



01248/07/DA
WP 136

Udtalelse nr. 4/2007 om begrebet personoplysninger

Vedtaget den 20. juni 2007

Artikel 29-Gruppen er nedsat ved artikel 29 i direktiv 95/46/EF. Den er et uafhængigt EU-rådgivningsorgan vedrørende databeskyttelse og beskyttelse af privatlivets fred. Dens opgave er beskrevet i artikel 30 i direktiv 95/46/EF og artikel 15 i direktiv 2002/58/EF.

Sekretariatet varetages af Direktorat C (Civilret, grundlæggende rettigheder og EU-borgerskab) i Europa-Kommissionen, Generaldirektoratet for Retfærdighed, Frihed og Sikkerhed, B-1049 Bruxelles, Belgien, kontor LX-46 01/43.

Websted: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

**GRUPPEN VEDRØRENDE BESKYTTELSE AF FYSISKE PERSONER I FORBINDELSE MED
BEHANDLING AF PERSONOPLYSNINGER,**

som er nedsat ved Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995¹,

som henviser til artikel 29 og artikel 30, stk. 1, litra a), og stk. 3, i ovennævnte direktiv og artikel 15, stk. 3, i Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002,

som henviser til EF-traktatens artikel 255 og til Europa-Parlamentets og Rådets forordning (EF) nr. 1049/2001 af 30. marts 2001 om aktindsigt i Europa-Parlamentets, Rådets og Kommissionens dokumenter,

som henviser til sin forretningsorden,

HAR VEDTAGET FØLGENDE UDTALELSE:

¹ EFT L 281 af 23.11.1995, s. 31, kan findes på:
http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

I. INDLEDNING	3
II. GENERELLE OVERVEJELSER OG POLITIKSPØRGSMÅL	4
III. ANALYSE AF DEFINITIONEN AF "PERSONOPLYSNINGER" IFØLGE DATABESKYTTELSESDIREKTIVET	6
1. FØRSTE ELEMENT: "ENHVER FORM FOR INFORMATION"	6
2. ANDET ELEMENT: "OM"	9
3. TREDJE ELEMENT: "IDENTIFICERET ELLER IDENTIFICERBAR" [FYSISK PERSON]	12
4. FJERDE ELEMENT: "FYSISK PERSON"	22
IV. HVAD SKER DER, HVIS OPLYSNINGERNE FALDER UDEN FOR DEFINITIONEN?	25
V. KONKLUSIONER	25

I. INDLEDNING

Artikel 29-Gruppen er bevidst om, at der er behov for at foretage en tilbundsgående analyse af begrebet personoplysninger. De foreliggende oplysninger om den nuværende praksis i EU's medlemsstater tyder på, at der er en vis usikkerhed og forskellig praksis i medlemsstaterne med hensyn til en række vigtige aspekter af dette begreb, hvilket kan have betydning for, om de nuværende databeskyttelsesregler fungerer ordentligt i forskellige sammenhænge. Resultatet af denne analyse af et element, som har afgørende betydning for anvendelsen og fortolkningen af databeskyttelsesreglerne, må nødvendigvis få stor indvirkning på en række vigtige spørgsmål og vil være særlig relevant for emner såsom identitetsstyring i forbindelse med e-forvaltning og e-sundhed og i forbindelse med RFID.

Formålet med denne udtalelse fra Artikel 29-Gruppen er at nå frem til en fælles forståelse af begrebet personoplysninger, de situationer, hvor den nationale databeskyttelseslovgivning skal anvendes, og den måde, den skal bruges på. At arbejde på en fælles definition af begrebet personoplysninger er ensbetydende med at definere, hvad der falder inden for og uden for databeskyttelsesreglernes anvendelsesområde. En naturlig følge af dette arbejde er, at der udstikkes retningslinjer for, hvordan databeskyttelsesreglerne bør anvendes på visse kategorier af situationer, som opstår i hele EU; det vil være med til at sikre en ensartet anvendelse af disse standarder, hvilket er en af Artikel 29-Gruppens vigtigste opgaver.

I dette dokument anvendes der eksempler, som er hentet fra de europæiske databeskyttelsesmyndigheders nationale praksis, til at underbygge og illustrere analysen. De fleste eksempler er kun blevet redigeret, så de kan anvendes i denne sammenhæng.

II. GENERELLE OVERVEJELSER OG POLITIKSPØRGSMÅL

Direktivet indeholder en bred definition af personoplysninger

Direktiv 95/46/EF (i det følgende benævnt "databeskyttelsesdirektivet" eller "direktivet") giver følgende definition af personoplysninger:

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

Det skal bemærkes, at denne definition afspejler den europæiske lovgivers ønske om en bred definition af "personoplysninger", som blev fastholdt i hele lovgivningsprocessen. I Kommissionens oprindelige forslag hedder det, at "*der ligesom i konvention 108 vedtages en bred definition for at dække alle oplysninger, som kan være knyttet til en person*"². I Kommissionens ændrede forslag hedder det, at "*det ændrede forslag imødekommer Parlamentets ønske om, at definitionen af "personoplysninger" skal være så generel som muligt, så man medtager alle oplysninger vedrørende en identificerbar person*"³, et ønske, som også Rådet tog hensyn til i den fælles holdning⁴.

Formålet med reglerne i direktivet er at beskytte det enkelte menneske

I artikel 1 i direktiv 95/46/EF og i direktiv 2002/58/EF anføres det klart, hvad det endelige formål med reglerne i disse direktiver er, nemlig at beskytte fysiske personers grundlæggende rettigheder og frihedsrettigheder, især retten til privatlivets fred, i forbindelse med behandling af personoplysninger. Dette er et meget vigtigt element, som der skal tages hensyn til ved fortolkningen og anvendelsen af reglerne i begge direktiverne. Det kan spille en væsentlig rolle, når man skal afgøre, hvordan direktivets bestemmelser skal anvendes i en række situationer, hvor det enkelte menneskes rettigheder ikke er i fare, og det kan mane til forsigtighed med en fortolkning af de samme regler, som ville fratage de pågældende beskyttelsen af deres rettigheder.

Direktivets anvendelsesområde udelukker en række aktiviteter, og teksten giver en vis smidighed, som gør det muligt at finde et passende juridisk svar på de enkelte situationer

På trods af, at begreberne "personoplysninger" og "behandling" er defineret bredt i direktivet, medfører det forhold, at en bestemt situation kan anses for at indebære "behandling af personoplysninger" som defineret i direktivet, ikke i sig selv, at denne situation er underlagt direktivets regler, specielt i henhold til artikel 3. Bortset fra de undtagelser, som skyldes fællesskabsrettens anvendelsesområde, tager undtagelserne i artikel 3 hensyn til den tekniske måde at behandle oplysningerne på (på en manuel,

² KOM(90) 314 endelig af 13.9.1990, s. 19 (bemærkningerne til artikel 2).

³ KOM(92) 422 endelig af 28.10.1992, s. 10 (bemærkningerne til artikel 2).

⁴ Fælles holdning (EF) nr. 1/95, vedtaget af Rådet den 20. februar 1995, EFT C 93 af 13.4.1995, s. 20.

ikke-struktureret måde) og hensigten med brugen (en fysisk persons behandling af oplysningerne med henblik på udøvelse af rent personlige eller familiemæssige aktiviteter). Selv når der er tale om behandling af personoplysninger inden for direktivets anvendelsesområde, er det ikke nødvendigvis alle direktivets regler, der finder anvendelse i det specifikke tilfælde. En række af direktivets bestemmelser rummer en betydelig fleksibilitet, som gør det muligt at opnå en passende balance mellem beskyttelsen af den registreredes rettigheder på den ene side og på den anden side registerførernes og tredjemands legitime interesser og eventuelle samfundsmæssige interesser. Der findes bl.a. eksempler på sådanne bestemmelser i artikel 6 (opbevaringsperioden afhænger af, om oplysningerne er nødvendige), artikel 7, litra f) (afvejning af de forskellige interesser som begrundelse for behandlingen), artikel 10, litra c), sidste led, og artikel 11, stk. 1, litra c) (information til den registrerede, når det er nødvendigt for at sikre en rimelig behandling), og artikel 18 (undtagelser fra anmeldelsespligten), for bare at nævne nogle få tilfælde.

Databeskyttelsesreglernes anvendelsesområde må ikke blive for bredt

Et uønsket resultat ville være, at man endte med at anvende databeskyttelsesreglerne på situationer, som ikke skulle have været omfattet af disse regler, og som lovgiveren ikke havde for øje ved udarbejdelsen af reglerne. De materielle undtagelser under artikel 3, som er nævnt ovenfor, og præciseringerne i direktivets betragtning 26 og 27 viser, hvordan lovgiveren ønskede databeskyttelsen anvendt.

En begrænsning vedrører måden at behandle oplysninger på. Det er nyttigt at huske på, at grundene til, at de første databeskyttelseslove blev indført i 1970'erne var, at den nye teknologi i form af elektronisk databehandling muliggør en lettere og mere udbredt adgang til personoplysninger end de traditionelle former for databehandling. Databeskyttelse i henhold til direktivet sigter derfor mod at beskytte de former for behandling, hvor der typisk er en højere risiko ved at "lette adgangen til personoplysninger" (betragtning 27). Ikke-elektronisk behandling af personoplysninger indgår kun i direktivets anvendelsesområde, når oplysningerne er eller vil blive indeholdt i et register (artikel 3).

En anden generel begrænsning i anvendelsen af databeskyttelse efter direktivet er behandling af oplysninger under omstændigheder, hvor hjælpemidler til identifikation af den registrerede ikke "med rimelighed kan tænkes bragt i anvendelse" (betragtning 26). Dette spørgsmål vil blive behandlet senere.

Men man må også undgå, at fortolkningen af begrebet personoplysninger begrænses for meget

I de tilfælde, hvor en mekanisk anvendelse af hver enkelt bestemmelse i direktivet umiddelbart synes at kunne få unødvendigt tunge eller måske endda absurde følger, må det først kontrolleres, 1) om situationen falder inden for direktivets anvendelsesområde, særlig i henhold til artikel 3, og 2) hvis den falder inden for direktivets anvendelsesområde, om direktivet selv eller den nationale lovgivning, som er vedtaget i medfør af direktivet, ikke giver mulighed for undtagelser eller forenklinger i forhold til specifikke situationer, så man kan finde et hensigtsmæssigt juridisk svar og samtidig sikre, at den enkeltes rettigheder og de forskellige interesser, der er på spil, beskyttes. Det er bedre at lade være med at begrænse fortolkningen af definitionen af personoplysninger for meget og i stedet konstatere, at der er en betydelig fleksibilitet i den måde, hvorpå reglerne anvendes på oplysningerne.

De nationale datatilsynsmyndigheder spiller en væsentlig rolle i denne forbindelse inden for rammerne af deres opgaver med at overvåge anvendelsen af databeskyttelseslovgivningen, som indebærer, at de skal fortolke de retlige bestemmelser og udstikke konkrete retningslinjer for de registeransvarlige og de registrerede. De bør anvende en definition, som er bred nok til, at den kan foregribe udviklingen og omfatte alle "gråzoner" inden for direktivets anvendelsesområde, samtidig med at den helt legitimt udnytter den fleksibilitet, som direktivet giver. Direktivets tekst opfordrer faktisk til, at der udvikles en politik, som kombinerer en bred fortolkning af begrebet personoplysninger og en passende balance i anvendelsen af direktivets regler.

III. ANALYSE AF DEFINITIONEN AF "PERSONOPLYSNINGER" IFØLGE DATABESKYTTELSESDIREKTIVET

Definitionen i direktivet indeholder fire hovedelementer, der vil blive analyseret hver for sig i dette dokument. Der er tale om følgende elementer:

- "enhver form for information"
- "om"
- "en identificeret eller identificerbar"
- "fysisk person".

De fire elementer hænger nøje sammen og påvirker hinanden. Af hensyn til den metode, som anvendes i dette dokument, vil hvert af disse elementer dog blive behandlet separat.

1. FØRSTE ELEMENT: "ENHVER FORM FOR INFORMATION"

Begrebet "enhver form for information", som anvendes i direktivet, viser klart, at lovgiveren er villig til at indføre en bred definition af personoplysninger. Denne formulering lægger op til en bred fortolkning.

Når man ser på oplysningernes art, omfatter begrebet personoplysninger enhver form for udsagn om en person. Det omfatter "objektive" oplysninger, såsom tilstedeværelsen af et bestemt stof i den pågældendes blod. Det omfatter også "subjektive" oplysninger, udtalelser eller vurderinger. Sidstnævnte form for udsagn udgør en betydelig del af behandlingen af personoplysninger, bl.a. i banksektoren i forbindelse med vurderingen af låntagernes pålidelighed ("Titius er en pålidelig låntager"), i forsikringssektoren ("Titius forventes ikke at dø foreløbig") og på arbejdsmarkedet ("Titius er en god medarbejder og fortjener at blive forfremmet").

Oplysninger behøver ikke at være sande eller bevist, for at der skal være tale om "personoplysninger". Databeskyttelsesreglerne omfatter således allerede den mulighed, at oplysningerne er ukorrekte, og giver den registrerede ret til aktindsigt i oplysningerne og til at bestride oplysningerne ved hjælp af passende retsmidler⁵.

⁵ Berigtigelse kan ske ved, at der tilføjes modsatrettede bemærkninger, eller ved brug af passende retsmidler, såsom klageordninger.

Når man ser på oplysningernes indhold, omfatter begrebet personoplysninger oplysninger, som giver enhver form for information. Dette omfatter selvfølgelig personoplysninger, der ifølge direktivets artikel 8 betragtes som "følsomme oplysninger" på grund af deres særlig risikofyldte art, men også mere generelle former for oplysninger. Begrebet "personoplysninger" omfatter oplysninger, der vedrører den pågældendes privatliv og familieliv i snæver forstand, men også oplysninger vedrørende de former for aktiviteter, som den pågældende foretager sig, f.eks. i forbindelse med den pågældendes arbejdsforhold eller økonomiske eller sociale adfærd. De omfatter derfor oplysninger om personer, uanset de pågældendes stilling eller egenskab (som forbruger, patient, medarbejder, kunde mv.).

Eksempel 1: Arbejdsmæssige vaner og praksis

Oplysninger om ordinerings af lægemidler (f.eks. lægemiddelnummer, lægemiddelnavn, lægemidlets styrke, producent, salgspris, nyordinerings eller receptfornyelse, grunde til brugen, begrundelse for ikke-substitution, den ordinerende læges fornavn og efternavn, telefonnummer osv.), enten i form af en individuel recept eller i form af de mønstre, som fremgår af en række recepter, kan betragtes som personoplysninger om den læge, der ordinerer lægemidlet, selv om patienten er anonym. Det at give oplysninger om recepter, som er udstedt af identificerede eller identificerbare læger, til producenter af receptpligtige lægemidler udgør således en videregivelse af personoplysninger til tredjemand i direktivets forstand.

Denne fortolkning støttes af selve direktivets ordlyd. På den ene side må privatliv og familieliv betragtes som brede begreber, hvilket Den Europæiske Menneskerettighedsdomstol da også har fastslået⁶. På den anden side går reglerne om beskyttelse af personoplysninger videre end beskyttelse af det brede begreb "ret til respekt for privatliv og familieliv". Det skal bemærkes, at beskyttelse af personoplysninger i artikel 8 i Den Europæiske Unions charter om grundlæggende rettigheder knæsesættes som en selvstændig rettighed, der er adskilt og forskellig fra retten til respekt for privatliv, der er omhandlet i chartrets artikel 7, og det samme gælder på nationalt plan i visse medlemsstater. Dette stemmer overens med ordlyden i artikel 1, stk. 1, der vedrører beskyttelse af "fysiske personers grundlæggende rettigheder og frihedsrettigheder, især [men ikke udelukkende] retten til privatlivets fred". I direktivet henvises der således specifikt til behandlingen af personoplysninger i sammenhænge uden for hjemmet og familien, f.eks. i forbindelse med arbejdsret (artikel 8, stk. 2, litra b)), straffedomme, administrative sanktioner eller domme i civile retssager (artikel 8, stk. 5) eller direkte markedsføring (artikel 14, litra b)). De Europæiske Fællesskabers Domstol⁷ har tilsluttet sig denne brede tilgang.

⁶ Den Europæiske Menneskerettighedsdomstols dom af 16.2.2000 i sagen Amann mod Schweiz, præmis 65: "[...] begrebet "privatliv" må ikke fortolkes restriktivt. Specielt omfatter respekten for privatlivets fred retten til et etablere og udvikle forhold til andre mennesker; desuden er der ingen principielle grunde til at udelukke faglige eller erhvervmæssige aktiviteter fra begrebet "privatliv" (se dommen af 16. december 1992 i sagen Niemietz mod Tyskland, serie A, nr. 251-B, s. 33-34, præmis 29, og ovennævnte dom i Halford-sagen, s. 1015-16, præmis 42). Denne brede fortolkning stemmer overens med fortolkningen i Europarådets konvention af 28. januar 1981 [...]."

⁷ Dom afsagt den 6.11.2003 af De Europæiske Fællesskabers Domstol i sag C-101/2001 (Lindquist), præmis 24: "Begrebet "personoplysninger" i artikel 3, stk. 1, i direktiv 95/46 omfatter i overensstemmelse med definitionen i artikel 2, litra a), "enhver form for information om en identificeret eller identificerbar fysisk person". Dette begreb omfatter uden tvivl navnet på en person sammen med oplysninger om dennes telefonnummer, eller oplysninger vedrørende dennes arbejdsforhold eller fritidsinteresser."

Med hensyn til formatet eller det medium, som oplysningerne opbevares på, omfatter begrebet personoplysninger de foreliggende oplysninger uanset form, hvad enten de er f.eks. alfabetiske, numeriske, grafiske, fotografiske eller akustiske. Det omfatter bl.a. oplysninger, der opbevares på papir, og oplysninger, der opbevares i en computers hukommelse i form af en binær kode eller på et videobånd. Dette er en logisk følge af, at direktivets anvendelsesområde omfatter elektronisk behandling af personoplysninger. Specielt betragtes lyd og billeddata ud fra dette synspunkt som personoplysninger, da de kan indeholde oplysninger om en person. I den forbindelse skal den særlige henvisning til lyd og billeddata i direktivets artikel 33 forstås som en bekræftelse og præcisering af, at denne form for data rent faktisk indgår i direktivets anvendelsesområde (hvis alle de andre betingelser er opfyldt), og at direktivet finder anvendelse på dem. Dette er en logisk antagelse med hensyn til den bestemmelse i artiklen, som forsøger at vurdere, om direktivets regler giver passende juridiske svar på disse områder. Dette præciseres yderligere af betragtning 14, hvori det hedder: "*der gøres for tiden betydelige fremskridt inden for informationssamfundet med hensyn til udvikling af metoder til at registrere, udsende, bearbejde, lagre, opbevare og videregive oplysninger om fysiske personer via lyd og billede, og det er derfor nødvendigt, at dette direktiv finder anvendelse på behandling af sådanne oplysninger*". På den anden side er det ikke nødvendigt, at oplysningerne opbevares i en struktureret database eller et struktureret register, for at de kan betragtes som personoplysninger. Også oplysninger, som findes i fri tekst i et elektronisk dokument, kan betragtes som personoplysninger, hvis de andre kriterier i definitionen af personoplysninger er opfyldt. F.eks. indeholder e-mail "personoplysninger".

Eksempel 2: Telefonbanker

Når de instrukser, som kunderne giver banken via telefonbanken, optages på bånd, bør de optagne instrukser betragtes som personoplysninger.

Eksempel 3: Videoovervågning

Billeder af personer, som er optaget af videoovervågningssystemer, kan være personoplysninger, i det omfang de pågældende kan genkendes.

Eksempel 4: En børnetegning

Som følge af en neuropsykiatrisk undersøgelse af en pige i forbindelse med en retssag om forældremyndigheden over hende fremlægges der en tegning, hun har lavet, som forestiller hendes familie. Tegningen giver oplysninger om pigens sindsstemning og om hendes følelser i forhold til forskellige familiemedlemmer. Den kan således betragtes som "personoplysninger". Tegningen vil nemlig afsløre oplysninger om barnet (hendes sundhedstilstand ud fra et psykiatrisk synspunkt) og også om f.eks. hendes fars eller mors adfærd. Det betyder, at forældrene i dette tilfælde muligvis kan udøve deres ret til aktindsigt i disse specifikke oplysninger.

Det er relevant specifikt at nævne biometriske oplysninger. Disse oplysninger kan defineres som biologiske egenskaber, fysiologiske karakteristika, særlige træk eller gentagelige handlinger, hvor disse karakteristika og/eller handlinger entydigt vedrører den pågældende og samtidig er målelige, selv om de mønstre, som i praksis bruges til den tekniske måling heraf, indebærer en vis grad af sandsynlighed. Typiske eksempler på sådanne biometriske oplysninger er fingeraftryk, nethindemønstre, ansigtsstruktur og stemme, men også håndgeometri, blodåremønstre eller endog en dybt rodfæstet

færdighed eller andre karakteristiske former for adfærd (såsom en håndskreven underskrift, anslaget på et tastatur eller en særlig måde at gå eller tale på).

Det særlige ved biometriske oplysninger er, at de både kan betragtes som *indholdet* i oplysningerne om en bestemt person (Titius har disse fingeraftryk) og som et element, der gør det muligt at etablere en *forbindelse* mellem en oplysning og den pågældende person (denne genstand er blevet rørt af en person med disse fingeraftryk, og disse fingeraftryk svarer til Titius; denne genstand er derfor blevet rørt af Titius). De kan derfor fungere som "identifikatorer". På grund af deres entydige forbindelse til en bestemt person kan biometriske oplysninger bruges til at identificere den pågældende. Disse to aspekter optræder også i forbindelse med dna-oplysninger, der giver information om menneskekroppen og muliggør en klar og entydig identifikation af en person.

Prøver på menneskeligt væv (f.eks. en blodprøve) er i sig selv kilder, hvorfra der udtrækkes biometriske oplysninger, men de er ikke selv biometriske oplysninger (ligesom f.eks. et fingeraftryksmønster er biometriske oplysninger, mens selve fingeren ikke er det). Udtrækningen af oplysninger fra prøverne er dermed indsamling af personoplysninger, som direktivets regler finder anvendelse på. Indsamling, opbevaring og anvendelse af selve vævsprøverne kan være underlagt særskilte regler⁸.

2. ANDET ELEMENT: "OM"

Denne del af definitionen er afgørende, da det er meget vigtigt præcist at finde ud af, hvilke relationer/forbindelser der har betydning, og hvordan de adskiller sig fra hinanden.

Generelt kan man sige, at der er tale om oplysninger "om" en person, når de *vedrører* den pågældende.

I mange situationer er det let at fastslå denne forbindelse. For eksempel er de oplysninger, som er registreret i éns personlige dossier i personaleafdelingen, tydeligvis oplysninger "om" personens situation som medarbejder. Det samme gælder oplysninger om resultaterne af en patients lægeundersøgelser, som indgår i hans patientjournal, eller billedet af en person, som er optaget under en videosamtale med den pågældende.

Man kan imidlertid nævne en række andre situationer, hvor det ikke altid er så let at afgøre, om der er tale om oplysninger "om" en person, som det var i de nævnte tilfælde.

I nogle situationer vedrører den information, som oplysningerne giver, i første omgang genstande og ikke personer. Disse genstande tilhører som regel en person eller er genstand for en særlig indflydelse fra personer eller har særlig indflydelse på personer, eller de har en eller anden form for fysisk eller geografisk nærhed til personer eller andre genstande. Man kan således kun indirekte sige, at der er tale om oplysninger om de pågældende personer eller genstande.

⁸ Se Europarådets Ministerudvalgs henstilling nr. Rec (2006) 4 af 15.3.2006 om forskning i biologisk materiale af menneskelig oprindelse.

Eksempel 5: Værdien af et hus

Værdien af et bestemt hus er oplysninger om en genstand. Databeskyttelsesreglerne finder tydeligvis ikke anvendelse, når disse oplysninger udelukkende vil blive brugt til at illustrere ejendomspriserne i et bestemt område. Under visse omstændigheder bør sådanne oplysninger imidlertid også betragtes som personoplysninger. Huset er jo et aktiv, der tilhører en ejer, og oplysningerne vil derfor f.eks. blive brugt til at afgøre, i hvilket omfang den pågældende skal betale visse skatter. I den forbindelse er der ingen tvivl om, at disse oplysninger bør betragtes som personoplysninger.

Der skal foretages en tilsvarende analyse, når oplysningerne i første omgang drejer sig om processer eller begivenheder, f.eks. oplysninger om, hvordan en maskine fungerer, når der kræves menneskelig medvirken. Under visse omstændigheder må disse oplysninger også betragtes som oplysninger "om" en person.

Eksempel 6: Servicebog for en bil

De oplysninger, som en mekaniker eller et værksted opbevarer om service på en bil, indeholder information om bilen, kilometertal, datoerne for serviceeftersyn, tekniske problemer og materiel tilstand. Disse oplysninger er i servicebogen knyttet sammen med indregistreringsnummer og motornummer, som igen kan knyttes sammen med ejeren. Når værkstedet etablerer en forbindelse mellem køretøjet og ejeren med henblik på at udskrive en faktura, vil der være tale om oplysninger "om" ejeren eller føreren. Hvis der etableres en forbindelse med den mekaniker, som har arbejdet på bilen, for at vurdere hans produktivitet, er der også tale om oplysninger "om" mekanikeren.

Artikel 29-Gruppen har allerede beskæftiget sig med spørgsmålet om, hvornår der kan siges at være tale om oplysninger "om" en person. I forbindelse med drøftelserne om de databeskyttelsesspørgsmål, som opstår i forbindelse med RFID-tags, bemærkede Artikel 29-Gruppen, at *"der er tale om oplysninger om en person, hvis de henviser til en persons identitet, karakteristika eller adfærd, eller hvis sådanne oplysninger bruges til at bestemme eller påvirke den måde, hvorpå den pågældende behandles eller evalueres"*⁹.

I betragtning af ovennævnte tilfælde kan det efter samme principper påpeges, at der, for at man kan sige, at der er tale om oplysninger "om" en person, skal være et **"indholdselement"** ELLER et **"formålselement"** ELLER et **"resultatelement"**.

"Indholdselementet" er til stede i de tilfælde, hvor der – svarende til den mest indlysende og almindelige forståelse i samfundet af ordet "om" – gives oplysninger vedrørende en bestemt person, uanset registerførers eller tredjemands formål eller oplysningernes indvirkning på den registrerede. Der er tale om oplysninger "om" en person, når oplysningerne "vedrører" den pågældende, og dette skal vurderes i lyset af alle omstændighederne i sagen. For eksempel er resultaterne af en medicinsk analyse tydeligvis oplysninger om patienten, og oplysningerne i en virksomheds kunderegister under en bestemt kundes navn er tydeligvis oplysninger om ham. Og oplysningerne i en RFID-tag eller en strejkode, som er inkorporeret i et identitetsdokument for en bestemt person, er oplysninger om den pågældende. Det gælder bl.a. de fremtidige pas med RFID-chip.

⁹ Artikel 29-Gruppens dokument nr. WP 105: "Working document on data protection issues related to RFID technology", vedtaget den 19.1.2005, s. 8.

Et "**formålselement**" kan også være ansvarligt for, at der er tale om oplysninger "om" en bestemt person. "Formålselementet" kan anses for at eksistere, når oplysningerne bruges eller - under hensyntagen til alle omstændighederne i den pågældende sag - kan forventes at blive brugt med det formål at vurdere en person, behandle den pågældende på en bestemt måde eller påvirke den pågældendes status eller adfærd.

Eksempel 7: Opkaldsregister for en telefon

Opkaldsregistret for en telefon på et kontor i en virksomhed giver oplysninger om de opkald, som er foretaget fra den pågældende telefon, der er forbundet med en bestemt linje. Oplysningerne kan sættes i forbindelse med forskellige personer. På den ene side er linjen stillet til rådighed for virksomheden, og virksomheden er kontraktligt forpligtet til at betale for de pågældende opkald. Telefonapparatet er under en bestemt medarbejders kontrol i arbejdstiden, og det formodes, at det er ham, der har foretaget opkaldene. Opkaldsregistret kan også give oplysninger om den person, som der blev ringet til. Telefonen kan også bruges af andre personer, der har adgang til lokalerne i medarbejderens fravær (f.eks. af rengøringspersonalet). Med forskellige formål kan oplysningerne om brugen af det pågældende telefonapparat sættes i forbindelse med virksomheden, medarbejderen eller rengøringspersonalet (f.eks. for at kontrollere, hvornår rengøringspersonalet forlader arbejdsstedet, når det er meningen, at de telefonisk skal bekræfte, hvad tid de forlader stedet, inden de aflåser lokalerne). Det skal nævnes, at begrebet personoplysninger her både omfatter udgående og indgående opkald, da de alle indeholder oplysninger vedrørende de pågældendes privatliv, sociale forbindelser og kontakter.

En tredje situation, hvor der er tale om oplysninger "om" bestemte personer, opstår, når der er et "**resultatelement**". På trods af, at der ikke er noget "indholdselement" eller "formålselement", kan oplysninger anses for at være oplysninger "om" en person, fordi anvendelsen af oplysningerne kan forventes at få indvirkning på en bestemt persons rettigheder og interesser under hensyntagen til alle omstændighederne i den pågældende sag. Det skal bemærkes, at det ikke er nødvendigt, at det mulige resultat er en stor indvirkning. Det er nok, at personen kan blive behandlet anderledes end andre personer som følge af behandlingen af de pågældende oplysninger.

Eksempel 8: Overvågning af taxaers position for at optimere servicen får indvirkning på chaufførerne

Et taxaselskab opretter et satellitlokaliseringssystem, der gør det muligt at bestemme de disponible taxaers position i realtid. Formålet med behandlingen er at yde bedre service og spare brændstof ved at sende hver kunde, der bestiller en taxa, den bil, som er nærmest på kundens adresse. Strengt taget er de oplysninger, som skal bruges i systemet, oplysninger om bilerne, ikke om chaufførerne. Formålet med behandlingen er ikke at vurdere taxachaufførernes resultater, f.eks. ved at optimere deres ruter. Men systemet gør det muligt at kontrollere taxachaufførernes resultater og tjekke, om de overholder hastighedsgrænserne, forsøger at finde hensigtsmæssige ruter, sidder ved rattet eller holder pause udenfor osv. Det kan derfor have en betydelig indvirkning på disse personer, og derfor kan oplysningerne anses for også at være oplysninger om fysiske personer. Behandlingen bør være underlagt databeskyttelsesreglerne.

Disse tre elementer (indhold, formål og resultat) skal betragtes som alternative betingelser, ikke som kumulative betingelser. Specielt er det, når indholdselementet er til stede, ikke nødvendigt, at de andre elementer er til stede, for at man kan anse

oplysningerne for at være oplysninger om personen. Det betyder, at de samme oplysninger kan vedrøre forskellige personer samtidig, afhængig af hvilket element der er til stede med hensyn til hver af dem. De samme oplysninger kan vedrøre personen Titius på grund af "indholdselementet" (der er tydeligvis tale om oplysninger vedrørende Titius) OG Gaius på grund af "formålselementet" (de vil blive brugt med henblik på at behandle Gaius på en bestemt måde) OG Sempronius på grund af "resultatelementet" (de kan forventes at få indvirkning på Sempronius' rettigheder og interesser). Det betyder også, at det ikke er nødvendigt, at oplysningerne "fokuserer" på en person, for at man kan anse dem for at være oplysninger om ham. Det følger af den foregående analyse, at spørgsmålet om, hvorvidt der er tale om oplysninger om en bestemt person, må besvares særskilt for hver enkelt oplysning. Tilsvarende bør man ved anvendelsen af materielle bestemmelser (f.eks. om anvendelsesområdet for retten til aktindsigt) holde sig for øje, at oplysningerne kan vedrøre forskellige personer.

Eksempel 9: Oplysninger i et mødereferat

Et eksempel på, at det er nødvendigt at foretage den førnævnte analyse med hensyn til hver enkelt oplysning for sig, vedrører oplysningerne i et mødereferat, der typisk registrerer tilstedeværelsen af deltagerne Titius, Gaius og Sempronius og de erklæringer, som Titius og Gaius har fremsat, og indeholder en rapport om drøftelserne af visse spørgsmål, opsummeret af forfatteren til referatet, Sempronius. Det er kun oplysningerne om, at Titius deltog i mødet på et bestemt tidspunkt og et bestemt sted, og at han fremsatte bestemte erklæringer, der kan betragtes som personoplysninger om ham. Gaius' deltagelse i mødet, hans erklæringer og drøftelserne om et spørgsmål, der er opsummeret af Sempronius, er IKKE personoplysninger om Titius. Det gælder, selv om disse oplysninger findes i det samme dokument, og selv om det var Titius, der var ophavsmand til det spørgsmål, som skulle drøftes på mødet. Disse oplysninger er derfor udelukket fra Titius' ret til aktindsigt i sine egne personoplysninger. Det må ved hjælp af ovennævnte analyse separat afgøres, om og i hvilket omfang disse oplysninger kan betragtes som personoplysninger om Gaius og Sempronius.

3. TREDJE ELEMENT: "IDENTIFICERET ELLER IDENTIFICERBAR" [FYSISK PERSON]

Ifølge direktivet skal der være tale om oplysninger om en fysisk person, som er "identificeret eller identificerbar". Dette giver anledning til følgende betragtninger.

Generelt kan en person betragtes som "identificeret", når den pågældende inden for en gruppe af personer kan "skelnes" fra alle de andre medlemmer af gruppen. Den fysiske person er således "identificerbar", når det er muligt at identificere den pågældende (det er betydningen af endelsen "-bar"), selv om det endnu ikke er sket. Dette andet alternativ er derfor i praksis den grænsebetingelse, som afgør, om oplysningerne ligger inden for anvendelsesområdet for det tredje element.

Identifikationen foretages normalt ved hjælp af særlige oplysninger, som vi kan kalde "identifikatorer", og som har en særligt privilegeret og tæt forbindelse med den pågældende person. Eksempler herpå er den pågældendes ydre træk, såsom højde, hårfarve og påklædning, eller en egenskab ved den pågældende, som man ikke umiddelbart kan se, såsom erhverv, stilling og navn. I direktivet nævnes disse "identifikatorer" i definitionen af personoplysninger i artikel 2, hvor det hedder, at en fysisk person "*direkte eller indirekte kan identificeres, bl.a. ved et*

identifikationsnummer eller et eller flere elementer, der er særlige for denne persons fysiske, fysiologiske, psykiske, økonomiske, kulturelle eller sociale identitet".

"Direkte" eller "indirekte" kan identificeres

Bemærkningerne til artiklerne i Kommissionens ændrede forslag indeholder yderligere præciseringer, idet det fastslås, at *"en person kan identificeres direkte med navn eller indirekte med et telefonnummer, et indregistreringsnummer for en bil, et socialsikringsnummer, et pasnummer eller en kombination af væsentlige kriterier, som gør det muligt at genkende ham ved at indsnævre den gruppe, han tilhører (alder, erhverv, bopæl mv.)"*. Denne formulering viser klart, at spørgsmålet om, hvorvidt visse identifikatorer er nok til at sikre en identifikation, afhænger af forholdene i den bestemte situation. Et meget almindeligt efternavn vil ikke være nok til at identificere en person – dvs. udskille den pågældende – når man ser på et lands samlede befolkning, mens det formodentlig vil være nok til at sikre identifikation af en elev i et klasseværelse. Selv mindre væsentlige oplysninger, såsom "manden i sort jakkesæt", kan identificere en person blandt de forbipasserende, der står i et lyskryds. Så spørgsmålet om, hvorvidt den person, som oplysningerne vedrører, er identificeret eller ej, afhænger af omstændighederne i det pågældende tilfælde.

Med hensyn til "direkte" identificerede eller identificerbare personer er personens **navn** den mest almindelige identifikator, og i praksis indebærer begrebet "identificeret person" som oftest en henvisning til den pågældendes navn.

For at fastslå denne identitet skal personens navn sommetider kombineres med andre oplysninger (fødselsdato, forældrenes navne, adresse eller et ansigtsbillede) for at undgå sammenblanding mellem den pågældende og eventuelle navnefæller. For eksempel kan den oplysning, at Titius skylder et bestemt beløb, anses for at vedrøre en identificeret person, fordi den er forbundet med personens navn. Navnet er en oplysning, som viser, at den pågældende bruger den kombination af bogstaver og lyde til at adskille sig fra andre og gøre det muligt for andre personer, som han etablerer forbindelser med, at adskille ham fra andre. Navnet kan også være et udgangspunkt, som fører til oplysninger om, hvor den pågældende bor eller kan findes, og kan også give oplysninger om personer i hans familie (gennem efternavnet) og et antal forskellige juridiske og sociale forbindelser, der er knyttet til navnet (uddannelse, patientjournal, bankkonti). Det kan endda være muligt at finde ud af, hvordan en person ser ud, hvis hans billede knyttes sammen med det pågældende navn. Alle disse nye oplysninger, som er knyttet til navnet, kan gøre det muligt at zoome ind på en person af kød og blod, og gennem identifikatorerne knyttes de oprindelige oplysninger således sammen med en fysisk person, der kan adskilles fra andre personer.

Med hensyn til "indirekte" identificerede eller identificerbare personer vedrører denne kategori typisk fænomenet "entydige kombinationer", uanset om de er små eller store. I tilfælde, hvor de foreliggende identifikators omfang i første omgang ikke gør det muligt at finde frem til en bestemt person, kan den pågældende stadig være "identificerbar", fordi disse oplysninger kombineret med andre oplysninger (uanset om registerføreren har sidstnævnte oplysninger eller ej) vil gøre det muligt at adskille den pågældende fra andre. Her kommer direktivet ind med "et eller flere elementer, der er særlige for denne persons fysiske, fysiologiske, psykiske, økonomiske, kulturelle eller sociale identitet". Nogle karakteristika er så entydige, at en person kan identificeres uden problemer ("den nuværende spanske premierminister"), men en kombination af oplysninger på kategoriniveau (alderskategori, regional oprindelse osv.) kan også være

temmelig entydige under visse omstændigheder, specielt hvis man har adgang til en eller anden slags supplerende oplysninger. Dette fænomen er blevet nøje undersøgt af statistikere, der altid bestræber sig på at undgå brud på fortroligheden.

Eksempel 10: Fragmentariske oplysninger i pressen

Der offentliggøres oplysninger om en tidligere straffesag, som dengang tiltrak sig stor opmærksomhed i offentligheden. Den nuværende artikel indeholder ikke nogen af de traditionelle identifikatorer, specielt ikke de involverede personers navn og fødselsdato.

Det er ikke særlig vanskeligt at få yderligere oplysninger, som gør det muligt at finde ud af, hvem de vigtigste involverede personer er, f.eks. ved at finde frem til aviser fra den relevante periode. Man må gå ud fra, at det ikke er helt usandsynligt, at en eller anden vil træffe sådanne foranstaltninger (såsom at finde frem til gamle aviser), som formodentlig vil give navnene og andre identifikatorer for de personer, der er nævnt i eksemplet. Det er derfor rimeligt at anse oplysningerne i eksemplet for at være "oplysninger om identificerbare personer" og dermed "personoplysninger".

Det skal her bemærkes, at et navn i sig selv ikke i alle tilfælde er nødvendigt for at identificere en person, selv om identifikation ved hjælp af navnet er den mest almindelige metode i praksis. Dette kan forekomme, når der anvendes andre "identifikatorer" til at indkredse en person. I edb-registre, som indeholder personoplysninger, anvendes der som regel en entydig identifikator for de registrerede personer for at undgå sammenblanding af to personer i registret. På internettet gør redskaber til overvågning af internettrafikken det også let at identificere en maskines adfærd og, bag ved maskinen, brugerens adfærd. Den enkeltes personlighed stykkes således sammen, så visse beslutninger kan tillægges den pågældende. Uden overhovedet at spørge om personens navn og adresse er det muligt at kategorisere den pågældende på grundlag af socioøkonomiske, psykologiske, filosofiske eller andre kriterier og tillægge den pågældende visse beslutninger, da vedkommendes kontaktpunkt (en computer) ikke længere nødvendigvis kræver, at vedkommendes identitet i snæver forstand afsløres. Med andre ord er muligheden for at identificere en person ikke længere nødvendigvis lig med muligheden for at finde frem til den pågældendes navn. Definitionen af personoplysninger afspejler dette forhold¹⁰.

De Europæiske Fællesskabers Domstol har bekræftet dette, idet den har udtalt, at "*en operation, der består i på en internetside at henvise til forskellige personer, og i at identificere dem ved navn eller på anden måde, f.eks. ved at oplyse deres telefonnummer eller ved at give oplysninger om deres arbejdsforhold og fritidsinteresser, udgør en behandling af personoplysninger [...] i den forstand, hvori udtrykket er anvendt i direktiv 95/46/EF*"¹¹.

Eksempel 11: Asylansøgere

Asylansøgere, der skjuler deres rigtige navne på et asylcenter, har fået et kodenummer til administrativ brug. Dette nummer bruges som identifikator, så forskellige

¹⁰ Rapport om anvendelsen af databaseskyttelsesprincipperne på de verdensomspændende telekommunikationsnet af Yves Pouillet og hans team for Europarådets Rådgivende Komité (T-PD), punkt 2.3.1, T-PD (2004) 04 endelig.

¹¹ Dom afsagt den 6.11.2003 af De Europæiske Fællesskabers Domstol i sag C-101/2001 (Lindquist), præmis 27.

oplysninger om asylansøgernes ophold på centret kan knyttes til det, og ved hjælp af et fotografi eller andre biometriske indikatorer har kodenummeret en tæt og direkte forbindelse med den fysiske person, så han kan adskilles fra andre asylansøgere, og der kan registreres forskellige oplysninger om ham, der så henviser til en "identificeret" fysisk person.

I artikel 8, stk. 7, hedder det, at "medlemsstaterne bestemmer, på hvilke betingelser et nationalt identifikationsnummer eller andre almene midler til identifikation kan gøres til genstand for behandling". Det er værd at lægge mærke til betydningen af denne bestemmelse, som ikke indeholder nogen særlige oplysninger om, hvilke former for betingelser medlemsstaterne bør indføre, men dog er anbragt i artiklen om følsomme oplysninger. I betragtning 33 omtales denne form for oplysninger som "*oplysninger, som ifølge deres art kan krænke de grundlæggende frihedsrettigheder eller privatlivets fred*". Det er rimeligt at antage, at lovgiveren har haft tilsvarende hensyn for øje i forbindelse med nationale identifikationsnumre, fordi de giver gode muligheder for let og utvetydigt at forbinde forskellige oplysninger om en bestemt person.

Identifikationsmidler

I betragtning 26 i direktivet lægges der særlig vægt på ordet "identificerbar", idet det hedder: "*for at afgøre, om en person er identificerbar, tages alle de hjælpemidler i betragtning, der med rimelighed kan tænkes bragt i anvendelse for at identificere den pågældende enten af den registeransvarlige eller af enhver anden person*". Det betyder, at det, at der blot er en hypotetisk mulighed for at udskille den pågældende, ikke er nok til, at personen kan betragtes som "identificerbar". Hvis muligheden under hensyntagen til "*alle de hjælpemidler, der med rimelighed kan tænkes bragt i anvendelse af den registeransvarlige eller af enhver anden person*", enten ikke eksisterer eller er forsvindende lille, bør personen ikke betragtes som "identificerbar", og oplysningerne betragtes ikke som "personoplysninger". Kriteriet om "*alle de hjælpemidler, der med rimelighed kan tænkes bragt i anvendelse enten af den registeransvarlige eller af enhver anden person*", bør specielt tage hensyn til alle de involverede faktorer. Omkostningerne ved at foretage en identifikation er én faktor, men ikke den eneste. Der bør tages hensyn til det tilsigtede formål, den måde, behandlingen er struktureret på, den fordel, som registerføreren forventer, de interesser, som er på spil for de pågældende personer, samt risikoen for organisationsmæssige fejl (f.eks. brud på tavshedspligten) og tekniske fejl. På den anden side er denne test dynamisk og bør tage hensyn til den seneste nye teknologi på tidspunktet for behandlingen og mulighederne for udvikling i den periode, hvor oplysningerne vil blive behandlet. Identifikation er måske ikke på nuværende tidspunkt mulig med alle de hjælpemidler, der med rimelighed kan tænkes bragt i anvendelse i dag. Hvis det er meningen, at oplysningerne skal opbevares i en måned, kan det ikke forventes, at en identifikation vil være mulig i oplysningernes "levetid", og de bør ikke betragtes som personoplysninger. Men hvis de skal opbevares i 10 år, bør den registeransvarlige overveje den mulighed for identifikation, som også kan opstå i det niende år af oplysningernes levetid, og som på det tidspunkt kan gøre dem til personoplysninger. Systemet bør kunne tilpasses til en sådan udvikling, efterhånden som den sker, og man bør så efterhånden kunne inkorporere passende tekniske og organisationsmæssige foranstaltninger.

Eksempel 12: Offentliggørelse af røntgenbilleder sammen med patientens fornavn

En kvindes røntgenbillede var blevet offentliggjort i et videnskabeligt tidsskrift sammen med hendes fornavn, der var meget usædvanligt. Personens fornavn

kombineret med hendes slægtnings eller bekendtes viden om, at hun led af en bestemt sygdom, gjorde hende identificerbar for en række personer, og røntgenbilledet skulle derfor betragtes som personoplysninger.

Eksempel 13: Oplysninger om lægemiddelforskning

Hospitalerne eller de enkelte læger overfører oplysninger fra deres patienters journaler til en virksomhed med henblik på medicinsk forskning. Man anvender ikke patienternes navne, men kun serienumre, som vilkårligt tildeles hvert klinisk tilfælde, så man sikrer sammenhæng og undgår sammenblanding af oplysninger om forskellige patienter. Det er udelukkende de respektive læger, som har tavshedspligt, der har patienternes navne. Oplysningerne indeholder ikke yderligere information, som gør det muligt at identificere patienterne ved at kombinere oplysningerne. Desuden har man truffet alle andre nødvendige juridiske, tekniske og organisationsmæssige foranstaltninger for at forhindre, at de registrerede identificeres eller bliver identificerbare. Under disse omstændigheder kan en databeskyttelsesmyndighed være af den opfattelse, at der i den behandling, som foretages af medicinalfirmaet, ikke findes nogen hjælpemidler, som gør det sandsynligt, at oplysningerne med rimelighed kan tænkes bragt i anvendelse for at identificere de registrerede.

Som allerede nævnt er en relevant faktor for vurderingen af "*alle de hjælpemidler, der med rimelighed kan tænkes bragt i anvendelse*" for at identificere de pågældende det formål, som den registeransvarlige har med databehandlingen. De nationale databeskyttelsesmyndigheder har stået over for tilfælde, hvor den registeransvarlige på den ene side hævder, at der kun behandles spredte oplysninger uden henvisning til et navn eller andre direkte identifikatorer, og taler for, at oplysningerne ikke bør betragtes som personoplysninger og ikke bør være underlagt databeskyttelsesreglerne. På den anden side giver behandlingen af de pågældende oplysninger kun mening, hvis den gør det muligt at identificere specifikke personer og at behandle dem på en bestemt måde. I disse tilfælde, hvor formålet med behandlingen indebærer identifikation af personer, kan det antages, at den registeransvarlige eller en anden involveret person har eller vil få de hjælpemidler, der "*med rimelighed kan tænkes bragt i anvendelse*" for at identificere den registrerede. Det er selvmodsigende at påstå, at personer ikke er identificerbare, når formålet med behandlingen netop er at identificere dem. Oplysningerne bør derfor betragtes som oplysninger om identificerbare personer, og behandlingen bør være underlagt databeskyttelsesreglerne.

Eksempel 14: Videoovervågning

Dette er særlig relevant i forbindelse med videoovervågning, hvor de registeransvarlige ofte hævder, at der kun vil ske identifikation i forbindelse med en lille procentdel af det indsamlede materiale, og at der derfor ikke behandles personoplysninger, før identifikationen i disse få tilfælde rent faktisk finder sted. Da formålet med videoovervågning imidlertid er at identificere de personer, som kan ses på videobillederne i alle de tilfælde, hvor den registeransvarlige anser en sådan identifikation for nødvendig, må hele applikationen som sådan betragtes som behandling af oplysninger om identificerbare personer, selv om nogle af de personer, som er blevet optaget, ikke er identificerbare i praksis.

Eksempel 15: Dynamiske IP-adresser

Artikel 29-Gruppen har anset IP-adresser for at være oplysninger om en identificerbar person. Den har udtalt, at *"internetadgangsudbydere og administratorer af lokale netværk med forholdsvis enkle midler kan identificere de internetbrugere, de har tildelt IP-adresser, da de normalt systematisk "logger" dato, tidspunkt, varighed og den dynamiske IP-adresse, som er tildelt internetbrugeren, i en fil. Det samme kan siges om internettjenesteudbyderen, der fører en log på HTTP-serveren. I disse tilfælde er der ingen tvivl om, at man kan tale om personoplysninger i betydningen efter direktivets artikel 2, litra a)"¹².*

Specielt i de tilfælde, hvor behandlingen af IP-adresser foretages med henblik på at identificere brugerne af computeren (for eksempel når indehavere af ophavsrettigheder ønsker at retsforfølge computerbrugere for krænkelse af intellektuelle ejendomsrettigheder), foregriber den registeransvarlige, at de "hjælpemidler, der med rimelighed kan tænkes bragt i anvendelse" for at identificere de pågældende, vil være til rådighed, f.eks. gennem de domstole, som sagen indbringes for (ellers giver indsamlingen af oplysningerne ikke mening), og oplysningerne bør derfor betragtes som personoplysninger.

Et særligt tilfælde ville være visse former for IP-adresser, som under visse omstændigheder rent faktisk ikke gør det muligt at identificere brugeren af forskellige tekniske og organisationsmæssige grunde. Et eksempel er de IP-adresser, som tildeles en computer på en internetcafé, hvor der ikke kræves nogen identifikation af kunderne. Man kan hævde, at de oplysninger, som indsamles om brugen af computer X i et vist tidsrum, ikke gør det muligt at identificere brugerne med rimelige midler, og at de derfor ikke er personoplysninger. Det skal imidlertid bemærkes, at internetudbyderne formodentlig heller ikke ved, om den pågældende IP-adresse muliggør identifikation eller ej, og at de vil behandle de oplysninger, som er knyttet til den pågældende IP, på samme måde, som de behandler oplysninger, der er knyttet til IP-adresser for brugere, der er registreret og er identificerbare. Så medmindre internetudbyderen med 100 % sikkerhed kan fastslå, at oplysningerne svarer til brugere, der ikke kan identificeres, vil det være nødvendigt at behandle alle IP-oplysninger som personoplysninger for at være på den sikre side.

Eksempel 16: Skader på grund af graffiti

En række busser, der tilhører et busselskab, bliver jævnligt beskadiget, når de svines til med graffiti. For at kunne vurdere skaderne og gøre det lettere at rejse erstatningskrav mod gerningsmændene opretter selskabet et register, som indeholder oplysninger om omstændighederne i forbindelse med skaderne og billeder af de beskadigede busser og af graffitimalerens "tags" eller "signatur". På det tidspunkt, hvor oplysningerne optages i registret, kendes gerningsmændene ikke, og man ved ikke, hvem "signaturen" svarer til. Det kan meget vel tænkes, at man aldrig finder ud af det. Men formålet med behandlingen er netop at identificere de personer, som oplysningerne vedrører, som dem, der har forvoldt skaden, så man kan rejse erstatningskrav mod dem. En sådan behandling giver mening, hvis den registeransvarlige forventer, at det er "rimeligt sandsynligt", at det en dag vil være muligt at identificere den pågældende. De oplysninger, som findes i billederne, bør betragtes som oplysninger om

¹² WP 37: Beskyttelse af privatlivets fred på Internettet – En integreret EU-strategi til beskyttelse af onlineoplysninger – vedtaget den 21.11.2000.

"identificerbare" personer, oplysningerne i registret bør betragtes som "personoplysninger", og behandlingen bør være underlagt databeskyttelsesreglerne, der tillader en sådan behandling under visse omstændigheder, hvis de nødvendige garantier overholdes.

Når identifikation af den registrerede ikke indgår i formålet med behandlingen, spiller de tekniske foranstaltninger, der skal forhindre identifikation, en meget vigtig rolle. Indførelsen af passende nye teknologiske og organisationsmæssige foranstaltninger med henblik på at beskytte oplysningerne mod identifikation kan betyde, at man kan gå ud fra, at personerne ikke er identificerbare under hensyntagen til *alle de hjælpemidler, der med rimelighed kan tænkes bragt i anvendelse for at identificere de pågældende af den registeransvarlige eller af enhver anden person*. I dette tilfælde er gennemførelsen af de pågældende foranstaltninger ikke en *følge* af en juridisk forpligtelse, som følger af direktivets artikel 17 (der kun finder anvendelse, hvis der er tale om personoplysninger), men snarere en *betingelse* for, at oplysningerne netop ikke skal betragtes som personoplysninger, og at behandlingen af oplysningerne ikke er underlagt direktivet.

Pseudonymiserede oplysninger

Pseudonymisering er den proces, hvor man tilslører identiteter. Formålet med denne proces er at kunne indsamle yderligere oplysninger om den samme person, uden at man behøver at kende den pågældendes identitet. Dette er særlig relevant i forbindelse med forskning og statistikker.

Pseudonymiseringen kan gøres på en måde, så oplysningerne kan spores tilbage, ved at man anvender lister, som viser sammenhængen mellem identiteterne og deres pseudonymer, eller ved, at man anvender tovejskrypteringsalgoritmer til pseudonymisering. Identiteterne kan også tilsløres på en måde, som ikke muliggør genidentifikation, f.eks. ved hjælp af envejskryptering, som generelt skaber anonymiserede oplysninger.

Pseudonymiseringsprocedurens effektivitet afhænger af en række faktorer (i hvilken fase den bruges, hvor sikker den er i forhold til baglæns sporing, størrelsen af den population, som personen er skjult i, muligheden for at forbinde individuelle transaktioner eller optegnelser med den samme person mv.). Pseudonymerne bør være vilkårlige og uforudsigelige. Antallet af mulige pseudonymer bør være så stort, at det samme pseudonym aldrig vælges vilkårligt to gange. Hvis der kræves et højt sikkerhedsniveau, skal sættet af mulige pseudonymer mindst svare til antallet af værdier af sikre kryptografiske hashfunktioner¹³.

Pseudonymiserede oplysninger, som kan spores tilbage, kan betragtes som oplysninger om personer, der er *indirekte identificerbare*. Når man bruger et pseudonym, betyder det, at det er muligt at finde tilbage til den pågældende, så vedkommendes identitet kan opdages, men kun under omstændigheder, som er fastsat på forhånd. I så fald gælder databeskyttelsesreglerne, men risiciene for de pågældende med hensyn til behandlingen af sådanne indirekte identificerbare oplysninger er som oftest små, så der er grund til at

¹³ Se "Working document "Privacy-enhancing technologies" by the Working Group on "privacy enhancing technologies" of the Committee on "Technical and organisational aspects of data protection" of the German Federal and State Data Protection Commissioners (October 1997)", offentliggjort på http://ec.europa.eu/justice_home/fsj/privacy/studies/index_en.htm

anvende disse regler på en mere smidig måde, end hvis man havde behandlet oplysninger om direkte identificerbare personer.

Oplysninger med nøglekode

Oplysninger med nøglekode er et klassisk eksempel på pseudonymisering. Oplysningerne vedrører personer, som er markeret med en kode, mens den nøgle, som udgør forbindelsen mellem koden og de almindelige identifikatorer for personerne (såsom navn, fødselsdato og adresse), opbevares separat.

Eksempel 17: Ikke-aggregerede oplysninger til statistikker

Et eksempel, der illustrerer betydningen af at tage hensyn til alle omstændighederne, når man skal vurdere, om midlerne til identifikation "med rimelighed kan tænkes bragt i anvendelse", er personoplysninger, der behandles af det nationale statistiske kontor, hvor oplysningerne i en bestemt fase opbevares i ikke-aggregeret form og vedrører specifikke personer, men disse nævnes med en kode i stedet for et navn (f.eks. drikker den person, som har koden X1234, et glas vin mere end tre gange om ugen). Det statistiske kontor opbevarer nøglen til disse koder (listen, som forbinder koderne med personernes navne) separat. Nøglen kan "med rimelighed tænkes bragt i anvendelse" af det statistiske kontor, og sættet af personrelaterede oplysninger kan derfor betragtes som personoplysninger, og det statistiske kontor bør behandle dem i overensstemmelse med databeskyttelsesreglerne. Man kan så forestille sig, at en liste med oplysninger om forbrugernes drikkevaner med hensyn til vin overføres til den nationale vinproducentorganisation, så den kan underbygge sin officielle holdning med statistiske tal. For at afgøre, om listen med oplysninger stadig er personoplysninger, bør det vurderes, om de enkelte vindrikkere kan identificeres *"i betragtning af alle de hjælpemidler, der med rimelighed kan tænkes bragt i anvendelse af den registeransvarlige eller af enhver anden person"*.

Hvis der anvendes en entydig kode for hver enkelt person, opstår risikoen for identifikation, når det er muligt at få adgang til den nøgle, som er anvendt til krypteringen. Risikoen for et eksternt hack, sandsynligheden for, at en person i afsenderens organisation – på trods af sin tavshedspligt – ville give nogen nøglen og muligheden for indirekte identifikation er faktorer, som der må tages hensyn til, når man skal afgøre, om personerne kan identificeres *i betragtning af alle de hjælpemidler, der med rimelighed kan tænkes bragt i anvendelse af den registeransvarlige eller af enhver anden person*, og derfor, om oplysningerne skal betragtes som "personoplysninger". Hvis det er tilfældet, finder databeskyttelsesreglerne anvendelse. Et andet spørgsmål er, at disse databeskyttelsesregler kan tage hensyn til, om risiciene for de pågældende personer er begrænsede, og underlægge behandlingen mere eller mindre strenge betingelser på grundlag af den fleksibilitet, som direktivets regler giver.

Hvis koderne på den anden side ikke er entydige, men det samme kodenummer (f.eks. "123") bruges til at betegne personer i forskellige byer og oplysninger fra forskellige år (så man kun indkredser en bestemt person inden for et år og inden for populationen i samme by), vil den registeransvarlige eller en tredjemand kun kunne identificere en bestemt person, hvis han ved, hvilket år og hvilken by oplysningerne henviser til. Hvis disse yderligere oplysninger er forsvundet, og det ikke med rimelighed kan forventes, at man kan finde frem til dem igen, kan man anse, at oplysningerne ikke henviser til identificerbare oplysninger og ikke er underlagt databeskyttelsesreglerne.

Denne form for oplysninger anvendes sædvanligvis til kliniske forsøg med lægemidler. I direktiv 2001/20/EF af 4. april 2001 om anvendelse af god klinisk praksis ved gennemførelse af kliniske forsøg¹⁴ fastlægges der en juridisk ramme for gennemførelsen af sådanne aktiviteter. Den sundhedsperson/forsker ("undersøger"), der afprøver lægemidlerne, indsamler oplysningerne om de kliniske resultater for hver patient og tildeler den pågældende en kode. Forskeren giver kun oplysningerne til medicinalfirmaet eller andre involverede parter ("sponsorer") i denne kodede form, da de kun er interesseret i biostatistiske oplysninger. Men undersøgeren opbevarer separat en nøgle, som forbinder denne kode med almindelige oplysninger, så det er muligt at identificere patienterne hver for sig. For at beskytte patienternes helbred i tilfælde af, at lægemidlerne viser sig at udgøre en fare, er undersøgeren forpligtet til at opbevare denne nøgle, så de enkelte patienter om nødvendigt kan identificeres og få den rette behandling.

Spørgsmålet er her, om de oplysninger, der bruges til det kliniske forsøg, kan anses for at vedrøre "identificerbare" fysiske personer og dermed er underlagt databeskyttelsesreglerne. Ifølge ovenstående analyse skal der, når man skal afgøre, om en person er identificerbar, tages hensyn til alle hjælpemidler, der med rimelighed kan tænkes bragt i anvendelse for at identificere den pågældende af den registeransvarlige eller af enhver anden person. I dette tilfælde er identifikationen af personer (så man om nødvendigt kan give den rigtige behandling) et af formålene med behandlingen af oplysningerne med nøglekode. Medicinalfirmaet har opbygget de midler, som skal bruges til databehandlingen, herunder de organisationsmæssige foranstaltninger og firmaets forbindelser med forskeren, der har nøglen, på en sådan måde, at identifikationen af personer ikke blot er noget, der *kan* ske, men snarere noget, der *skal* ske under visse omstændigheder. Identifikationen af patienterne er således en del af formålene med og midlerne til databehandlingen. I dette tilfælde kan man konkludere, at sådanne oplysninger med nøglekode udgør oplysninger vedrørende identificerbare fysiske personer for alle parter, der kan være involveret i en mulig identifikation, og at databeskyttelseslovgivningens regler bør finde anvendelse. Det betyder dog ikke, at enhver anden registeransvarlig, som behandler det samme sæt af kodede oplysninger, behandler personoplysninger, hvis genidentifikation udtrykkeligt er udelukket inden for den specifikke ordning, hvor de pågældende andre registeransvarlige arbejder, og der er truffet passende tekniske foranstaltninger med henblik herpå.

På andre forskningsområder eller inden for andre områder af samme projekt kan genidentifikation af den registrerede være blevet udelukket i udformningen af protokollerne og proceduren, f.eks. fordi der ikke er nogen terapeutiske aspekter involveret. Af tekniske eller andre grunde kan der stadig være en måde, hvorpå man kan finde ud af, hvilke personer der svarer til hvilke kliniske oplysninger, men identifikationen formodes eller forventes ikke at finde sted under nogen omstændigheder, og der er indført passende tekniske foranstaltninger (f.eks. kryptografisk, irreversibel hashing) for at forhindre, at det sker. Selv om identifikation af visse registrerede i dette tilfælde kan forekomme på trods af alle disse protokoller og foranstaltninger (på grund af uforudsete omstændigheder, såsom tilfældig matchning af karakteristika ved den registrerede, som afslører den pågældendes identitet), kan de oplysninger, som den oprindelige registeransvarlige behandler, ikke anses for at vedrøre identificerede eller identificerbare personer, når man tager *alle de hjælpemidler i betragtning, der med rimelighed kan tænkes bragt i anvendelse af den registeransvarlige eller af enhver anden person*. Behandlingen af oplysningerne

¹⁴

EFT L 121 af 1.5.2001, s. 34.

behøver således ikke være underlagt direktivets bestemmelser. En anden sag er, at for den nye registeransvarlige, som rent faktisk har fået adgang til de identificerbare oplysninger, vil de utvivlsomt vil blive betragtet som "personoplysninger".

FAQ 14-7 i safe harbor-ordningen

Spørgsmålet om oplysninger med nøglekode inden for lægemiddelforskning er blevet behandlet i safe harbor-ordningen¹⁵. FAQ 14-7 har følgende ordlyd:

FAQ 14 – Farmaceutiske og medicinske produkter

7. spørgsmål: Som regel koder undersøgeren forskningsoplysningerne entydigt ved kilden for ikke at afsløre de registreredes identitet. De farmaceutiske virksomheder, der sponsorerer en sådan forskning, modtager ikke en nøgle til denne kode. Det er udelukkende forskeren, der er i besiddelse af den entydige nøgle, således at han/hun under særlige forhold er i stand til at identificere den enkelte forskningsdeltager (f.eks. hvis der er behov for efterfølgende medicinsk kontrol). Skal en overførsel fra EU til USA af oplysninger, der er kodet på denne måde, betragtes som en overførsel af personoplysninger, der er underlagt safe harbor-principperne?

7. svar: Nej, det vil ikke kunne karakteriseres som en overførsel af personoplysninger, der kræver overholdelse af safe harbor-principperne.

Artikel 29-Gruppen mener ikke, at denne erklæring i safe harbor-ordningen er uforenelig med ovenstående argumentation for, at sådanne oplysninger bør betragtes som personoplysninger, der er underlagt direktivet. Rent faktisk er dette spørgsmål ikke tilstrækkeligt præcist, da det ikke anføres, til hvem og under hvilke omstændigheder oplysningerne overføres. Artikel 29-Gruppen forstår, at spørgsmålet henviser til det tilfælde, hvor oplysningerne med nøglekode sendes til en modtager i USA (f.eks. den farmaceutiske virksomhed), der kun modtager oplysningerne med nøglekode og aldrig vil få kendskab til patienternes identitet, som kun kendes (og i tilfælde af, at der er behov for behandling, kun vil blive kendt) af sundhedspersonen/forskeren i EU, men aldrig vil blive kendt af virksomheden i USA.

Anonyme oplysninger

"Anonyme oplysninger" i direktivets forstand kan defineres som alle oplysninger om en fysisk person, hvor den pågældende ikke kan identificeres af den registeransvarlige eller af nogen anden person *i betragtning af alle de hjælpemidler, der med rimelighed kan tænkes bragt i anvendelse til at identificere den pågældende enten af den registeransvarlige eller af enhver anden person*. "Anonymiserede oplysninger" er derfor anonyme oplysninger, som tidligere henviste til en identificerbar person, men hvor identifikation ikke længere er mulig. Betragtning 26 henviser også til dette begreb, idet det hedder, at "*beskyttelsesprincipperne gælder ikke oplysninger, som er gjort anonyme på en sådan måde, at den registrerede ikke længere kan identificeres*". Vurderingen af, hvorvidt oplysningerne muliggør identifikation af en person, og om oplysningerne kan betragtes som anonyme eller ej, afhænger også her af omstændighederne, og der bør foretages en analyse af de enkelte tilfælde med særlig vægt på, i hvilket omfang hjælpemidlerne med rimelighed kan tænkes bragt i anvendelse til identifikation som beskrevet i betragtning 26. Dette er særlig relevant, når der er tale om statistiske oplysninger, hvor den oprindelige population ikke er stor

¹⁵ Kommissionens beslutning 2000/520/EF af 26.7.2000, EFT L 215 af 25.8.2000, s. 7.

nok, og andre oplysninger kan muliggøre identifikation af de pågældende på trods af, at oplysningerne fremlægges som aggregerede oplysninger.

Eksempel 18: Statistiske undersøgelser og kombination af spredte oplysninger

Bortset fra deres generelle pligt til at respektere databeskyttelsesreglerne er statistikerne for at sikre anonymiteten i de statistiske undersøgelser underlagt en særlig tavshedspligt, og disse regler forbyder dem at offentliggøre ikke-anonyme oplysninger. Dette tvinger dem til at offentliggøre aggregerede statistiske oplysninger, som det ikke er muligt at forbinde med en identificeret person bag statistikkerne. Denne regel er særlig relevant, når der er tale om offentliggørelse af folketællingsdata. I hver situation bør der fastlægges en grænse, hvorunder det anses for at være muligt at identificere de pågældende personer. Hvis et kriterium ser ud til at medføre identifikation i en given kategori af personer, uanset hvor stor den er (f.eks. hvis der kun er én læge i en by med 6 000 indbyggere), bør dette "diskriminerende" kriterium helt udelades, eller der bør tilføjes andre kriterier for at "udvande" resultaterne om en given person, så den statistiske tavshedspligt overholdes.

Eksempel 19: Offentliggørelse af videoovervågning

En butiksindehaver installerer et videoovervågningssystem i sin butik. Han offentliggør i sin butik billederne af de tyve, der er blevet fanget ved hjælp af kameraovervågningssystemet. Efter en henvendelse fra politiet tilslører han tyvenes ansigter ved at gøre dem mørke. Men selv efter at dette er gjort, er der stadig en mulighed for, at personer på billederne kan genkendes af deres venner, slægtninge eller naboer, fordi f.eks. deres skikkelse, frisure og tøj stadig kan genkendes.

4. FJERDE ELEMENT: "FYSISK PERSON"

Den beskyttelse, som direktivets regler giver, finder anvendelse på fysiske personer, dvs. mennesker. Retten til beskyttelse af personoplysninger er i den forstand en universel rettighed, som ikke er begrænset til personer, der er statsborgere eller har bopæl i et bestemt land. I betragtning 2 i direktivet fastslås dette udtrykkeligt, idet det hedder, at "*databehandlingssystemer er til for menneskets skyld*", og at de "*skal være i overensstemmelse med de grundlæggende rettigheder og frihedsrettigheder, der gælder for fysiske personer, uanset statsborgerskab og bopæl*".

Begrebet fysisk person er omhandlet i artikel 6 i verdenserklæringen om menneskerettigheder, hvori det hedder: "*Ethvert menneske har overalt i verden ret til at blive anerkendt som retssubjekt*". Medlemsstaternes lovgivning, normalt inden for civilretten, giver en mere præcis definition af begrebet menneskers personlighed, der forstås som evnen til at være subjekt i retsforhold, der begynder med den pågældendes fødsel og slutter med vedkommendes død. Personoplysninger er derfor i princippet oplysninger om identificerede eller identificerbare levende personer. Det rejser et antal spørgsmål i forbindelse med denne analyse.

Oplysninger om døde personer

Oplysninger om døde personer skal derfor i princippet ikke betragtes som personoplysninger, der er underlagt direktivets regler, da døde personer ikke længere civilretligt er fysiske personer. Men oplysningerne om afdøde kan stadig indirekte nyde en vis beskyttelse i visse tilfælde.

På den ene side er den registeransvarlige ikke altid i stand til at finde ud af, om den person, som oplysningerne vedrører, stadig lever eller måske er død. Og selv om han er i stand til det, kan oplysningerne om døde personer forskelsløst behandles efter de samme regler som oplysningerne om levende personer. Da den registeransvarlige er underlagt de databeskyttelsesforpligtelser, som direktivet fastsætter, med hensyn til oplysninger om levende personer, er det formodentlig i praksis lettere for ham også at behandle oplysninger om døde personer på den måde, som databeskyttelsesreglerne kræver, i stedet for at adskille de to sæt oplysninger.

På den anden side kan oplysningerne om døde personer også henvise til levende personer. For eksempel tyder oplysningen om, at afdøde Gaia led af hæmofili, på, at hendes søn Titus også lider af samme sygdom, da den er knyttet til et gen, som findes på X-kromosomet. Når den information, som udgør oplysninger om den døde person, samtidig kan anses for også at vedrøre en levende person og for at være personoplysninger, der er underlagt direktivet, kan afdødes personoplysninger indirekte være beskyttet af databeskyttelsesreglerne.

For det tredje kan oplysninger om døde personer være underlagt en særlig beskyttelse, som findes i et andet sæt regler end databeskyttelseslovgivningen, og som indeholder bestemmelser om, hvad nogle kalder "*personalitas praeterita*". Sundhedspersonernes tavshedspligt slutter ikke med patientens død. Den nationale lovgivning om retten til sit rygte og sin ære kan også være med til at beskytte afdødes minde.

Og for det fjerde er der som fastslået af De Europæiske Fællesskabers Domstol intet til hinder for, at en medlemsstat udvider rækkevidden af den nationale lovgivning, der gennemfører bestemmelserne i direktiv 95/46/EF, til områder, der ikke er omfattet af dette direktivs anvendelsesområde, for så vidt som ingen anden fællesskabsretlig bestemmelse er til hinder herfor¹⁶. Det er muligt, at en national lovgiver vil beslutte at udvide bestemmelserne i den nationale databeskyttelseslovgivning til visse aspekter vedrørende behandling af oplysninger om døde personer, når en legitim interesse retfærdiggør det¹⁷.

Ufødte børn

I hvilket omfang databeskyttelsesreglerne kan finde anvendelse inden fødslen afhænger af den generelle holdning i de nationale retssystemer vedrørende beskyttelse af ufødte børn. For især at tage hensyn til arverettigheder anerkender visse medlemsstater det princip, at børn, som er undfanget, men endnu ikke er født, betragtes, som om de havde været født med hensyn til fordele (og således kan modtage en arv eller en gave), på betingelse af, at de rent faktisk bliver født. I andre medlemsstater giver særlige retlige bestemmelser specifik beskyttelse, også på samme betingelse. For at afgøre, om de nationale databeskyttelsesbestemmelser også beskytter oplysninger om ufødte børn, bør man se på den generelle tilgang i det nationale retssystem sammen med idéen om, at formålet med databeskyttelsesreglerne er at beskytte den enkelte person.

Et andet spørgsmål opstår i forbindelse med overvejelsen om, at retssystemets generelle svar hviler på en forventning om, at ufødte børns situation er tidsbegrænset til

¹⁶ Dom afsagt den 6.11.2003 af De Europæiske Fællesskabers Domstol i sag C-101/2001 (Lindquist), præmis 98.

¹⁷ Referat af mødet i Rådet for Den Europæiske Råd den 8.2.1995, dokument 4730/95: "Ad artikel 2, litra a): Rådet og Kommissionen bekræfter, at det er medlemsstaterne, der skal fastlægge, om og i hvilket omfang dette direktiv skal anvendes på afdøde personer".

graviditetsperioden. Der tages ikke hensyn til, at denne situation rent faktisk kan være betydeligt længere, f.eks. i forbindelse med frosne embryoner. Endelig kan man finde specifikke juridiske svar i særlige bestemmelser om reproduktionsteknikker, der beskæftiger sig med anvendelsen af lægelige eller genetiske oplysninger om embryoner.

Juridiske personer

Da definitionen af personoplysninger vedrører enkeltpersoner, dvs. fysiske personer, er oplysninger om juridiske personer i princippet ikke omfattet af direktivet, og den beskyttelse, det giver, finder ikke anvendelse¹⁸. Visse databeskyttelsesregler kan dog stadig indirekte finde anvendelse på oplysninger om virksomheder eller juridiske personer under forskellige omstændigheder.

Visse bestemmelser i direktivet om e-kommunikation (direktiv 2002/58/EF) omfatter også juridiske personer. Artikel 1, stk. 2, har følgende ordlyd: *"Med henblik på at nå de i stk. 1 omhandlede mål specificerer og supplerer dette direktivs bestemmelser direktiv 95/46/EF. Nærværende bestemmelser beskytter desuden legitime interesser hos abonnenter, der er juridiske personer."* I overensstemmelse hermed udvider artikel 12 og 13 anvendelsen af visse bestemmelser vedrørende abonnentfortegnelser og uanmodet kommunikation til også at omfatte juridiske personer.

Oplysninger om juridiske personer kan også i sig selv betragtes som oplysninger "om" fysiske personer i overensstemmelse med de kriterier, der er beskrevet i dette dokument. Dette kan være tilfældet, når den juridiske persons navn bygger på navnet på en fysisk person. Et andet tilfælde kan være virksomheds-e-mail, der normalt bruges af en bestemt medarbejder, eller oplysninger om en lille virksomhed (juridisk set en "genstand" snarere end en juridisk person), som kan beskrive ejerens adfærd. I alle disse tilfælde, hvor kriterierne "indhold", "formål" eller "resultat" betyder, at oplysningerne om den juridiske person eller virksomheden kan betragtes som oplysninger "om" en fysisk person, bør oplysningerne betragtes som personoplysninger, og databeskyttelsesreglerne bør finde anvendelse.

De Europæiske Fællesskabers Domstol har fastslået, at der intet er til hinder for, at medlemsstaterne udvider rækkevidden af den nationale lovgivning, der gennemfører direktivets bestemmelser, til områder, der ikke er omfattet af direktivet, for så vidt som ingen anden fællesskabsretlig bestemmelse er til hinder herfor¹⁹. I overensstemmelse hermed har visse medlemsstater, såsom Italien, Østrig og Luxembourg, udvidet anvendelsen af visse bestemmelser i den nationale lovgivning i henhold til direktivet (bl.a. bestemmelserne om sikkerhedsforanstaltninger) til også at omfatte behandlingen af oplysninger om juridiske personer.

Ligesom i forbindelse med oplysninger om døde personer kan praktiske foranstaltninger, som er truffet af den registeransvarlige, også medføre, at oplysninger om juridiske personer i praksis er underlagt databeskyttelsesreglerne. Når den registeransvarlige indsamler oplysninger om fysiske og juridiske personer uden at skelne mellem dem og medtager dem i de samme datasæt, kan databehandlingsmekanismerne og revisionssystemet være udformet sådan, at de

¹⁸ Betragtning 24 i direktivet: *"Dette direktiv berører ikke national lovgivning, der beskytter juridiske personer i forbindelse med behandlingen af oplysninger, som vedrører dem"*.

¹⁹ Dom afsagt den 6.11.2003 af De Europæiske Fællesskabers Domstol i sag C-101/2001 (Lindquist), præmis 98.

overholder databeskyttelsesreglerne. Det kan nemlig være lettere for den registeransvarlige at anvende databeskyttelsesreglerne på alle former for oplysninger i sine registre end at forsøge at finde ud af, hvilke oplysninger der vedrører henholdsvis fysiske og juridiske personer.

IV. HVAD SKER DER, HVIS OPLYSNINGERNE FALDER UDEN FOR DEFINITIONEN?

Som vi har set i hele dette dokument, kan oplysninger under forskellige omstændigheder anses for ikke at være personoplysninger. Det er tilfældet, når oplysningerne ikke kan anses for at vedrøre en person, eller når personen ikke kan betragtes som identificeret eller identificerbar. Når de oplysninger, som behandles, ikke falder ind under begrebet "personoplysninger", medfører det, at direktivet ikke finder anvendelse, jf. direktivets artikel 3. Det betyder imidlertid ikke, at personer kan fratages enhver form for beskyttelse i den bestemte situation. Der må tages hensyn til følgende betragtninger.

Hvis direktivet ikke finder anvendelse, kan den nationale databeskyttelseslovgivning eventuelt finde anvendelse. Som fastsat i artikel 34 er direktivet rettet til medlemsstaterne. Uden for direktivets anvendelsesområde er medlemsstaterne ikke underlagt de forpligtelser, direktivet pålægger dem, dvs. hovedsagelig pligten til at sætte de nødvendige love og administrative bestemmelser i kraft for at efterkomme det. Som De Europæiske Fællesskabers Domstol har fastslået, er der imidlertid intet til hinder for, at medlemsstaterne udvider rækkevidden af den nationale lovgivning, der gennemfører direktivets bestemmelser, til områder, der ikke er omfattet af direktivet, for så vidt som ingen anden fællesskabsretlig bestemmelse er til hinder herfor. Det kan derfor sagtens ske, at visse situationer, som ikke involverer behandling af personoplysninger som defineret i direktivet, alligevel er underlagt beskyttelsesforanstaltninger i henhold til national lovgivning. Det kan f.eks. gælde for et spørgsmål som oplysninger med nøglekode, uanset om der er tale om personoplysninger eller ej.

Når databeskyttelsesreglerne ikke finder anvendelse, kan visse aktiviteter stadig udgøre en overtrædelse af artikel 8 i den europæiske menneskerettighedskonvention, der beskytter retten til respekt for privatlivet og familielivet, i lyset af Den Europæiske Menneskerettighedsdomstols vidtgående retspraksis. Andre regelsæt, såsom erstatningsretten, strafferetten og antidiskriminationslovgivningen, kan også yde beskyttelse til personer i de tilfælde, hvor databeskyttelsesreglerne ikke finder anvendelse, og forskellige legitime interesser kan være på spil.

V. KONKLUSIONER

I denne udtalelse har Artikel 29-Gruppen udstukket retningslinjer for, hvordan begrebet personoplysninger i direktiv 95/46/EF og beslægtet fællesskabslovgivning skal forstås, og hvordan det skal anvendes i forskellige situationer.

En generel overvejelse er, at den europæiske lovgiver ønskede at fastsætte en bred definition af begrebet personoplysninger, men begrebet er ikke ubegrænset. Man må altid holde sig for øje, at formålet med direktivets regler er at beskytte den enkeltes grundlæggende rettigheder og frihedsrettigheder, specielt deres ret til privatlivets fred, i forbindelse med behandling af personoplysninger. Disse regler er derfor beregnet til at finde anvendelse på situationer, hvor den enkeltes rettigheder kan være i fare og derfor

har brug for beskyttelse. Anvendelsesområdet for databeskyttelsesreglerne bør ikke gøres for bredt, men man bør også undgå at begrænse begrebet personoplysninger for meget. Direktivet har fastlagt anvendelsesområdet, som udelukker en række aktiviteter, og muliggør en vis smidighed i anvendelsen af reglerne på aktiviteter, der falder inden for anvendelsesområdet. Databeskyttelsesmyndighederne spiller en vigtig rolle med hensyn til at finde en passende ligevægt i anvendelsen (se afsnit II).

Artikel 29-Gruppens analyse er baseret på de fire vigtigste elementer i definitionen af "personoplysninger", nemlig "enhver form for information", "om", "en identificeret eller identificerbar" og "fysisk person". Disse elementer hænger nøje sammen og påvirker hinanden, men tilsammen afgør de, som en oplysning skal betragtes som "personoplysninger". Analysen underbygges med eksempler fra de europæiske databeskyttelsesmyndigheders nationale praksis.

- Det første element – "enhver form for information" – lægger op til en bred fortolkning af begrebet, uanset oplysningernes art eller indhold og det tekniske format, de foreligger i. Det betyder, at både objektive og subjektive oplysninger om en person, uanset den pågældendes egenskab, kan betragtes som "personoplysninger", uafhængigt af det tekniske medium, de opbevares på. I udtalelsen behandles også spørgsmålet om biometriske oplysninger og de juridiske sondringer med hensyn til menneskelige prøver, som de kan uddrages af (se afsnit III.1).
- Det andet element – "om" – er indtil nu ofte blevet overset, men spiller en afgørende rolle, når man skal fastlægge begrebets materielle anvendelsesområde, specielt i forbindelse med genstande og nye teknologier. Udtalelsen gennemgår tre alternative elementer, nemlig indhold, formål og resultat, der kan bruges til at afgøre, om der er tale om oplysninger "om" en person. Dette omfatter også oplysninger, som kan have en klar indvirkning på den måde, hvorpå en person behandles eller vurderes (se afsnit III.2).
- Det tredje element – "identificeret eller identificerbar" – fokuserer på betingelserne for, at en person kan betragtes som "identificerbar", og specielt på "de hjælpemidler, der med rimelighed kan tænkes bragt i anvendelse" til at identificere den pågældende af den registeransvarlige eller af enhver anden person. De særlige forhold og omstændigheder i et bestemt tilfælde spiller en vigtig rolle i denne analyse. Udtalelsen kommer også ind på "pseudonymiserede oplysninger" og anvendelsen af "oplysninger med nøglekode" i statistisk forskning og lægemiddelforskning (se afsnit III.3).
- Det fjerde element – "fysisk person" – beskæftiger sig med kravet om, at "personoplysninger" skal vedrøre "levende personer". I udtalelsen drøftes også grænsefladerne med oplysninger om døde personer, ufødte børn og juridiske personer (se afsnit III.4).

Endelig drøftes det, hvad der sker, hvis oplysningerne falder uden for anvendelsesområdet for definitionen af "personoplysninger". Der er forskellige løsninger, som kan bruges til at behandle spørgsmålene i disse tilfælde, herunder national lovgivning uden for direktivets anvendelsesområde, for så vidt som alle andre fællesskabsretlige bestemmelser overholdes (se afsnit IV).

Artikel 29-Gruppen opfordrer alle interesserede parter til at sætte sig grundigt ind i de retningslinjer, som udstikkes i denne udtalelse, og til at tage hensyn til dem, når de fortolker og anvender bestemmelserne i national lovgivning i overensstemmelse med direktiv 95/46/EF.

Artikel 29-Gruppens medlemmer, hvoraf de fleste er repræsentanter for datatilsynsmyndighederne på nationalt plan, vil udbygge de retningslinjer, som udstikkes i denne udtalelse, inden for deres egne kompetenceområder og sikre, at deres nationale lovgivning anvendes korrekt i overensstemmelse med direktiv 95/46/EF.

Artikel 29-Gruppen har til hensigt at anvende og videreudvikle de retningslinjer, som udstikkes i denne udtalelse, når det er hensigtsmæssigt, og at tage fuldt hensyn til dem i sit videre arbejde, specielt når den beskæftiger sig med emner såsom identitetsstyring i forbindelse med e-forvaltning samt i forbindelse med RFID. Med hensyn til sidstnævnte spørgsmål har Artikel 29-Gruppen til hensigt at bidrage til en yderligere analyse af, hvordan databeskyttelsesreglerne kan påvirke anvendelsen af RFID, og af, om der er behov for yderligere foranstaltninger, som kan være nødvendige for at sikre, at databeskyttelsesrettighederne og interesserne overholdes korrekt i denne sammenhæng.

Endelig vil Artikel 29-Gruppen gerne have feedback fra interesserede parter og fra overvågningsmyndighederne om deres praktiske erfaringer med de retningslinjer, som fremsættes i denne udtalelse, herunder andre eksempler end dem, der er nævnt i dette dokument. Den har til hensigt at tage spørgsmålet op igen på et senere tidspunkt med henblik på at forbedre den fælles forståelse af nøglebegrebet personoplysninger yderligere og sikre en harmoniseret anvendelse og en bedre gennemførelse af direktiv 95/46/EF og beslægtet fællesskabslovgivning på dette grundlag.

På Artikel 29-Gruppens vegne

Peter Schaar
Formand