemmelser, der er fastlagt i medlemsstatens lovgivning i overensstemmelse med fællesskabsretten.

Artikel 7

1. Alle personoplysninger, der behandles i forbindelse med telenet og -tjenester, skal principielt behandles fortroligt.

2. Personoplysninger må ikke videregives uden for teleselskabets tjenester og net uden særlig hjemmel ved lov eller anden retsforskrift eller uden abonnentens forudgående udtrykkelige samtykke. Et sådant samtykke betragtes kun som meddelt, når abonnenten har givet det efter anmodning fra teleselskabet. Uden abonnentens forudgående samtykke må personlige oplysninger vedrørende ham ikke røbes til personer i teleselskabet, der ikke er beskæftiget med de pågældende tjenester.

3. Teleselskaber må ikke som betingelse for at stille tjenester til rådighed stille krav om, at et sådant samtykke gives.

Artikel 8

1. Teleselskaber skal påse, at personoplysninger på betryggende og tidssvarende måde beskyttes mod, at uvedkommende skaffer sig adgang hertil eller gør brug heraf.

2. Hvor der er særlig risiko for brud på netsikkerheden, f.eks. inden for mobilradiotelefoni, skal teleselskabet informere abonnenterne herom og tilbyde kryptering fra abonnentterminal til abonnentterminal.

Artikel 9

1. Det er tilladt at opbevare og behandle debiteringsdata, der indeholder abonnentterminalens telefonnummer eller identifikationsnummer, abonnentens adresse og terminaltype, det samlede antal debiteringsenheder for afregningsperioden, det kaldte apparats nummer, samtalernes type og varighed og/eller mængden af transmitterede data, samt anden information, der er nødvendig i forbindelse med debiteringen, herunder oplysninger om forudbetaling, ratevis afregning, lukning og rykkerskrivelser.

2. En sådan generel opbevaring af debiteringsdata er tilladt indtil udløbet af den lovhjemlede forældelsesfrist for sådanne gældsforpligtelser.

Artikel 10

1. Det er tilladt at indsamle, opbevare og behandle trafikdata, der indeholder personoplysninger, hvor disse data er nødvendige for at opsætte et kald eller af hensyn til debiteringen eller andre driftsmæssige formål, herunder oplysninger om den kaldende og den kaldte abonnents nummer, den enkelte samtales begyndelses- og sluttidspunkt, og den af abonnenten anvendte teletjeneste, i den udstrækning, dette er nødvendigt for at stille den pågældende teletjeneste til rådighed.

2. Trafikdata, der opbevares i teleselskabets centraler, skal slettes efter samtalens afslutning, medmindre de pågældende data anonymiseres eller fortsat er nødvendige af hensyn til debitering eller andre legitime formål, jf. artikel 4.

Artikel 11

På abonnentens anmodning kan der udskrives en specificeret samtaleopgørelse, der blandt andet kan indeholde telefonnummeret på de kaldte abonnenter, dog uden de fire sidste cifre.

Artikel 12

1. For så vidt angår kommunikation mellem abonnenter, der er tilknyttet digitale centraler, skal den kaldende abonnent, hver gang han foretager et opkald, have mulighed for ved hjælp af en simpel teknisk blokeringsfacilitet at forhindre, at hans telefonnummer vises på det kaldte terminaludstyrs skærm eller registreres i en lageranordning heri.

   Teleselskabet kan foretage en permanent blokering af overførslen af telefonnummeret, dersom abonnenten anmoder herom.

2. Den kaldte abonnent kan anmode om, at der iværksættes en permanent blokering af identificeringsfunktionen for alle indkommende opkald; den kaldte abonnent skal også have mulighed for, hver gang han modtager et opkald, at frakoble skærmen på sit terminaludstyr eller blokere registreringen i terminalens lageranordning, således at indkommende opkald forbliver uidentificerede.

   Den kaldte abonnent skal have mulighed for kun at acceptere opkald med identifikation, dvs. den kaldende abonnents nummer.

3. For så vidt angår kommunikation mellem abonnenter under analoge centraler og abonnenter under digitale centraler, skal abonnenterne under de analoge centraler informeres om identificeringsfunktionen og om, at de kan få denne funktion blokeret permanent ved at anmode herom. De skal også have mulighed for at blokere identificeringsfunktionen i forbindelse med det enkelte opkald.

Artikel 13

1. Er identificeringsfunktionen blokeret, kan teleselskabet i et begrænset tidsrum suspendere denne blokering

   a) når en abonnent, der ønsker chicaneopkald eftersporet, anmoder herom. I så tilfælde skal de data, hvorved den kaldende abonnent identificeres, opbevares af teleselskabet og efter anmodning stilles til rådighed for de offentlige myndigheder, der i den pågældende medlemsstat er ansvarlige for forebyggelse og retsforfølgelse af kriminalitet

   b) når der foreligger retskendelse herom med henblik på at forebygge eller retsforfølge alvorlig kriminalitet.

2. Når der anmodes herom, skal der stilles en permanent suspenderingsfunktion til rådighed for

   a) organisationer, der med den pågældende medlemsstats godkendelse modtager og tager sig af nødopkald

   b) brandvæsensenheder, der forvaltes eller er godkendt af den pågældende medlemsstat.

3. Teleselskabet skal træffe de nødvendige foranstaltninger for at sikre, at suspenderings-funktionen fungerer både indenlands og i EF som helhed.

Artikel 14

1. Opkald må kun viderestilles fra den kaldte abonnent til en tredjepart, hvis tredjeparten har givet samtykke hertil; tredjeparten skal have mulighed for at specificere, at der kun må viderestilles opkald med identifikation, dvs. den kaldende abonnents nummer; tredjeparten skal ved hjælp af et særligt signal adviseres om, at der er tale om et viderestillet opkald.

2. Den kaldende abonnent skal under kaldets opsætning automatisk adviseres om, at samtalen viderestilles til en tredjepart.

Artikel 15

1. Hvis indholdet af en telefonsamtale gøres tilgængeligt for tredjepart ved hjælp af tekniske anordninger, f.eks. højtalere eller andet udstyr, der fungerer uden afløftning, eller indspilles på bånd til abonnentens eget brug eller til brug for tredjepart, skal det sikres, at de berørte parter på passende vis informeres herom, inden en sådan formidling eller indspilning indledes, og det sålænge denne varer.

2. Stk. 1 finder ikke anvendelse på de tilfælde, der er omhandlet i artikel 13, stk. 1.

Artikel 16

1. Det påhviler teleselskabet at sikre, at abonnentens telefonnummer samt andre personlige oplysninger vedrørende abonnenten, herunder oplysninger om omfanget og arten af dennes teleindkøb og om dennes konsultation af information via en teledatatjeneste, kun registreres i det omfang, disse oplysninger er nødvendige for, at den pågældende tjeneste kan stilles til rådighed, samt at de af tjenesteleverandøren kun anvendes til formål, der er godkendt af abonnenten.

2. Tjenesteleverandøren må ikke uden abonnentens forudgående udtrykkelige samtykke etablere elektroniske profiler over abonnenterne eller klassificere de individuelle abonnenter i kategorier, jf. dog artikel 20.

Artikel 17

1. Abonnenter, der modtager uopfordrede opkald med reklame for eller tilbud om levering af varer og tjenesteydelser, skal kunne advisere de teleselskaber, der formidler disse meddelelser, om, at de ikke ønsker at modtage sådanne opkald.

2. Teleselskabet træffer de fornødne foranstaltninger til at standse formidling af sådanne henvendelser til de pågældende abonnenter. Teleselskabet skal endvidere med henblik på tilsynsmyndighedernes inspektion føre en liste over disse adviseringer i en form, der fastlægges af tilsynsmyndighederne, således at sådanne opkald forhindres i fremtiden.

Artikel 18

1. Ved gennemførelsen af bestemmelserne i dette direktiv drager medlemsstaterne omsorg for, at der ikke stilles bindende krav om, at terminaludstyr eller andet teleudstyr skal indeholde specifikke funktioner, hvorved markedsføring af udstyr og den frie bevægelighed for sådant udstyr i medlemsstaterne og mellem disse hindres, jf. dog stk. 2 og 3.

2. I tilfælde, hvor bestemmelser kun kan gennemføres ved et krav om specifikke tekniske funktioner, underretter medlemsstaterne Kommissionen herom efter den procedure, der er fastlagt ved Rådets direktiv 83/189/EØF [10] vedrørende en informationsprocedure med hensyn til tekniske standarder og forskrifter.

10) EFT nr. L 109 af 26.4.1983, s. 8.

3. Hvor der er behov herfor, sørger Kommissionen for, at der udarbejdes fælles europæiske standarder for, hvorledes specifikke tekniske funktioner skal implementeres, jf. Rådets direktiv . . . [om indbyrdes tilnærmelse af medlemsstaternes lovgivning om teleterminaludstyr samt gensidig anerkendelse af udstyrets overensstemmelse][11], og Rådets beslutning 87/95/EØF om standardisering inden for informationsteknologi og telekommunikation[12].

Artikel 19

1. Dette direktivs bestemmelser vedrørende telefontjenesten gælder også for andre offentlige digitale teletjenester i det omfang, brugernes kommunikationshemmelighed udsættes for risici i sådanne tjenester.

2. De nærmere bestemmelser for gennemførelsen af stk. 1 vedtages af Kommissionen efter høring af den i artikel 22 nævnte gruppe og efter den i artikel 23 fastsatte procedure.

Artikel 20

I det omfang, en fuldstændig virkeliggørelse af dette direktivs målsætninger kræver, at bestemmelserne i direktivet bringes i anvendelse over for andre tjenesteleverandører end teleselskaberne, kan Kommissionen vedtage sådanne foranstaltninger, som er nødvendige for, at dette direktiv kan finde anvendelse på nævnte tjenesteleverandører, efter høring af den i artikel 22 omhandlede gruppe og efter den i artikel 23 fastsatte procedure.

---

11) EFT nr. C

12) EFT nr. L 36 af 7.2.1987, s. 31.

Artikel 21

De nærmere bestemmelser for anvendelsen af dette direktiv og ændringer, der er nødvendige for at tilpasse direktivet til den tekniske udvikling, fastsættes af Kommissionen efter den i artikel 23 fastsatte procedure.

Artikel 22

1. Den gruppe til beskyttelse af personoplysninger, der er nedsat ved artikel 27 i Rådets direktiv om beskyttelse af personer i forbindelse med behandling af personoplysninger, varetager også de i artikel 28 i nævnte direktiv omhandlede opgaver for så vidt angår de databeskyttelsesforanstaltninger, der henhører under nærværende direktiv.

2. Gruppen konstitueres specifikt med henblik på nærværende direktiv.

Artikel 23

1. Den i artikel 30 i direktiv .... om beskyttelse af personer i forbindelse med behandling af personoplysninger fastsatte procedure finder anvendelse.

2. Det udvalg, der er oprettet i forbindelse med den i stk. 1 omhandlede procedure, konstitueres specifikt med henblik på dette direktiv.

Artikel 24

1. Medlemsstaterne sætter de nødvendige love og administrative bestemmelser i kraft for at efterkomme dette direktiv senest den 1. januar 1993.

De i henhold til første afsnit vedtagne bestemmelser skal indeholde en udtrykkelig henvisning til dette direktiv.

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

Artikel 25

Dette direktiv er rettet til medlemsstaterne.

Udfærdiget i Bruxelles, den

På Rådets vegne

Formand

FICHE FINANCIERE

PROJET DE PROPOSITION DE DIRECTIVE DU CONSEIL CONCERNANT LA PROTECTION DES DONNEES A CARACTERE PERSONNEL ET DE LA VIE PRIVEE DANS LE CONTEXTE DES RESEAUX DE TELECOMMUNICATIONS NUMERIQUES PUBLICS, ET EN PARTICULIER DU RESEAU NUMERIQUE A INTEGRATION DE SERVICES (RNIS) ET DES RESEAUX NUMERIQUES MOBILES PUBLICS.

1. Ligne budgétaire concernée

   En 1990 : B 7700

   En 1991 et exercices ultérieurs : B5-4010

2. Base légale

   Article 100 A

3. Proposition de classification en dépense obligatoire /non obligatoire

   non -obligatoire

4. Description et justification de l'action :

   4.1. Objectifs : - assurer la protection des personnes à l'égard des données à caractère personnel,

   - permettre la circulation transfrontalière de données à caractère personnel dans la Communauté,

   - permettre le bon fonctionnement du marché intérieur.

   4.2. Réunions spécifiques du groupe de protection des données à caractère personnel (Art. 22) et du Comité consultatif (Art. 23), créés par la directive, représentant les Etats membres .

4.3. Un représentant de la Commission préside le groupe de protection des données à caractère personnel et le Comité consultatif. Le secrétariat du groupe et du Comité de protection des données à caractère personnel est assuré par les services de la Commission.

5. Nature de la dépense et mode de calcul :

5.1. **Nature : réunions**

(frais de participation des membres des 2 Comités)

5.2. **Calcul : - Groupe de protection des données : (cf. fiche financière de la directive générale)**

- Comité consultatif :

24 membres (gouvernementaux) x 3 réunions x 2 jours x 390 ECU/jour = 56.160 ECU *

6. Incidence financière de l'action sur les crédits d'intervention :

6.1. Echéancier des crédits d'engagement et de paiement

CE-CP

1993 : 56.160 ECU

1994 : 56.160 *

1995 : 56.160 *

1996 : 56.160 *

1997 : 56.160 *

6.2. Part du financement communautaire dans le coût total : 100 %

---

* estimation

7. Observations :

1. Le groupe de protection des données à caractère personnel (Art. 22):

Il est institué ce groupe à caractère consultatif et indépendant et est composé de représentants de l'autorité de contrôle de tous les Etats membres, présidé par un représentant de la Commission.

Ce groupe établit son règlement intérieur. Le secrétariat du groupe est assuré par les services de la Commission.

Missions de ce groupe : voir Art. 22

2. Le Comité consultatif (Art . 23)

Il est institué un Comité consultatif composé des représentants des Etats Membres, présidé par le représentant de la Commission.

La Commission est assistée par ce Comité afin de prendre les éventuelles mesures complémentaires nécessaires pour adapter les dispositions de la directive aux spécificités de certains secteurs.

Henstilling med henblik på

RÅDETS AFGØRELSE

om åbning af forhandlinger
med henblik på De Europæiske Fællesskabers tiltrædelse af Europarådets konvention om beskyttelse af individet i forbindelse med automatisk behandling af personlige data

BEGRUNDELSE:

1. Beskyttelse af individet i forbindelse med behandling af personlige data er både en personlig rettighed og en nødvendig betingelse for udviklingen af den internationale handel.

2. Behandlingen af personlige data er absolut nødvendig for at kunne foretage international udveksling af goder og tjenesteydelser og for at opnå et snævere samarbejde mellem landene.

3. Kommissionen har forelagt Rådet et forslag til direktiv om i Fællesskabet som helhed at sikre individet en omfattende beskyttelse i forbindelse med behandling af personlige data. Det er ønskeligt, at denne aktion følges op af initiativer med henblik på at sikre, at individet får samme grad af beskyttelse, når der er tale om udveksling af data mellem Fællesskabet og tredjelande.

4. Der blev i 1981 i Europarådet indgået en konvention om beskyttelse af individet i forbindelse med automatisk behandling af personlige data. Formålet med denne konvention er på den enkelte parts område at sikre, at der uanset nationalitet og bopæl sker overholdelse af enhver fysisk persons grundlæggende rettigheder og frihedsrettigheder og særlig af privatlivets fred i forbindelse med automatisk behandling af personlige data om den pågældende. Det bestemmes ligeledes i denne konvention, at en part ikke alene under henvisning til beskyttelse af privatlivets fred kan modsætte sig, at personlige data overskrider grænsen til en anden parts område, eller gøre dette betinget af en særlig tilladelse.

5. Kommisisonen opfordrede i sin henstilling af 29. juli 1981 Fællesskabets medlemsstater til at ratificere Europarådets konvention om beskyttelse af individet i forbindelse med automatisk behandling af personlige data; i henstillingen understregede Kommisisonen, at den forbeholdt sig ret til at forelægge Rådet et udkast til retsakt baseret på EØF-Traktaten, hvis alle medlemsstater ikke inden for et passende tidsrum skulle have undertegnet og ratificeret konventionen.

6. Endnu ikke alle Fællesskabets medlemsstater har på nuværende tidspunkt ratificeret konventionen[1]). Det er ønskeligt og nødvendigt, at Fællesskabet tiltræder konventionen for at sikre beskyttelsen af personlige data og for at sikre, at personlige data kan overskride grænserne i forhold til tredjelande, samt for at øge interessen for konventionen i tredjelande, der ønsker en så fri udveksling af data med Fællesskabet som muligt.

7. Kommisisonen henstiller derfor til Rådet, at dette giver Kommissionen bemyndigelse til med Europarådet og de stater, der er parter i konventionen om beskyttelse af individet i forbindelse med automatisk behandling af personlige data, at forhandle om en tillægsprotokol, hvorefter De Europæiske Fællesskaber inden for deres kompetenceområder kan bliver parter i denne konvention.

8. Kommissionen vil i samråd med repræsentanterne for medlemsstaterne føre disse forhandlinger inden for rammerne af de retningslinjer, der er vedlagt som bilag til denne meddelelse, eller efter de retningslinjer, Rådet eventuelt måtte give Kommissonen.

9. Fællesskabets medlemsstater, der er medlemmer af Europarådet, vil fuldt ud støtte Fællesskabets aktion under forhandlingerne med henblik på Det Europæiske Fællesskabs tiltrædelse, når dette spørgsmål behandles i Europarådets organer.

Bilag: Retningslinjer for forhandlingerne.

---

1) Hvad angår Fællesskabets medlemsstater er konventionen (STE 108 af 28. januar 1981) undertegnet af Belgien, Grækenland, Irland, Italien, Nederlandene og Portugal; konventionen er ratificeret af Danmark, Frankrig, Forbundsrepublikken Tyskland, Luxembourg, Spanien og Det Forenede Kongerige.

BILAG

RETNINGSLINJER FOR FORHANDLINGERNE

1. Formålet med forhandlingerne er at nå frem til indgåelse af en tillægsprotokol, således at Fællesskabet bliver kontraherende part i konventionen på de områder, der henhører under dettes kompetence, idet følgende principper overholdes:

2. I det rådgivende udvalg, der er nedsat i henhold til konventionens artikel 18, repræsenteres Det Europæiske Fællesskab som medlem af udvalget af Kommissionen for De Europæiske Fællesskaber.

Efter fælles koordination på initiativ af Kommissionen skal repræsentanten for Det Europæiske Fællesskab i alle spørgsmål vedrørende behandling af personlige data inden for Fællesskabets kompetenceområder råde over et antal stemmer, der svarer til summen af de stemmer, der er indrømmet de nationale delegationer for de EF-medlemsstater, der er parter i konventionen.

I alle andre spørgsmål har den enkelte nationale delegation en stemme.

3. For at den tillægsprotokol, hvorefter Fællesskabet kan blive kontraherende part i konventionen, kan træde i kraft inden for en rimelig frist, foreslår Kommissionen med støtte fra medlemsstaterne, at der i protokollens tekst indføjes en "opting out procedure"-bestemmelse med henblik på tillægsprotokollens vedtagelse.

Forslag til

RÅDETS AFGØRELSE

om

informationssikkerhed

RESUMÉ

Information i forskellig form bidrager mere og mere til både den enkeltes, erhvervslivets, og samfundets velstand. Det skønnes, at vækst og produktion i op mod to tredjedele af erhvervslivet er stærk afhængig af informationsteknologi, telekommunikation og rundspredning, og dermed af informationens nøjagtighed, sikkerhed og "troværdighed". Dette aspekt er af stor betydning og interesse både for den enkelte og for handelen, industrien og den offentlige administration. Beskyttelse af information i alle dens former - i det følgende omtalt som informationssikkerhed[1] – er dermed blevet et centralt politisk emne, der er genstand for stor opmærksomhed i hele verden.

I løbet af de seneste tiår er der sket store ændringer, og der er måske endnu større omvæltninger undervejs. Desk-top superdatamater, direkte satellittransmission, digital mobilradio, integreret bredbåndskommunikation samt andre nye former for udnyttelse af teknologien er under udvikling, hvilket vil resultere i billig, mobil, højperformant kommunikation på verdensplan i et hidtil ukendt omfang. Fremkomsten af en effektiv verdensomspændende kommunikation gør, at der må lægges endnu større vægt på behovet for at tilvejebringen en passende beskyttelse for så vidt angår tjenestedisponibilitet, meddelelsesintegritet og kommunikationshemmelighed, således at de forventede administrative og tekniske risici kan imødegås.

Dette område har stor betydning for Det Europæiske Fællesskabs samfundsøkonomiske udvikling og for realiseringen af det indre marked i 1992. En kohærent fremgangsmåde på europæisk plan vil tilskynde til en større brug af ny informationsteknologi og nye teletjenester og samtidig hjælpe med til at undgå, at der opstår nye barrierer mellem de enkelte medlemsstater og i forholdet til andre lande. Der er et presserende behov for konstatere behovene og de forskellige muligheder for aktion på EF-niveau i nært samarbejde med aktørerne i de forskellige sektorer og medlemsstaterne. Enhver form for tiltag må tage hensyn til den kommercielle, retlige og tekniske udvikling, såvel nationalt som internationalt. Informationssikkerhed vedrører ikke blot beskyttelse af ejendom og personer, men også af selve samfundet, og betragtes derfor af medlemsstaterne som noget, der henhører under landets egen suverænitet.

Samtidig er det imidlertid af afgørende betydning for Fællesskabet og for medlemsstaterne, at informationsikkerhed ikke går hen og bliver en hæmsko for udviklingen i Fællesskabet og for forholdet til andre lande. En harmoniseret strategi på informationssikkerhedsområdet må indgå som en integrerende del af Fællesskabets politik, dvs. de dele heraf, der tager sigte på en styrkelse af Det Europæiske Fællesskabs samfundsøkonomiske performans og internationale konkurrenceevne samt realiseringen af det indre marked.

Det vigtigste er at sørge for, at bpde de almindelige brugere, administrationerne og erhvervslivet sikres en effektiv og praktisk beskyttelse af information lagret i elektronisk form, uden at den brede offentligheds interesser tilsidesættes.

1) Informationssikkerhed (IS) vedrører beskyttelse af information, der lagres, behandles eller transmitteres i elektronisk form, mod hændelige eller forsætlige trusler. Elektroniske informationstjenester kræve både sikre teleinfrastrukturer, sikre terminaler (herunder tekstbehandlere og databaser) og sikker anvendelse.

Der kræves en samordnet indsats I EF-regi for at de fornødne foranstaltninger med hensyn til teknologi, standarder, verificerings- og certificeringsprocedurer og –bestemmelser (hvor noget sådant kræves) inden for rammerne af EF's politik.

Kommissionens hensigt er at opfordre til en debat med de forskellige sektoraktører i Fællesskabet om informationsikkerhedsmæssige aspekter og at nå frem til enighed om, hvilke skridt der bør overvejes. En sådan debat kan tage sit udgangspunkt i vedlagte redegørelse over områder og aktionslinjer. I denne debat er det på baggrund af medlemsstaternes ansvar på området vigtigt at basere EF's tiltag på et nært samarbejde med højstående embedsmænd i medlemsstaterne.

Det foreslås derfor, at Kommissionen lader sig bistå af et udvalg af rådgivende art, bestående af repræsentanter for medlemsstaterne under Kommissionens formandsskab. Arbejdet i udvalget skal afspejle områdets specificitet. Det foreslås, at udvalget navngives Gruppen af Højtstående Embedsmænd vedrørende Informationssikkerhed (SOGIS). Udvalgets kommisorium og sammensætning fremgår af pkt. 37-39 i denne meddelelse.

Det meget vigtige område vedrørende beskyttelse af personoplysninger er behandlet i et direktivforslag, der fremsendes sideløbende med denne meddelelse.

A. Nye udfordringer - Informationssikkerhedens samfundsmæssige, økonomiske, strategiske og politiske betydning

1. Inden for alle økonomiske, samfundsmæssige og politiske sfærer gør man brug af informationsteknologi og edb, når man skal anvende og forvalte information. Dette gør det muligt at integrere aktiviteter via globale kommunikationssystemer ved hjælp af sammenkobling af industrivirksomheder, forskningsinstitutioner, databaser, edb-centre, tjenesteleverandører samt centre for politisk og økonomisk beslutningstagning.

2. Denne større integration af særskilte aktiviteter giver en stor værditilvækst i form af besparelser og større effektivitet. Integration er derfor en nøglefaktor for den internationale konkurrenceevne, men øger samtidig behovet for en beskyttelse af individets, offentlighedens, handelens, industriens, operatørernes, tjenesteleverandørernes og de nationale administrationers interesser.

3. Hvis servicesektoren skal vokse, og der skal investeres i elektronisk udstyr, telekommunikation, rundspredning, edb- og terminaludstyr og diverse telematikapplikationer, må der skabes et sikkert europæisk miljø for elektronisk information. Det er vigtigt at opnå en generel accept og at inddrage alle parter med henblik på at beskytte legitime interesser og forebygge forkert brug og misbrug af information. Dette må ske på en måde, som er både effektiv og fyldestgørende for alle brugere, uanset hvilken lovgivning de er undergivet. Informationssikkerhedssystemer må beskytte kommunikationshemmeligheden, den intellektuelle ejendomsret, konkurrencen, den nationale sikkerhed og andre interesser.

4. Med indførelsen af mikrodatamater er informationsteknologi, telekommunikation og rundspredning ikke længere kun en aktivitet for professionelle. Der er nu tale om en *forbrugeraktivitet* med dertil hørende *forbrugerservice*. Denne forandring i kvantitativ henseende følges af en meget vigtig ændring af kvalitativ art, idet telekommunikation nu åbner mulighed for sammenkobling og kommunikation på globalt niveau.

5. I løbet af de seneste tiår er der sket store ændringer, og der er måske endnu større omvæltninger undervejs. Desk-top superdatamater, direkte satellittransmission, digital mobilradio, integreret bredbåndskommunikation samt andre nye former for udnyttelse af teknologien er under udvikling, hvilket vil resultere i billig, mobil, højperformant kommunikation på verdensplan i et hidtil ukendt omfang.

6. Fremkomsten af en effektiv verdensomspændende kommunikation gør, at nødvendigheden af at tilvejebringen en passende beskyttelse med hensyn til tjenestedisponibilitet, meddelelsesintegritet og kommunikationshemmelighed må tillægges endnu større vægt, således at de forventede administrative og tekniske risici kan imødegås.

7. Både industrien, det offentlige og samfundet som helhed er begyndt at udvise større interesse i at bruge informationstjenester, og dette gør, at sådanne tjenester er i færd med at blive en integrerende del af dagligdagen. Både styring, kommunikation og kontrol generelt, processtyring inden for industrien, transport, finansverdenen, og kontorautomation kræver en disponibilitet og en driftsmæssig robusthed, som endnu ikke er indbygget i tjenesterne eller i komponenternes design.

8. Der vil blive opfundet nye applikationer, der måske ikke er realiserbare inden for de nuværende arkitekturer. Det bliver måske påkrævet med en fundamental omdefinering af arkitekturer og performansstandarder (herunder behovet for at garantere opfyldelsen heraf) for tjenester og tilgrundliggende komponenter.

9. Der må etableres nye discipliner og understøttende organisationer/aktiviteter for at tilfredsstille disse større forventninger. De vigtigste af de nye behov tager imidlertid ikke udgangspunkt i tekniske, men i kulturelle forandringer. Den globale udnyttelse af informationstjenesterne, som udbyggede telenet muliggør, vil ændre samfundets opfattelse af organisatoriske/menneskelige forhold.

10. Kommunikation vil stadig hyppigere blive formidlet via en tredjepart, jf. de forskellige niveauer af forædlede IT-støttede tjenester, eller vil ske, så snart en tredjepart har godkendt kontakten. I sådanne tilfælde må tillidsforholdet baseres på en eksplicit definition inden for rammerne af organisatoriske relationer, myndigheder/privilegier og kvalitetsstyring med hensyn til tjenesteydelser/varer. Det er vigtigt, at individets og virksomhedernes rettigheder tilgodeses i lovgivning og bestemmelser. Sideløbende hermed må ny teknologi implementeres på en måde, der tilgodeser behovet for sikkerhed.

B. Behovet for EF-aktion i samarbejde med medlemsstaterne

11. Da der er tale om beskyttelse af ejendom, personer, og i visse tilfælde selve samfundets sikkerhed, er det klart, at informationssikkerheden vejer tungt for medlemsstaterne. Enhver medlemsstat er direkte involveret i sikkerhedsaspektet, både på forsvarsområdet og og med hensyn til samfundsinstitutionernes funktionsdygtighed. Disse overvejelser har traditionelt tilskyndet myndigheder til en vidtgående magtudøvelse på informationssikkerhedsområdet, idet staten har søgt at holde teknologi og teknik under kontrol for at hindre spredning af følsomt materiale. Selv om den enkelte bruger i sidste ende selv må være ansvarlig for, hvor stor sikkerhed han ønsker, afhænger hans muligheder for selv at bestemme i alt væsentligt af, hvilke garantier myndighederne fastlægger, f.eks. de grænser, de fastsætter gennem lovgivningen.

12. EF's politik og programmer for udvikling af informations- og telekommunikationsindustrien og for realiseringen af det indre marked kan komme i alvorlige vanskeligheder, hvis ikke der vedtages en aktiv politik for udarbejdelse og fremme af standarder med sigte på sikre informationstjenester. For EF er det væsentligt, at informationsikkerheden ikke går hen og bliver en hæmsko for udviklingen i Fællesskabet og for forholdet til andre lande. Fastlæggelse af en harmoniseret strategi på informationssikkerhedsområdet må indgå som en integrerende del af Fællesskabets politik, dvs. de dele heraf, der tager sigte på en styrkelse af Det Europæiske Fællesskabs samfundsøkonomiske performans og internationale konkurrenceevne samt realiseringen af det indre marked.

13. Mere specifikt er der tale om en samordnet indsats med sigte på at fastlægge de fornødne standarder, verificerings- og certificeringsprocedurer og –bestemmelser (hvor noget sådant kræves) inden for rammerne af EF's politik. På grund af de underliggende aspekters yderst tekniske karakter implicerer en samordnet af arbejdet et tæt samarbejde mellem aktører på et prækompetitivt F&U-stade.

14. Det forhold, at forskellige regeringer (US/UK GOSIP), Vestens forsvarsfællesskab (NATO/NOSI), edb- og telekommunikationsindustrien, samt netoperatørerne (ISO's OSI-standarder) går ind for "åbne standarder", gør, at der må lægges større vægt på sikkerheds-aspektet i informationssystemer, arkitekturer, standarder, kommunikationsprotokoller og komponentteknik.

15. Kun henved 2% af de tjenester, der vil blive stillet til rådighed i EF i år 2000, findes idag. Fremtidens tids tjenester vil kunne tage større hensyn til brugernes behov og og vil byde på mange nye funktioner, blandt andet fleksibel tale-, data- og billedformidling. Dette går det så meget mere vanskeligt at tilgodese brugernes behov for informationssikkerhed for så vidt angår databeskyttelse, kommunikationshemmelighed, autentificering, autorisation, debitering osv. Dette er grunden til, at informationssikkerhed og hermed beslægtede tekniske funktioner, såsom integritet, må gøres til genstand for systematisk udvikling og udforskning. De amerikanske myndigheder finansierer diverse programmer, såsom Trusted Computer Systems, åbne systemers arkitektur, protokoller og teknik, der vil fremskynde brugen af producentspecifikke sikkerhedsløsninger også inden for det internationale brugerfællesskab. Det må være af vital interesse for medlemsstaterne at indgå som partner på lige fod, når der skal udføres standardiseringsarbejde på dette felt. At acceptere en de-facto standard medfører en risiko for fornyet teknologisk afhængighed, hvilket kan være til alvorlig skade for EF-landenes internationale konkurrenceevne. Dette indebærer, at der også i Fællesskabet må udføres et vist arbejde, hvis der skal etableres et konstruktivt samspil med lande uden for EF, blandt andet med De Forenede Stater.

16. Det kan konkluderes, at både EF og medlemsstaterne på grund af deres respektive ansvar har stor interesse i at få afklaret følgende vigtige spørgsmål:

    - Hvorledes kan man på effektiv måde udforme og håndhæve specifikationer og standarder på informationssikkerhedsområdet?
    - Hvordan kan man implementere en formel evaluering og certificering af, at varer og systemer opfylder sikkerhedsstandarderne (både med hensyn til funktioner og skabelse af tillid)?
    - Hvordan kan man implementere, tilvejebringe og bruge sikre produkter og systemer?

17. Informationssikkerhed er et typisk eksempel på et område, hvor subsidiaritetsprincippet bør finde anvendelse, både på grund af emnet iboende kompleksitet, det forhold at flere forskellige aktører er involveret, og nødvendigheden af at gøre brug af flere forskellige politiske virkemidler. En handlingsplan er nødvendig for at kunne fastlægge, hvem der skal gøre hvad og hvornår. På den ene side er det op til medlemsstaterne at tage sig af disse spørgsmål, men på den anden side har også Fællesskabet en klar interesse i, at der fastlægges vilkår, der sikrer, at realiseringen af det indre marked, opbygningen af borgernes Europa, implementeringen af telekommunikationspolitikken og den europæiske elektronikindustris og de europæiske informationsleverandørers konkurrencedygtighed er forenelig med ønsket om at tilgodese individets og erhvervslivets fundamentale behov for informationssikkerhed. Med henblik herpå og med henblik på at koncentrere indsatsen stilles der hermed forslag om forskellige typer aktioner og om en procedurestruktur, der kan tjene som grundlag for yderligere indgående undersøgelser med sigte på gennemførelse af foranstaltninger på rette niveau.

Forslag til

RÅDETS AFGØRELSE

om informationssikkerhed

RÅDET FOR DE EUROPÆISKE FÆLLESSKABER HAR -

under henvisning til Traktaten om oprettelse af Det Europæiske Økonomiske Fællesskab, særlig artikel 235,

under henvisning til forslag fra Kommissionen[1],

under henvisning til udtalelse fra Europa-Parlamentet[2],

under henvisning til udtalelse fra Det Økonomiske og Sociale Udvalg[3], og

ud fra følgende betragtninger:

Fællesskabet har til opgave gennem oprettelsen af et fællesmarked og gennem gradvis tilnærmelse af medlemsstaternes økonomiske politik at fremme en harmonisk udvikling af den økonomiske virksomhed i Fællesskabet som helhed, en varig og afbalanceret ekspansion, en øget stabilitet, en hurtigere højnelse af levestandarden og snævrere forbindelser mellem medlemsstaterne;

elektronisk lagring, behandling og formidling af information spiller en stadig større rolle for samfundet og erhvervslivet;

med fremkomsten af en effektiv verdensomspændende kommunikation og den udstrakte brug af elektronisk behandling af information forstærkes behovet for en passende beskyttelse;

Europa-Parlamentet har i sine drøftelser og beslutninger ved flere lejligheder understreget vigtigheden af informationssikkerheden;

Det Økonomiske og Sociale Udvalg har fremhævet behovet for at behandle de informationssikkerhedsmæssige aspekter i forbindelse med Fællesskabets foranstaltninger, blandt andet på baggrund af de virkninger, realiseringen af det indre marked må forventes at få;

(1) EFT nr. C ...
(2) EFT nr. C ...
(3) EFT nr. C ...

der må fastlægges en global strategi for informationssikkerheden for at garantere brugernes sikkerhed på EF-niveau og for at hindre, at der opstår nye tekniske hindringer for kommunikationen;

de komplekse aspekter i forbindelse med informationssikkerheden gør det nødvendigt at bringe subsidiaritetsprincippet i anvendelse, at involvere aktører i forskellige sektorer samt at samordne politikken på forskellige områder;

aktioner på nationalt, internationalt og EF-niveau danner et formålstjenligt udgangspunkt;

nævnte område er nært knyttet til telekommunikation, standardisering, informationsmarkedet og FU&T-politikken samt andet arbejde, som Det Europæiske Fællesskab allerede har indledt på dette felt;

der bør sikres en samordning af indsatsen på grundlag af allerede igangværende nationalt og internationalt arbejde, og samarbejdet mellem hovedaktørerne bør fremmes med henblik på denne samordning, der bør finde sted inden for rammerne af en sammenhængende handlingsplan;

medlemsstaternes ansvar på dette område indebærer en samordnet indsats på grundlag af et snævert samarbejde med højtstående embedsmænd fra medlemsstaterne —

TRUFFET FØLGENDE AFGØRELSE:

Artikel 1

1. Der vedtages herved en handlingsplan på informationssikkerhedsområdet (INFOSEC) for en periode på 24 måneder startende fra d. .....

2. Handlingsplanen tager sigte på at fastlægge en global strategi, hvorved brugerne af elektronisk lagret, behandlet og transmitteret information beskyttes mod hændelige eller forsætlige trusler mod information og informationssystemer.

3. Planen skal tage hesyn til og understøtte det standardiseringsarbejde, der er indledt på dette område både på europæisk og verdensomspændende plan.

Artikel 2

Den i artikel 1 omhandlede plan, hvis detaljer er anført i bilaget, omfatter følgende felter:

I. etablering af rammerne for en informationssikkerhedstrategi
II. analyse af behovet for informationssikkerhed
III. udarbejdelse af løsninger på visse prioriterede behov
IV. specificering, standardisering og verificering af informationssikkerhed
V. teknologisk og driftsmæssig udvikling med henblik på informationssikkerhed som led i en generel strategi
VI. realisering af informationssikkerhed.

Artikel 3

Handlingsplanen gennemføres af Kommissionen i samarbejde med de berørte organisationer og i nært samarbejde med medlemsstaterne.

Artikel 4

Det beløb, der afsættes til denne aktion, fastsættes inden for rammerne af den årlige budgetprocedure.

Artikel 5

Kommissionen sender senest tre måneder efter planens afslutning Europa-Parlamentet og Rådet en rapport over resultaterne heraf.

Artikel 6

I forbindelse med gennemførelsen af handlingsplanen hører Kommissionen i fornødent omfang Gruppen af Højtstående Embedsmænd vedrørende Informationssikkerhed (SOGIS). Denne gruppe består af to repræsentanter for hver medlemsstat og for Kommissionen. Kommissionens repræsentant er formand for gruppen.

Medlemmerne af gruppen kan lade sig bistå af eksperter eller rådgivere alt efter karakteren af de problemer, der skal løses.

Gruppens drøftelser og beslutninger er fortrolige. Gruppen fastsætter selv sin forretningsorden. Sekretariatsforretningerne varetages af Kommissionen.

Udfærdiget i Bruxelles, den

På Rådets vegne

Formand

BILAG

Resumé af aktionslinjer

1. Aktionslinje I - Etablering af informationssikkerhedsstrategiens rammer

1.1. Område

1. Det er klart, at informationssikkerhed er en nødvendighed for det moderne samfund i mange sammenhænge. Elektroniske informationstjenester gør det nødvendigt med sikre telekommunikationsinfrastrukturer, sikre terminaler (herunder tekstbehandlingsanlæg og databaser) samt sikker brug. Der må etableres en overordnet strategi, der tager hensyn til alle aspekter af informationssikkerhed, således at der undgås en splittelse mellem forskellige metoder. Enhver form for strategi vedrørende information, der behandles i elektronisk form, må afspejle samfundets behov for at kunne fungere effektivt, samtidig med at det er beskyttet under de forskellige skiftende forhold.

1.2. Mål

2. Der må fastlægges strategiske rammer, således at de samfundsmæssige, økonomiske og politiske målsætninger kan forenes med de muligheder, der findes på teknisk, driftsmæssigt og lovgivningsmæssigt plan. Der må findes en balance mellem de forskellige ønsker, målsætninger og begrænsninger. Dette bliver en opgave for sektoraktørerne gennem et samarbejde med sigte på fastlæggelse af et fælles synspunkt og en fælles strategi. Dette er en forudsætning for at kunne forene modstridende interesser og behov både inden for den politiske beslutningstagning og i forbindelse med industriens udvikling.

1.3. Status og tendenser

3. Situationen præges af en voksende erkendelse af, at der er behov for handling. Sålænge der ikke foreligger foranstaltninger med sigte på at samordne indsatsen, er det sandsynligt, at der vil blive taget forskellige initiativer inden for de forskellige sektorer, og at dette konkret vil ytre sig i en situation med indbyrdes modsætninger, idet der efterhånden vil opstå alvorligere juridiske, samfundsmæssige og økonomiske problemer.

1.4. Behov, muligheder og prioriteter

4. Inden for sådanne fælles rammer må der tages stilling til risikoanalyse og risikostyring afhængigt af informationens og informationstjenesternes følsomhed, den indbyrdes tilnærmelse af lovgivninger og bestemmelser vedrørende forkert brug og misbrug af edb og telekommunikation, de administrative infrastrukturer, herunder sikkerhedspolitik, og hvorledes disse kan implementeres effektivt inden for de forskellige brancher/fagområder, samt samfundsmæssige aspekter og aspekter i forbindelse med kommunikationshemmeligheden (blandt andet spørgsmålet om identificerings-, autentificerings- og eventuelt autorisationsordninger i et demokratisk miljø).

5. Der må opstilles klare bestemmelser for udarbejdelse af fysiske og logiske arkitekturer med sigte på sikre distribuerede informationstjenester, standarder, retningslinjer for og definitioner af garanteret sikre produkter og tjenester, pilotforsøg og prototyper til konstatering af gennemførligheden af de forskellige aministrative strukturer, arkitekturer og standarder med henblik på specifikke sektorers behov.

6. Der må skabes opmærksomhed omkring sikkerhedsproblematikken med henblik på at gøre brugerne mere agtpågivende med hensyn til sikkerheden inden for IT- og telekommunikationssystemer.

2. Aktionslinje II - behovet for informationssikkerhed

2.1. Område

7. Informationssikkerheden er en klar forudsætning for beskyttelse af kommunikationshemmelighed, den intellektuelle ejendomsret, kommerciel fortrolighed og den nationale sikkerhed. Dette gør det vanskeligt at finde en balance i valget mellem ønsket om fri handel og ønsket om at sikre kommunikationshemmeligheden og den intellektuelle ejendomsret. Denne afgørelse og de hermed forbundne kompromisløsninger må baseres på en komplet vurdering af behovene og mulighederne for at udnytte forskellige informationssikkerhedsløsninger.

8. Brugerbehov indebærer, at de informationssikkerhedsmæssige funktionaliteter afspejler de teknologiske, driftsmæssige og regulatoriske aspekter. Det vil sige, at en systematisk undersøgelse af behovet for informationssikkerhed udgør en væsentlig del af arbejdet med at udvikle passende og effektive foranstaltninger.

2.2. Mål

9. Målet er at konstatere brugerbehovenes art og karakteristika samt disses forhold til de informationssikkerhedsmæssige foranstaltninger.

2.3. Status og tendenser

10. Indtil nu har der ikke været igangsat noget samordnet forsøg på at konstatere, hvilke behov hovedaktører har for informationssikkerhed, idet disse behov udvikler og ændrer sig meget hurtigt. Medlemsstaterne har konstateret, at der er behov for harmonisering af de enkelte landes aktiviteter (specielt for så vidt angår sikkerhedskriterier for IT). Ensartede evalueringskriterier og regler for gensidig anerkendelse af evalueringsresultater og –certifikater er af stor betydning.

2.4. Behov, muligheder og prioriteter

11. Som grundlag for en konsekvent og transparent behandling af sektoraktørernes behov bør der vedtages en klassificering af brugerbehovene og konsekvenserne af denne for etableringen af informationssikkerhed.

12. Det betragtes også som vigtigt at få konstateret behovene for lovgivning, bestemmelser og kodekser på baggrund af en vurdering af tendenserne inden for tjenestekarakteristika og tjenesteteknologi, at få indkredset alternative strategier for, hvordan målsætningerne kan tilgodeses gennem administrative, tjenesterelaterede, driftsmæssige og tekniske bestemmelser, og at få vurderet , hvor effektive og brugervenlige samt hvor bekostelige eventuelle alternative løsninger med hensyn til informationssikkerhed og strategier for brugere, tjenesteleverandører og operatører vil være.

3. Aktionslinje III - Løsninger på umiddelbare og midlertidige behov

3.1. Område

13. Det er idag muligt at beskytte datamater effektivt mod indtrængen af uvedkommende ved hjælp af "isolerende" foranstaltninger, dvs. ved hjælp af konventionelle organisatoriske og fysiske tiltag. Dette gælder også for elektronisk kommunikation inden for en lukket brugergruppe på et dedikeret net. Forholdene er meget anderledes, dersom informationen er fælles mellem brugergrupper, eller hvis den udveksles via et offentligt net eller et net, hvortil flere har adgang. I dette tilfælde mangler både teknologi, terminaler og tjenester, for slet ikke at nævne standarder og procedurer, hvorfor der ikke er mulighed for at opnå en tilsvarende informationssikkerhed

3.2. Mål

14. Målet har været at at finde frem til hurtige løsninger, der kan tilgodese brugernes mest presserende behov. Disse bør opfattes som åbne over for fremtidige behov og løsninger.

3.3. Status og tendenser

15. Visse brugergrupper har udviklet forskellige former for teknik og procedurer til deres egne specifikke behov, blandt andet behovet for autentificering, integritet og "ikke-afvisning" (non-repudiation). Normalt anvendes der magnetkort eller intelligente kort. Nogle anvender mere eller mindre sofistikeret krypteringsteknik. Dette indebærer ofte, at der må etableres brugergruppespecifikke "myndigheder". Det er imidlertid vanskeligt at generalisere denne teknik og disse metoder, således at behovene i et mere åbent miljø kan tilgodeses.

16. ISO arbejder med OSI-informationssikkerhed (ISO DIS 7498-2), og CCITT er også beskæftiget hermed inden for rammerne af X.400. Det er også muligt at indsætte informationssikkerhedssegmenter i meddelelser. Autentificering, integritet og ikke-afvisning behandles som led i meddelelser (EDIFACT) og som en del af X.400 MHS.

17. De retlige rammer omkring EDI er endnu ikke fuldt fastlagte. Det Internationale Handelskammer har fastlagt ensartede regler i en kodeks for udveksling af handelsdata via telenet.

18. Flere lande (f.eks. Frankrig, Tyskland, UK og US) er i færd med at fastlægge eller har allerede fastlagt kriterier for evaluering af IT- og telekommunikationsprodukters og –systemers troværdighed og procedurer for gennemførelse af evalueringer. Disse kriterier er blevet koordineret med landenes egne fabrikanter og vil resultere i et voksende antal pålidelige produkter og systemer, i første omgang simplere produkter. Oprettelsen af nationale organisationer til gennemførelse af evalueringer og udstedelse af certifikater vil støtte denne tendens.

19. Bestemmelser vedrørende fortrolighedsaspektet betragtes af de fleste brugere som knap så vigtige i første omgang. Det kan imidlertid forventes, at dette vil ændre sig, efterhånden som avancerede kommunikationstjenester, herunder specielt mobiltjenester, bliver mere almindelige.

3.4. Behov, muligheder og prioriteter

20. Det er vigtigt, at der hurtigst muligt etableres procedurer, standarder, produkter og værktøjer til beskyttelse af informationssikkerheden i offentlige kommunikationsnet. Autentificering, integritet og ikke-afvisning bør prioriteres højt. Der bør udføres pilotprojekter til konstatering af, om de foreslåede løsning er de bedste. Løsninger på prioriteringsbehov vedrørende EDI er genstand for undersøgelse inden for TEDIS-programmet som led i denne handlingsplans mere generelle indhold.

4. Aktionslinje IV - specificering, standardisering og verificering af informationssikkerhed

4.1. Område

Behovet for informationssikkerhed er alment, og det er således vigtigt med ensartede specifikationer og standarder. Mangelen på standarder og specifikationer kan være en stor hindring for indførslen af informationsbaserede processer og tjenester i erhvervslivet og i samfundet som helhed. Der må tages skridt til en hurtigere udvikling og brug af teknologi og standarder inden for flere indbyrdes beslægtede kommunikations- og datamatnetsområder, der er af kritisk betydning for brugerne, industrien og det offentlige.

4.2. Mål

22. Der må gøres en indsats for at understøtte og varetage specifikke funktioner inden for generelle område, såsom OSI, ONP, ISDN/IBC, netstyring og netsikkerhed, for så vidt angår oplysninger, der måske ikke er hemmeligtstemplede, men dog følsomme. Verifikationsteknik og -metoder er tæt knyttede til standardisering og specificering.

4.3. Status og tendenser

23. I USA er der taget store initiativer med henblik på informationssikkerheden inden for det civile område. I Europa behandles spørgsmålet inden for standardiseringen på IT- og telekommunikationsområdet af blandt andre ETSI og CEN/CENELEC som forberedelse af CCITT's og ISO's arbejde på området.

24. På baggrund af den voksende bekymring på området sker der for øjeblikket en udbygning af arbejdet i USA, og både handlende og tjenesteleverandører er i færd med at intensivere deres indsats på området. I Europa har Frankrig, Tyskland og Det Forenede Kongerige uafhængigt af hinanden indledt tilsvarende aktiviteter. En samlet indsats på linje med den amerikanske er dog kun langsomt ved at forme sig.

4.4. Behov, muligheder og prioriteter

25. Inden for informationssikkerhed er der en naturlig tæt sammenhæng mellem regulatoriske, driftsmæssige, administrative og tekniske aspekter. Regulativer må udmøntes i standarder, og bestemmelser vedrørende informationssikkerheden må på kontrollerbar måde være i overensstemmelse med standarder og regulativer. I flere henseende kræver regulativerne specifikationer, der går ud over standardiseringens konventionelle sigte, idet de f.eks. kan indeholde adfærdskodekser. Behovet for standarder og adfærdskodekser er til stede inden for alle områder af informationssikkerheden, og der må skelnes mellem de beskyttelseskrav, der beror på sikkerhedsmålsætningen, og de tekniske krav, der kan varetages af de de europæiske standardiseringsorganer med beføjelser på området (CEN/CENELEC/ETSI).

26. Specifikationer og standarder må omfatte informationssikkerhedstjenester (autentificiering af personer og virksomheder, protokoller for ikke-afvisning, juridisk bindende elektronisk bevis, autorisationskontrol), kommunikationstjenester (kommunikationshemmelighed for billeder og for mobilkommunikation af tale og data, beskyttelse af data/billedbaser, beskyttelse af integrerede tjenester), kommunikations- og sikkerhedsstyring (systemer baseret på offentlig/privat nøgle inden for åbne net, beskyttelse af netstyring, beskyttelse af tjenesteleverandører) samt certificering (kriterier og niveauer for beskyttelse af informationssikkerheden, procedurer for sikkerhedsbeskyttelse).

5. **Aktionslinje V - Teknologisk og driftsmæssig udvikling med henblik på informationssikkerhed**

5.1. Område

5.1. Systematisk udforskning og udvikling af teknologien med henblik på økonomisk rentable og driftsmæssigt tilfredsstillende løsninger på en række nutidige og fremtidige behov for informationssikkerhed er en forudsætning for at kunne udvide tjenestemarkedet og forbedre konkurrenceevnen inden for den europæiske industri som helhed betragtet.

28. Enhver form for teknologisk udvikling af informationssystemernes sikkerhed må nødvendigvis indbefatte såvel datamatsikkerhed som kommunikationssikkerhed, idet de fleste moderne systemer er distribuerede systemer, hvortil man får adgang via kommunikationstjenesterne .

5.2. Mål

29. Målet er en systematisk udforskning og udvikling af teknologien med henblik på økonomisk rentable og driftsmæssigt tilfredsstillende løsninger på en række nutidige og fremtidige behov for informationssikkerhed.

5.3. Behov, muligheder og prioriteter

30. Arbejdet inden for informationssikkerhed må omfatte udviklings- og implementeringsstrategi, teknologi, og integration og verificering.

31. Det strategiske F&U-arbejde må indbefatte konceptuelle modeller til sikre systemer (sikre mod kompromis'er), modeller for funktionsbehov, risikomodeller og sikkerhedsorienterede arkitekturer.

32. Det teknologiske F&U-arbejde bør omfatte bruger- og meddelelsesautentificering (f.eks. ved hjælp af stemmeanalyse og elektronisk underskrift), tekniske grænseflader og protokoller for kryptering, adgangskontrolordninger, og metoder til implementering af efterprøveligt sikre systemer.

33. Verificering og validering af tekniske systemers sikkerhed og anvendeligheden heraf skal udforskes inden for integrations- og verificeringsprojekter

34. Udover konsolidering og udvikling sikkerhedsteknologi er det påkrævet med en række ledsageforanstaltninger af hensyn til udarbejdelse, vedligehold og korrekt anvendelse af standarder, samt validering og certificering af IT- og telekommunikationsprodukter med hensyn til deres sikkerhedsegenskaber, herunder validering og certificering af metoder til udformning og implementering af systemer.

35. Fællesskabets tredje rammprogram for FT&U kan eventuelt finde anvendelse med henblik på at fremme samarbejdsbaserede projekter på prækompetitivt og prænormativt niveau.

6. Aktionslinje VI - Realisering af informationssikkerhed

6.1 Område

36. Afhængigt af informationens art er der behov for inkorporering af sikkerhedsfunktioner i forskellige dele af kommunikationssystemerne, blandt andet terminaler og datamater, tjenester, netstyring, krypteringsanordninger, smart cards, offentlige og private nøgler osv. Nogle af disse kan forventes indbygget i hardware og software af producenterne, mens andre kan indgå som en del af distribuerede systemer (f.eks. netstyring), være i den enkelte brugers besiddelse (f.eks. smart cards) eller stilles til rådighed af særlige organisationer (f.eks. offentlige/private nøgler).

37. Det kan forventes, at de fleste informationssikkerhedsprodukter vil blive stillet til rådighed af producenter, tjenesteleverandører og operatører. Med hensyn til specifikke funktioner (f.eks. etablering af offentlige/private nøgler, revision og autorisation) kan det blive nødvendigt at udpege og bemyndige særlige organisationer.

38. Det samme gælder med hensyn til certificering, evaluering og verificering af tjenestens kvalitet, dvs. funktioner, der må kontrolleres af organisationer, der er uafhængige af producenternes. tjenesteleverandørernes og operatørernes interesser. Disse organisationer kan være private, statslige eller være koncessioneret af det offentlige med henblik på varetagelse af bestemte uddelegerede funktioner.

6.2. Mål

39. For at sørge for, at informationssikkerhed stilles til rådighed i Fællesskabet på harmonisk måde, således at offentlighedens og erhvervslivets interesser tilgodeses, må der fastlægge en kohærent fremgangsmåde for, hvorledes dette skal ske. I de tilfælde, hvor der må udpeges uafhængige organisationer, må deres funktioner og vilkår fastlægges og vedtages og i givet fald indføjes i de regulatoriske ramme. Målet bør være at nå frem til en klart defineret og alment accepteret fordeling af ansvaret mellem de forskellige aktører på fællesskabsniveau som en forudsætning for gensidig anerkendelse.

6.3. Status og tendenser

40. Idag er informationssikkerheden kun tilgodeset på specifikke områder, og normalt kun med sigte på tilfredsstillelse af specifikke behov. Tilrettelæggelsen heraf på europæisk niveau er for det meste af uformel art, og man har endnu ikke etableret gensidig anerkendelse af verifikation og certificering uden for visse lukkede grupper. Med informationssikkerhedens voksende betydning begynder der at opstå en presserende behov for at få fastlagt en kohærent fremgangsmåde med hensyn til, hvorledes informationssikkerheden skal tilgodeses i Europa og på internationalt plan.

6.4. Behov, muligheder og prioriteter

41. Da der er mange forskellige aktører involveret, og der er en nær tilknytning til spørgsmål af regulatorisk og lovgivningsmæssig art, er det meget vigtigt på forhånd at nå frem til enighed om, hvilke principper der bør lægges til grund for informationssikkerheden.

For at kunne behandle dette spørgsmål, er det nødvendigt at tage stilling til forskellige aspekter, herunder indkredsning og specificering af, hvilke funktioner der i kraft af deres art kræver, at der står en uafhængig organisation (eller samarbejdende organisationer) til rådighed. Herunder hører eventuelt funktioner såsom administration af et system for offentlige/private nøgler.