ARTIKEL 29 – ARBETSGRUPPEN FÖR SKYDD AV PERSONUPPGIFTER

01248/07/EN
WP 136

Yttrande 4/2007 om begreppet personuppgifter

Antaget den 20 juni

Denna arbetsgrupp inrättades genom artikel 29 i direktiv 95/46/EG. Arbetsgruppen är en oberoende rådgivande EU-instans för skydd av personuppgifter och privatlivet.
Dess arbetsuppgifter framgår av artikel 30 i direktiv 95/46/EG och artikel 15 i direktiv 2002/58/EG.

För sekretariatet svarar direktorat C (Civilrättsliga frågor, grundläggande rättigheter och medborgarskap) inom Europeiska kommissionens
generaldirektorat för rättvisa, frihet och säkerhet, B-1049 Bryssel, Belgien, Kontor LX-46 01/43.

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

ARBETSGRUPPEN FÖR SKYDD FÖR ENSKILDA VID BEHANDLING AV PERSONUPPGIFTER HAR ANTAGIT DETTA YTTRANDE

med beaktande av Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995, genom vilket arbetsgruppen inrättades[1],

med beaktande av artiklarna 29 och 30.1 a och 30.3 i det direktivet och artikel 15.3 i Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002,

med beaktande av artikel 255 i EG-fördraget och av Europaparlamentets och rådets förordning (EG) nr 1049/2001 av den 30 maj 2001 om allmänhetens tillgång till Europaparlamentets, rådets och kommissionens handlingar,

med beaktande av dess arbetsordning,

HAR ANTAGIT FÖLJANDE YTTRANDE:

[1] EGT L 281, 23.11.1995, s. 31. Kan hämtas på http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

I. INLEDNING

Arbetsgruppen är medveten om behovet av att göra en grundlig analys av begreppet personuppgifter. Uppgifter om gällande praxis i medlemsstaterna tyder på att det råder en viss osäkerhet och olika uppfattningar om vissa viktiga delar av detta begrepp, vilket skulle kunna ha betydelse för om den befintliga ramen för uppgiftsskydd fungerar tillfredsställande i olika sammanhang. Resultatet av denna analys av centrala delar av tillämpningen och tolkningen av bestämmelserna om uppgiftsskydd kommer troligen att få stor inverkan på många viktiga frågor och kommer att vara särskilt relevant för frågor som rör identitetshantering i samband med e-förvaltning och e-hälsa, samt vid radiofrekvensidentifiering (RFID).

Syftet med detta yttrande från arbetsgruppen är att nå fram till en gemensam tolkning av begreppet personuppgifter, och i vilka situationer som nationell lagstiftning om uppgiftsskydd ska tillämpas och i vilka fall den inte ska tillämpas. Att arbeta på en gemensam definition av begreppet personuppgifter är detsamma som att definiera vad som faller inom eller utanför tillämpningsområdet för uppgiftsskyddsbestämmelserna. En naturlig följd av detta arbete är att ge vägledning om hur nationella uppgiftsskyddsbestämmelser ska tillämpas i vissa typer av situationer som inträffar i hela EU och på så sätt bidra till att sådana regler tillämpas på samma sätt, vilket är artikel 29-arbetsgruppens huvuduppgift.

I detta dokument används exempel från nationell praxis vid medlemsstaternas dataskyddsmyndigheter för att underbygga och illustrera analysen. De flesta exempel har endast redigerats för att kunna användas i detta sammanhang.

II. ALLMÄNNA ÖVERVÄGANDEN OCH STRATEGISKA FRÅGOR

Direktivet innefattar ett brett begrepp av personuppgifter

Definitionen av personuppgifter i direktiv 95/46/EG (nedan kallat ”direktivet om uppgiftsskydd” eller ”direktivet” lyder på följande sätt:

”personuppgifter: varje upplysning som avser en identifierad eller identifierbar fysisk person (den registrerade). En identifierbar person är en person som kan identifieras, direkt eller indirekt, framför allt genom hänvisning till ett identifikationsnummer eller till en eller flera faktorer som är specifika för hans fysiska, fysiologiska, psykiska, ekonomiska, kulturella eller sociala identitet.”

Det bör noteras att denna definition återspeglar lagstiftarens avsikt att hålla begreppet ”personuppgifter” så brett som möjligt under hela lagstiftningsgången. I kommissionens ursprungliga förslag förklarades att man liksom i konvention 108 antog en bred definition för att kunna täcka in all information som skulle kunna kopplas till en enskild individ[2]. I kommissionens ändringsförslag noterades att det ändrade förslaget uppfyllde parlamentets önskan om att definitionen av ”personuppgifter” borde hållas så bred som möjligt för att omfatta all information rörande en identifierbar individ[3], vilket rådet också tog i beaktande i den gemensamma ståndpunkten[4].

Syftet med bestämmelserna i direktivet är att skydda enskilda individer

I artikel 1 i direktiv 95/46/EG och i direktiv 2002/58/EG anges tydligt vad bestämmelsernas slutgiltiga syfte är: ”Att skydda fysiska personers grundläggande fri- och rättigheter, särskilt rätten till privatliv, i samband med behandling av personuppgifter”. Detta är en mycket viktig punkt att beakta vid tolkningen och tillämpningen av de båda instrumenten. Det kan spela en avgörande roll för att bestämma hur man ska tillämpa bestämmelserna i direktivet i ett antal situationer där en persons rättigheter inte är utsatta för risk, och det kan också varna för en tolkning av bestämmelserna som skulle frånta enskilda personers skydd av sina rättigheter.

Direktivets tillämpningsområde utesluter ett antal verksamhetsområden och texten har en viss flexibilitet för att möjliggöra en lämplig rättslig åtgärd under ett visst förhållande

Trots den breda definitionen av ”personuppgifter” och ”behandling” i direktivet kan man inte enbart utifrån det faktum att en viss situation skulle kunna anses innebära ”behandling av personuppgifter” enligt definitionen avgöra om situationen ska omfattas av bestämmelserna i direktivet, och då särskilt artikel 3. Bortsett från de undantag som har med gemenskapsrättens räckvidd att göra omfattar undantagen enligt artikel 3 den tekniska behandlingen (på ett manuellt icke-strukturerat sätt) och avsikten med användandet (av en fysisk person som ett led i verksamhet av rent privat natur

---

2 KOM(90) 314 slutlig, 13.9.1990, s. 19 (kommentar till artikel 2)

3 KOM(92) 422 slutlig, 13.9.1990, s. 10 (kommentar till artikel 2)

4 Gemensam ståndpunkt (EG) nr 1/95, antagen av rådet den 20 februari 1995, EGT C 93, 13.4.1995, s. 20.

eller som har samband med hans hushåll). Även om behandlingen av personuppgifter ligger inom direktivets tillämpningsområde behöver inte alla bestämmelser vara tillämpliga i det aktuella fallet. Flera av bestämmelserna i direktivet ger uttryck för en avsevärd grad av flexibilitet för att uppnå en lämplig balans mellan skydd av den registrerade och de berättigade intressen som registeransvariga, tredje parter och allmänheten har. Vissa exempel på sådana bestämmelser finns i artikel 6 (nödvändig arkiveringstid för vissa uppgifter), 7 f (avvägning av intressen för att rättfärdiga behandling), sista stycket i 10 c och 11.1 c (information till den registrerade vid behov för att tillförsäkra den registrerade en korrekt behandling) och 18 (undantag från anmälningsplikten), bara för att nämna några fall.

Tillämpningsområdet för uppgiftsskyddsbestämmelserna bör inte sträckas för långt

Det skulle vara ett oönskat resultat om man skulle tillämpa uppgiftsskyddsbestämmelserna i situationer som de inte var avsedda för och som de inte har utformats för av lagstiftaren. De materiella undantagen i artikel 3 som nämns ovan och förtydligandena i skälen 26 och 27 i direktivet visar hur lagstiftaren ville att bestämmelserna skulle tillämpas.

En begränsning gäller sättet att behandla uppgifter. Man bör tänka på att anledningen till att de första uppgiftsskyddslagarna stiftades var att ny teknik i form av elektronisk databehandling underlättade tillgången till personuppgifter och gjorde dessa mer allmänt tillgängliga än de traditionella formerna för databehandling. Syftet med uppgiftsskyddet enligt detta direktiv är att skydda mot sådana former av behandling som är typiska när det finns en större risk för att man lätt ger tillgång till personuppgifter (skäl 27). Behandling av personuppgifter som inte är automatisk omfattas bara av direktivet om uppgifterna ingår i eller kommer att ingå i ett register (se artikel 3).

En annan allmän begränsning för tillämpningen av uppgiftsskydd enligt direktivet skulle vara behandling av uppgifter under omständigheter där medlen för att identifiera den registrerade inte ”rimligen kan komma att användas” (skäl 26). Denna fråga kommer att diskuteras längre fram.

Man ska dock inte heller begränsa tolkningen av begreppet personuppgifter mer än nödvändigt

I de fall där en mekanistisk tillämpning av varje enskild bestämmelse i direktivet skulle leda till alltför betungande eller kanske till och med absurda konsekvenser måste man först kontrollera om 1) situationen faller inom direktivets tillämpningsområde, särskilt enligt artikel 3, och 2) om direktivet självt eller nationell lagstiftning som antagits i enlighet med direktivet inte medger undantag eller förenklingar i särskilda situationer för att kunna nå fram till lämpliga rättsliga lösningar samtidigt som man säkerställer skyddet av individens rättigheter och av de berörda intressena. Det är bättre att inte begränsa tolkningen av definitionen av personuppgifter onödigt mycket och i stället notera att det finns en avsevärd flexibilitet i tillämpningen av bestämmelserna som rör dessa uppgifter.

Nationella tillsynsmyndigheter för uppgiftsskydd spelar en viktig roll i sitt arbete med att övervaka tillämpningen av uppgiftsskyddslagstiftningen, vilket inbegriper att tolka rättsliga bestämmelser och ge konkret vägledning till registeransvariga och registrerade personer. De bör stödja en definition som är så bred att den kan förekomma

utvecklingen och nå alla ”gråzoner” inom tillämpningsområdet samtidigt som man utnyttjar den rättsliga flexibiliteten i direktivet. Direktivet uppmanar till en politik som kombinerar en bred tolkning av begreppet personuppgifter och en lämplig balans i tillämpningen av direktivets bestämmelser.

III. ANALYS AV DEFINITIONEN PERSONUPPGIFTER ENLIGT DIREKTIVET OM UPPGIFTSSKYDD

Definitionen i direktivet består av fyra viktiga beståndsdelar som kommer att analyseras var och en för sig i detta dokument. Dessa är följande:

- ”varje upplysning”
- ”som avser en”
- ”identifierad eller identifierbar”
- ”fysisk person”.

Dessa fyra beståndsdelar är nära sammankopplade och beroende av varandra men av metodskäl kommer de att behandlas var för sig i det här dokumentet.

1. FÖRSTA BESTÅNDSDELEN: ”VARJE UPPLYSNING”

Begreppet ”varje upplysning” i direktivet signalerar tydligt lagstiftarens vilja att utforma ett brett begrepp för personuppgifter. Detta begrepp kräver en vid tolkning.

När det gäller upplysningens natur omfattar begreppet personuppgifter alla typer av information om en person. Det omfattar ”objektiva” upplysningar, såsom t.ex. förekomst av ett visst ämne i någons blod. Det omfattar även ”subjektiva” upplysningar, åsikter eller bedömningar. Den sistnämnda typen av information utgör en betydande andel av de personuppgifter som behandlas, t.ex. i banksektorn för att bedöma tillförlitligheten hos låntagare (”Titus är en pålitlig låntagare”), i försäkringsbranschen (”Titus förväntas inte dö inom kort”) eller i en arbetssituation (”Titus är en duktig medarbetare och förtjänar en befordran”).

För att en upplysning ska utgöra en ”personuppgift” behöver den inte vara sann eller bekräftad. Uppgiftsskyddsbestämmelserna förutser redan möjligheten att en upplysning är felaktig och ger den registrerade rätt att få tillgång till upplysningen och att protestera mot den genom lämpliga åtgärder[5].

När det gäller innehållet i en upplysning omfattar begreppet personuppgifter uppgifter som ger alla typer av upplysningar. Detta omfattar givetvis personliga upplysningar som anses utgöra ”känsliga uppgifter” enligt artikel 8 i direktivet på grund av att de är särskilt riskabla, men även information av mer allmän art. Begreppet ”personuppgifter” omfattar information som rör individens privat- och familjeliv i egentlig bemärkelse men även information om olika typer av aktiviteter som rör personen i fråga t.ex. arbetsförhållanden eller personens ekonomiska eller sociala beteende. Det omfattar således upplysningar om individer, oavsett deras ställning eller kapacitet (som konsument, patient, anställd, kund osv.)

[5] Man skulle kunna göra en rättelse genom att lägga till kontrasterande kommentarer eller genom lämpliga rättsliga åtgärder, t.ex. överklagandeförfaranden.

Exempel nr 1: Yrkesmässiga vanor och beteenden

Information om receptbelagda läkemedel (t.ex. läkemedelsidentifikationsnummer, läkemedelsnamn, läkemedelsstyrka, tillverkare, försäljningspris, ny förpackning eller refill, skäl till användning, skäl till att det inte är utbytbart, utskrivarens för- och efternamn, telefonnummer osv.), oavsett om det gäller ett enskilt recept eller om det är ett mönster som urskiljs från ett antal recept, kan anses som personuppgifter om den läkare som skriver ut läkemedlet, även om patienten är anonym. Att ge upplysningar om recept som skrivits ut av en identifierad eller identifierbar läkare till tillverkare av receptbelagda läkemedel utgör således ett meddelande om personuppgifter till en mottagare som är tredje part enligt direktivet.

Denna tolkning stöds av ordalydelsen i själva direktivet. Å ena sidan måste man beakta att begreppet privatliv och familjeliv är brett, vilket Europeiska domstolen för de mänskliga rättigheterna har klargjort[6]. Å andra sidan går bestämmelserna om skydd av personuppgifter längre än skyddet av det vida begreppet om rätten till respekt för privatliv och familjeliv. Det bör noteras att Europeiska unionens stadga om de grundläggande rättigheterna tar upp skyddet av personuppgifter i artikel 8 som en självständig rättighet, som är separat och skild från den rätt till privatliv som omnämns i artikel 7 i stadgan och samma sak gäller på nationell nivå i medlemsstaterna. Detta överensstämmer med villkoren i artikel 1.1 som syftar till att ”skydda fysiska personers grundläggande fri- och rättigheter, *särskilt* [men inte enbart] rätten till privatliv”. I enlighet med detta hänvisas det i direktivet särskilt till behandling av personuppgifter i situationer utanför hemmet och familjen såsom den som omfattas av arbetsmarknadslagstiftning (artikel 8.2 b), brottmålsdomar, administrativa sanktioner eller avgöranden i tvistemål (artikel 8.5) eller direkt marknadsföring (artikel 14 b). EG-domstolen stödjer denna breda definition[7].

När det gäller formatet eller medlet som informationen lagras på omfattar begreppet personuppgifter upplysningar som är tillgängliga i vilken form som helst, t.ex. alfabetisk, numerisk, grafisk, fotografisk eller akustisk. De omfattar både upplysningar på papper och information som lagras på ett datorminne genom en binär kod eller t.ex. på en videokassett. Det är en logisk konsekvens av att automatisk behandling av personuppgifter omfattas av direktivet. Ur detta perspektiv är ljud- och bilduppgifter personuppgifter eftersom de kan utgöra information om en person. I detta hänseende måste man se den särskilda hänvisningen till ljud- och bilduppgifter i artikel 33 i direktivet som en bekräftelse på och ett förtydligande av att denna typ av upplysningar faktiskt omfattas av direktivets tillämpningsområde (förutsatt att alla andra villkor är uppfyllda) och att direktivet gäller dessa uppgifter. Detta är också ett följdriktigt antagande för bestämmelsen i denna artikel som försöker bedöma om direktivet kan

6 Dom i Europeiska domstolen för de mänskliga rättigheterna i målet Amann mot Schweiz av den 16 februari 2000, §65: [...] begreppet ”privatliv” får inte tolkas restriktivt. Respekt för privatlivet gäller särskilt rätten att bygga upp och utveckla förhållanden med andra människor. Dessutom finns det inga principiella skäl som rättfärdigar att man undantar verksamhet av yrkesmässig eller affärsmässig karaktär från begreppet ”privatliv” (se domen i målet Niemietz mot Tyskland av den 16 december 1992, serie A nr 251-B s. 33–34 och domen I Halford-målet som citeras ovan, s. 1015–1016, § 42). Denna vida definition överensstämmer med den som återfinns i Europarådets konvention av den 28 januari 1981 [...]”.

7 EG-domstolens dom av den 6 november 2003 i mål C-101/2001, (Lindqvist), punkt 24: Begreppet personuppgifter, som används i artikel 3.1 i direktiv 95/46, omfattar i enlighet med definitionen i artikel 2 a i direktivet i fråga ”varje upplysning som avser en identifierad eller identifierbar fysisk person”. Detta begrepp omfattar förvisso en persons namn tillsammans med dennes telefonnummer eller med uppgifter om vederbörandes arbetsförhållanden eller fritidsintressen.”

möjliggöra lämpliga rättsliga lösningar på dessa områden. Detta klargörs ytterligare i skäl 14: ”*för närvarande görs inom ramen för informationssamhället betydande framsteg såvitt avser tekniken för att uppta, överföra, bearbeta, registrera, lagra eller lämna ut ljud- eller bilduppgifter om fysiska personer; detta direktiv bör därför tillämpas på behandling av sådana uppgifter*”. Å andra sidan är det inte är nödvändigt att se upplysningar som finns i en strukturerad databas eller en fil som personuppgifter. Upplysningar som återfinns i fritexten i ett elektroniskt dokument kan ses som personuppgifter förutsatt att övriga kriterier i definitionen av personuppgifter är uppfyllda. E-postmeddelanden innehåller t.ex. personuppgifter.

Exempel nr 2: Telefonbank

Vid telefonbankärenden där kundens röst ger instruktioner till banken och dessa registreras på band ska inspelningarna anses utgöra personuppgifter.

Exempel nr 3: Videoövervakning

Bilder av personer tagna av övervakningskameror kan utgöra personuppgifter om personerna går att känna igen.

Exempel nr 4: En barnteckning

Efter ett neuropsykiatriskt test som gjorts på en flicka i ett domstolsförfarande angående vårdnaden om henne lämnas en teckning som hon gjort av sin familj in till domstolen. Teckningen ger upplysningar om flickans känsloläge och vad hon tycker om de olika familjemedlemmarna. Som sådan skulle den kunna betraktas som ”personuppgift”. Teckningen kommer att avslöja information om barnet (hennes psykiska hälsotillstånd) och också t.ex. om hennes fars eller mors uppträdande. Föräldrarna kan därför utnyttja sin rätt att få tillgång till denna upplysning.

Man bör särskilt beakta biometriska uppgifter. Dessa uppgifter kan definieras som biologiska egenskaper, fysiologiska kännetecken, särdrag eller repeterbara handlingar där dessa kännetecken eller handlingar är både unika för individen och mätbara, även om de mönster som används i praktiken för att tekniskt mäta dessa bygger på ett visst mått av sannolikhet. Typiska exempel på sådana biometriska uppgifter är fingeravtryck, näthinnemönster, ansiktsform, röster, men även handgeometri, venmönster eller djupt förankrade kunskaps- eller beteenderelaterade kännetecken (såsom en handskriven namnteckning, tangentnedslag, ett särskilt sätt att gå eller tala osv.).

Ett utmärkande drag för biometriska uppgifter är att de kan ses både som *innehållande* upplysningar om en viss individ (Titus har dessa fingeravtryck) liksom som ett element för att skapa en *länk* mellan en upplysning och individen (detta föremål har vidrörts av någon med dessa fingeravtryck och dessa fingeravtryck motsvarar Titus fingeravtryck; därför har detta föremål vidrörts av Titus). De kan fungera som ”identifierare”. Biometriska uppgifter kan på grund av sin unika länk till en särskild individ användas för att identifiera en person. Denna dubbelkaraktär har även DNA-uppgifter eftersom de ger information om människokroppen och möjliggör en otvetydig och unik identifiering av en person.

Vävnadsprov (t.ex. blodprov) är källor som biometriska uppgifter kan utvinnas ur, men de är inte biometriska uppgifter i sig. Därför utgör utvinnandet av information från

sådana prov insamling av personuppgifter som omfattas av bestämmelserna i direktivet. Insamling, lagring och användande av vävnadsprov kan i sig omfattas av olika bestämmelser[8].

2. ANDRA BESTÅNDSDELEN: ”SOM AVSER EN”

Denna beståndsdel i definitionen är avgörande och det är mycket viktigt att man exakt tar reda på vilka relationer eller länkar som spelar roll och hur man kan urskilja dem.

I allmänna termer kan information anses ”avse” en person när det *handlar om* den personen.

I många situationer kan man lätt se detta förhållande. Detta innebär t.ex. att uppgifter som registreras i en persons akt på ett personalkontor ”avser” personens situation som anställd. Samma sak gäller för uppgifter om resultatet av en patients medicinska test i personens patientjournal eller bilden av en person som filmas vid en videointervju med denna person.

Ett antal andra situationer kan nämnas där det dock inte är lika uppenbart som i de föregående fallen att upplysningarna ”avser” en individ.

I vissa situationer angår informationen som framgår av uppgifterna i första hand föremål och inte enskilda personer. Dessa föremål tillhör vanligtvis någon, eller är utsatta för eller har ett särskilt inflytande på personer, eller har en sorts fysisk eller geografisk närhet till personer eller andra föremål. Då är det endast möjligt att indirekt avgöra om upplysningarna rör dessa personer eller andra föremål.

Exempel nr 5: Värdet på ett hus

Uppgifter om värdet på ett hus är information om ett föremål. Det är klart att bestämmelserna om uppgiftsskydd inte är tillämpliga om denna information endast kommer att användas som illustration för fastighetspriserna i ett visst område. Under vissa omständigheter bör emellertid sådan information också kunna betraktas som personuppgifter. Huset utgör ju en ägares tillgångar, och följaktligen kommer informationen om värdet att användas för att t.ex. avgöra den här personens skyldighet att betala skatt. I detta sammanhang är det inget tvivel om att sådan information bör betraktas som personuppgifter.

Man kan göra en liknande analys av uppgifter som först och främst gäller processer eller händelser, t.ex. information om hur en maskin fungerar när det krävs mänskligt ingripande. Under vissa omständigheter får denna information också betraktas som information som ”avser” en individ.

Exempel nr 6: Serviceboken för en bil

Bilmekanikers eller bilverkstäders register om service som utförts på en viss bil innehåller information om bilen, körsträcka, datum för service, tekniska problem och bilens allmänna skick. Informationen i registret är knuten till ett registreringsnummer och ett motornummer, som i sin tur kan kopplas till en ägare. När bilverkstaden gör denna koppling mellan fordonet och ägaren, t.ex. för fakturering, kommer

[8] Se Europarådets ministerkommittés rekommendation Rec (2006) 4 till medlemsstaterna beträffande forskning om biologiskt material av mänsklig härkomst av den 15.3.2006

informationen att ”avse” ägaren eller bilföraren. Om informationen kopplas till den mekaniker som utförde arbetet på bilen för att fastställa hans produktivitet kommer informationen också att ”avse” mekanikern.

Arbetsgruppen har redan uppmärksammat frågan om när information kan anses ”avse” en person. I samband med diskussionerna kring de dataskyddsfrågor som uppstod i samband med RFID-etiketter konstaterade arbetsgruppen att uppgifter avser en enskild individ om de hänför sig till en individs identitet, utmärkande egenskaper eller uppträdande, eller om sådan information används för att avgöra eller inverka på hur denna person behandlas eller bedöms[9].

Mot bakgrund av exemplen ovan och i linje med dessa bör det framhållas att för att uppgifterna ska anses ”avse” en individ bör beståndsdelarna ”**innehåll”** ELLER ”**syfte”** ELLER ”**resultat**” finnas med i bilden.

Beståndsdelen ”**innehåll”** finns med i alla de fall när det – enligt den mest uppenbara och den vanligaste tolkningen av ordet ”avse” i ett samhälle – ges information om en särskild person, oavsett vilken avsikt den registeransvarige eller tredje part har med detta eller hur informationen inverkar på den person som informationen gäller. Information ”avser” en person när den ”handlar” om denna, och detta måste bedömas mot bakgrund av alla omständigheter i det aktuella fallet. Exempelvis är det otvivelaktigt att resultaten av en läkarundersökning handlar om patienten, liksom att informationen i ett företags mapp med namnet på en specifik kund otvivelaktigt gäller denne. Informationen i en RFID-etikett eller i en streckkod i en viss individs identitetshandling avser den personen, som t.ex. i de framtida passen med RFID-chips.

Även beståndsdelen ”**syfte”** kan bära ansvaret för att information ”avser” en viss person. Beståndsdelen ”syfte” kan anses vara befintlig när uppgifterna används eller sannolikt kommer att användas, med beaktande av alla omständigheter i det enskilda fallet, i syfte att bedöma, behandla på ett särskilt sätt eller påverka en enskild persons ställning eller uppträdande.

[9] Arbetsgruppens dokument nr WP 105: ”Working document on data protection issues related to RFID technology”, antaget den 19 januari 2005, s. 8.

Exempel nr 7: Samtalslistan för en telefon

Samtalslistan för en telefon på ett företagskontor ger information om vilka samtal som har ringts från den aktuella telefonen som är kopplad till en särskild linje. Informationen kan sättas i relation till olika personer. Telefonlinjen har gjorts tillgänglig för företaget, och företaget är enligt kontrakt skyldigt att betala samtalen. Telefonen kontrolleras av en särskild anställd under arbetstid och det förmodas att det är han som ringer samtalen. Samtalslistan kan också ge information om den person som blev uppringd. Telefonen kan dessutom användas av alla som har tillstånd att komma in i byggnaden när den anställde inte är där (t.ex. lokalvårdare). Informationen om användningen av den aktuella telefonen kan, i olika syften, sättas i relation till företaget, den anställde, eller lokalvårdarna (t.ex. för att kontrollera vilken tid dessa lämnar arbetsplatsen eftersom de förväntas bekräfta per telefon vilken tid de lämnar byggnaden innan denna låses). Det bör framhållas att begreppet personuppgifter här utvidgas till att omfatta både utgående och inkommande samtal eftersom alla samtal innehåller information om personers privatliv, sociala relationer och kommunikation.

En tredje sorts uppgifter som ”avser” bestämda personer uppstår när det finns en ”**resultat”-**beståndsdel. Även i avsaknad av beståndsdelarna ”innehåll” eller ”syfte” kan uppgifter anses ”avse” en enskild individ eftersom deras användning sannolikt kommer att få inverkan på en viss persons rättigheter och intressen, med hänsyn till alla omständigheter i det enskilda fallet. Det bör noteras att det inte är nödvändigt att det eventuella resultatet får stor inverkan. Det räcker om individen behandlas annorlunda än andra till följd av behandlingen av sådana uppgifter.

Exempel nr 8: Övervakning av taxibilars position för att optimera servicen inverkar på taxiförarna

Ett taxiföretag har installerat ett system för positionsbestämning med hjälp av satellit som gör det möjligt att lokalisera lediga taxibilar i realtid. Syftet med behandlingen av data är att ge bättre service och spara bränsle genom att alla kunder som beställer taxi anvisas den bil som är närmast kundens adress. I strikt mening är de uppgifter som behövs för detta system uppgifter om bilarna, inte om förarna. Syftet med databehandlingen är inte att bedöma taxiförarnas resultat, t.ex. genom optimera deras rutter. Men systemet gör det ändå möjligt att övervaka förarnas resultat och kontrollera om de håller hastigheten, söker lämpliga rutter, sitter vid ratten eller vilar utanför bilen, osv. Det kan därför få stor inverkan för dessa individer, och mot denna bakgrund kan uppgifterna också anses avse fysiska personer. Databehandlingen bör därför omfattas av bestämmelserna om uppgiftsskydd.

Dessa tre beståndsdelar (innehåll, syfte, resultat) måste betraktas som alternativa förutsättningar, inte kumulativa. Framför allt gäller att när beståndsdelen innehåll finns med i bilden är inte de andra beståndsdelarna nödvändiga för att informationen ska avse individen. Detta innebär att en och samma upplysning samtidigt kan avse olika individer beroende på vilken beståndsdel den innehåller avseende var och en av dessa individer. Samma information kan gälla individen Titius på grund av ”innehållet” (uppgifterna handlar otvivelaktigt om Titius) OCH Gaius på grund av ”syftet” (den kommer att användas i syfte att behandla Gaius på ett visst sätt) OCH Sempronius på grund av ”resultatet” (informationen kommer sannolikt att få inverkan på Sempronius rättigheter och intressen). Detta innebär också att det inte är nödvändigt att uppgifterna

”fokuserar” på någon för att de ska anses avse denna individ. Det följer av den föregående analysen att frågan om huruvida uppgifter avser en viss person måste besvaras specifikt för varje enskild upplysning. På liknande sätt bör man vid tillämpningen av viktiga bestämmelser (t.ex. om räckvidden av rätten till tillgång) hålla i minnet att information kan avse olika personer.

Exempel nr 9: Informationen i ett mötesprotokoll

Behovet av att göra en separat analys för varje enskild upplysning enligt modellen ovan illustreras av följande exempel om informationen i ett mötesprotokoll, som innehåller uppgifter om deltagarna Titius, Gaius och Sempronius närvaro, Titius och Gaius uttalanden, och en redogörelse för diskussionerna om vissa ämnen sammanfattade av protokollföraren Sempronius. Det är endast informationen om att Titius var närvarande vid mötet vid en särskild tidpunkt och på en särskild plats och att han gjorde vissa uttalanden som kan anses som personuppgifter avseende Titius. Gaius närvaro vid mötet, hans uttalanden och diskussionerna i en fråga sammanfattade av Sempronius är INTE personuppgifter som avser Titius. Detta gäller även om denna information finns i samma dokument och även om det var Titius som tog upp den fråga som diskuterades vid mötet. Den omfattas därför inte av Titius rätt till tillgång till sina egna personuppgifter. Huruvida och i vilken omfattning den informationen kan anses som personuppgifter om Gaius och Sempronius måste avgöras var för sig, med hjälp av ovannämnda analys.

3. TREDJE BESTÅNDSDELEN: ”IDENTIFIERAD ELLER IDENTIFIERBAR” [FYSISK PERSON]

Enligt direktivet måste upplysningen avse en fysisk person som är ”identifierad eller identifierbar”. Detta ger upphov till följande reflektioner:

I allmänna termer kan en fysisk person i en grupp anses ”identifierad” när han eller hon på något sätt kan ”särskiljas” från alla de övriga medlemmarna i gruppen. I enlighet med detta är en fysisk person ”identifierbar” om, även om personen ännu inte har blivit identifierad, det är möjligt att göra detta (vilket är innebörden av suffixet ”-bar”). Detta andra alternativ är därför i praktiken minimivillkoret för att avgöra om information omfattas av den tredje beståndsdelen.

Identifiering sker vanligen genom vissa upplysningar som vi kan kalla ”identifierare” och som har en särskild och nära relation med den specifika individen. Exempel på dessa är yttre kännetecken i personens utseende, som t.ex. längd, hårfärg, klädsel osv. … eller en egenskap hos personen som inte omedelbart märks, t.ex. yrke, befattning, namn osv. Direktivet nämner ”identifierarna” i definitionen av ”personuppgifter” i artikel 2 där det fastställs att en fysisk person ”*kan identifieras, direkt eller indirekt, framför allt genom hänvisning till ett identifikationsnummer eller till en eller flera faktorer som är specifika för hans fysiska, fysiologiska, psykiska, ekonomiska, kulturella eller sociala identitet.*”

”Direkt” eller ”indirekt” identifierbar

Ytterligare klargöranden finns i kommentaren till artiklarna i kommissionens ändringsförslag genom att det där fastställs att en person kan identifieras direkt genom ett namn eller indirekt genom ett telefonnummer, bilnummer, personnummer, passnummer eller av en kombination av väsentliga kriterier som gör att personen känns

igen genom att den grupp som han tillhör ringas in (ålder, yrkesverksamhet, bostadsort, osv.). Denna lydelse anger klart och tydligt att frågan om huruvida vissa identifierare är tillräckliga för att identifiera en person beror på förhållandena i den bestämda situationen. Ett mycket vanligt efternamn kommer inte att vara tillräckligt för att identifiera, dvs. särskilja, någon från hela befolkningen i ett land, medan det sannolikt kan identifiera en elev i ett klassrum. Även mindre viktig information, som t.ex. ”mannen i svart kostym” kan identifiera någon av de förbipasserande som står vid ett trafikljus. Frågan om huruvida den individ som informationen avser identifieras eller inte beror på omständigheterna i det aktuella fallet.

När det gäller ”direkt” identifierade eller identifierbara personer är personens **namn** den vanligaste identifieraren, och i praktiken innebär begreppet ”identifierad person” oftast en referens till personens namn.

För att fastställa identiteten måste personens namn ibland kombineras med andra upplysningar (födelsedatum, föräldrarnas namn, adress eller ett fotografi av ansiktet) för att förhindra att han eller hon blandas ihop med eventuella andra personer med samma namn. Exempelvis kan informationen att Titius äger en summa pengar anses avse en identifierad individ eftersom den är kopplad till personens namn. Namnet är en upplysning som säger oss att individen använder denna kombination av bokstäver och ljud för att utmärka sig själv och för att andra personer med vilka han eller hon etablerar kontakt ska kunna särskilja honom eller henne från andra. Namnet kan också vara en utgångspunkt som leder till information om var personen bor eller kan hittas. Det kan också ge information om personerna i hans eller hennes familj (genom efternamnet) och ett antal olika rättsliga och sociala förhållanden som är knutna till namnet (skolgång/utbildning, patientjournaler, bankkonton). Det kan till och med vara möjligt att få reda på hur personen ser ut om det finns en bild som är knuten till namnet. Alla dessa nya upplysningar som är knutna till namnet kan göra det möjligt för någon att zooma in en levande person, och genom identifierarna knyts således den ursprungliga informationen samman med en fysisk person som kan särskiljas från andra individer.

När det gäller ”indirekt” identifierade eller identifierbara personer gäller denna kategori vanligen fenomenet ”unika kombinationer”, oavsett om de är små eller stora. I fall där de tillgängliga identifierarna vid första anblicken inte gör det möjligt för någon att särskilja en specifik person kan denne ändå vara ”identifierbar” eftersom den informationen tillsammans med andra upplysningar (oavsett om dessa registrerats av den registeransvarige eller inte) kommer att göra det möjligt att särskilja individen från andra individer. Det är i detta sammanhang som direktivet nämner ”en eller flera faktorer som är specifika för hans fysiska, fysiologiska, psykiska, ekonomiska, kulturella eller sociala identitet”. Vissa utmärkande egenskaper är så unika att en person lätt kan identifieras (”den nuvarande spanske premiärministern”), men en kombination av upplysningar på kategorinivå (ålderskategori, regionalt ursprung, osv.) kan också vara tämligen avgörande under vissa omständigheter, särskilt om man har tillgång till någon form av ytterligare information. Detta fenomen har studerats ingående av statistiker, som alltid är måna om att undvika brott mot sekretessen.

Exempel nr 10: Fragmentarisk information i pressen

Information om ett gammalt kriminalfall som tidigare rönte stort intresse från allmänheten blir offentliggjord. I det aktuella offentliggörandet ges ingen av de traditionella identifierarna, i synnerhet inga namn eller födelsedatum för någon av de inblandade.

Det verkar inte orimligt svårt att få fram mer information som gör det möjligt att lista ut vilka personer som huvudsakligen var inblandade, t.ex. genom att se i tidningar från den aktuella tidsperioden. Man kan till och med anta att det inte är helt osannolikt att någon skulle vidta sådana åtgärder (som att titta i gamla tidningar) vilket högst sannolikt skulle ge namn och andra identifierare för de personer som avses i exemplet. Det förefaller därför motiverat att anse informationen i exemplet som ”information om identifierbara personer” och som sådan som ”personuppgifter”.

I detta sammanhang bör det noteras att även om identifiering genom namnet i praktiken är det oftast förekommande så är ett namn i sig inte alltid nödvändigt för att identifiera en individ. Detta kan vara fallet när andra ”identifierare” används för att särskilja någon. I datafiler för registrering av personuppgifter ges de registrerade personerna vanligen en unik identifierare för att undvika sammanblandning mellan två personer i filen. Även på nätet blir det tack vare verktyg för övervakning av Internettrafiken lätt att identifiera en dators beteende och bakom denna, datoranvändarens beteende. På detta sättet pusslar man ihop individens personlighet för att tillskriva individen vissa beslut. Utan att ens fråga efter en individs namn och adress är det möjligt att kategorisera personen på grundval av socioekonomiska, psykologiska, filosofiska eller andra kriterier och tillskriva honom eller henne vissa beslut eftersom individens kontaktpunkt (en dator) inte längre nödvändigtvis kräver att individens identitet i snäv bemärkelse avslöjas. Med andra ord, möjligheten att identifiera en individ betyder inte längre nödvändigtvis att kunna ta reda på hans eller hennes namn. Definitionen av personuppgifter speglar detta förhållande[10].
EG-domstolen har gjort uttalanden i samma avseende genom att fastslå att ”*omnämnandet av olika personer – med namn eller på annat sätt, till exempel med telefonnummer eller med uppgifter om deras arbetsförhållanden och fritidsintressen – på en hemsida på Internet utgör en "behandling av personuppgifter [...]” i den mening som avses i [...] direktiv 95/46”*[11].

Exempel nr 11: Asylsökande

Asylsökande som inte talar om sitt riktiga namn på ett mottagningscenter har getts en kod för administrativa ändamål. Kodnumret kommer att vara en identifierare på så sätt att olika upplysningar om den asylsökandes vistelse på centret kommer att knytas till detta, och genom ett fotografi eller andra biometriska indikatorer kommer kodnumret att ha en nära och omedelbar anknytning till den fysiska personen. Därigenom kan han särskiljas från andra asylsökande och olika upplysningar kan tilldelas honom, som sedan kommer att referera till en ”identifierad” fysisk person.

[10] *Report on the application of data protection principles to the worldwide telecommunication networks* av Yves Poullet och hans arbetsgrupp för Europarådets rådgivande kommitté för konvention 108 (T-PD), punkt 2.3.1, T-PD (2004) 04 slutlig.

[11] EG-domstolens dom av den 6 november 2003 i mål C-101/2001, (Lindqvist), punkt 27.

I artikel 8.7 föreskrivs att ”medlemsstaterna skall bestämma på vilka villkor ett nationellt identifikationsnummer eller något annat vedertaget sätt för identifiering får behandlas”. Det är värt att notera innebörden av denna bestämmelse, som inte klart anger vilken sorts villkor som medlemsstaterna bör anta, men som ändå finns med i artikeln som handlar om känsliga uppgifter. I skäl 33 omnämns denna typ av uppgifter som *”uppgifter som på grund av sin natur kan kränka grundläggande fri- och rättigheter eller privatlivets helgd”*. Det är rimligt att tänka sig att lagstiftaren upplevde samma oro när det gäller nationella identifikationsnummer på grund av de stora möjligheter de ger att lätt och otvetydigt kombinera olika upplysningar om en viss individ.

Hjälpmedel för identifiering

Skäl 26 i direktivet ägnar särskild uppmärksamhet åt begreppet ”identifierbar” och det står att *”för att avgöra om en person är identifierbar skall härvid beaktas alla hjälpmedel som i syfte att identifiera vederbörande rimligen kan komma att användas antingen av den registeransvarige eller av någon annan person”*. Detta innebär att enbart en hypotetisk möjlighet att särskilja en individ inte är tillräcklig för att anse personen som ”identifierbar”. Om denna möjlighet inte existerar eller är försumbar när man beaktar *”alla hjälpmedel som i syfte att identifiera vederbörande rimligen kan komma att användas antingen av den registeransvarige eller av någon annan person*” bör personen inte anses som ”identifierbar” och informationen skulle inte anses som ”personuppgifter”. Kriteriet *”alla hjälpmedel som i syfte att identifiera vederbörande rimligen kan komma att användas antingen av den registeransvarige eller av någon annan person”* bör framför allt ta hänsyn till alla faktorer som spelar in. Kostnaderna för att göra en identifiering är en faktor men inte den enda. Faktorer som det avsedda ändamålet, det sätt på vilket behandlingen är strukturerad, den fördel som den registeransvarige förväntar sig, de intressen som står på spel för individerna liksom risken för organisatoriska störningar (t.ex. brott mot tystnadsplikten) och tekniska problem bör samtliga beaktas. Å andra sidan är denna test dynamisk och bör ta hänsyn till den tekniska utvecklingsnivån vid den tidpunkt då uppgifterna behandlas och möjligheterna till utveckling under den period under vilken uppgifterna kommer att behandlas. Identifiering är eventuellt inte möjlig för närvarande med alla hjälpmedel som rimligen kan komma att användas idag. Om uppgifterna är avsedda att sparas en månad kanske identifiering inte kan förväntas under uppgifternas livstid och de bör därför inte anses som personuppgifter. Om de emellertid är avsedda att sparas i 10 år bör den registeransvarige överväga möjligheten till identifiering som också kan inträffa under det nionde året av uppgifternas livstid, och som förvandlar dem till personuppgifter vid den tidpunkten. Systemet bör vara i stånd att anpassa sig till denna utveckling allt eftersom den äger rum och införliva lämpliga tekniska och organisatoriska åtgärder när det är aktuellt.

Exempel nr 12: Offentliggörande av röntgenbilder tillsammans med patientens förnamn

En kvinnas röntgenbild hade offentliggjorts i en vetenskaplig tidskrift tillsammans med hennes förnamn, som var mycket ovanligt. Kvinnans förnamn, i kombination med att släktingar eller bekanta kände till att hon led av en viss sjukdom gjorde henne identifierbar för ett antal personer och röntgenbilden skulle då betraktas som personuppgifter.

Exempel nr 13: Uppgifter om läkemedelsforskning

Sjukhus eller enskilda läkare överför uppgifter från sina patienters journaler till ett företag för medicinska forskningsändamål. Inga namn på patienterna används utan bara serienummer som slumpmässigt tilldelas varje kliniskt fall för att säkerställa sammanhang och undvika sammanblandning av information om olika patienter. Endast patienternas respektive läkare, som är bundna av tystnadsplikt, har tillgång till deras namn. Uppgifterna innehåller ingen ytterligare information som gör att patienterna kan identifieras genom att uppgifterna kombineras. Dessutom har alla andra rättsliga, tekniska eller organisatoriska åtgärder vidtagits för att förhindra att de registrerade identifieras eller blir identifierbara. Under dessa omständigheter kan en dataskyddsmyndighet anse att läkemedelsföretaget inte använder några hjälpmedel vid databehandlingen som rimligen skulle kunna användas i syfte att identifiera de registrerade.

Som redan nämnts ovan kommer i själva verket den registeransvariges syfte med databehandlingen att vara en relevant faktor för bedömningen av alla hjälpmedel som rimligen kan komma att användas för att identifiera personer. Nationella dataskyddsmyndigheter har stött på fall där den registeransvarige hävdar att det enbart är spridda upplysningar som behandlas, utan några referenser till namn eller andra direkta identifierare, och förespråkar att uppgifterna inte bör anses som personuppgifter och inte omfattas av uppgiftsskyddsbestämmelser. Samtidigt är behandlingen av uppgifterna meningsfull endast om den gör det möjligt att identifiera specifika individer och behandla dem på ett visst sätt. I dessa fall där syftet med databehandlingen innebär identifiering av individer kan man förutsätta att den registeransvarige eller någon annan delaktig person har eller kommer att ha hjälpmedel som ”rimligen kan komma att användas” för att identifiera den registrerade. Att hävda att enskilda individer inte är identifierbara när syftet med databehandlingen just är att identifiera individer, vore oerhört motsägelsefullt. Därför bör informationen anses avse identifierbara individer och behandlingen omfattas av uppgiftsskyddsbestämmelser.

Exempel nr 14: Videoövervakning

Detta är särskilt relevant i samband med videoövervakning, där de registeransvariga ofta hävdar att identifiering bara kommer att äga rum för en liten andel av det insamlade materialet, och att det följaktligen inte behandlas några personuppgifter innan identifieringen i dessa få fall faktiskt äger rum. Eftersom syftet med videoövervakning emellertid är att identifiera de personer som syns på videobilderna i samtliga fall där sådan identifiering bedöms nödvändig av den registeransvarige, måste hela företeelsen som sådan anses som databehandling om identifierbara personer, även om vissa personer som spelats in i praktiken inte är identifierbara.

Exempel nr 15: Dynamiska IP-adresser

Arbetsgruppen har ansett IP-adresser som uppgifter som avser en identifierbar person. Den har fastslagit att "*nätleverantörer och förvaltare av lokala nätverk (LAN) med rimliga medel kan identifiera de Internet-användare som de har tilldelat IP-adresser eftersom de i allmänhet i en fil bokför datum, tidpunkt, varaktighet och den dynamiska IP-adress som Internet-användaren har fått. Samma sak gäller för Internet-leverantörer som för en loggbok på HTTP-servern. I dessa fall råder det inga tvivel om*

att man kan tala om personuppgifter i den mening som avses i artikel 2 a i direktivet."[12]

Särskilt i de fall när behandlingen av IP-adresser sker i syfte att identifiera användarna av en dator (t.ex. av innehavare av upphovsrätter som underlag för åtal mot datoranvändare som kränker immateriella rättigheter) förutsätter den registeransvarige att "medel som rimligen kan komma att användas" för att identifiera personerna kommer att finnas tillgängliga t.ex. genom de domstolar där talan väcks (i annat fall är insamlingen av informationen inte meningsfull), och informationen bör därför betraktas som personuppgifter.

En slags IP-adresser som under vissa omständigheter inte gör det möjligt att identifiera användaren av olika tekniska och organisatoriska skäl skulle utgöra ett särfall. Ett exempel på detta kan vara IP-adresser som tilldelas en dator på ett Internetkafé där det inte krävs identifiering av gästerna. Man kan hävda att de uppgifter som samlas in angående användningen av datorn X under en viss tid inte gör det möjligt att identifiera användaren med rimliga medel och därför inte är personuppgifter. Det bör emellertid noteras att Internetleverantörerna med största sannolikhet inte vet varken om den aktuella IP-adressen är möjlig att identifiera eller inte, och att de kommer att behandla de uppgifter som är knutna till den IP-adressen på samma sätt som de behandlar information som är knuten till registrerade och identifierbara användares IP-adresser. Om inte Internetleverantören med absolut säkerhet kan särskilja att uppgifterna svarar mot användare som inte kan identifieras måste den följaktligen behandla all IP-information som personuppgifter för att vara på den säkra sidan.

Exempel nr 16: Skadegörelse orsakad av graffiti

Passagerarfordon som ägs av transportföretag utsätts för skadegörelse om och om igen genom att de målas med graffiti. I syfte att bedöma skadegörelsen och underlätta att göra gällande rättsliga anspråk mot förövarna inrättar företaget ett register med information om omständigheterna för skadegörelsen och med bilder på de fördärvade fordonen och på förövarnas "taggar" eller "signatur". När informationen matas in i registret är förövarna inte kända och inte heller vems "signatur" som är vems. Det kan mycket väl vara så att det aldrig kommer att bli känt. Avsikten med databehandlingen är emellertid just att identifiera de individer som informationen avser i deras egenskap av gärningsmän, så att de kan rikta rättsliga anspråk mot dem. Sådan databehandling blir meningsfull om den registeransvarige anser att det "rimligen" en dag kommer att finnas medel att identifiera individen. Informationen i bilderna bör anses avse "identifierbara" individer, informationen i registret som bedömas som "personuppgifter" och databehandlingen bör omfattas av uppgiftsskyddsbestämmelserna som tillåter sådan databehandling under vissa omständigheter och om den omfattas av vissa skyddsåtgärder.

Om identifiering av den registrerade inte ingår i syftet med databehandlingen blir de tekniska åtgärderna för att förhindra identifiering av mycket stor betydelse. Att vidta lämpliga avancerade tekniska och organisatoriska åtgärder för att skydda uppgifterna mot identifiering kan vara det som gör att personerna inte anses identifierbara, med beaktande av *alla hjälpmedel som rimligen kan komma att användas antingen av den registeransvarige eller av någon annan person* i syfte att identifiera individerna. I detta

[12] WP 37: Skydd av privatlivet på Internet – Ett integrerat förhållningssätt till dataskydd på Internet – Antaget den 21 november 2000.

fall är genomförandet av dessa åtgärder inte *följden* av en rättslig förpliktelse enligt artikel 17 i direktivet (som i första hand är tillämplig endast om informationen i fråga utgörs av personuppgifter) utan snarare ett *villkor* för att informationen inte ska anses som just personuppgifter och behandlingen av denna inte omfattas av direktivet.

Pseudonymiserade uppgifter

Pseudonymisering är en process för att dölja identiteter. Syftet med processen är att kunna samla ytterligare uppgifter om en och samma individ utan att behöva känna till hans identitet. Detta är särskilt relevant när det gäller forskning och statistik.

Pseudonymisering kan ske på ett sätt som går att spåra genom användning av förteckningar över identiteter och deras motsvarande pseudonymer eller genom att använda tvåvägs krypteringsalgoritmer för pseudonymisering. Att dölja identiteter kan också ske på ett sätt så att återidentifiering inte är möjlig, t.ex. genom envägskryptering, som i allmänhet skapar anonymiserade uppgifter.

Hur pass effektiv pseudonymiseringen är beror på ett antal faktorer (i vilket skede den används, hur säker den är mot spårning bakåt, hur stor den population är där individen ska avidentifieras, möjligheten att länka individuella transaktioner eller register till samma person, osv.). Pseudonymer bör vara slumpmässiga och omöjliga att förutsäga. Antalet möjliga pseudonymer bör vara så stort att samma pseudonym aldrig slumpmässigt väljs två gånger. Om det krävs hög säkerhetsnivå måste uppsättningen möjliga pseudonymer minst vara lika stort som antalet olika värden på säkra kryptografiska hashfunktioner[13].

Spårbara pseudonymiserade uppgifter kan anses som information om individer som är *indirekt identifierbara*. Användning av en pseudonym innebär ju att det är möjligt att följa spåren tillbaka till individen så att dennes identitet kan avslöjas, men endast på i förväg fastställda villkor. I det här fallet kommer riskerna för individerna när det gäller behandlingen av sådan indirekt identifierbar information i de flesta fall att vara låga, så fastän uppgiftsskyddsbestämmelserna gäller kommer tillämpningen av bestämmelserna med rätta att vara mer flexibel än vid behandling av information om direkt identifierbara individer.

Kodade uppgifter

Kodade uppgifter är ett klassiskt exempel på pseudonymisering. Informationen avser individer som har betecknats med en kod, medan nyckeln för att koppla samman koden och de vanliga identifierarna (namn, födelsedatum, adress) för individerna förvaras för sig.

Exempel nr 17: Icke-aggregerade uppgifter för statistik

För att illustrera vikten av att ta hänsyn till alla omständigheter i syfte att bedöma huruvida hjälpmedlen för identifiering ”rimligen” kommer att användas kan man som exempel ta personuppgifter som behandlas av den nationella statistikbyrån när, i ett visst skede, informationen sparas i icke-aggregerad form och avser specifika individer,

[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

som dock är betecknade med en kod i stället för ett namn (t.ex. individen med koden X1234 dricker ett glas vin oftare än tre gånger per vecka). Statistikbyrån förvarar nyckeln till dessa koder för sig (den förteckning som beskriver vilka koder som hör ihop med vilka namn). Nyckeln kan anses att ”rimligen komma att användas” av statistikbyrån, och den individrelaterade informationen kan därför anses som personuppgifter och bör hanteras i enlighet med uppgiftsskyddsbestämmelserna av statistikbyrån. Nu tänker vi oss att förteckningen med uppgifter om konsumenternas dryckesvanor när det gäller vin överlämnas till den nationella vinproducentorganisationen så att de kan backa upp sin offentliga hållning med statistik. För att avgöra om förteckningen med uppgifter fortfarande är personuppgifter bör det göras en bedömning av om den enskilde vinkonsumenten kan identifieras *”med beaktande av alla hjälpmedel som rimligen kan komma att användas antingen av den registeransvarige eller av någon annan person”*.

Om de koder som används är unika för varje enskild person uppstår en risk för identifiering vid varje tillfälle som det är möjligt att få tillgång till den nyckel som används för krypteringen. Därför är riskerna för angrepp av en extern hackare, sannolikheten för att någon inom sändarens organisation – trots sin tystnadsplikt – skulle tillhandahålla nyckeln *och* möjligheten till indirekt identifiering faktorer att ta hänsyn till vid bedömningen av huruvida personerna kan identifieras *med beaktande av alla hjälpmedel som rimligen kan komma att användas antingen av den registeransvarige eller av någon annan person*, och följaktligen huruvida information bör anses som ”personuppgifter”. Om de konstateras vara personuppgifter ska bestämmelserna om uppgiftsskydd tillämpas. En annan aspekt är att uppgiftsskyddsbestämmelserna ger möjlighet att ta hänsyn till eventuellt reducerad risk för individerna och låter behandlingen omfattas av mer eller mindre strikta villkor på grundval av den flexibilitet som ges i direktivet.

Om däremot koderna inte är unika, utan samma kodnummer (t.ex. ”123”) används för att beteckna individer i olika städer och för uppgifter från olika år (dvs. bara för att särskilja en specifik individ ett visst år och inom urvalet i en och samma stad) kan den registeransvarige eller en tredje part endast identifiera en viss individ om de vet vilket år och vilken stad som uppgifterna avser. Om denna tilläggsinformation har försvunnit, och den rimligen inte kommer att återfinnas, kan det anses att informationen inte avser identifierbara individer och därför inte omfattas av uppgiftsskyddsbestämmelserna.

Denna sorts information är vanligt förekommande vid klinisk prövning av läkemedel. En rättslig ram för denna typ av verksamhet fastställs i direktiv 2001/20 av den 4 april 2001 om tillnärmning av medlemsstaternas lagar och andra författningar rörande tillämpning av god klinisk sed vid kliniska prövningar av humanläkemedel[14]. Den läkare/forskare (”prövare”) som prövar läkemedel samlar in information om de kliniska resultaten för varje patient, och betecknar denne med en kod. Forskaren ger informationen till läkemedelsföretaget eller andra berörda parter (”sponsorer”) endast i denna kodade form, eftersom de bara är intresserade av den biostatistiska informationen. Prövaren förvarar separat en nyckel som förbinder koderna med allmän information för att identifiera patienterna var för sig. För att skydda patienternas hälsa om det visar sig att medicinerna kan innebära risker är prövaren skyldig att förvara denna nyckel så att de enskilda patienterna vid behov kan identifieras och få rätt behandling.

[14] EGT L 121, 1.5.2001, s. 34.

Frågan i det här fallet är om de uppgifter som används för den kliniska prövningen kan anses avse ”identifierbara” fysiska personer och sålunda omfattas av uppgiftsskyddsbestämmelserna. För att avgöra om en person är identifierbar bör, enligt analysen ovan, alla hjälpmedel beaktas som i syfte att identifiera vederbörande rimligen kan komma att användas antingen av den registeransvarige eller av någon annan person. I detta fall är identifieringen av enskilda (för att ge lämplig behandling om behovet skulle uppstå) ett av syftena med att behandla de kodade uppgifterna. Läkemedelsföretaget har utformat medlen för databehandlingen, däribland de organisatoriska åtgärderna och företagets kontakter med den forskare som har nyckeln så att identifieringen av enskilda inte enbart är något som *kan* ske utan snarare något som *måste* ske under vissa omständigheter. Identifieringen av patienter ingår följaktligen i databehandlingens syften och i medlen för denna. I detta fall kan man utgå från att sådana kodade uppgifter utgör information som avser identifierbara fysiska personer för samtliga som tar del i den eventuella identifieringen och uppgifterna bör omfattas av lagstiftningen för uppgiftsskydd. Detta betyder dock inte att alla andra registeransvariga som behandlar samma uppsättning kodade uppgifter skulle behandla personuppgifter, om återidentifiering inom det specifika system inom vilket de övriga registeransvariga verkar uttryckligen är uteslutet och lämpliga tekniska åtgärder har vidtagits i detta avseende.

Inom andra forskningsområden eller andra områden inom ramen för samma projekt kan återidentifiering av den registrerade ha uteslutits vid utformningen av protokoll och förfaranden, t.ex. på grund av att det inte finns några terapeutiska aspekter att ta hänsyn till. Av tekniska eller andra skäl kan det fortfarande finnas ett sätt att ta reda på vilka personer som motsvarar vilka kliniska uppgifter men identifieringen förmodas inte, eller förväntas inte, äga rum under några omständigheter och lämpliga tekniska åtgärder (t.ex. kryptografisk, oåterkallelig hashfunktion) har vidtagits för att förhindra att detta inträffar. Även om identifiering av vissa registrerade kan äga rum trots alla dessa protokoll och åtgärder (på grund av oförutsedda omständigheter som t.ex. oavsiktlig matchning av den registrerades egenskaper som avslöjar hans eller hennes identitet), behöver den information som behandlas av den ursprunglige registeransvarige i detta fall inte anses avse identifierade eller identifierbara individer med beaktande av *alla hjälpmedel som rimligen kan komma att användas antingen av den registeransvarige eller av någon annan person*. Behandlingen av uppgifterna behöver följaktligen inte omfattas av direktivet. För den nya registeransvarige som i praktiken har haft tillgång till den identifierbar informationen är det en annan fråga och informationen kommer utan tvivel att anses som ”personuppgifter”.

FAQ 14-7 om Safe Harbour-systemet

Frågan om kodade uppgifter inom läkemedelsforskningen har behandlats inom ramen för Safe Harbour-systemet[15]. FAQ 1 -7 har följande lydelse**:**

FoS 14 - Farmaceutiska och medicinska produkter

F7: Forskningsrön kodas alltid inledningsvis av ansvarig forskningsledare för att enskilda försökspersoners identitet inte skall avslöjas. De läkemedelsföretag, som sponsrar sådan forskning, får ej tillgång till kodnyckeln. Den enda kodnyckeln finns endast hos forskaren, för att han/hon under vissa omständigheter skall kunna identifiera försökspersonen (t.ex. om medicinsk uppföljning erfordras). Utgör en

[15] Rådets beslut 2000/520/EG av den 26 juli 2000, EGT L 215, 25.8.2000, s. 7.

överföring från EU till USA av uppgifter, som kodats på detta sätt, en sådan överöring av personuppgifter som omfattas av safe harbour-principerna?

S: Nej, den utgör inte en sådan överföring av personuppgifter som omfattas av dessa principer.

Arbetsgruppen anser inte att detta påstående inom ramen för safe harbour-systemet är förenligt med resonemanget ovan, vilket förespråkar att sådan information bör anses som personuppgifter och omfattas av direktivet. I själva verket är denna fråga inte tillräckligt stringent eftersom den inte anger till vem eller på vilka villkor som uppgifterna överförs. Arbetsgruppen är införstådd med att frågan refererar till det fall då kodade uppgifter sänds till en mottagare i USA (till exempel ett läkemedelsföretag) som bara får de kodade uppgifterna och aldrig kommer att känna till patienternas identitet, som är känd och kommer att delges enbart läkaren/forskaren i EU om det uppstår behov av medicinsk behandling, men aldrig till företaget i USA.

Anonyma uppgifter

”Anonyma uppgifter” i den mening som avses i direktivet kan definieras som all information som avser en fysisk person som inte kan identifieras varken av den registeransvarige eller av någon annan, *med beaktande av alla hjälpmedel som i syfte att identifiera vederbörande rimligen kan komma att användas antingen av den registeransvarige eller av någon annan person.* ”Anonymiserade uppgifter” är därför anonyma uppgifter som tidigare hänvisade till en identifierad person men där denna identifiering inte längre är möjlig. I skäl 26 tar också upp detta begrepp genom följande formulering: *”Skyddsprinciperna gäller inte för uppgifter som gjorts anonyma på ett sådant sätt att den registrerade inte längre är identifierbar”*. Bedömningen av om uppgifterna gör det möjligt att identifiera en individ och huruvida informationen kan anses anonym eller inte beror återigen på omständigheterna, och varje enskilt fall bör analyseras för sig med särskild tonvikt vid i vilken utsträckning hjälpmedlen rimligen kommer att användas för identifiering enligt skäl 26. Detta är särskilt relevant när det gäller statistisk information när, trots det faktum att informationen får presenteras som aggregerade uppgifter, det ursprungliga urvalet inte är tillräckligt omfattande och andra upplysningar kan möjliggöra identifiering av individer.

Exempel nr 18: Statistiska undersökningar och kombination av spridda upplysningar

Utöver deras allmänna skyldighet att följa uppgiftsskyddsbestämmelser i syfte att säkerställa anonymiteten i statistiska undersökningar omfattas statistiker av en särskild tystnadsplikt, och enligt de reglerna är de förbjudna att offentliggöra uppgifter som inte är anonyma. Detta tvingar dem att offentliggöra aggregerade statistiska uppgifter som omöjligen kan tillskrivas en identifierad person bakom statistiken. Denna bestämmelse är särskilt relevant när det gäller offentliggörande av folkräkningsuppgifter. I varje situation bör det fastställas en tröskel under vilken det bedöms vara möjligt att identifiera de personer som berörs. Om ett kriterium verkar leda till identifiering i en given grupp personer, även om denna är stor (t.ex. en läkare arbetar i en stad med 6 000 invånare) bör detta ”diskriminerande” kriterium strykas eller andra kriterier läggas till för att ”tunna ut” resultaten om en viss person så att den statistiska sekretessen upprätthålls.

Exempel nr 19: Offentliggörande av videoövervakning

En affärsinnehavare installerar ett kameraövervakningssystem i sin affär. I affären sätter han upp bilderna på tjuvar som har tagits tack vare kameraövervakningssystemet. Efter polisingripande döljer han tjuvarnas ansikten genom att göra dem mörkare. Även efter detta är det emellertid fortfarande möjligt för vänner, släktingar eller grannar till personerna på bilderna att känna igen dem eftersom deras siluett, frisyr och kläder fortfarande är igenkännliga.

4. FJÄRDE BESTÅNDSDELEN: ”FYSISK PERSON”

Det skydd som bestämmelserna i direktivet ger gäller fysiska personer, dvs. människor. Rätten till skydd av personuppgifter är i den meningen en universell rätt som inte är begränsad till medborgarna eller invånarna i ett visst land. I skäl 2 i direktivet står det uttryckligen att ”*systemen för databehandling av uppgifter är till för människornas skull*” och att de ”*oavsett fysiska personers medborgarskap eller hemvist måste […] respektera dessa personers grundläggande fri- och rättigheter*”.

Begreppet fysisk person omnämns i artikel 6 i den allmänna förklaring om de mänskliga rättigheterna enligt vilken ”*envar har rätt att allestädes erkännas som person i lagens mening*”. I medlemsstaternas lagstiftning, vanligen inom civilrättens område, ges en mer precis definition av begreppet människans personlighet i betydelsen förmågan att vara subjekt i rättsförhållanden, som tar sin början med individens födelse och slutar med dennes bortgång. Personuppgifter avser därför i princip identifierade eller identifierbara *levande personer*. Detta ger upphov till en rad frågor i samband med denna analys.

Uppgifter om avlidna personer

Följaktligen bör information som avser avlidna personer i princip inte anses som personuppgifter enligt bestämmelserna i direktivet, eftersom avlidna inte längre är fysiska personer enligt civilrätten. Personuppgifter om en avliden person kan emellertid fortfarande åtnjuta skydd i vissa fall.

För det första kanske den registeransvarige inte har möjlighet att ta reda på om den person som uppgifterna avser fortfarande lever eller eventuellt har avlidit. Eller även om han gör detta kanske informationen om den avlidne behandlas enligt samma system som informationen om individen i livet, utan åtskillnad. Eftersom den registeransvarige omfattas av skyldigheterna beträffande uppgiftsskydd enligt direktivet i fråga om uppgifter om levande personer, är det i praktiken förmodligen lättare för honom att behandla även uppgifterna om den avlidne på det sätt som föreskrivs av uppgiftsskyddsbestämmelserna än att göra åtskillnad mellan två uppsättningar uppgifter.

För det andra kan informationen om avlidna också hänvisa till levande personer. Informationen om att den döda Gaia led av blödarsjuka tyder exempelvis på att hennes son Titius också lider av samma sjukdom eftersom den är knuten till en gen som finns i X-kromosomen. När information som är uppgifter om en avliden person samtidigt kan anses avse en levande person och följaktligen vara personuppgifter enligt direktivet, kan personuppgifterna gällande den avlidne indirekt skyddas genom uppgiftsskyddsbestämmelserna.

För det tredje kan information om avlidna personer omfattas av ett särskilt skydd genom andra bestämmelser än lagstiftningen om uppgiftsskydd, med hjälp av

gränsdragningar enligt vad vissa kallar *”personalitas praeterita”*. Sjukvårdspersonals tystnadsplikt upphör inte när en patient avlider. Nationell lagstiftning om en människas rätt till ett rättvist eftermäle och oantastad ära kan också ge skydd till den avlidnes minne.

Och, för det fjärde, ingenting hindrar att en medlemsstat utökar räckvidden av den nationella lagstiftning varigenom bestämmelserna i direktiv 95/46 har införlivats till att omfatta områden som inte ingår i direktivets tillämpningsområde, såvida ingen annan gemenskapsrättslig bestämmelse utgör hinder för detta, vilket EG-domstolen har erinrat om[16]. Det är möjligt att någon nationell lagstiftare beslutar utöka räckvidden för nationell lagstiftning och dataskydd till några av de aspekter som rör behandling av uppgifter om avlidna personer, i de fall då det finns ett berättigat intresse av detta[17].

Ofödda barn

I vilken omfattning uppgiftsskyddsbestämmelser får tillämpas före födseln beror på den allmänna inställningen i de nationella rättsordningarna när det gäller skyddet för ofödda barn. Om vi främst tittar på arvsrätt erkänner vissa medlemsstater principen att det avlade men ännu ej födda barnet betraktas som om det var fött när det gäller förmåner (och kan följaktligen motta ett arv eller en gåva), under förutsättning att de faktiskt föds. I andra medlemsstater ges specifikt skydd genom särskilda bestämmelser i lagstiftningen, under samma förutsättning. För att fastställa huruvida nationella bestämmelser om uppgiftsskydd också omfattar information om ofödda barn bör man titta närmare på den allmänna inställningen i den nationella rättsordningen mot bakgrund av den grundläggande tanken att syftet med uppgiftsskyddsbestämmelser är att skydda individen.

En andra fråga uppstår när man tar i beaktande att rättsordningens allmänna svar grundar sig på att situationen med ett ofött barn är begränsad till den tid graviditeten varar. Det tas inte hänsyn till det faktum att denna situation i själva verket kan vara betydligt längre, vilket är fallet med frysta embryon. Slutligen kan man hitta specifika rättsliga svar i särskilda bestämmelser om fortplantningsteknik, som tar upp användningen av medicinsk eller genetisk information om embryon.

Juridiska personer

Eftersom definitionen av personuppgifter avser individer, dvs. fysiska personer, är information om juridiska personer i princip inte täckta av direktivet, och det skydd som direktivet ger är inte tillämpligt[18]. Vissa bestämmelser om uppgiftsskydd kan emellertid fortfarande gälla indirekt för information om företag eller juridiska personer under en rad omständigheter.

Vissa bestämmelser i direktiv 2002/58/EG om integritet och elektronisk kommunikation omfattar även juridiska personer. I artikel 1.2 i detta föreskrivs följande: *”Bestämmelserna i detta direktiv skall precisera och komplettera direktiv 95/46/EG för de ändamål som avses i punkt 1. Bestämmelserna är vidare avsedda att*

---

16 EG-domstolens dom av den 6 november 2003 i mål C-101/2001, (Lindqvist), punkt 98.

17 Protokoll från mötet i Europeiska Unionens råd den 8 februari 1995, dokument 4730/95: ”Angående artikel 2 a ”Rådet och kommissionen bekräftar att det är medlemsstaterna som ska fastställa huruvida och i vilken utsträckning detta direktiv ska tillämpas på avlidna personer.”

18 Se skäl 24 i direktivet. ”Sådan lagstiftning som rör skydd för juridiska personer med avseende på behandling av uppgifter som angår dem berörs inte av detta direktiv.”

skydda berättigade intressen för de abonnenter som är juridiska personer." Tillämpningen av några av bestämmelserna som rör abonnentförteckningar och icke begärd kommunikation utsträcks i enlighet med detta till att omfatta även juridiska personer genom artiklarna 12 och 13.

Information om juridiska personer kan också från fall till fall anses ”avse” fysiska personer i enlighet med kriterierna i detta dokument. Detta kan vara fallet när namnet på en juridisk person härrör från namnet på en fysisk person. Ett annat fall kan vara företags-epost, som vanligen används av en viss anställd, eller information om ett litet företag (rättsligt sett snarare ett ”objekt” än en juridisk person), som beskriver sin ägares beteende. I alla dessa fall, där kriterierna ”innehåll”, ”syfte” eller ”resultat” gör att informationen om den juridiska personen eller företaget anses ”avse” en fysisk person, bör informationen anses som personuppgifter och uppgiftsskyddsbestämmelserna gälla.

EG-domstolen har klargjort att ingenting hindrar att en medlemsstat utökar räckvidden av den nationella lagstiftning varigenom bestämmelserna i direktivet har införlivats till att omfatta områden som inte ingår i direktivets tillämpningsområde, såvida ingen annan gemenskapsrättslig bestämmelse utgör hinder för detta[19]. I enlighet med detta har några medlemsstater, bl.a. Italien, Österrike och Luxemburg, utökat räckvidden av vissa bestämmelser i den nationella lagstiftning som antagits i enlighet med direktivet (exempelvis bestämmelserna om säkerhetsåtgärder) till att omfatta behandling av uppgifter om juridiska personer.

Liksom när det gäller uppgifter om avlidna personer kan den registeransvariges praktiska arrangemang resultera i att personuppgifter om juridiska personer i praktiken omfattas av uppgiftsskyddsbestämmelserna. Om den registeransvarige samlar in uppgifter både om fysiska och juridiska personer utan att göra åtskillnad och matar in dem i samma datauppsättningar kan utformningen av databehandlingsmekanismerna och revisionssystemet utformas så att de uppfyller uppgiftsskyddsbestämmelserna. Det kan faktiskt vara lättare för den registeransvarige att tillämpa uppgiftsskyddsbestämmelserna på alla typer av information som finns i datafilerna än att försöka sortera vad som gäller fysiska respektive juridiska personer.

IV. VAD HÄNDER OM UPPGIFTERNA FALLER UTANFÖR DEFINITIONEN?

Som vi har sett i hela dokumentet betraktas information under olika omständigheter inte som personuppgifter. Detta är fallet när uppgifterna inte kan anses avse en individ, eller om individen inte kan anses identifierad eller identifierbar. Om den information som behandlas inte faller under begreppet ”personuppgifter” får detta till följd att direktivet inte är tillämpligt i enlighet med artikel 3 i detsamma. Detta behöver dock inte betyda att individer går miste om någon form av skydd i en särskild situation. Följande bör vägas in.

Om direktivet inte är tillämpligt kan eventuellt den nationella uppgiftsskyddslagstiftningen vara det. Enligt artikel 34 riktar sig detta direktiv till medlemsstaterna. Utanför dess tillämpningsområde omfattas medlemsstaterna inte av skyldigheterna enligt direktivet, dvs. främst att sätta i kraft de lagar och andra författningar som är nödvändiga för att följa direktivet. EG-domstolen har emellertid

[19] EG-domstolens dom av 6 november 2003 i mål C-101/2001, (Lindqvist), punkt 98.

klargjort att ingenting hindrar att en medlemsstat utökar räckvidden av den nationella lagstiftning varigenom bestämmelserna i direktivet har införlivats till att omfatta områden som inte ingår i direktivets tillämpningsområde, såvida ingen annan gemenskapsrättslig bestämmelse utgör hinder för detta. Det kan därför mycket väl inträffa att vissa situationer, som inte gäller behandling av personuppgifter enligt definitionen i direktivet, ändå omfattas av skydd enligt nationell lagstiftning. Detta kan t.ex. gälla kodade uppgifter, oavsett om dessa är personuppgifter eller inte.

I de fall där uppgiftsskyddsbestämmelser inte gäller kan vissa verksamheter ändå vara i strid med artikel 8 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna, som handlar om rätten till skydd för privat- och familjeliv, mot bakgrund av Europadomstolens omfattande rättspraxis. Andra regelverk, t.ex. skadeståndsbestämmelser, straffrätt eller antidiskrimineringslagstiftning kan också ge skydd till individer i de fall där uppgiftsskyddsbestämmelserna inte är tillämpliga och olika rättmätiga intressen kan stå på spel.

V. SLUTSATSER

I detta yttrande har arbetsgruppen gett vägledning om hur begreppet personuppgifter i direktiv 95/46/EG och relaterad gemenskapslagstiftning ska tolkas och hur det ska tillämpas i olika situationer.

Som en allmän synpunkt har det konstaterats att den europeiska lagstiftaren avsåg att anta en bred definition av begreppet personuppgifter men att begreppet inte har en obegränsad räckvidd. Man måste hela tiden beakta att målet med direktivet är att skydda individers grundläggande rättigheter och friheter, särskilt deras rätt till privatliv, när det gäller behandling av personuppgifter. Bestämmelserna har därför utformats för att gälla i situationer där individens rättigheter kan vara i fara och följaktligen i behov av skydd. Tillämpningsområdet för dataskyddsbestämmelserna bör inte sträckas för långt men man bör inte heller begränsa tolkningen av begreppet personuppgifter mer än nödvändigt. Direktivet har definierat tillämpningsområdet, genom att utesluta en rad verksamheter från detta, och ger utrymme för flexibilitet vid tillämpningen av bestämmelserna på verksamhet som faller inom dess tillämpningsområde. Dataskyddsmyndigheterna spelar en avgörande roll för att finna en lämplig balans i tillämpningen (se avsnitt II).

Arbetsgruppens analys bygger på de fyra huvudsakliga ”beståndsdelar” som kan särskiljas i definitionen av ”personuppgifter”, dvs. "varje upplysning”, ”som avser”, ”en identifierad eller identifierbar”, ”fysisk person”. Dessa beståndsdelar är nära sammankopplade och beroende av varandra, men avgör tillsammans om en upplysning bör anses som ”personuppgifter”. Analysen illustreras av exempel från nationell praxis vid medlemsstaternas dataskyddsmyndigheter.

- Den första beståndsdelen, ”varje upplysning” uppmanar till en bred tolkning av begreppet, oavsett informationens natur eller innehåll och i vilket tekniskt format den presenteras. Detta betyder att både objektiv och subjektiv information om en person oavsett egenskaper kan anses som ”personuppgifter” oberoende av på vilket tekniskt medium de förvaras. Yttrandet tar även upp biometriska uppgifter och de rättsliga distinktionerna i fråga om humanprover som de kan vara hämtade från(se avsnitt III.1).

- Den andra beståndsdelen, ”som avser”, har hittills ofta förbisetts men spelar en avgörande roll för att avgöra begreppets faktiska räckvidd, särskilt när det gäller objekt och ny teknik. I yttrandet anges tre alternativa beståndsdelar, dvs. innehåll, syfte och resultat, som är avgörande för huruvida information ”avser” en individ. Detta omfattar även information som kan ha en klar inverkan på hur en individ behandlas eller bedöms (se avsnitt III.2).

- Den tredje beståndsdelen, ”identifierad eller identifierbar”, riktar uppmärksamheten mot de omständigheter under vilka en individ bör anses ”identifierad", särskilt ”de hjälpmedel som i syfte att identifiera vederbörande rimligen kan komma att användas” antingen av den registeransvarige eller av någon annan person. Det särskilda sammanhanget och omständigheterna i ett specifikt fall spelar en viktig roll i denna analys. Yttrandet behandlar också ”pseudonymiserade uppgifter” och användningen av ”kodade uppgifter” i statistisk forskning eller läkemedelsforskning (se avsnitt III.3).

- Den fjärde beståndsdelen, ”fysisk person”, handlar om kravet att ”personuppgifter” ska gälla ”levande personer”. I yttrandet diskuteras också kopplingarna till uppgifter om avlida personer, ofödda barn och juridiska personer (se avsnitt III.4).

Slutligen tar yttrandet upp vad som händer om uppgifter faller utanför definitionen av ”personuppgifter”. Det kan finnas olika lösningar till hands för att hantera sådana fall, däribland nationell lagstiftning utanför direktivets tillämpningsområde, under förutsättning att gemenskapslagstiftningen följs (se avsnitt IV).

Arbetsgruppen uppmanar alla berörda parter att noggrant studera den vägledning som ges i detta yttrande och att ta hänsyn till denna vid tolkning och tillämpning av nationell lagstiftning i enlighet med direktiv 95/46/EG.

Medlemmarna i arbetsgruppen, de flesta företrädare för nationella tillsynsmyndigheter för uppgiftsskydd, har åtagit sig att vidareutveckla vägledningen i detta yttrande inom sina egna behörighetsområden och att säkerställa en korrekt tillämpning av sin nationella lagstiftning i enlighet med direktiv 95/46/EG.

Arbetsgruppen avser att tillämpa och utveckla vägledningen i yttrandet när detta är lämpligt, och att noggrant ta hänsyn till den i sitt fortsatta arbete, särskilt i frågor som rör identitetshantering i samband med e-förvaltning och e-hälsa samt vid radiofrekvensidentifiering (RFID). När det gäller radiofrekvensidentifiering planerar arbetsgruppen att bidra till ytterligare en analys av hur uppgiftsskyddsbestämmelser kan inverka på användningen av radiofrekvensidentifiering, och om eventuella behov av ytterligare åtgärder som kan bli nödvändiga för att säkerställa vederbörlig respekt för rättigheter och intressen i fråga om dataskydd i detta sammanhang.

Slutligen välkomnar arbetsgruppen också all typ av feedback från berörda parter och tillsynsmyndigheter om deras praktiska erfarenheter av vägledningen i detta yttrande, gärna med fler exempel utöver de som nämns i det här dokumentet. Den planerar att se över frågan längre fram i syfte att ytterligare öka den allmänna förståelsen av nyckelbegreppet personuppgifter, och säkerställa en harmoniserad tillämpning och ett bättre genomförande av direktiv 95/46/EG och relaterad gemenskapslagstiftning som bygger på detta.

På arbetsgruppens vägnar

Ordförande
Peter Schaar