ISSN 1725-2504

Europeiska unionens officiella tidning

C 128

Svensk utgåva

femtioandra årgången

6 juni 2009

Meddelanden och upplysningar

Informationsnummer — Innehållsförteckning — Sida

SV

(forts. på nästa sida)

IV *Upplysningar*

UPPLYSNINGAR FRÅN EUROPEISKA UNIONENS INSTITUTIONER OCH ORGAN

Kommissionen

Rättelser

SV

I

(Resolutioner, rekommendationer och yttranden)

YTTRANDEN

EUROPEISKA DATATILLSYNSMANNEN

Yttrande från Europeiska datatillsynsmannen om slutrapporten från EU–USA-kontaktgruppen på hög nivå för informationsutbyte, integritetsskydd och skydd av personuppgifter

(2009/C 128/01)

EUROPEISKA DATATILLSYNSMANNEN HAR ANTAGIT DETTA YTTRANDE

med beaktande av fördraget om upprättandet av Europeiska gemenskapen, särskilt artikel 286,

med beaktande av Europeiska unionens stadga om de grundläggande rättigheterna, särskilt artikel 8,

med beaktande av Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter,

med beaktande av Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter, särskilt artikel 41.

HÄRIGENOM FRAMFÖRS FÖLJANDE.

I. INLEDNING – BAKGRUND TILL YTTRANDET

1. Inför EU-toppmötet den 12 juni 2008 meddelade ordförandeskapet för Europeiska unionens råd den 28 maj 2008 Coreper att EU–USA-kontaktgruppen på hög nivå (nedan kallad *kontaktgruppen*) för informationsutbyte, integritetsskydd och skydd av personuppgifter hade färdigställt sin rapport. Rapporten offentliggjordes den 26 juni 2008. [1]

2. Rapporten syftar till att fastställa gemensamma principer för integritetsskydd och uppgiftsskydd som ett första steg mot informationsutbyte med Förenta staterna för att bekämpa terrorism och allvarlig gränsöverskridande brottslighet.

3. I meddelandet förklarar rådets ordförandeskap att det välkomnar alla synpunkter som rör uppföljningen av rapporten, särskilt reaktioner på de rekommendationer för det fortsatta arbetet som anges i rapporten. Europeiska datatillsynsmannen svarar på denna uppmaning genom att avge följande yttrande som bygger på den lägesbeskrivning som offentliggjorts och som inte föregriper någon ståndpunkt som han eventuellt kommer att inta senare när det gäller frågans utveckling.

4. Datatillsynsmannen noterar att kontaktgruppen har utfört sitt arbete mot bakgrund av att utbytet av uppgifter mellan USA och EU har förändrats, särskilt sedan den 11 september 2001, genom internationella avtal eller andra typer av instrument. Bland dessa finns Europols och Eurojusts avtal med Förenta staterna samt PNR-avtalet och Swift-fallet som ledde till en skriftväxling mellan tjänstemän i EU och USA för att fastställa minimigarantier för uppgiftsskydd [2].

[1] Rådets dokument 9831/08 finns tillgängligt på http://ec.europa.eu/justice_home/fsj/privacy/news/index_en.htm.

[2] — Avtal mellan Amerikas förenta stater och Europeiska polisbyrån av den 6 december 2001 samt tilläggsavtal mellan Europol och USA om utbyte av personuppgifter och relaterade upplysningar, offentliggjorda på Europols webbplats.
— Avtal mellan Amerikas förenta stater och Eurojust om rättsligt samarbete av den 6 november 2006, offentliggjort på Eurojusts webbplats.
— Avtal mellan Europeiska unionen och Amerikas förenta stater om lufttrafikföretags behandling av passageraruppgifter (PNR) och överföring av dessa till Förenta staternas Department of Homeland Security (DHS) (2007 års PNR-avtal), undertecknat i Bryssel den 23 juli 2007 och i Washington den 26 juli 2007, EUT L 204, 4.8.2007, s. 18.
— Skriftväxling mellan myndigheter i USA och EU om programmet för att spåra finansiering av terrorism, den 28 juni 2007.

5. Dessutom förhandlar EU också om och godkänner liknande instrument för utbyte av personuppgifter med andra tredjeländer. Ett exempel nyligen är avtalet mellan Europeiska unionen och Australien om lufttrafikföretags behandling av passageraruppgifter (PNR) från Europeiska unionen och överföring av dessa till Australiens tullmyndighet ([3]).

6. Det framgår i detta sammanhang att framställningar om personuppgifter från brottsbekämpande myndigheter i tredjeländer ständigt ökar, och att de också utvidgats från traditionella statliga databaser till andra typer av register, särskilt dataregister i den privata sektorn.

7. Som en viktig bakgrundsfaktor erinrar datatillsynsmannen också om att frågan om överföring av personuppgifter till tredjeländer inom ramen för polissamarbete och straffrättsligt samarbete omfattas av rådets rambeslut om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete ([4]), vilket sannolikt kommer att antas före utgången av 2008.

8. Det transatlantiska informationsutbytet kan endast förväntas öka och beröra ytterligare sektorer där personuppgifter behandlas. I detta sammanhang är en dialog om ”transatlantisk brottsbekämpning” välkommen men samtidigt känslig. Den är välkommen i den meningen att den kan ge en tydligare ram för det uppgiftsutbyte som äger rum eller som kommer att äga rum. Den är också känslig, eftersom en sådan ram kan legitimera omfattande överföringar av uppgifter på ett område, brottsbekämpning, där konsekvenserna för enskilda personer är särskilt allvarliga och där det är särskilt nödvändigt med strikta och tillförlitliga säkerhetsåtgärder och garantier. ([5])

9. Det följande kapitlet i detta yttrande behandlar det nuvarande läget och det tänkbara framtida arbetet. Kapitel III inriktas på omfattningen och arten av ett instrument som möjliggör informationsutbyte. I kapitel IV i yttrandet analyseras ur ett allmänt perspektiv de rättsliga frågor som har anknytning till innehållet i ett eventuellt avtal. Det behandlar frågor som villkoren för bedömning av den skyddsnivå som erbjuds i Förenta staterna och diskuterar frågan om användningen av EU:s regelverk som riktmärke för att bedöma denna skyddsnivå. I det kapitlet förtecknas också de grundläggande krav som ska ingå i ett sådant avtal. Slutligen innehåller kapitel V i yttrandet en analys av de principer för integritetsskydd som bifogas rapporten.

II. DET NUVARANDE LÄGET OCH DET TÄNKBARA FRAMTIDA ARBETET

10. Datatillsynsmannen bedömer det nuvarande läget på följande sätt. Vissa framsteg har gjorts för att fastställa gemensamma standarder för informationsutbyte, integritetsskydd och skydd av personuppgifter.

11. Förberedelsearbetet för någon typ av avtal mellan EU och USA har emellertid ännu inte slutförts. Det behövs ytterligare arbete. I kontaktgruppens rapport nämns också flera kvarstående frågor, varav frågan om ”möjlighet till rättslig prövning” är den mest framträdande. Det råder fortfarande oenighet om vilken omfattning som krävs för möjligheten till rättslig prövning ([6]). Fem andra kvarstående frågor fastställs i kapitel 3 i rapporten. Det framgår dessutom av detta yttrande att många andra frågor ännu inte har lösts, till exempel omfattningen och arten av ett instrument om informationsutbyte.

12. Eftersom det alternativ som förordas i rapporten är ett bindande avtal, vilket också datatillsynsmannen föredrar, är det särskilt nödvändigt med försiktighet. Ytterligare noggranna och ingående förberedelser behövs innan ett avtal kan uppnås.

13. Enligt datatillsynsmannen skulle det slutligen vara bäst att ett avtal ingås enligt Lissabonfördraget, givetvis under förutsättning att detta träder i kraft. Enligt Lissabonfördraget skulle det nämligen inte råda någon rättslig osäkerhet om avgränsningen mellan EU:s olika pelare. Dessutom skulle det garanteras att Europaparlamentet deltar fullt ut samt att domstolen utövar rättslig kontroll.

14. Under dessa förhållanden skulle det framtida arbetet bäst kunna bestå i utarbetandet av en färdplan mot ett eventuellt senare avtal. En sådan färdplan kan innehålla följande delar:

— Riktlinjer för det fortsatta arbetet i kontaktgruppen (eller någon annan grupp) samt en tidsplan.

— I ett tidigt skede, diskussion och eventuell överenskommelse om grundläggande frågor, till exempel avtalets omfattning och art.

— På grundval av en gemensam uppfattning av dessa grundläggande frågor, vidareutveckling av principerna för uppgiftsskydd.

— De berörda parternas medverkan i olika skeden i förfarandet.

— På den europeiska sidan, behandling av de institutionella begränsningarna.

([3]) EUT L 213, 8.8.2008, s. 49.

([4]) Rådets rambeslut om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete, versionen av den 24 juni 2008 är tillgänglig på http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=sv&DosId=193371.

([5]) När det gäller behovet av en tydlig rättslig ram, se kapitlen III och IV i detta yttrande.

([6]) Sidan 5 i rapporten, avsnitt C.

III. **OMFATTNINGEN OCH ARTEN AV ETT INSTRUMENT OM INFORMATIONSUTBYTE**

15. Datatillsynsmannen anser att det är av avgörande betydelse att omfattningen och arten av ett eventuellt instrument, inklusive principer för uppgiftsskydd, fastställs tydligt, som ett första steg i vidareutvecklingen av ett sådant instrument.

16. När det gäller omfattningen är det viktigt att följande frågor besvaras:

— Vilka aktörer som berörs, inom och utanför brottsbekämpningsområdet.

— Vad som avses med ”brottsbekämpningssyfte” och dess förhållande till andra syften som nationell säkerhet, och mer specifikt gränskontroll och folkhälsa.

— Hur instrumentet passar in i ett övergripande transatlantiskt säkerhetsområde.

17. När det gäller fastställandet av arten bör följande frågor klargöras:

— Om det är tillämpligt, inom vilken pelare förhandlingarna om instrumentet ska föras.

— Huruvida instrumentet ska vara bindande för EU och USA.

— Huruvida det ska få direkt effekt i den meningen att det innehåller rättigheter och skyldigheter för enskilda personer vilka kan göras gällande inför en rättslig myndighet.

— Huruvida instrumentet i sig ska möjliggöra informationsutbyte eller om det ska fastställa minimistandarder för informationsutbyte, vilka ska kompletteras genom särskilda avtal.

— Instrumentets förhållande till befintliga instrument, huruvida det ska respektera, ersätta eller komplettera dem.

III.1 **Instrumentets omfattning**

Berörda aktörer

18. Även om den exakta omfattningen av det framtida instrumentet inte anges klart i kontaktgruppens rapport kan man av de principer som nämns i den dra slutsatsen att avsikten är att det ska omfatta överföringar såväl mellan privata och offentliga aktörer ([7]) som mellan offentliga myndigheter.

— Mellan privata och offentliga aktörer

19. Datatillsynsmannen anser att det är logiskt att ett framtida instrument ska vara tillämpligt på överföringar mellan privata och offentliga aktörer. Ett sådant instrument utarbetas mot bakgrund av USA:s framställningar om information från privata parter under de senaste åren. Datatillsynsmannen noterar att privata aktörer håller på att bli en systematisk informationskälla i brottsbekämpningssammanhang, såväl på EU-nivå som på internationell nivå ([8]). Swift-fallet är ett viktigt tidigare exempel där ett privat företag anmodades att systematiskt överföra stora mängder uppgifter till brottsbekämpande myndigheter i en tredjestat ([9]). Insamlingen av PNR-uppgifter från flygbolag följer samma logik. Redan i sitt yttrande om utkastet till rambeslut om ett europeiskt PNR-system ifrågasatte datatillsynsmannen lagenligheten av denna tendens ([10]).

20. Det finns ytterligare två skäl till att hysa betänkligheter mot att överföringar mellan privata och offentliga aktörer införs i tillämpningsområdet för ett framtida instrument.

21. För det första kan införandet få en oönskad effekt inom EU:s eget territorium. Om uppgifter från privata företag (till exempel finansinstitut) i princip kan överföras till tredjeländer, hyser datatillsynsmannen allvarliga farhågor om att detta kan ge upphov till starka påtryckningar för att samma typ av uppgifter ska bli tillgängliga för de brottsbekämpande myndigheterna också inom EU. PNR-systemet är ett exempel på en sådan oönskad utveckling som startade med USA:s insamling av stora mängder passageraruppgifter och därefter överfördes också till ett internt europeiskt sammanhang ([11]), utan att systemets nödvändighet och rimlighet visats på ett tydligt sätt.

22. För det andra tar datatillsynsmannen i sitt yttrande om kommissionens förslag till EU:s PNR-system också

([7]) Se särskilt kapitel 3 i rapporten, ”Kvarstående frågor rörande transatlantiska förbindelser”, punkt 1: ”Enhetlighet i privata enheters skyldigheter i samband med överföring av uppgifter”.

([8]) När det gäller denna fråga, se yttrandet från Europeiska datatillsynsmannen av den 20 december 2007 om förslaget till rådets rambeslut om användande av passageraruppgifter (PNR-uppgifter) i brottsbekämpningssyfte, EUT C 110, 1.5.2008, s. 1. ”Av tradition har det funnits en tydlig åtskillnad mellan brottsbekämpning och verksamhet inom den privata sektorn, varvid brottsbekämpningsuppgifter har utförts av särskilt avdelade myndigheter, särskilt polisen, medan privata aktörer från fall till fall anmodas överföra personuppgifter till dessa brottsbekämpande myndigheter. Det finns nu en tendens att systematiskt kräva samarbete av privata aktörer i brottsbekämpningssyfte.”

([9]) Se yttrande 10/2006 av den 22 november 2006 från arbetsgruppen för skydd av enskilda med avseende på behandlingen av personuppgifter (artikel 29-gruppen) om behandling av personuppgifter av Society for Worldwide Interbank Financial Telecommunication (Swift), WP 128.

([10]) Yttrande av den 20 december 2007, op.cit.

([11]) Se förslaget till rådets rambeslut om användande av passageraruppgifter (PNR-uppgifter) i brottsbekämpningssyfte, se fotnot 8, som för närvarande diskuteras i rådet.

upp frågan om vilket regelverk för uppgiftsskydd (den första eller den tredje pelaren) som är tillämpligt på villkoren för samarbetet mellan offentliga och privata aktörer: Bör reglerna bygga på kategorin av registeransvarig (privat sektor) eller på det eftersträvade målet (brottsbekämpning)? Avgränsningen mellan den första och den tredje pelaren är långt ifrån tydlig i situationer där privata aktörer åläggs skyldigheter att behandla personuppgifter för brottsbekämpningssyften. I detta sammanhang är det signifikativt att generaladvokat Bot nyligen i sitt förslag till avgörande i målet om lagring av uppgifter ([12]) föreslår en avgränsning för dessa situationer, men gör följande tillägg: ”Visserligen kan denna avgränsning kritiseras och i vissa avseenden förefalla konstgjord.” Datatillsynsmannen konstaterar också att domstolen i sin dom i PNR-målet ([13]) inte fullständigt besvarar frågan om det tillämpliga regelverket. Det faktum att vissa verksamheter inte omfattas av direktiv 95/46/EG innebär till exempel inte automatiskt att dessa verksamheter kan regleras inom den tredje pelaren. Detta kan därför lämna ett kryphål när det gäller tillämplig lag och leder under alla omständigheter till rättslig osäkerhet när det gäller de rättsliga garantier som de registrerade personerna omfattas av.

23. Mot bakgrund av detta betonar datatillsynsmannen att det måste säkerställas att ett framtida instrument med allmänna principer för uppgiftsskydd inte kan legitimera den transatlantiska överföringen av personuppgifter mellan privata och offentliga parter som sådan. Denna överföring kan endast införas i ett framtida instrument under förutsättning att

— det fastställs i det framtida instrument att överföringen endast är tillåten om den har visats vara absolut nödvändig för ett specifikt syfte, vilket ska beslutas från fall till fall,

— själva överföringen omfattas av strikta garantier för uppgiftsskydd (vilka beskrivs i detta yttrande).

Datatillsynsmannen konstaterar dessutom att det råder osäkerhet om vilket regelverk som ska tillämpas på uppgiftsskydd och vädjar därför under alla omständigheter om att överföringen av personuppgifter mellan privata och offentliga parter inte ska införas enligt den nu gällande EU-lagstiftningen.

— Mellan offentliga myndigheter

24. Den exakta omfattningen av informationsutbytet är oklar. Som ett första steg i det framtida arbetet mot ett gemensamt instrument bör den planerade omfattningen av ett sådant instrument klargöras. I synnerhet följande frågor kvarstår:

— När det gäller databaser i EU, huruvida instrumentet ska omfatta centraliserade databaser som (delvis) förvaltas av EU, till exempel Europols och Eurojusts databaser, eller decentraliserade databaser som förvaltas av medlemsstaterna, eller båda.

— Huruvida instrumentet också ska omfatta sammanlänkade nät, dvs. huruvida de planerade garantierna ska omfatta uppgifter som utbyts mellan medlemsstater eller myndigheter, såväl i EU som i USA.

— Huruvida instrumentet endast ska omfatta utbyte mellan databaser på brottsbekämpningsområdet (polis, rättsväsende, eventuellt tullen) eller också andra databaser som skattedatabaser.

— Huruvida instrumentet också ska gälla nationella säkerhetsorgans databaser eller ge dessa organ tillgång till databaser för brottsbekämpning på den andra avtalsslutande partens territorium (EU till USA och omvänt).

— Huruvida instrumentet ska omfatta överföring av information från fall till fall eller ständig tillgång till befintliga databaser. Det sistnämnda alternativet skulle givetvis väcka frågor om proportionalitet, vilka diskuteras närmare i kapitel V punkt 3.

Brottsbekämpningssyfte

25. Fastställandet av syftet med ett eventuellt avtal ger också utrymme för osäkerhet. Brottsbekämpningssyften anges klart såväl i inledningen som i den första principen som bifogas rapporten, och kommer att analyseras närmare i kapitel IV i detta yttrande. Datatillsynsmannen noterar redan att det av dessa förklaringar framgår att utbytet av uppgifter ska inriktas på frågor inom den tredje pelaren, men man kan fråga sig om detta endast är ett första steg mot ett mer omfattande informationsutbyte. Det förefaller klart att de syften avseende ”allmän säkerhet” som anges i rapporten omfattar kampen mot terrorism, organiserad brottslighet och andra typer av brott. Är avsikten emellertid att utbyte av uppgifter också ska vara möjligt för andra allmänintressen, exempelvis risker för folkhälsan?

26. Datatillsynsmannen rekommenderar att syftet ska begränsas till exakt identifierad behandling av uppgifter och att de policyval som leder till detta fastställande av syftet ska motiveras.

([12]) Generaladvokat Bots förslag till avgörande av den 14 oktober 2008, Irland mot Europaparlamentet och rådet (mål C-301/06), punkt 108.

([13]) Domstolens dom av den 30 maj 2006, Europaparlamentet mot Europeiska unionens råd (mål C-317/04) och Europeiska gemenskapernas kommission (mål C-318/04, förenade målen C-317/04 och C-318/04, REG 2006, s. I-4721).

Ett övergripande transatlantiskt säkerhetsområde

27. Rapportens breda räckvidd bör sättas i förhållande till det övergripande transatlantiska säkerhetsområde som diskuteras av den s.k. framtidsgruppen ([14]). Rapporten från denna grupp, som lämnades i juni 2008, inriktas i viss utsträckning på den yttre dimensionen i politiken för inrikes frågor. I rapporten förespråkas följande: *"Senast 2014 bör Europeiska unionen fatta beslut om det politiska målet att förverkliga ett Euroatlantiskt samarbetsområde när det gäller frihet, säkerhet och rättvisa med Förenta staterna."* Ett sådant samarbete skulle gå utöver säkerhet i strikt mening och åtminstone omfatta de frågor som behandlas i nuvarande avdelning IV i EG-fördraget, till exempel invandring, visering och asyl samt civilrättsligt samarbete. Det måste ifrågasättas i vilken utsträckning ett avtal om grundläggande principer för uppgiftsskydd, som de principer som nämns i kontaktgruppens rapport, kan och bör ligga till grund för ett informationsutbyte på ett så brett område.

28. Normalt kommer pelarstrukturen att ha upphört att existera 2014 och det kommer att finnas en enda rättslig grund för uppgiftsskydd inom själva EU (enligt Lissabonfördraget, artikel 16 i fördraget om Europeiska unionens funktionssätt). Det faktum att *lagstiftningen* om uppgiftsskydd är harmoniserad på EU-nivå innebär dock inte att *överföringen* av personuppgifter kan tillåtas enligt ett avtal med ett tredjeland, oavsett syfte. Beroende på sammanhanget och villkoren för behandling kan det krävas anpassade garantier för uppgiftsskydd för särskilda områden, till exempel brottsbekämpning. Datatillsynsmannen rekommenderar att konsekvenserna av dessa olika perspektiv ska beaktas i samband med utarbetandet av ett framtida avtal.

III.2 **Avtalets art**

Den europeiska institutionella ramen

29. Åtminstone på kort sikt är det väsentligt att avgöra inom vilken pelare förhandlingarna om avtalet ska föras. Detta är nödvändigt särskilt på grund av det interna regelverket för uppgiftsskydd som kommer att påverkas av ett sådant avtal. Ska förhandlingarna föras inom ramen för den första pelaren, huvudsakligen direktiv 95/46/EG med sitt specifika system för överföring av uppgifter till tredjeländer, eller inom ramen för den tredje pelaren med ett mindre strikt system för överföringar till tredjeländer? ([15])

30. Som redan sagts överväger brottsbekämpningssyftena, men i kontaktgruppens rapport nämns ändå insamling av uppgifter från privata aktörer, och syftena kan också tolkas så brett att de går utöver ren säkerhet, inklusive till exempel invandrings- och gränskontrollfrågor, men också eventuellt folkhälsa. Med hänsyn till denna osäkerhet skulle det i hög grad vara att föredra att invänta harmoniseringen av pelarna enligt EU-lagstiftningen, vilket föreskrivs i Lissabonfördraget, för att klart fastställa den rättsliga grunden för förhandlingarna och den exakta rollen för de europeiska institutionerna, särskilt Europaparlamentet och kommissionen.

Instrumentets bindande karaktär

31. Det bör klargöras om de avslutade diskussionerna ska leda till ett samförståndsavtal eller något annat icke bindande instrument eller till ett bindande internationellt avtal.

32. Datatillsynsmannen stöder rapportens preferens för ett bindande avtal. Datatillsynsmannen anser att ett officiellt bindande avtal är en nödvändig förutsättning för all överföring av uppgifter utanför EU, oavsett för vilket syfte uppgifterna överförs. Ingen överföring av uppgifter till ett tredjeland kan ske utan adekvata villkor och garantier som ingår i ett specifikt (och bindande) regelverk. Ett samförståndsavtal eller något annat icke bindande instrument kan med andra ord vara användbart för att ge riktlinjer för förhandlingar om ytterligare bindande avtal, men kan aldrig ersätta behovet av ett bindande avtal.

Direkt effekt

33. Bestämmelserna i instrumentet bör vara bindande såväl för USA som för EU och dess medlemsstater.

34. Det bör dessutom säkerställas att enskilda personer får utöva sina rättigheter, och särskilt få möjlighet till rättslig prövning, på grundval av överenskomna principer. Datatillsynsmannen anser att detta resultat bäst kan uppnås om de materiella bestämmelserna i instrumentet utformas så att de har direkt effekt gentemot invånarna i Europeiska unionen och kan åberopas inför en domstol. Den direkta effekten av bestämmelserna i det internationella avtalet, samt villkoren för införlivandet i intern europeisk och nationell lagstiftning för att säkerställa bestämmelsernas verkningsfullhet, måste därför klargöras i instrumentet.

Förhållandet till andra instrument

35. Det är också en grundläggande fråga i vilken utsträckning avtalet står ensamt eller om det från fall till fall måste kompletteras med ytterligare avtal om specifika utbyten av uppgifter. Det kan verkligen ifrågasättas om ett enda avtal, med en enda uppsättning standarder, på ett tillfredsställande sätt kan täcka mångfalden av särdrag när det gäller behandlingen av uppgifter inom den tredje pelaren.

([14]) Rapport från den informella rådgivande högnivågruppen avseende framtiden för den europeiska politiken för inrikes frågor, "Frihet, säkerhet och personlig integritet – europeiska inrikes frågor i en öppen värld", juni 2008, tillgänglig på register.consilium.europa.eu.

([15]) Se artiklarna 11 och 13 i det rambeslut som nämns i punkt 7 i detta yttrande.

Det är ändå mera tveksamt om det kan *tillåta*, utan ytterligare diskussioner och garantier, ett allmänt godkännande av alla överföringar av uppgifter, oavsett de berörda uppgifternas syfte och art. Dessutom är avtal med tredjeländer inte nödvändigtvis permanenta, eftersom de kan kopplas till specifika hot, bli föremål för översyn eller omfattas av klausuler om automatiskt upphörande. Å andra sidan kan gemensamma minimistandarder som erkänns i ett bindande avtal underlätta eventuella senare diskussioner om överföring av personuppgifter i förhållande till en specifik databas eller uppgiftsbehandling.

36. Datatillsynsmannen vill därför förespråka att en miniuppsättning kriterier för uppgiftsskydd utarbetas vilka från fall till fall kompletteras med specifika tilläggsbestämmelser, så som nämns i kontaktgruppens rapport, i stället för alternativet med ett enda avtal. Dessa specifika tilläggsbestämmelser är en förutsättning för att överföringen av uppgifter ska vara tillåten i ett specifikt fall. Detta skulle främja en harmoniserad strategi för uppgiftsskydd.

Tillämpning på befintliga instrument

37. Det bör också undersökas hur ett eventuellt allmänt avtal skulle samverka med redan befintliga avtal som ingåtts mellan EU och USA. Det bör noteras att dessa befintliga avtal inte har samma bindande karaktär; särskilt bör nämnas PNR-avtalet (det avtal som erbjuder störst rättslig säkerhet), Europol- och Eurojustavtalen samt Swift-skriftväxlingen ([16]). Kommer ett nytt allmänt regelverk att komplettera dessa befintliga instrument eller kommer de att förbli opåverkade och det nya regelverket endast vara tillämpligt på andra framtida utbyten av personuppgifter? Datatillsynsmannen anser att det för rättslig enhetlighet krävs en harmoniserad uppsättning bestämmelser som är tillämpliga på och kompletterar både befintliga och framtida bindande avtal om överföring av uppgifter.

38. Tillämpningen av det allmänna avtalet på befintliga instrument skulle medföra fördelen att den stärker deras bindande karaktär. Detta skulle vara särskilt välkommet när det gäller instrument som inte är rättsligt bindande, till exempel Swift-skriftväxlingen, eftersom det åtminstone skulle föreskrivas att en uppsättning allmänna principer för integritetsskydd ska följas.

IV. **ALLMÄN RÄTTSLIG BEDÖMNING**

39. I detta kapitel kommer det att diskuteras hur skyddsnivån inom ett specifikt regelverk eller i ett specifikt instrument ska bedömas, inklusive frågan om vilka riktmärken som ska användas och de nödvändiga grundläggande kraven.

([16]) Se fotnot 2.

Adekvat skyddsnivå

40. Datatillsynsmannen anser att det bör stå klart att ett av de viktigaste resultaten av ett framtida instrument ska vara att överföring av personuppgifter till Förenta staterna endast får ske om myndigheterna i Förenta staterna garanterar en adekvat skyddsnivå (och vice versa).

41. Datatillsynsmannen anser att endast en verklig prövning av att skyddsnivån är adekvat skulle säkerställa tillräckliga garantier när det gäller skyddsnivån för personuppgifter. Han anser att ett allmänt ramavtal med en så bred räckvidd som i kontaktgruppens rapport skulle ha svårt att som sådant klara en verklig prövning av att skyddsnivån är adekvat. Det allmänna avtalet kan endast erkännas ha en adekvat skyddsnivå om det kombineras med en adekvat skyddsnivå i särskilda avtal som ingås från fall till fall.

42. Det är inte ovanligt att den skyddsnivå som erbjuds av tredjeländer bedöms, särskilt av Europeiska kommissionen: inom den första pelaren är adekvat skyddsnivå ett krav för överföring. Den har mätts vid flera tillfällen enligt artikel 25 i direktiv 95/46/EG på grundval av specifika kriterier och bekräftats genom beslut av Europeiska kommissionen ([17]). Inom den tredje pelaren fastställs inte uttryckligen något sådant system: mätning av adekvat skyddsnivå föreskrivs endast i den specifika situation som behandlas i artiklarna 11 och 13 i det ännu inte antagna ramdirektivet om uppgiftsskydd ([18]) och överlåts till medlemsstaterna.

43. I det aktuella fallet omfattar bedömningen brottsbekämpningssyften och diskussionerna förs av kommissionen under rådets överinseende. Sammanhanget skiljer sig från bedömningen av principerna om integritetsskydd (Safe Harbour Principles) eller bedömningen av om den kanadensiska lagstiftningen föreskriver en adekvat skyddsnivå, och har ett närmare samband med de PNR-förhandlingar som nyligen fördes med USA och Australien, vilka ägde rum inom den tredje pelarens regelverk. Kontaktgruppens principer har emellertid också nämnts i samband med programmet för viseringsundantag som gäller gränser och invandring och därmed frågor inom den första pelaren.

44. Datatillsynsmannen rekommenderar att alla konstateranden av adekvat skyddsnivå enligt ett framtida instrument bör bygga på erfarenheterna inom dessa olika områden.

([17]) Kommissionens beslut om adekvat skydd för personuppgifter i tredjeländer, bland annat Argentina, Kanada, Schweiz, Förenta staterna, Guernsey, Isle of Man och Jersey, finns tillgängliga på http://ec.europa.eu/justice_home/fsj/privacy/thirdcountries/index_sv.htm.

([18]) Begränsat till en medlemsstats överföring till ett tredjeland eller ett internationellt organ av uppgifter som erhållits från en behörig myndighet i en annan medlemsstat.

Han rekommenderar en vidareutveckling av begreppet ”adekvat skyddsnivå” i samband med ett framtida instrument, på grundval av liknande kriterier som de som använts i tidigare bedömningar av adekvat skyddsnivå.

Ömsesidigt erkännande – ömsesidighet

45. Ett andra inslag i skyddsnivån gäller det ömsesidiga erkännandet av EU:s och USA:s system. I kontaktgruppens rapport nämns i detta sammanhang att målet kommer att vara att ”erhålla erkännande att motpartens system för integritets- och uppgiftsskydd är verkningsfullt på de områden som omfattas av dessa principer” ([19]) och att uppnå ”likvärdig och ömsesidig tillämpning av lagstiftningen om integritetsskydd och skydd av personuppgifter”.

46. För datatillsynsmannen är det uppenbart att ömsesidigt erkännande (eller ömsesidighet) endast är möjligt om en adekvat skyddsnivå garanteras. Med andra ord bör det framtida instrumentet harmonisera en minimiskyddsnivå (genom ett konstaterande av adekvat skyddsnivå, med beaktande av behovet av särskilda avtal från fall till fall). Endast under denna förutsättning kan ömsesidighet erkännas.

47. Den första faktorn som ska beaktas är ömsesidigheten i materiella bestämmelser om uppgiftsskydd. Datatillsynsmannen anser att ett avtal bör behandla begreppet ömsesidighet i materiella bestämmelser om uppgiftsskydd på ett sätt som säkerställer dels att behandling av uppgifter inom EU:s (och USA:s) territorium fullt ut följer de inhemska lagarna om uppgiftsskydd, dels att sådan behandling utanför det land varifrån uppgifter kommer vilken omfattas av avtalet följer de principer om uppgiftsskydd som fastställs i avtalet.

48. Den andra faktorn är ömsesidighet när det gäller systemen för tillgång till rättslig prövning. Det bör säkerställas att europeiska medborgare har tillfredsställande möjligheter till rättslig prövning när uppgifter som rör dem behandlas i Förenta staterna (oberoende av den lag som är tillämplig på den behandlingen), men också att Europeiska unionen och dess medlemsstater ger likvärdiga rättigheter till USA-medborgare.

49. Den tredje faktorn är ömsesidighet när det gäller de brottsbekämpande myndigheternas tillgång till personuppgifter. Om något instrument tillåter myndigheterna i Förenta staterna att få tillgång till uppgifter från Europeiska unionen skulle ömsesidigheten medföra att myndigheterna i EU ges samma tillgång när det gäller uppgifter från USA. Ömsesidigheten får inte skada ett verkningsfullt skydd av de registrerade personerna. Detta är en nödvändig förutsättning för att de brottsbekämpande myndigheterna ska tillåtas få ”transatlantisk” tillgång. Detta innebär konkret följande:

— Direkt tillgång för myndigheter i Förenta staterna till uppgifter inom EU:s territorium (och vice versa) bör inte tillåtas. Tillgång bör endast ges indirekt enligt ett ”pushsystem”.

— Denna tillgång bör ske under kontroll av datatskyddsmyndigheterna och de rättsliga myndigheterna i det land där uppgifterna behandlas.

— Tillgång för myndigheterna i Förenta staterna till databaser inom EU bör följa de materiella bestämmelserna om uppgiftsskydd (se ovan) och garantera fullständiga möjligheter till rättslig prövning för de registrerade personerna.

Instrumentets exakthet

50. Specificeringen av villkoren för bedömningen (adekvat skyddsnivå, likvärdighet, ömsesidigt erkännande) är viktig eftersom den bestämmer innehållet, när det gäller exakthet, rättslig säkerhet och skyddets verkningsfullhet. Innehållet i ett framtida instrument måste vara exakt och noggrant.

51. Dessutom bör det stå klart att alla särskilda avtal som ingås i ett senare skede fortfarande måste innehålla detaljerade och fullständiga garantier för uppgiftsskydd i förhållande till de registrerade personer som berörs av det planerade uppgiftsutbytet. Endast en sådan dubbel nivå av konkreta principer för uppgiftsskydd kommer att säkerställa den nödvändiga ”nära anpassningen” mellan det allmänna avtalet och särskilda avtal, vilket redan noteras i punkterna 35 och 36 i detta yttrande.

Utarbetande av en modell för andra tredjeländer

52. Det förtjänar att särskilt uppmärksammas i vilken utsträckning ett avtal med USA kan stå som modell för andra tredjeländer. Datatillsynsmannen noterar att i den ovannämnda rapporten från framtidsgruppen anges utöver USA också Ryssland som en strategisk partner för EU. I den mån principerna är neutrala och överensstämmer med grundläggande EU-garantier kan de utgöra ett användbart prejudikat. Särskilda egenskaper som är knutna till exempelvis mottagarlandets regelverk eller syftet med överföringen kommer dock att hindra en ren överföring av avtalet. Lika avgörande kommer den demokratiska situationen i tredjeländerna att vara: det bör säkerställas att de överenskomna principerna kommer att garanteras och genomföras på ett verkningsfullt sätt i mottagarlandet.

Vilka riktmärken ska användas för att bedöma skyddsnivån?

53. En underförstådd eller uttrycklig adekvat skyddsnivå bör under alla omständigheter överensstämma med det internationella och europeiska regelverket och särskilt de gemensamt överenskomna garantierna för uppgiftsskydd.

([19]) Kapitel A, Bindande internationella avtal, s. 8.

Dessa fastställs i Förenta nationernas riktlinjer, Europarådets konvention 108 och tilläggsprotokollet till denna, OECD-riktlinjerna och utkastet till rambeslut om uppgiftsskydd samt, när det gäller aspekter inom den första pelaren, direktiv 95/46/EG ([20]). Alla dessa instrument innehåller likartade principer som är mer allmänt erkända som kärnan i skyddet för personuppgifter.

54. Med hänsyn till effekterna av ett potentiellt avtal som det som avses i kontaktgruppens rapport är det särskilt viktigt att de ovannämnda principerna beaktas. Ett instrument som omfattar hela den *brottsbekämpande* sektorn i ett tredjeland skulle verkligen vara en situation som saknar motstycke. Befintliga beslut om adekvat skyddsnivå inom den första pelaren och avtal som ingåtts med tredjeländer inom EU:s tredje pelare (Europol, Eurojust) har alltid varit knutna till en specifik överföring av uppgifter, medan överföring av mycket bredare omfattning kan bli möjlig här, med hänsyn till det breda syftet (brottsbekämpning, nationell och allmän säkerhet, hävdande av gränser) och det okända antal databaser som berörs.

Grundläggande krav

55. De villkor som ska uppfyllas i samband med överföring av personuppgifter till tredjeländer har utformats i ett arbetsdokument från arbetsgruppen för skydd av enskilda med avseende på behandlingen av personuppgifter ([21]). Alla avtal om minimiprinciper för integritetsskydd bör klara en prövning för att säkerställa överensstämmelsen med verkningsfulla garantier för uppgiftsskydd.

— Avseende sakinnehåll: Principerna för uppgiftsskydd bör medge en hög skyddsnivå och uppfylla standarder som överensstämmer med EU:s principer. De tolv principerna i kontaktgruppens rapport kommer att analyseras mer ingående ur denna synvinkel i kapitel V i detta yttrande.

— Avseende exakthet: Beroende på avtalets karaktär, och särskilt om det utgör ett officiellt internationellt avtal, bör bestämmelserna och förfarandena vara så detaljerade att en verkningsfull tillämpning blir möjlig.

— Avseende tillsyn: För att säkerställa att de överenskomna bestämmelserna följs bör särskilda kontrollmekanismer införas, både internt (revisioner) och externt (översyner). Båda parter i avtalet måste få lika tillgång till dessa mekanismer. Tillsyn omfattar mekanismer för att säkerställa efterlevnad på makronivå, till exempel gemensamma mekanismer för översyn, och på mikronivå, till exempel individuell möjlighet till rättslig prövning.

56. Utöver dessa tre grundläggande krav bör särskild uppmärksamhet ägnas åt de särdrag som är knutna till behandlingen av personuppgifter i brottsbekämpningssammanhang. Detta är verkligen ett område där de grundläggande rättigheterna kan drabbas av vissa restriktioner. Garantier för att kompensera restriktionerna av de enskilda personernas rättigheter bör därför införas, särskilt med avseende på följande aspekter, med hänsyn till effekterna på de enskilda personerna:

— Öppenhet: Information och tillgång till personuppgifter kan begränsas i ett brottsbekämpningssammanhang, till exempel på grund av att det är nödvändigt med diskreta utredningar. Inom EU har traditionsenligt kompletterande mekanismer införts för att kompensera denna begränsning av de grundläggande rättigheterna (ofta med hjälp av oberoende dataskyddsmyndigheter), men det måste säkerställas att liknande kompensationsmekanismer finns tillgängliga när information har överförts till ett tredjeland.

— Möjlighet till rättslig prövning: Av de ovannämnda skälen bör enskilda personer kunna utnyttja alternativa möjligheter för att försvara sina rättigheter, särskilt genom en oberoende tillsynsmyndighet och inför en domstol.

— Bevarande av uppgifter: Motiveringen till den period under vilken uppgifterna bevaras är eventuellt inte klar och tydlig. Åtgärder måste vidtas så att detta inte hindrar de registrerade personerna eller tillsynsmyndigheterna från att faktiskt utöva sina rättigheter.

([20]) — Förenta nationernas riktlinjer avseende datoriserade personuppgiftsregister, som antogs av generalförsamlingen den 14 december 1990, tillgängliga på www.unhchr.ch/html/menu3/b/71.htm.
— Europarådets konvention om skydd för enskilda vid automatisk databehandling av personuppgifter av den 28 januari 1981, tillgänglig på www.conventions.coe.int/treaty/en/Treaties/html/108.htm.
— OECD:s riktlinjer för integritetsskydd och gränsöverskridande flöden av personuppgifter, som antogs den 23 september 1980, tillgängliga på www.oecd.org/document/20/0,3343.en_2649_34255_15589524_1_1_1_1,00.html.
— Utkast till rådets rambeslut om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete, tillgängligt på http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=sv&DosId=193371.
— Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter, EGT L 281, 23.11.1995, s. 31.

([21]) Arbetsdokument av den 24 juli 1998 om överföring av personuppgifter till tredjeländer: tillämpning av artiklarna 25 och 26 i EU:s direktiv om uppgiftsskydd, WP12.

— De brottsbekämpande myndigheternas redovisningsskyldighet: I avsaknad av faktisk öppenhet kan kontrollmekanismerna inte på något sätt vara heltäckande, vare sig för de enskilda eller de institutionella berörda parterna. Det kommer ändå att vara av avgörande betydelse att sådana kontroller fastställs strikt, med hänsyn till uppgifternas känslighet och de tvångsåtgärder som kan vidtas mot enskilda personer på grundval av behandlingen av uppgifterna. Redovisningsskyldighet är en avgörande fråga i förhållande till nationella kontrollmekanismer i mottagarlandet, men också i förhållande till översynsmöjligheterna för det land eller den region varifrån uppgifter kommer. Sådana översynsmekanismer föreskrivs i särskilda avtal som PNR-avtalet och datatillsynsmannen rekommenderar starkt att de ska införas också i det allmänna instrumentet.

V. **ANALYS AV PRINCIPERNA**

Inledning

57. I detta kapitel analyseras de tolv principerna i kontaktgruppens dokument med utgångspunkt i följande:

— Dessa principer visar att USA:s och EU:s synsätt när det gäller principernas nivå i viss mån sammanfaller, eftersom likheter kan noteras med principerna i konvention 108.

— Enighet om principernas nivå är dock inte tillräckligt. Ett rättsligt instrument måste vara så starkt att efterlevnaden säkerställs.

— Datatillsynsmannen beklagar att principerna inte åtföljs av en motivering.

— Innan beskrivningen av principerna diskuteras bör det klargöras att båda parter har samma tolkning av den formulering som används, till exempel när det gäller begreppen personuppgifter och enskilda personer som skyddas. Det skulle vara välkommet med definitioner i detta avseende.

1. Specificering av syftet

58. I den första principen som förtecknas i bilagan till kontaktgruppens rapport anges att personuppgifter ska behandlas för lagenliga brottsbekämpningssyften. Som nämns ovan gäller detta för Europeiska unionens del förebyggande, upptäckt, utredning eller lagföring av brott. För USA:s del går dock tolkningen av brottsbekämpning utöver straffbara gärningar och omfattar ”hävdande av gränser, allmän säkerhet och nationell säkerhet”. Konsekvenserna av sådana skillnader mellan EU:s och USA:s angivna syften är inte tydliga. I rapporten anges att syftena i stor utsträckning kan sammanfalla i praktiken, men det är avgörande att veta exakt i vilken utsträckning de *inte* sammanfaller. Med tanke på konsekvenserna av de åtgärder som vidtas mot enskilda personer måste principen om begränsning av syftet följas strikt på brottsbekämpningsområdet och de angivna syftena måste vara tydliga och begränsade. Med hänsyn till den ömsesidighet som avses i rapporten förefaller det också vara väsentligt med en tillnärmning av dessa syften. Kort sagt måste tolkningen av denna princip klargöras.

2. Integritetsskydd/uppgiftskvalitet

59. Datatillsynsmannen välkomnar bestämmelsen om att det för lagenlig behandling är nödvändigt med krav på korrekta, relevanta och fullständiga personuppgifter i rätt tid. En sådan princip är ett grundläggande villkor för all effektiv behandling av uppgifter.

3. Nödvändighet/proportionalitet

60. Principen innebär en nära koppling mellan den insamlade informationen och denna informations nödvändighet för att uppfylla ett brottsbekämpningssyfte som fastställs enligt lag. Detta krav på en rättslig grund är en positiv faktor när det gäller att garantera behandlingens lagenlighet. Trots att detta stärker behandlingens rättsliga säkerhet noterar dock datatillsynsmannen att den rättsliga grunden för denna behandling utgörs av en lag i ett tredjeland. En lag i ett tredjeland kan inte i sig utgöra en legitim grund för en överföring av personuppgifter ([22]). I kontaktgruppens rapport förefaller det förutsättas att legitimiteten av lagen i ett tredjeland, till exempel Förenta staterna, i princip erkänns. Det bör hållas i åtanke att om ett sådant resonemang kan vara berättigat här, med hänsyn till att Förenta staterna är en demokratisk stat, skulle samma system inte vara giltigt för och kunna överföras till förbindelserna med något annat tredjeland.

61. Enligt bilagan till kontaktgruppens rapport måste alla överföringar av personuppgifter vara relevanta, nödvändiga och lämpliga. Datatillsynsmannen betonar att om behandlingen ska vara proportionell får den inte vara onödigt inkräktande och förfarandena för behandlingen måste vara väl avvägda, med beaktande av de registrerade personernas rättigheter och intressen.

62. Av detta skäl bör tillgång ges till information från fall till fall, beroende på de praktiska behoven i samband med en specifik utredning. Permanent tillgång för brottsbekämpande myndigheter i ett tredjeland till databaser i EU bör betraktas som oproportionell och otillräckligt motiverad.

([22]) Se särskilt artikel 7 c och e i direktiv 95/46/EG. I sitt yttrande 6/2002 av den 24 oktober 2002 om överföring av passagerarlistor och andra uppgifter från flygbolag till Förenta staterna förklarade arbetsgruppen för skydd av enskilda med avseende på behandlingen av personuppgifter att ”det inte förefaller godtagbart att ett ensidigt beslut som fattats av ett tredjeland av skäl som hänför sig till dess eget allmänintresse ska leda till rutinmässig och omfattande överföring av uppgifter som skyddas enligt det direktivet”.

Datatillsynsmannen erinrar om att även i samband med befintliga avtal om utbyte av uppgifter, till exempel när det gäller PNR-avtalet, baseras utbytet av uppgifter på särskilda omständigheter och avtal har ingåtts för en begränsad tidsperiod ([23]).

63. Enligt samma logik bör tidsperioden för bevarandet av uppgifter regleras: uppgifterna bör bevaras endast så länge de behövs med hänsyn till det specifika syftet. Om de inte längre är relevanta i förhållande till det fastställda syftet bör de raderas. Datatillsynsmannen motsätter sig starkt upprättandet av datalager där information om icke misstänkta personer skulle lagras med tanke på ett eventuellt kommande behov.

4. Informationssäkerhet

64. Åtgärder och förfaranden för att skydda uppgifter från missbruk, ändring och andra risker utvecklas i principerna, liksom en bestämmelse om att endast behöriga personer ska få tillgång till uppgifterna. Datatillsynsmannen anser att detta är tillfredsställande.

65. Principen kan också kompletteras med en bestämmelse om att register ska föras över de personer som konsulterar uppgifterna. Detta skulle stärka verkningsfullheten av garantierna för att begränsa tillgången och förhindra missbruk av uppgifterna.

66. Dessutom bör det föreskrivas ömsesidig information vid fall av säkerhetsöverträdelser: mottagare såväl i USA som i EU skulle vara ansvariga för att informera sina motparter i det fall att uppgifter som de har erhållit lämnats ut olagligen. Detta kommer att bidra till ökat ansvar för en säker behandling av uppgifterna.

5. Särskilda kategorier av personuppgifter

67. Datatillsynsmannen anser att principen om förbud mot behandling av känsliga uppgifter försvagas avsevärt genom det undantag som tillåter behandling av känsliga uppgifter om den inhemska lagen föreskriver ”lämpliga garantier” i samband med detta. Just på grund av uppgifternas känsliga karaktär måste alla undantag från principen om förbud motiveras tillfredsställande och exakt, och det bör finnas en förteckning över vilka syften och omständigheter som medför att det är tillåtet att behandla en fastställd typ av känsliga uppgifter, samt uppgift om vilka kategorier av registeransvariga som har rätt att behandla dessa typer av uppgifter. Bland de garantier som ska införas anser datatillsynsmannen att det bör ingå att känsliga uppgifter som sådana inte bör utgöra en utlösande faktor för en utredning. Uppgifterna kan göras tillgängliga under särskilda omständigheter, men endast som kompletterande information om en registrerad person som redan är föremål för utredning. Dessa garantier och villkor måste förtecknas på ett begränsande sätt i texten till principen.

6. Redovisningsskyldighet

68. Enligt diskussionen i punkterna 55–56 i detta yttrande måste redovisningsskyldigheten för de offentliga myndigheter som behandlar personuppgifter säkerställas på ett verkningsfullt sätt, och garantier måste ges i avtalet för hur denna redovisningsskyldighet ska ombesörjas. Detta är alldeles särskilt viktigt med tanke på den brist på öppenhet som traditionellt är förknippad med behandlingen av personuppgifter i brottsbekämpningssammanhang. Med hänsyn till detta är ett omnämnande, som nu är fallet i bilagan, av att de offentliga myndigheterna ska vara redovisningsskyldiga, men utan att någon ytterligare förklaring ges av förfarandena för och konsekvenserna av denna redovisningsskyldighet, ingen tillfredsställande garanti. Datatillsynsmannen rekommenderar att en sådan förklaring ska ges i texten till instrumentet.

7. Oberoende och verkningsfull tillsyn

69. Datatillsynsmannen stöder fullt ut att det införs en bestämmelse som föreskriver oberoende och verkningsfull tillsyn av en eller flera offentliga tillsynsmyndigheter. Han anser att tolkningen av oberoende bör klargöras, särskilt vem dessa myndigheter är oberoende av och vem de ska rapportera till. Det behövs kriterier i detta avseende, vilka bör beakta institutionellt och funktionellt oberoende i förhållande till de verkställande och lagstiftande organen. Datatillsynsmannen erinrar om att detta är en väsentlig faktor för att säkerställa att de överenskomna principerna följs på ett verkningsfullt sätt. Dessa myndigheters befogenheter när det gäller intervention och säkerställande av efterlevnad är också avgörande i samband med frågan om redovisningsskyldigheten för de offentliga myndigheter som behandlar personuppgifter, vilket nämns ovan. Deras existens och behörighet bör göras tydligt synbara för de registrerade personerna, så att det blir möjligt för dessa att utöva sina rättigheter, särskilt om flera myndigheter är behöriga beroende på i vilket sammanhang behandlingen sker.

70. Datatillsynsmannen rekommenderar dessutom att det i ett framtida avtal också ska fastställas samarbetsmekanismer mellan tillsynsmyndigheterna.

8. Individuell tillgång och rättelse

71. Specifika garantier krävs när det gäller tillgång och rättelse i brottsbekämpningssammanhang. Datatillsynsmannen välkomnar därför den princip i vilken det konstateras att enskilda personer ska/bör få tillgång till och möjligheter att söka ”rättelse och/eller radering av sina personuppgifter”. Viss osäkerhet kvarstår dock när det gäller definitionen av enskilda personer (alla registrerade personer bör skyddas och inte endast medborgare i det berörda landet)

([23]) Avtalet ska upphöra att gälla sju år efter den dag då det undertecknades, om inte parterna ömsesidigt beslutar att ersätta det.

samt de villkor som gäller för att enskilda personer ska kunna göra invändningar mot behandlingen av uppgifter som rör dem. Det bör preciseras i vilka ”lämpliga fall” en invändning kan eller inte kan göras. Det bör stå klart för de registrerade personerna under vilka omständigheter, beroende till exempel på typen av myndighet, typen av utredning eller andra kriterier, som de kommer att kunna utöva sina rättigheter.

72. Om det av berättigade skäl inte finns någon direkt möjlighet att invända mot en behandling bör vidare en indirekt kontroll finnas tillgänglig, genom den oberoende myndighet som ansvarar för tillsynen av behandlingen.

9. Öppenhet och meddelande

73. Datatillsynsmannen betonar ännu en gång vikten av faktisk öppenhet, för att de enskilda personerna ska kunna utöva sina rättigheter och för att bidra till den allmänna redovisningsskyldigheten för offentliga myndigheter som behandlar personuppgifter. Han stöder principerna, så som de utformats, och insisterar särskilt på behovet av allmänt *och* individuellt meddelande till den enskilda personen. Detta återspeglas i den princip som utformas i punkt 9 i bilagan.

74. I kapitel 2 punkt A.B i rapporten (”Överenskomna principer”) anges emellertid att i USA kan öppenhet omfatta ”enbart eller i kombination med varandra, offentliggörande i det federala registret, personligt meddelande och avslöjande vid en rättegång”. Det måste stå klart att ett offentliggörande i en officiell tidning inte i sig är tillräckligt för att garantera lämplig information till den registrerade personen. Utöver behovet av personligt meddelande erinrar datatillsynsmannen om att informationen måste lämnas i en form och på ett språk som är lätt att förstå för den registrerade personen.

10. Möjlighet till rättslig prövning

75. För att garantera att enskilda personer faktiskt ska kunna utöva sina rättigheter måste dessa personer ha möjlighet att lämna in ett klagomål till en oberoende dataskyddsmyndighet samt ha tillgång till ett rättsmedel inför en oberoende och opartisk domstol. Båda möjligheterna till rättslig prövning bör vara tillgängliga i lika stor utsträckning.

76. Det är nödvändigt med tillgång till en oberoende dataskyddsmyndighet, eftersom detta erbjuder en flexibel och mindre kostsam hjälp i ett sammanhang, brottsbekämpning, som kan vara ganska ogenomskinligt för enskilda personer. Dataskyddsmyndigheterna kan också ge bistånd när det gäller att utöva rättigheten till tillgång på de registrerade personernas vägnar, när undantag hindrar dessa från att få direkt tillgång till de personuppgifter som rör dem.

77. Tillgång till det rättsliga systemet är en ytterligare och oundgänglig garanti för att de registrerade personerna ska kunna få tillgång till rättslig prövning inför en myndighet som tillhör en gren av det demokratiska systemet som är skild från de offentliga institutioner som faktiskt behandlar deras uppgifter. EG-domstolen ([24]) har fastställt att ett sådant verkningsfullt rättsmedel inför en domstol är viktigt ”så att den enskildes rättigheter kan ges ett effektivt skydd. (…) [Det] utgör en allmän gemenskapsrättslig princip som härrör från de konstitutionella traditioner som är gemensamma för medlemsstaterna och som fastställs i artiklarna 6 och 13 i Europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna.” Förekomsten av ett rättsmedel anges också uttryckligen i artikel 47 i Europeiska unionens stadga om de grundläggande rättigheterna och i artikel 22 i direktiv 95/46/EG, utan att det påverkar möjligheten att utnyttja något administrativt förfarande.

11. Databehandlade enskilda beslut

78. Datatillsynsmannen välkomnar bestämmelsen om lämpliga garantier vid databehandling av personuppgifter. Han noterar att en gemensam tolkning av vad som betraktas som en ”betydande skadlig åtgärd som rör den enskilda personens relevanta intressen” skulle klargöra villkoren för tillämpningen av denna princip.

12. Vidareöverföringar

79. Villkoren för vissa vidareöverföringar är oklara. Särskilt när vidareöverföringen ska överensstämma med internationella avtal och avtal mellan de sändande och mottagande länderna bör det anges huruvida det gäller avtal mellan de båda länder som har tagit initiativ till den första överföringen eller mellan de båda länder som är inblandade i vidareöverföringen. Datatillsynsmannen anser att det under alla omständigheter krävs avtal mellan de båda länder som har tagit initiativ till den första överföringen.

80. Datatillsynsmannen noterar också en mycket bred definition av de ”legitima allmänna intressen” som medger en vidareöverföring. Räckvidden för allmän säkerhet förblir oklar och utvidgningen till överföringar vid fall av brott mot etiska regler eller reglerade yrken förefaller oberättigad och alltför omfattande i ett brottsbekämpningssammanhang.

VI. **SLUTSATS**

81. Datatillsynsmannen välkomnar EU- och USA-myndigheternas gemensamma arbete på området för brottsbekämpning, där uppgiftsskydd är av avgörande betydelse. Han vill dock framhålla att frågan är komplicerad, särskilt

([24]) Mål 222/84, Johnston, REG 1986, s. 1651, mål 222/86, Heylens, REG 1987, s. 4097, och mål C-97/91, Borelli, REG 1992, s. I-6313.

när det gäller dess exakta omfattning och art, och att den därför förtjänar noggrann och ingående analys. Ett transatlantiskt instruments effekter på uppgiftsskyddet bör övervägas noggrant i förhållande till det befintliga regelverket och konsekvenserna för medborgarna.

82. Datatillsynsmannen uppmanar till större tydlighet och konkreta bestämmelser, särskilt när det gäller följande aspekter:

— Förtydligande när det gäller instrumentets karaktär, som bör vara rättsligt bindande för att erbjuda tillräcklig rättslig säkerhet.

— Ett noggrant konstaterande av adekvat skyddsnivå, på grundval av väsentliga krav rörande systemets innehåll, särdrag och tillsyn. Datatillsynsmannen anser att det allmänna instrumentets adekvata skyddsnivå kan erkännas endast om det kombineras med adekvata särskilda avtal från fall till fall.

— Ett begränsat tillämpningsområde, med en tydlig och gemensam definition av de brottsbekämpningssyften som berörs.

— Preciseringar av villkoren för att privata enheter ska kunna medverka i system för uppgiftsöverföring.

— Överensstämmelse med proportionalitetsprincipen, vilket innebär utbyte av uppgifter från fall till fall när det finns ett konkret behov.

— Kraftfulla tillsynssystem samt system för rättslig prövning som är tillgängliga för registrerade personer, inklusive administrativa förfaranden och rättsmedel.

— Verkningsfulla åtgärder som garanterar att alla registrerade personer kan utöva sina rättigheter, oberoende av deras medborgarskap.

— Medverkan av oberoende dataskyddsmyndigheter, särskilt i samband med tillsyn och bistånd till registrerade personer.

83. Datatillsynsmannen insisterar på att all brådska bör undvikas när principerna utarbetas, eftersom detta endast kan leda till otillfredsställande lösningar, med effekter som är motsatta dem som avses i fråga om uppgiftsskydd. Den bästa vägen framåt skulle därför i detta skede vara utarbetandet av en färdplan mot ett eventuellt avtal vid en senare tidpunkt.

84. Datatillsynsmannen uppmanar också till större öppenhet när det gäller utarbetandet av principerna för uppgiftsskydd. Endast om samtliga berörda parter, inklusive Europaparlamentet, medverkar kan instrumentet dra fördel av en demokratisk debatt och få det nödvändiga stödet och erkännandet.

Utfärdat i Bryssel den 11 november 2008

Peter HUSTINX

Europeisk datatillsynsman

Yttrande från Europeiska datatillsynsmannen om meddelandet från kommissionen till rådet, Europaparlamentet och Europeiska ekonomiska och sociala kommittén – *Mot en europeisk strategi för e-juridik*

(2009/C 128/02)

EUROPEISKA DATATILLSYNSMANNEN HAR ANTAGIT DETTA YTTRANDE

med beaktande av fördraget om upprättandet av Europeiska gemenskapen, särskilt artikel 286,

med beaktande av Europeiska unionens stadga om de grundläggande rättigheterna, särskilt artikel 8,

med beaktande av Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter ([1]),

med beaktande av Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter ([2]), särskilt artikel 41.

HÄRIGENOM FRAMFÖRS FÖLJANDE.

I. **INLEDNING**

1. Den 30 maj antogs meddelandet från kommissionen till rådet, Europaparlamentet och Europeiska ekonomiska och sociala kommittén – *Mot en europeisk strategi för e-juridik* (nedan kallat *meddelandet*). Europeiska datatillsynsmannen lämnar detta yttrande i enlighet med artikel 41 i förordning (EG) nr 45/2001.

2. Syftet med meddelandet är att föreslå en strategi för e-juridik som är tänkt att stärka medborgarnas förtroende för det europeiska området med rättvisa. E-juridikens huvudsyfte bör vara att se till att rättvisa skipas på ett effektivare sätt i hela Europa till förmån för medborgarna. Genom EU:s insatser bör medborgarna få tillgång till information utan att hindras av språkliga, kulturella eller rättsliga hinder som härrör från mångfalden av system. Till meddelandet har fogats ett utkast till handlingsplan och tidsplan för de olika projekten.

3. I detta yttrande lämnar datatillsynsmannen synpunkter på meddelandet i fråga om behandling av personuppgifter, integritetsskyddet i sektorn för elektroniska kommunikationer och om det fria flödet av uppgifter.

([1]) EGT L 281, 23.11.1995, s. 31.
([2]) EGT L 8, 12.1.2001, s. 1.

II. **BAKGRUND OCH SAMMANHANG**

4. Rådet (rättsliga och inrikes frågor) ([3]) fastställde ett antal prioriteringar för utvecklingen av e-juridik i juni 2007:

— att inrätta ett europeiskt gränssnitt (e-juridikportalen),

— att skapa förutsättningar för länkning mellan flera register, t.ex. kriminalregister, register för insolvensförfaranden, handels- och företagsregister och fastighetsregister,

— att inleda förberedelserna inför användningen av informations- och kommunikationsteknik för det europeiska betalningsföreläggandet,

— att förbättra användningen av videokonferensteknik vid gränsöverskridande förfaranden, särskilt när det gäller bevisupptagning,

— att utforma stödverktyg för översättning och tolkning.

5. Sedan dess har arbetet med e-juridiken fortsatt i jämn takt. Enligt kommissionen måste det i detta sammanhang under arbetets gång sörjas för att operativa projekt och decentraliserade strukturer prioriteras, med samordning på europeisk nivå, varvid befintliga rättsliga instrument bör användas och IT-verktyg utnyttjas för att effektivisera dem. Även Europaparlamentet har uttryckt sitt stöd för e-juridikprojektet ([4]).

6. Såväl på det civilrättsliga som det straffrättsliga området har kommissionen konsekvent stött användning av modern informationsteknik. Detta ledde fram till instrument som det europeiska betalningsföreläggandet. Kommissionen har alltsedan 2003 förvaltat portalen för det europeiska rättsliga nätverket på privaträttens område som medborgarna nu har tillgång till på 22 olika språk. Kommissionen har även utformat och tagit fram den europeiska rättsliga atlasen. Dessa verktyg förebådar en kommande europeisk ram för e-juridik. På det straffrättsliga området har kommissionen arbetat på ett verktyg som ska gör det möjligt att utväxla uppgifter i medlemsstaternas kriminalregister ([5]). Inte bara kommissionen utan även Eurojust har utvecklat säkra kommunikationssystem med de nationella myndigheterna.

([3]) Dok. 10393/07 JURINFO 21.
([4]) Se utkastet till betänkande från Europaparlamentets utskott för rättsliga frågor.
([5]) Se särskilt det nedan nämnda europeiska informationssystemet för utbyte av uppgifter ur kriminalregister (Ecrissystemet).

7. E-juridiken är avsedd att ge många möjligheter under de kommande åren till ett europeiskt rättsligt område som har en mer konkret innebörd för medborgarna. För att skapa en övergripande strategi på detta viktiga område antog kommissionen detta meddelande om e-juridik. I meddelandet fastställs objektiva kriterier för fastställande av prioriteringar, särskilt för framtida projekt på europeisk nivå, för konkreta resultat inom rimlig tid.

8. Ett arbetsdokument från kommissionens avdelningar, ett dokument som åtföljer meddelandet och innehåller en sammanfattning av konsekvensbedömningen ger också viss bakgrundsinformation ([6]). Rapporten om konsekvensbedömningen har utarbetats med beaktande av synpunkterna från medlemsstaterna, de rättsliga myndigheterna, rättsutövarna, medborgarna och företagen. Inget samråd med Europeiska datatillsynsmannen förekom. I rapporten om konsekvensbedömningen förordas ett politiskt alternativ där en EU-dimension kombineras med nationell behörighet för att lösa problemen. Det är detta politiska alternativ som valts i meddelandet. Strategin ska inriktas på användning av videokonferenser; upprättande av en e-juridikportal, förbättrade översättningsmöjligheter genom utveckling av automatiska elektroniska översättningshjälpmedel, förbättring av kommunikationen mellan rättsliga myndigheter, ökad sammankoppling av nationella register och elektroniska verktyg för EU-förfaranden (t.ex. det europeiska betalningsföreläggandet).

9. Datatillsynsmannen stöder inriktningen på dessa åtgärder. Han stöder generellt ett heltäckande upplägg för e-juridiken. Han instämmer därför i det tredelade behovet att förbättra tillgången till rättvisa, samarbetet mellan europeiska rättsliga myndigheter och själva rättssystemets effektivitet. Detta upplägg påverkar därigenom ett antal institutioner och enskilda:

   — Medlemsstaterna som har huvudansvaret för effektiva och trovärdiga rättssystem.

   — Europeiska kommissionen, i egenskap av fördragens väktare.

   — Medlemsstaternas rättsliga myndigheter, som behöver förfinade verktyg för sin kommunikation, särskilt i gränsöverskridande ärenden.

   — Rättsutövarna, medborgarna och företagen, som alla förordar bättre användning av IT-verktyg för att deras behov av ”rättvisa” ska tillgodoses på ett mer tillfredsställande sätt.

10. Meddelandet har nära anknytning till förslaget till rådets beslut om inrättande av det europeiska informationssystemet för utbyte av uppgifter ur kriminalregister (Ecris). Den 16 september 2008 antog Europeiska datatillsynsmannen ett yttrande om detta förslag ([7]). Han stödde förslaget, förutsatt att ett antal överväganden beaktades. Han framhöll särskilt att nya dataskyddsgarantier bör kompensera för avsaknaden för närvarande av en heltäckande rättslig ram för dataskydd vid samarbetet mellan polis och rättsliga myndigheter. Han betonade därför behovet av effektiv samordning av datatillsynen i systemet, vilket omfattar medlemsstaternas myndigheter och kommissionen i egenskap av den som tillhandahåller den gemensamma kommunikationsinfrastrukturen.

11. Några rekommendationer i det yttrandet som förtjänar att erinras om är följande:

   — Det bör finnas en hänvisning till att en hög nivå av dataskydd är en förutsättning för de genomförandeåtgärder som ska antas.

   — För ökad rättssäkerhet bör dels kommissionens ansvar för den gemensamma kommunikationsinfrastrukturen i systemet, dels tillämpligheten för förordning (EG) nr 45/2001 klargöras i texten.

   — Kommissionen – och inte medlemsstaterna – bör även ansvara för anslutningsprogramvaran för att effektivisera utbytet och möjliggöra bättre tillsyn av systemet.

   — Användningen av automatisk översättning bör vara klart definierad och begränsad för att gynna den ömsesidiga förståelsen av brott utan att försämra kvaliteten på den överförda informationen.

12. Dessa rekommendationer är fortfarande belysande för det sammanhang i vilket meddelandet kommer att analyseras.

III. INFORMATIONSUTBYTE I ENLIGHET MED MEDDELANDET

13. E-juridik har ett mycket vitt tillämpningsområde, som i allmänhet inbegriper användningen av informations- och kommunikationsteknik inom rättsväsendet i Europeiska unionen. Det omfattar ett antal frågor, såsom projekt för att förbättra informationen till parterna. Det innefattar upplysningar online om rättssystem, lagstiftning och rättspraxis, system för elektronisk kommunikation mellan

([6]) Kommissionens arbetsdokument: Dokument som åtföljer meddelandet till rådet, Europaparlamentet och Europeiska ekonomiska och sociala kommittén – *Mot en europeisk strategi för e-juridik* – Sammanfattning av konsekvensbedömningen, 30.5.2008, SEK(2008) 1944.

([7]) Se Yttrande från Europeiska datatillsynsmannen om förslaget till rådets beslut om inrättande av Europeiska informationssystemet för utbyte av uppgifter ur kriminalregister (Ecris) i enlighet med artikel 11 i rambeslut 2008/XX/RIF på Europeiska datatillsynsmannens webbplats under *Consultation* och sedan *Opinions* och *2008*.

parterna och domstolarna samt inrättandet av fullständigt elektroniska förfaranden. Det omfattar även sådana europeiska projekt som användningen av elektroniska medel för upptagning av rättegångsförhandlingar samt projekt för informationsutbyte eller sammankoppling.

14. Även om tillämpningsområdet är mycket vitt, har Europeiska datatillsynsmannen noterat att det kommer att finnas information om straffrättsliga förfaranden och privaträttsliga system men inte om förvaltningsrättsliga system. Det kommer dessutom att finnas en länk till en straffrättslig och en civilrättslig atlas men inte till en förvaltningsrättslig atlas, även om det skulle vara bättre för medborgare och företag att ha tillgång till förvaltningsrättsliga system, dvs. förvaltningsrätt och klagomålsförfaranden. Det bör även finnas en länk till sammanslutningen av de högsta förvaltningsdomstolarna. Dessa tillägg skulle göra det lättare för medborgarna att hitta vägen i den snårskog som förvaltningsrätten med alla sina domstolar ofta utgör och på så sätt bli mer välinformerade om de förvaltningsrättsliga systemen.

15. Europeiska datatillsynsmannen rekommenderar därför att förvaltningsrättsliga förfaranden ska ingå i e-juridiken. Som en del av denna nya aspekt bör e-juridikprojekt lanseras för att synliggöra reglerna för dataskydd samt nationella dataskyddsmyndigheter, särskilt i förbindelse med sådana data som behandlas inom ramen för e-juridik. Detta vore i linje med det s.k. Londoninitiativet, vilket lanserades av dataskyddsmyndigheterna i november 2006 och vilket syftar till ”Att förmedla uppgiftsskydd och göra det mer effektivt”.

IV. **DET NYA RAMBESLUTET OM DATASKYDD INOM RAMEN FÖR POLISSAMARBETE OCH STRAFFRÄTTSLIGT SAMARBETE**

16. Med tanke på det ökande utbyte av personuppgifter mellan rättsliga myndigheter som förutses i meddelandet framstår de tillämpliga rättsliga dataskyddsramarna som allt viktigare. I sammanhanget noterar Europeiska datatillsynsmannen att Europeiska unionens råd - tre år efter det ursprungliga kommissionsförslaget - den 27 november 2008 antog ett rambeslut om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete ([8]). Denna nya rättsakt kommer att tillhandahålla generella rättsliga ramar för dataskydd i frågor som rör den tredje pelaren, jämte bestämmelserna om dataskydd i frågor som rör den första pelaren i direktiv 95/46/EG.

17. Europeiska datatillsynsmannen välkomnar detta rättsinstrument som ett första betydande framsteg för dataskyddet inom polissamarbete och rättsligt samarbete. Den dataskyddsnivå som har uppnåtts i den slutgiltiga texten är emellertid inte helt tillfredsställande. I synnerhet omfattar rambeslutet endast polisuppgifter och rättsliga uppgifter som utbyts mellan medlemsstaterna, EU-myndigheter och EU-system och innefattar inte inhemska uppgifter. Vidare innehåller det antagna rambeslutet ingen skyldighet att skilja mellan olika kategorier av registrerade personer, såsom misstänkta personer, brottslingar, vittnen och offer, för att säkerställa att deras uppgifter skyddas på lämpligt sätt. Det innebär ingen fullständig överensstämmelse med direktiv 95/46/EG, särskilt vad avser att begränsa de syften för vilka personuppgifter får behandlas ytterligare. Inte heller föreskriver det inrättandet av en oberoende grupp av berörda nationella dataskyddsmyndigheter och EU-dataskyddsmyndigheter, vilken skulle säkerställa såväl bättre samordning mellan dataskyddsmyndigheterna som ett betydande bidrag till den enhetliga tillämpningen av rambeslutet.

18. Detta torde innebära att det i ett sammanhang där många insatser görs för att utveckla gemensamma system för gränsöverskridande utbyte av personuppgifter fortfarande finns skiljaktigheter i fråga om reglerna för uppgiftsbehandling och för medborgarnas utövande av sina rättigheter i olika EU-länder.

19. Europeiska datatillsynsmannen erinrar ånyo om att säkerställandet av en hög dataskyddsnivå inom polissamarbete och rättsligt samarbete samt överensstämmelse med direktiv 95/46/EG utgör ett nödvändigt komplement till andra införda eller påtänkta åtgärder för att underlätta det gränsöverskridande utbytet av personuppgifter som ett led i brottsbekämpningen. Detta bottnar inte endast i medborgarens fundamentala rätt till personuppgiftsskydd utan även i de brottsbekämpande myndigheternas behov av att säkerställa kvaliteten på de uppgifter som utbyts - såsom bekräftas i meddelandets bilaga när det gäller sammankopplingen av kriminalregister -, förtroende mellan myndigheterna i olika länder samt rättslig giltighet för de bevis som samlas in i ett gränsöverskridande sammanhang.

20. Europeiska datatillsynsmannen uppmanar därför EU-institutionerna att särskilt beakta dessa aspekter inte endast vid genomförandet av de åtgärder som avses i meddelandet utan även inför inledandet snarast möjligt av reflektioner om ytterligare förbättringar av de rättsliga ramarna för dataskydd inom brottsbekämpning.

V. **E-JURIDIKPROJEKT**

E-juridikverktyg på europeisk nivå

21. Europeiska datatillsynsmannen inser att utbytet av personuppgifter utgör en viktig del av inrättandet av ett område med frihet, säkerhet och rättvisa och stöder därför förslaget

([8]) Ännu ej offentliggjort i EUT.

till strategi för e-juridik samtidigt som han framhåller vikten av dataskydd i detta sammanhang. Respekten för dataskydd är förvisso inte endast en rättslig skyldighet utan är även av avgörande betydelse för de planerade systemens framgång, exempelvis när det gäller att säkerställa kvaliteten på de uppgifter som överförs. Detta gäller såväl för institutioner och organ när de behandlar personuppgifter som när nya strategier utarbetas. Regler och principer bör tillämpas och följas i praktiken och särskilt beaktas vid utformningen och konstruktionen av informationssystem. Integritetsskydd och dataskydd är i sig nyckelfaktorer för ett framgångsrikt, välfungerande och balanserat informationssamhälle. Det är därför meningsfullt att i ett så tidigt skede som möjligt investera i dessa faktorer.

22. Europeiska datatillsynsmannen betonar i sammanhanget att meddelandet inte föreskriver någon central europeisk databas. Han noterar med tillfredsställelse att man föredrar decentraliserade strukturer. Europeiska datatillsynsmannen erinrar om sina yttranden om Ecris ([9]) och Prüm-initiativet ([10]). I sitt yttrande om Ecris hävdade han att man med en decentraliserad struktur undviker ytterligare duplicering av personuppgifter i en central databas. I sitt yttrande om Prüm-initiativet förespråkade han att man vederbörligen ska beakta systemets omfattning när man diskuterar sammankoppling av databaser. Det bör utformas särskilda format för förmedling av uppgifter, såsom begäran online om tillgång till kriminalregister, som även beaktar språkliga skillnader, och de utbytta uppgifternas korrekthet bör kontrolleras ständigt. Dessa aspekter bör även beaktas i samband med initiativ som går tillbaka på e-juridikstrategin.

23. Europeiska kommissionen har för avsikt att i nära samarbete med medlemsstaterna och andra partner bidra till att stärka och utveckla e-juridikverktyg på europeisk nivå. Samtidigt som kommissionen stöder medlemsstaternas ansträngningar kommer den att på egen hand ta fram ett antal datorverktyg för att öka systemens interoperabilitet, underlätta allmänhetens tillgång till rättsväsendet och kommunikationen mellan rättsliga myndigheter samt åstadkomma betydande skalfördelar på europeisk nivå. När det gäller interoperabiliteten för den programvara som medlemsstaterna använder, måste inte samtliga medlemsstater nödvändigtvis använda samma programvara – även om detta är det mest praktiska alternativet – men denna måste vara fullt interoperabel.

24. Europeiska datatillsynsmannen rekommenderar att man för systemens sammankoppling och interoperabilitet vederbörligen ska beakta principen om ändamålsbegränsning, och dessa bör konstrueras enligt dataskyddsnormer (dvs. att skydd av privatlivet ska ingå som en del av utformningen, s.k. *privacy by design*). Varje form av interaktion mellan olika system bör dokumenteras grundligen. Interoperabilitet bör aldrig leda till en situation där en myndighet som inte har rätt att få tillgång till eller använda vissa uppgifter kan få tillgång till dessa via ett annat informationssystem. Europeiska datatillsynsmannen vill återigen betona att interoperabilitet inte i sig kan rättfärdiga ett frångående av principen om ändamålsbegränsning ([11]).

25. En annan avgörande punkt är vidare att se till att det förstärkta, gränsöverskridande utbytet av personuppgifter åtföljs av bättre övervakning från och samarbete mellan dataskyddsmyndigheterna. Europeiska datatillsynsmannen har redan i sitt yttrande av den 29 maj 2006 om rambeslutet om utbyte av uppgifter ur kriminalregistret ([12]) framhållit att det föreslagna rambeslutet inte bara bör ta upp samarbetet mellan centrala myndigheter utan även samarbetet mellan diverse behöriga dataskyddsmyndigheter. Detta har sedermera fått än större vikt, eftersom förhandlingarna om det nyligen antagna rambeslutet om skydd av personuppgifter som behandlas inom ramen för polissamarbete och rättsligt samarbete ([13]) har lett till att man strukit bestämmelsen om inrättande av en arbetsgrupp där man samlar EU-dataskyddsmyndigheter och samordnar deras verksamhet med avseende på uppgiftsbehandling inom ramen för polissamarbete och rättsligt samarbete. I syfte att säkerställa en effektiv övervakning samt god kvalitet på det gränsöverskridande utbytet av uppgifter från kriminalregistren bör det inrättas mekanismer för effektiv samordning mellan dataskyddsmyndigheter ([14]). Dessa mekanismer bör även beakta Europeiska datatillsynsmannens tillsynsbefogenhet i fråga om s-Testa-infrastruktur ([15]). E-juridikverktyg kan stödja dessa mekanismer, som kan utformas i nära samarbete med dataskyddsmyndigheterna.

26. I punkt 4.2.1 i meddelandet påpekas det att det är viktigt att utbytet av uppgifter från kriminalregistren utvidgas till att omfatta mer än det rättsliga samarbetet och även används för andra syften, t.ex. i fråga om tillgång till vissa befattningar. Europeiska datatillsynsmannen betonar att varje behandling av personuppgifter i andra syften än de för vilka uppgifterna har samlats in bör respektera de särskilda villkor som anges i tillämplig dataskyddslagstiftning. I synnerhet bör behandling av personuppgifter i andra syften endast tillåtas om detta är nödvändigt för

([9]) Se fotnot 4, punkt 18.
([10]) EUT C 89, 10.4.2008, s. 4.
([11]) EUT C 91, 19.4.2006, s. 53. Se även Europeiska datatillsynsmannens synpunkter på kommissionens meddelande om interoperabilitet mellan de europeiska databaserna, Bryssel, 10.3.2006.
([12]) EUT C 313, 20.12.2006, s. 26.
([13]) Se kapitel IV ovan.
([14]) Se Europeiska datatillsynsmannens yttrande om Ecris, punkterna 8 och 37–38.
([15]) Se punkterna 27-28 nedan.

att söka uppnå intressen som anges i gemenskapens dataskyddslagstiftning ([16]) och under förutsättning att de föreskrivs genom lagstiftningsåtgärder.

27. När det gäller sammankopplingen av kriminalregister anges det i meddelandet att som en del av förberedelserna inför ikraftträdandet av ramdirektivet om utbyte av uppgifter ur kriminalregister kommer kommissionen att inleda två genomförbarhetsstudier för att organisera projektets vidareutveckling och utvidga informationsutbytet till att också omfatta tredjelandsmedborgare som fällts för brott. Under 2009 kommer kommissionen att ställa programvara till medlemsstaternas förfogande som ska göra att alla kriminalregister snabbt kan ingå i informationsutbytet. I kombination med s-Testa-systemet för informationsutbyte kommer detta referenssystem att medföra skalfördelar, eftersom medlemsstaterna inte behöver ägna sig åt eget utvecklingsarbete. Det tekniska genomförandet av projektet förenklas också på detta sätt.

28. Europeiska datatillsynsmannen välkomnar i detta avseende utnyttjandet av s-Testa-infrastrukturen som har visat sig vara ett pålitligt system för utbyte av uppgifter och rekommenderar att de statistikuppgifter som avser de planerade systemen för uppgiftsutbyte bör definieras mer i detalj med vederbörlig hänsyn till behovet av att säkerställa att dataskyddet övervakas. Till exempel kan statistikuppgifter uttryckligen omfatta sådana faktorer som antalet ansökningar om tillgång till och rättelse av personuppgifter, uppdateringsprocessens längd och fullständighet, de personers ställning som har tillgång till dessa uppgifter samt fall av brott mot säkerheten. Vidare bör statistikuppgifter och rapporter baserade på dessa uppgifter göras tillgängliga fullt ut för de behöriga dataskyddsmyndigheterna.

Automatisk översättning och databas över översättare

29. Användningen av automatisk översättning är ett användbart instrument och kommer troligen att gynna den ömsesidiga förståelsen mellan relevanta aktörer i medlemsstaterna. Emellertid bör inte användningen av automatisk översättning resultera i att kvaliteten på de utbytta uppgifterna försämras, särskilt när dessa uppgifter används för att fatta beslut som har rättsliga verkningar för de berörda personerna. Europeiska datatillsynsmannen påpekar att det är viktigt att klart definiera och begränsa användningen av automatisk översättning. Användningen av automatisk översättning för att överföra uppgifter som inte har översatts korrekt, såsom ytterligare kommentarer eller specifikationer avseende ett enskilt fall, kommer sannolikt att påverka kvaliteten på de överförda uppgifterna – och således de beslut som fattas på grundval av dessa – och bör i princip uteslutas ([17]). Europeiska datatillsynsmannen föreslår att ta hänsyn till denna rekommendation i de åtgärder som vidtas enligt meddelandet.

30. Kommissionen vill upprätta en databas över rättstolkar och översättare så att kvaliteten på rättstolkningen och översättningen förbättras. Europeiska datatillsynsmannen stöder detta syfte men erinrar om att denna databas kommer att underställas relevant dataskyddslagstiftning. Framför allt om databasen skulle innehålla utvärderingsuppgifter om översättarnas prestationer bör den först kontrolleras av behöriga dataskyddsmyndigheter.

Mot en europeisk handlingsplan för e-juridik

31. I punkt 5 i meddelandet anges det att ansvaret måste tydligt fördelas mellan kommissionen, medlemsstaterna och de andra aktörerna i det rättsliga samarbetet. Kommissionen kommer att ta på sig en allmän samordningsroll och främja utbytet av bästa praxis och kommer att utarbeta, upprätta och samordna uppgifterna i e-juridikportalen. Dessutom kommer kommissionen att fortsätta att arbeta med att koppla samman kriminalregistren och ta på sig det direkta ansvaret för nätverket på civilrättens område och stödja det rättsliga nätverket på straffrättens område. Medlemsstaterna måste uppdatera de uppgifter om sina rättssystem som återfinns i e-juridikens webbplats. Andra aktörer är de civil- och straffrättsliga nätverken och Eurojust. De kommer att utveckla de verktyg som är nödvändiga för ett effektivare rättsligt samarbete, särskilt verktyg för automatisk översättning och ett säkert utbytessystem i nära kontakt med kommissionen. Ett utkast till en handlingsplan och en tidtabell för de olika projekten bifogas meddelandet.

32. Europeiska datatillsynsmannen understryker i detta sammanhang att i Ecris-systemet å ena sidan har ingen central europeisk databas upprättats och det planeras ingen direktåtkomst till sådana databaser som innehåller kriminalregister i andra medlemsstater, medan å den andra sidan ansvaret på nationell nivå för korrekt information har centraliserats till medlemsstaternas centrala myndigheter. Inom denna mekanism ansvarar medlemsstaterna för driften av de nationella databaserna och för att utbytet sker effektivt. Det är oklart om de ansvarar för anslutningsprogramvaran eller inte. Kommissionen kommer att förse medlemsstaterna med programvara som utformats så att uppgifter från alla kriminalregister kan utbytas inom en kort frist. Referenssystemet kommer att kombineras med användningen av s-Testa för informationsutbyte.

33. Europeiska datatillsynsmannen förstår också att i samband med analoga e-juridikinitiativ skulle liknande system kunna genomföras och kommissionen kommer att ansvara för den gemensamma infrastrukturen, även om detta inte klart

([16]) Se särskilt artikel 13 i direktiv 95/46/EG och artikel 20 i förordning nr 45/2001.

([17]) Se punkterna 39 och 40 i Europeiska datatillsynsmannens yttrande om Ecris.

anges i meddelandet. Datatillsynsmannen föreslår att detta ansvar av rättssäkerhetsskäl förtydligas för de åtgärder som härrör från meddelandet.

E-juridikprojekt

34. Bilagan innehåller en rad projekt som ska utvecklas under de kommande fem åren. Det första projektet, utveckling av sidor om e-juridik, avser e-juridikportalen. Åtgärden kräver en genomförbarhetsstudie och att portalen utvecklas. Därutöver behöver man införa metoder för handhavande och tillhandahållande av information på alla EU-språk på Internet. Det andra och det tredje projektet avser sammankopplingen av kriminalregister. Projekt 2 gäller sammankoppling av nationella kriminalregister. Projekt 3 avser upprättandet av en europeisk förteckning över dömda tredjelandsmedborgare utöver en genomförbarhetsstudie och framläggandet av ett förslag till rättsakt. Datatillsynsmannen noterar att sistnämnda projekt inte längre nämns i kommissionens arbetsprogram och undrar om detta avspeglar en ändring i kommissionens planerade projekt eller endast ett uppskjutande av detta specifika projekt.

35. I meddelandet förtecknas också tre projekt på området för elektroniska utbyten och tre projekt på området för översättningsstöd. Ett pilotprojekt kommer att inledas om att successivt upprätta en komparativ flerspråkig juridisk vokabulär. Andra relevanta projekt avser upprättandet av dynamiska formulär som ska åtfölja EU-rättsakterna liksom främjandet av de rättsliga myndigheternas utnyttjande av videokonferenser. Som en del av e-juridikforumet kommer slutligen årsmöten att hållas om e-juridikfrågor och rättstillämpare kommer att utbildas i rättsligt samarbete. Europeiska datatillsynsmannen föreslår att man vid sådana möten och utbildningar ägnar tillräcklig uppmärksamhet åt lagstiftning och praxis i fråga om dataskydd.

36. Bilagan innehåller därför en lång rad europeiska verktyg som syftar till att förenkla informationsutbytet mellan aktörer i olika medlemsstater. Bland dessa verktyg spelar e-juridikportalen, som kommissionen huvudsakligen ska ansvara för, en viktig roll.

37. En egenskap som är gemensam för många av dessa verktyg är att information, och personuppgifter, kommer att utbytas och handläggas av olika aktörer både på nationell nivå och EU-nivå vilka omfattas av de dataskyddsskyldigheter och de tillsynsmyndigheter som inrättas genom direktiv 95/46/EG eller förordning (EG) nr 45/2001. I detta avseende, och som Europeiska datatillsynsmannen redan klargjort i sitt yttrande om informationssystemet för den inre marknaden (IMI) ([18]), är det mycket viktigt att se till att ansvaret för att dataskyddsreglerna följs säkerställs på ett effektivt och problemfritt sätt.

38. I grunden kräver detta å ena sidan att ansvaret för behandlingen av personuppgifter inom dessa system är klart definierat och fördelat; å andra sidan att det fastställs lämpliga samordningsmekanismer – särskilt för övervakning – varje gång detta är nödvändigt.

39. Användningen av ny teknik utgör en av hörnstenarna i e-juridikinitiativet: sammankoppling av nationella register, utveckling av elektroniska signaturer, säkra nätverk, virtuellt utrymme för informationsutbyte och utökad användning av videokonferenser kommer att ingå som väsentliga delar av e-juridikinitiativet under de kommande åren.

40. I detta sammanhang är det mycket viktigt att dataskyddsfrågor beaktas så tidigt som möjligt och införlivas i de planerade verktygens struktur. Framför allt är såväl systemets uppbyggnad som genomförandet av lämpliga säkerhetsåtgärder särskilt viktiga. Detta *privacy by design* -upplägg skulle medge att det i relevanta e-juridikinitiativ föreskrivs en effektiv hantering av personuppgifter och samtidigt garantera att dataskyddsprinciperna följs och att uppgiftsutbytet mellan olika myndigheter är säkert.

41. Europeiska datatillsynsmannen understryker också att tekniska verktyg bör användas, inte bara för att säkerställa informationsutbytet, utan också för att förstärka de berörda personernas rättigheter. I detta avseende välkomnar Europeiska datatillsynsmannen att meddelandet hänvisar till medborgarnas möjlighet att begära utdrag ur kriminalregistret på valfritt språk ([19]). När det gäller denna fråga erinrar datatillsynsmannen om att han i sitt yttrande om kommissionens förslag att utbyta uppgifter ur kriminalregistren välkomnade möjligheten för den berörda personen att begära fram sina personliga uppgifter ur kriminalregistret av den centrala myndigheten i en medlemsstat, förutsatt att personen i fråga är eller har varit bosatt, eller är eller har varit medborgare i den anmodade eller den anmodande medlemsstaten. Tanken på att använda den myndighet som befinner sig närmast den berörda personen som en enda kontaktpunkt framfördes också av datatillsynsmannen i samband med samordningen av socialförsäkringssystemen. Europeiska datatillsynsmannen uppmanar därför kommissionen att fortsätta på samma väg och främja tekniska verktyg – framför allt åtkomst via Internet – så att

([18]) EUT C 270, 25.10.2008, s. 1.
([19]) Se punkt 6 i meddelandet.

medborgarna får bättre kontroll över sina personuppgifter även när de flyttar mellan olika medlemsstater.

VI. **SLUTSATSER**

42. Europeiska datatillsynsmannen stöder det nuvarande förslaget att upprätta e-juridiken och rekommenderar att följande kommentarer i detta yttrande beaktas:

— Beakta det nya rambeslutet om skydd för personuppgifter på området för polissamarbete och straffrättsligt samarbete – inklusive dess brister – inte bara vid genomförandet av de planerade åtgärderna enligt meddelandet utan också i syfte att så snart som möjligt inleda en planering av ytterligare förbättringar av den rättsliga ramen för dataskydd i brottsbekämpningen.

— Införliva administrativa förfaranden i e-juridiken. Som en del av denna nya faktor bör e-juridikprojekt inledas för att förbättra synligheten för dataskyddsreglerna och de nationella dataskyddsmyndigheterna, särskilt vad avser den typ av uppgifter som behandlas inom ramen för e-juridikprojekten.

— Fortsätta att prioritera decentraliserade strukturer.

— Säkerställa systemens sammankoppling och interoperabilitet med vederbörligt beaktande av principen om ändamålsbegränsning.

— Fördela ansvaret tydligt mellan alla aktörer som behandlar personuppgifter inom de planerade systemen och tillhandahålla mekanismer för en effektiv samordning mellan dataskyddsmyndigheterna.

— Se till att behandlingen av personuppgifter för andra syften än de som de samlades in för bör respektera de specifika villkor som fastställts i den tillämpliga dataskyddslagstiftningen.

— Klart definiera och begränsa användningen av automatiska översättningar för att främja en ömsesidig förståelse av brotten utan att det påverkar kvaliteten på överlämnad information.

— Klargör kommissionens ansvar för gemensamma infrastrukturer, t.ex. s-Testa.

— När det gäller användningen av ny teknik se till att dataskyddsfrågor beaktas så tidigt som möjligt (*privacy by design*) och främja tekniska verktyg som ger medborgarna möjlighet att bättre kontrollera sina personuppgifter även om de flyttar mellan olika medlemsstater.

Upprättat i Bryssel den 19 december 2008.

Peter HUSTINX

Europeiska datatillsynsmannen

Utkast till yttrande från Europeiska datatillsynsmannenom förslaget till Europaparlamentets och rådets direktiv om tillämpningen av patienträttigheter vid gränsöverskridande hälso- och sjukvård

(2009/C 128/03)

EUROPEISKA DATATILLSYNSMANNEN HAR ANTAGIT DETTA YTTRANDE

med beaktande av fördraget om upprättandet av Europeiska gemenskapen, särskilt artikel 286,

med beaktande av Europeiska unionens stadga om de grundläggande rättigheterna, särskilt artikel 8,

med beaktande av Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter,

med beaktande av Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter, särskilt artikel 41,

med beaktande av den begäran om ett yttrande i enlighet med artikel 28.2 i förordning (EG) nr 45/2001 som översändes till datatillsynsmannen den 2 juli 2008.

HÄRIGENOM FRAMFÖRS FÖLJANDE.

I. INLEDNING

Förslaget till direktiv om tillämpningen av patienträttigheter vid gränsöverskridande hälso- och sjukvård

1. Den 2 juli 2008 antog kommissionen ett förslag till Europaparlamentets och rådets direktiv om tillämpningen av patienträttigheter vid gränsöverskridande hälso- och sjukvård (nedan kallat *förslaget*) [1]. Kommissionen översände förslaget till datatillsynsmannen för samråd i enlighet med artikel 28.2 i förordning (EG) nr 45/2001.

2. Syftet med förslaget är att inrätta en gemenskapsram för tillhandahållande av gränsöverskridande hälso- och sjukvård i EU i de fall då den vård patienterna söker ges i en annan medlemsstat än deras hemland. Ramen består av följande tre huvudområden:

— Fastställande av gemensamma principer i alla hälso- och sjukvårdsystem i EU, med medlemsstaternas ansvarsområden tydligt angivna.

— Utarbetande av en särskild ram för gränsöverskridande hälso- och sjukvård, där patienternas rätt till hälso- och sjukvård i en annan medlemsstat klargörs.

— Främjande av EU-samarbete inom hälso- och sjukvård, på områden som erkännande av recept som skrivits ut i andra länder, europeiska referensnätverk, utvärdering av hälso- och sjukvårdsteknik, uppgiftsinsamling, kvalitet och säkerhet.

3. Det finns två syften med denna ram, nämligen att skapa tillräcklig klarhet när det gäller rätten till ersättning för hälso- och sjukvård som tillhandahålls i andra medlemsstater och att garantera att de nödvändiga kraven för högkvalitativ, säker och effektiv hälso- och sjukvård är uppfyllda när det gäller gränsöverskridande vård.

4. En förutsättning för genomförandet av ett gränsöverskridande hälso- och sjukvårdssystem är att relevanta personuppgifter som rör patienternas hälsa (nedan kallade *hälsouppgifter*) kan utbytas mellan behöriga organisationer och yrkesverksamma på hälsoområdet i de olika medlemsstaterna. Dessa uppgifter anses vara känsliga och omfattas av strängare dataskyddsbestämmelser i enlighet med artikel 8 i direktiv 95/46/EG som rör särskilda kategorier av uppgifter.

Samråd med datatillsynsmannen

5. Datatillsynsmannen välkomnar att kommissionen samråder med honom om detta ärende och att det hänvisas till dessa samråd i förslagets ingress i enlighet med artikel 28 i förordning (EG) nr 45/2001.

6. Detta är första gången som samråd formellt har hållits med datatillsynsmannen om ett förslag till direktiv på hälso- och sjukvårdsområdet. Detta yttrande innehåller därför ett antal mer generella synpunkter på allmänna frågor som rör skydd av personuppgifter på hälso- och sjukvårdsområdet, vilka även kan vara tillämpliga på andra relevanta (bindande och icke-bindande) rättsliga instrument.

[1] KOM(2008) 414 slutlig. Det bör noteras att ett kompletterade meddelande om tillämpning av patienträttigheter vid gränsöverskridande hälso- och sjukvård (KOM(2008) 415 slutlig) också antogs samma dag. Eftersom meddelandet är av ganska allmän karaktär har datatillsynsmannen dock valt att inrikta sig på förslaget till direktiv.

7. Datatillsynsmannen vill redan från början uttrycka sitt stöd för initiativen för att förbättra villkoren för gränsöverskridande hälso- och sjukvård. Detta förslag bör betraktas som ett inslag i EG:s övergripande program för att förbättra medborgarnas hälsa i informationssamhället. Andra initiativ på detta område är kommissionens planerade direktiv och meddelande om donation av mänskliga organ och transplantation ([1]) rekommendationen om interoperabilitet för elektroniska patientjournalsystem ([2]) samt det planerade meddelandet om telemedicin ([3]). Datatillsynsmannen är emellertid bekymrad över att alla dessa initiativ inom närliggande områden inte är nära sammankopplade och/eller sammanlänkade när det gäller integritet och datasäkerhet, vilket hindrar fastställandet av en enhetlig strategi för dataskydd inom hälso- och sjukvård, särskilt i fråga om användning av ny informations- och kommunikationsteknik. I det föreliggande förslaget till direktiv nämns exempelvis telemedicin uttryckligen i skäl 10, men förslaget innehåller ingen hänvisning till dataskyddsdimensionen i det relevanta kommissionsmeddelandet. Fastän elektroniska patientjournaler är ett möjligt sätt att utbyta hälsouppgifter över gränserna finns det vidare ingen koppling till de integritetsfrågor som tas upp i den relevanta rekommendationen från kommissionen ([4]). Detta ger intrycket att ett övergripande integritetsperspektiv inom hälso- och sjukvård ännu inte är tydligt fastställt och i vissa fall helt saknas.

8. Samma sak gäller det föreliggande förslaget där dataskyddsaspekterna tyvärr inte tas upp på ett konkret sätt. Förslaget innehåller naturligtvis hänvisningar till dataskydd, men dessa är huvudsakligen av allmän karaktär och återspeglar inte i tillräcklig utsträckning de specifika behoven och kraven i fråga om integritet inom gränsöverskridande hälso- och sjukvård.

9. Datatillsynsmannen vill betona att en enhetlig och genomtänkt strategi för dataskydd i samtliga föreslagna instrument inom hälso- och sjukvårdsområdet inte enbart kommer att skydda medborgarnas grundläggande rätt till skydd av personuppgifter utan även kommer att bidra till vidareutvecklingen av gränsöverskridande hälso- och sjukvård.

II. DATASKYDD INOM GRÄNSÖVERSKRIDANDE HÄLSO- OCH SJUKVÅRD

Allmän bakgrund

10. Det främsta syftet med Europeiska gemenskapen har varit att upprätta en inre marknad, ett område utan inre gränser där fri rörlighet för varor, personer, tjänster och kapital garanteras. När det blev lättare för medborgarna att flytta till och vistas i andra medlemsstater än ursprungsstaten uppstod naturligtvis problem som rör hälso- och sjukvård. På 1990-talet behandlade därför domstolen, inom ramen för den inre marknaden, frågor om eventuell ersättning för sjukvårdskostnader som uppkommit i en annan medlemsstat. Domstolen erkände att friheten att tillhandahålla tjänster i enlighet med artikel 49 i EG-fördraget inbegriper friheten för personer att flytta till en annan medlemsstat för att erhålla sjukvård ([5]). Som en följd av detta kunde patienter som sökte gränsöverskridande sjukvård inte längre behandlas annorlunda än medborgare i deras ursprungsland som erhöll samma sjukvård utan att lämna landet.

11. Dessa domar ligger till grund för det föreliggande förslaget. Eftersom domstolens praxis grundar sig på enskilda fall är avsikten med förslaget att öka tydligheten i syfte att säkerställa en mer allmän och effektivare tillämpning av friheten att erhålla och tillhandahålla hälso- och sjukvårdstjänster. Men som nämns ovan utgör förslaget också en del av ett mer ambitiöst program för att förbättra medborgarnas hälsa i informationssamhället, där EU ser stora möjligheter att förbättra den gränsöverskridande hälso- och sjukvården genom användning av informationsteknik.

12. Av lättförklarliga skäl är fastställandet av regler för gränsöverskridande hälso- och sjukvård en känslig fråga. Det berör ett känsligt område där medlemsstaterna har inrättat olika nationella system, exempelvis när det gäller försäkringar och ersättningar för kostnader eller uppbyggnaden av hälso- och sjukvårdsinfrastrukturen, inklusive nätverk och tillämpningar för hälso- och sjukvårdsinformation. I det föreliggande förslaget inriktar sig gemenskapslagstiftaren enbart på *gränsöverskridande* hälso- och sjukvård, men bestämmelserna kommer åtminstone att påverka det sätt på vilket nationella hälso- och sjukvårdssystem organiseras.

13. Medborgarna kommer att kunna dra nytta av förbättrade villkor för gränsöverskridande hälso- och sjukvård. Samtidigt kommer det emellertid också att medföra vissa risker för medborgarna. Många praktiska problem som uppstår vid gränsöverskridande samarbete mellan människor som kommer från olika länder och talar olika språk måste lösas. Eftersom god hälsa är av yttersta vikt för varje medborgare måste varje risk för missförstånd och felaktigheter till följd av detta elimineras. Förbättrad gränsöverskridande hälso- och sjukvård i kombination med användning av den senaste informationstekniken får naturligtvis stora följder när

([1]) Tillkännages i kommissionens arbetsprogram.

([2]) Kommissionens rekommendation av den 2 juli 2008 om gränsöverskridande interoperabilitet för elektroniska patientjournalsystem (delgivet med nr K(2008) 3282), EUT L 190, 18.7.2008, s. 37.

([3]) Tillkännages i kommissionens arbetsprogram.

([4]) I detta sammanhang är det belysande att det inte finns någon hänvisning till integritet eller dataskydd i meddelandet i fotnot 1, vars syfte är att lägga fram en gemenskapsram för tillämpningen av patienträttigheter vid gränsöverskridande hälso- och sjukvård.

([5]) Se mål 158/96, *Kohll*, REG 1998 s. I-1931, punkt 34. Se bl.a. även mål C-157/99, *Smits och Peerbooms*, REG 2001, s. I-5473 och mål C-385/99, *Müller-Fauré och Van Riet*, REG 2003 s. I-12403.

det gäller skyddet av personuppgifter. Ett effektivare och därmed ökande utbyte av hälsouppgifter, det ökande avståndet mellan berörda personer och instanser och de olika nationella lagar genom vilka dataskyddsbestämmelserna genomförs leder till frågor om datasäkerhet och rättslig säkerhet.

Skydd av hälsouppgifter

14. Det måste betonas att hälsouppgifter anses vara en särskild kategori av uppgifter för vilka en högre skyddsnivå bör gälla. Europeiska domstolen för de mänskliga rättigheterna gjorde nyligen följande uttalande mot bakgrund av artikel 8 i den europeiska konventionen om de mänskliga rättigheterna: ”Skyddet av personuppgifter, särskilt hälsouppgifter, är av grundläggande betydelse för en persons åtnjutande av sin rätt till skydd för privat- och familjeliv i enlighet med artikel 8 i konventionen” ([1]). De strängare reglerna för behandling av hälsouppgifter enligt direktiv 95/46/EG förklaras nedan, men först följer en kort diskussion om begreppet ”hälsouppgifter”.

15. Direktiv 95/46/EG innehåller inte någon uttrycklig definition av hälsouppgifter. Allmänt tillämpas en bred tolkning där hälsouppgifter ofta definieras som ”personuppgifter som har ett tydligt och nära samband med beskrivningen av personens hälsotillstånd” ([2]). I detta sammanhang infattar hälsouppgifter vanligen medicinska uppgifter (t.ex. remisser och recept, rapporter om läkarundersökningar, laboratorietester, röntgenbilder osv.) samt administrativa och finansiella uppgifter som rör hälsa (t.ex. handlingar rörande sjukhusintagning, socialförsäkringsnummer, tider för läkarbesök, räkningar för tillhandahållande av vårdstjänster osv.) Det bör noteras att termen ”medicinska uppgifter” ([3]) ibland också avser uppgifter om hälsa, liksom termen ”sjukvårdsuppgifter” ([4]). I detta yttrande kommer begreppet ”hälsouppgifter” att användas.

16. En användbar definition av ”hälsouppgifter” finns i ISO 27799: ”alla uppgifter som rör en persons fysiska eller mentala hälsa eller tillhandahållandet av hälso- och sjukvårdstjänster till personen, vilket kan innefatta: a) uppgifter om registrering av personen för tillhandahållande av hälso- och sjukvårdstjänster, b) uppgifter om betalning för eller rätt till hälso- och sjukvård avseende personen i fråga, c) ett nummer, en symbol eller ett kännetecken som personen tilldelats för att identifiera denne för hälso- och sjukvårdsändamål, d) alla uppgifter om personen som insamlats i samband med tillhandahållande av hälso- och sjukvårdstjänster till denne, e) uppgifter som härrör från tester eller undersökning av en kroppsdel eller kroppssubstans, och f) identifiering av en person (verksam inom hälso- och sjukvården) som tillhandahållare av hälso- och sjukvård till personen”.

17. Datatillsynsmannen förordar bestämt att man ska fastställa en särskild definition för begreppet ”hälsouppgifter” i samband med det föreliggande förslaget, vilken i framtiden också skulle kunna användas i andra relevanta EG-rättsakter (se avsnitt III nedan).

18. I artikel 8 i direktiv 95/46/EG fastställs bestämmelser för behandling av särskilda kategorier av uppgifter. Dessa bestämmelser är strängare än de som gäller för behandling av andra uppgifter i enlighet med artikel 7 i direktiv 95/46/EG. Detta framgår redan när det i artikel 8.1 uttryckligen anges att medlemsstaten *ska förbjuda* behandling av bl.a. personuppgifter som rör hälsa. I efterföljande punkter i artikeln anges flera undantag från detta förbud, men dessa är mer begränsade än grunderna för behandling av normala uppgifter enligt artikel 7. Förbudet gäller exempelvis inte om den registrerade har lämnat sitt *uttryckliga* samtycke (artikel 8.2 a), i motsats till det *otvetydiga* samtycke som krävs i artikel 7 a i direktiv 95/46/EG. Dessutom kan det i medlemsstaternas lagstiftning fastställas att förbudet i vissa fall inte kan upphävas ens genom den registrerades samtycke. Artikel 8.3 gäller endast behandling av uppgifter som rör hälsa. Enligt denna punkt gäller förbudet i punkt 1 inte när behandlingen av uppgifterna är nödvändig med hänsyn till förebyggande hälso- och sjukvård, medicinska diagnoser, vård eller behandling eller administration av hälso- eller sjukvård eller när dessa uppgifter behandlas av någon som är yrkesmässigt verksam på hälso- och sjukvårdsområdet och som enligt nationell lagstiftning eller bestämmelser som antagits av behöriga nationella organ är underkastad tystnadsplikt eller av en annan person som är ålagd en liknande tystnadsplikt.

19. I artikel 8 i direktiv 95/46/EG betonas starkt att medlemsstaterna bör sörja för lämpliga eller tillräckliga skyddsåtgärder. Enligt artikel 8.4 får exempelvis medlemsstaterna besluta om andra undantag från förbudet mot behandling av känsliga uppgifter av hänsyn till ett viktigt allmänt intresse, men under förutsättning av lämpliga skyddsåtgärder. Detta understryker allmänt medlemsstaternas ansvar för att känsliga uppgifter, t.ex. uppgifter som rör hälsa, behandlas med särskild försiktighet.

Skydd för hälsouppgifter i gränsöverskridande situationer

Medlemsstaternas gemensamma ansvarsområden

20. Medlemsstaterna bör var särskilt medvetna om det ansvar som nämns ovan när det gäller frågan om gränsöverskridande utbyte av hälsouppgifter. Såsom anges ovan leder gränsöverskridande utbyte av hälsouppgifter till att risken för felaktig eller otillåten databehandling ökar. Detta kan

([1]) Se Europadomstolen, 17.7.2008, *I mot Finland* (ans. nr 20511/03), punkt 38.

([2]) Se arbetsgruppen för skydd av enskilda med avseende på behandlingen av personuppgifter, arbetsdokument om behandling av personuppgifter rörande hälsa i elektroniska patientjournaler, februari 2007, WP 131, punkt II.2. När det gäller den vida betydelsen av ”personuppgifter” se även arbetsgruppen för skydd av enskilda med avseende på behandlingen av personuppgifter, yttrande nr 4/2007 om begreppet personuppgifter, WP 136.

([3]) Europarådet, rekommendation nr R(97) 5 om skydd av medicinska uppgifter.

([4]) ISO 27799:2008 ”Hälso- och sjukvårdsinformatik – Ledningssystem för informationssäkerhet i hälso- och sjukvården baserat på ISO/IEC 27002”.

naturligtvis få enorma negativa konsekvenser för den registrerade. Både den medlemsstat där patienten är försäkrad och den behandlande medlemsstaten (där den gränsöverskridande vården faktiskt tillhandahålls) deltar i denna process och delar därför ansvaret.

21. Säkerheten för hälsouppgifter är i detta sammanhang en viktig fråga. I det mål som nämns ovan fäste Europeiska domstolen för de mänskliga rättigheterna särskild vikt vid hälsouppgifternas konfidentialitet: ”Respekten för hälsouppgifters konfidentialitet är en mycket viktig princip i de rättsliga systemen i alla länder som är parter i konventionen. Den är av avgörande betydelse inte enbart för patientens integritet utan även när det gäller att upprätthålla dennes förtroende för läkaryrket och hälso- och sjukvården i allmänhet” ([1]).

22. Dataskyddsbestämmelserna i direktiv 95/46/EG kräver dessutom att den medlemsstat där patienten är försäkrad ger patienten tillräcklig, korrekt och uppdaterad information om överföringen av dennes personuppgifter till en annan medlemsstat samt sörjer för säker överföring av uppgifterna till denna medlemsstat. Den behandlande medlemsstaten ska också sörja för säker mottagning av dessa uppgifter och för en lämplig skyddsnivå när uppgifterna faktiskt behandlas, i enlighet med dess nationella dataskyddslagstiftning.

23. Datatillsynsmannen föreslår att medlemsstaternas gemensamma ansvarsområden ska klargöras i förslaget, även med hänsyn till elektronisk datakommunikation, särskilt i samband med nya IKT-tillämpningar, såsom anges nedan.

Elektronisk överföring av hälsouppgifter

24. Det gränsöverskridande utbytet av hälsouppgifter förbättras främst genom användning av informationsteknik. Även om utbytet av uppgifter i ett gränsöverskridande hälso- och sjukvårdssystem fortfarande kan ske i pappersform (t.ex. när patienten flyttar till en annan medlemsstat och tar med sig alla relevanta hälsouppgifter som laboratorieresultat, remisser etc.) är avsikten helt klart att elektroniska metoder ska användas. Elektronisk överföring av hälsouppgifter kommer att stödjas av vårdinformationssystem som har upprättats (eller kommer att upprättas) i medlemsstaterna (på sjukhus, kliniker osv.) samt användning av ny teknik, som tillämpningar för elektroniska patientjournaler (eventuellt via Internet) och andra verktyg som hälsokort för patienter och läkare. Det är naturligtvis också möjligt att använda en kombination av pappersbaserat och elektroniskt utbyte, beroende på medlemsstaternas sjukvårdssystem.

25. Tillämpningar för e-hälsa och telemedicin, som omfattas av förslaget till direktiv, kommer att vara helt beroende av elektroniskt utbyte av hälsouppgifter (t.ex. vitalparametrar, bilder osv.), vanligen i kombination med andra befintliga elektroniska vårdinformationssystem i den behandlande medlemsstaten och den medlemsstat där patienten är försäkrad. Detta innefattar system som används både för utbyte mellan patient och läkare (t.ex. fjärrövervakning och fjärrdiagnostik) och för utbyte mellan läkare (t.ex. distanskonsultation mellan sjukvårdpersonal för expertråd om specifika sjukvårdsfall). Andra mer specifika sjukvårdstillämpningar som stöder gränsöverskridande tillhandahållande av hälso- och sjukvård i allmänhet kan även vara helt beroende av elektroniskt uppgiftsutbyte, t.ex. elektroniska recept (e-recept) eller elektroniska remisser (e-remiss), som redan har genomförts i vissa medlemsstater ([2]).

Områden av intresse när det gäller gränsöverskridande utbyte av hälsouppgifter

26. Med beaktande av ovannämnda faktorer, tillsammans med de nuvarande olikheterna i medlemsstaternas sjukvårdssystem och den tilltagande utvecklingen av e-hälsa, framträder följande två huvudsakliga områden av intresse när det gäller skydd av personuppgifter i samband med gränsöverskridande vård: a) de olika skyddsnivåer som kan tillämpas av medlemsstaterna för skydd av personuppgifter (i form av tekniska och organisatoriska åtgärder) och b) införlivande av integritet i e-hälsa, särskilt när det gäller ny utveckling. Även andra aspekter såsom sekundär användning av uppgifter om hälsa, särskilt när det gäller statistikproduktion, kan behöva särskild uppmärksamhet. Dessa frågor analyseras närmare i resten av detta avsnitt.

Datasäkerhet i medlemsstaterna

27. Trots att direktiven 95/46/EG och 2002/58/EG tillämpas på ett enhetligt sätt i Europa kan tolkningen och genomförandet av vissa inslag variera mellan länderna, särskilt när det gäller områden där de rättsliga bestämmelserna är allmänna och överlåts till medlemsstaterna. I detta avseende är säkerheten i behandlingen det viktigaste området, dvs. de åtgärder (tekniska och organisatoriska) som medlemsstaterna vidtar för att trygga hälsouppgifternas säkerhet.

([1]) Europadomstolen, 17.7.2008, *I mot Finland* (ans. nr 20511/03), punkt 38.

([2]) eHealth ERA Report, Towards the Establishment of a European eHealth Research Area, European Commission, Information Society and Media, March 2007, http://ec.europa.eu/information_society/activities/health/docs/policy/ehealth-era-full-report.pdf

28. Även om alla medlemsstater har ansvar för att hälsouppgifter strikt skyddas finns det för närvarande inte någon allmänt godtagen definition av ”lämplig” säkerhetsnivå när det gäller hälso- och sjukvård inom EU och som skulle kunna tillämpas i fråga om gränsöverskridande vård. Således kan ett sjukhus i en medlemsstat, enligt nationellt införda dataskyddsbestämmelser, vara skyldigt att vidta särskilda säkerhetsåtgärder (t.ex. att fastställa en säkerhetspolitik och etiska regler, särskilda bestämmelser för utläggande på entreprenad och anlitande av utomstående uppdragstagare, redovisningskrav etc), medan detta i andra medlemsstater kanske inte är fallet. Denna inkonsekvens kan ha inverkan på det gränsöverskridande informationsutbytet, särskilt när det sker i elektronisk form, eftersom man inte kan garantera att uppgifterna är säkrade (ur teknisk och organisatorisk synvinkel) på samma nivå mellan olika medlemsstater.

29. Det finns därför ett behov av att ytterligare harmonisera detta område och utforma en gemensam uppsättning säkerhetskrav när det gäller hälso- och sjukvård, vilka bör antas gemensamt av medlemsstaternas leverantörer av hälso- och sjukvårdstjänster. Detta behov är helt klart i linje med det övergripande behovet av att fastställa gemensamma principer i EU:s hälso-och sjukvårdssystem, vilket anges i förslaget.

30. Detta bör göras rent allmänt utan att ålägga medlemsstaterna några särskilda tekniska lösningar. Det bör dock fastställas en grund för ömsesidigt erkännande och godtagande, t.ex. när det gäller fastställande av säkerhetspolitik, identifiering och autentisering av patienter och vårdpersonal etc. Gällande europeiska och internationella standarder (t.ex. ISO och CEN) när det gäller vård och säkerhet, liksom allmänt accepterade och rättsligt grundade tekniska begrepp (t.ex. elektroniska signaturer [1]) skulle kunna användas som en färdplan i ett sådant försök.

31. Datatillsynsmannen stöder idén om harmonisering av säkerheten när det gäller hälso- och sjukvård på gemenskapsnivå och anser att kommissionen, redan inom ramen för det aktuella förslaget, bör ta relevanta initiativ (se avsnitt III nedan).

Integritet i tillämpningar för e-hälsa

32. Integritet och säkerhet bör utgöra en del av utformningen och genomförandet av alla vårdssystem, och särskilt när det gäller e-hälsa såsom nämns i detta förslag (inbyggda skyddsmekanismer). Detta odiskutabla krav har redan fått stöd i andra relevanta policydokument [2], såväl allmänna som vårdspecifika [3].

33. I samband med den kompatibilitet för e-hälsa som diskuteras i förslaget bör begreppet ”inbyggda skyddsmekanismer” återigen framhävas som en grund för all planerad utveckling. Detta begrepp gäller för flera olika nivåer: organisatorisk, semantisk och teknisk nivå.

— På organisatorisk nivå bör integritet beaktas när man fastställer de nödvändiga förfarandena för utbyte av hälsouppgifter mellan medlemsstaternas vårdsystem. Detta kan ha direkt inverkan på typen av utbyte och omfatta vilka uppgifter som överförs (t.ex. användning av identifikationsnummer i stället för patienternas verkliga namn när detta är möjligt).

— På semantisk nivå bör krav på integritet och säkerhet införlivas i nya standarder och system, t.ex. vid utformningen av en elektronisk mall för recept när detta diskuteras i förslaget. Detta kan bygga på befintliga tekniska standarder på området, t.ex. standarder för datakonfidentialitet och digital signatur, och behandla vårdspecifika behov såsom rollbaserad autentisering av kvalificerad vårdpersonal.

— På teknisk nivå bör systemarkitektur och användartillämpningar anpassas till integritetsfrämjande teknik och genomföra ovannämnda semantiska definition.

34. Datatillsynsmannen anser att elektroniska recept skulle kunna utgöra utgångspunkten för att införliva integritets- och säkerhetskrav från och med det inledande utvecklingsstadiet (se avsnitt III nedan).

Övriga aspekter

35. Ytterligare en aspekt som skulle kunna övervägas inom ramen för gränsöverskridande utbyte av hälsouppgifter är sekundär användning av hälsouppgifter och i synnerhet användning av uppgifter för statistiska ändamål, såsom redan fastställs i det nuvarande förslaget.

36. Som tidigare nämnts i punkt 18 föreskrivs det i artikel 8.4 i direktiv 95/46 en möjlighet till sekundär användning av hälsouppgifter. Denna ytterligare behandling får dock endast göras av hänsyn till ett ”viktigt allmänt intresse” och ska vara föremål för ”lämpliga skyddsåtgärder” som föreskrivs i nationell lag eller efter beslut av tillsynsmyndigheten [4]. I händelse av statistisk uppgiftsbehandling uppstår det, vilket också nämns i datatillsynsmannens yttrande

[1] Europaparlamentets och rådets direktiv 1999/93/EG av den 13 december 1999 om ett gemenskapsramverk för elektroniska signaturer (EGT L 13, 19.1.2000, s. 12–20).

[2] Datatillsynsmannen och EU:s forskning och tekniska utveckling, policydokument, Datatillsynsmannen, April 2008, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/08-04-28_PP_RTD_EN.pdf

[3] Kommissionens rekommendation av den 2 juli 2008 om gränsöverskridande interoperabilitet för elektroniska patientjournalsystem (delgivet med nr K(2008) 3282), EUT L 190, 18.7.2008, s. 37.

[4] Se även skäl 34 i direktiv 95/46. När det gäller denna fråga, se även yttrande 29 om elektroniska hälsouppgifter från arbetsgruppen och som omnäms ovan i fotnot 8, sid. 16.

om förslaget till förordning om gemenskapsstatistik om folkhälsa och hälsa och säkerhet i arbetet ([1]), dessutom ytterligare en risk på grund av de olika innebörder som begreppen ”sekretess” och ”uppgiftsskydd” kan ha vid tillämpningen av dataskyddslagstiftningen å ena sidan och lagstiftningen om statistik å andra sidan.

37. Datatillsynsmannen vill framhäva ovanstående faktorer i samband med det aktuella förslaget. Det bör införas mer uttryckliga hänvisningar till dataskyddskraven om senare användning av hälsouppgifter (se avsnitt III nedan).

III. NÄRMARE ANALYS AV FÖRSLAGET

Förslagets bestämmelser om dataskydd

38. Förslaget innehåller ett antal hänvisningar till dataskydd och integritet i följande delar av dokumentet:

— I skäl 3 anges det bl.a. att direktivet måste genomföras och tillämpas med vederbörlig respekt för rätten till privat- och familjeliv och skydd av personuppgifter.

— I skäl 11 hänvisas det till den grundläggande rätten till personlig integritet vid behandling av personuppgifter och konfidentialitet som två av de operativa principer som är gemensamma för hälso- och sjukvårdssystemen i hela gemenskapen.

— I skäl 17 beskrivs rätten till skydd av personuppgifter för enskilda personer som en grundläggande rättighet som bör skyddas, och inriktas särskilt på den enskildes rätt till tillgång till hälsouppgifter, även i samband med gränsöverskridande hälso- och sjukvård, eftersom detta fastställs i direktiv 95/46/EG.

— I artikel 3, där förhållandet mellan direktivet och andra gemenskapsbestämmelser anges, hänvisas det i punkt 1a till direktiven 95/46/EG och 2002/58/EG.

— I artikel 5 om den behandlande medlemsstatens ansvar fastställs det i led 1f att skyddet av rätten till integritet omfattas av detta ansvar i överensstämmelse med nationella åtgärder för genomförande av direktiven 95/46/EG och 2002/58/EG.

— I artikel 6 om hälso- och sjukvård i en annan medlemsstat betonas det i punkt 5 att patienter har rätt till tillgång till sina patientjournaler när de reser till en annan medlemsstat för att få vård där eller för att söka vård som ges i en annan medlemsstat, återigen i överensstämmelse med nationella åtgärder för genomförande av direktiven 95/46/EG och 2002/58/EG.

— I artikel 12 om nationella kontaktpunkter för gränsöverskridande hälso- och sjukvård anges det i punkt 2 a att dessa kontaktpunkter bland annat ska ansvara för att ta fram och sprida information till patienter om de garantier för skydd av personuppgifter som ges i en annan medlemsstat.

— I artikel 16 om e-hälsa fastställs det att åtgärder för att uppnå driftskompatibilitet mellan systemen för informations- och kommunikationsteknik ska respektera den grundläggande rätten till skydd av personuppgifter i enlighet med tillämplig lag.

— Slutligen fastställs det i artikel 18.1 bl.a. att insamling av uppgifter för statistik- och övervakningsändamål ska ske i enlighet med nationell lagstiftning och gemenskapslagstiftning om skydd av personuppgifter.

39. Datatillsynsmannen välkomnar att uppgiftsskydd beaktades när förslaget utformades och att det har gjorts försök att påvisa det övergripande behovet av integritet i samband med gränsöverskridande hälso-och sjukvård. De befintliga bestämmelserna i förslaget om uppgiftsskydd är dock antingen för allmänna eller hänvisar till medlemsstaternas ansvar på ett ganska selektivt och uppsplittrat sätt:

— Skälen 3 och 11 berör, tillsammans med artiklarna 3.1 a, 16 och 18.1, i praktiken den allmänna rättsliga ramen för dataskydd (de två sista i samband med e-hälsa och insamling av statistisk men utan att det fastställs några särskilda krav i fråga om integritet).

— När det gäller medlemsstaternas ansvar görs det en allmän hänvisning i artikel 5.1 f.

— I skäl 17 och artikel 6.5 görs det en mer specifik hänvisning till patienternas rätt till tillgång i den behandlande medlemsstaten.

— Artikel 12.2 a innehåller slutligen en bestämmelse om patientens rätt till information i den medlemsstat där patienten är försäkrad (genom de nationella kontaktpunkternas försorg).

Såsom redan nämnts i inledningen i detta yttrande finns det dessutom inte någon koppling och/eller hänvisning till de integritetsaspekter som tas upp i andra (bindande eller icke bindande) gemenskapsrättsakter i fråga om hälso- och sjukvård, särskilt när det gäller användning av nya IKT-tillämpningar (t.ex. telemedicin eller elektroniska patientjournaler).

([1]) EUT C 295, 7.12.2007, s. 1.

40. Trots att integritet i allmänhet anges som ett krav för gränsöverskridande hälso- och sjukvård saknas det sålunda fortfarande en övergripande bild, både i fråga om medlemsstaternas skyldigheter och de särdrag som införs till följd av vårdtjänsternas gränsöverskridande karaktär (i motsats till nationella vårdtjänster). Närmare bestämt:

— Medlemsstaternas ansvar presenteras inte på något samlat sätt eftersom vissa skyldigheter (rätten till tillgång och information) ges en framträdande plats – dock i olika delar av förslaget – medan andra, såsom behandlingens säkerhet, utelämnas helt.

— Det görs inte någon hänvisning till problemet med medlemsstaternas olikartade säkerhetsåtgärder och behovet av en harmonisering på gemenskapsnivå av hälsouppgifternas säkerhet, inom ramen för den gränsöverskridande hälso- och sjukvården.

— Det görs inte någon hänvisning till införlivande av integritet i tillämpningar för e-hälsa. Inte heller när det gäller e-recept avspeglas detta.

41. Artikel 18, som handlar om insamling av uppgifter för statistik- och övervakningsändamål, ger dessutom anledning till särskilda farhågor. I punkt 1 hänvisas det till ”statistiska *och andra kompletterande uppgifter*”. Vidare hänvisas det i pluralis till ”övervakningsändamål” och därefter förtecknas de områden som omfattas av dessa övervakningsändamål, nämligen tillhandahållande av gränsöverskridande hälso- och sjukvård, den vård som givits, uppgifter om vårdgivare och patienter samt kostnader och resultat. I detta, redan mycket oklara, sammanhang görs det en allmän hänvisning till dataskyddslagstiftningen men det fastställs inte några särskilda krav för senare användning av hälsouppgifter enligt artikel 8.4 i direktiv 95/46/EG. Punkt 2 innehåller dessutom en ovillkorlig skyldighet att överföra stora mängder uppgifter till kommissionen minst en gång om året. Eftersom det inte uttryckligen hänvisas till någon bedömning av huruvida denna överföring är nödvändig verkar det som om gemenskapslagstiftaren själv redan har fastställt att dessa överföringar till kommissionen är nödvändiga.

Datatillsynsmannens rekommendationer

42. För att på ett lämpligt sätt ta itu med ovan nämnda faktorer ger datatillsynsmannens ett antal rekommendationer i form av fem grundläggande steg för ändringar, enligt nedanstående.

Steg 1 – Definition av hälsouppgifter

43. I artikel 4 definieras de grundläggande termer som används i förslaget. Datatillsynsmannen rekommenderar starkt att en definition av hälsouppgifter införs i denna artikel. Det bör tillämpas en bred tolkning av hälsouppgifter, i likhet med den som beskrivs i avsnitt II i detta yttrande (punkterna 14 och 15).

Steg 2 – Införande av en särskild artikel om dataskydd

44. Datatillsynsmannen rekommenderar också starkt att det införs en särskild artikel om dataskydd i förslaget där de övergripande aspekterna på integritet kan fastställas på ett klart och begripligt sätt. Man bör i denna artikel a) beskriva ansvaret för den medlemsstat där patienten är försäkrad respektive ansvaret för den behandlande medlemsstaten, bland annat behovet av behandlingssäkerhet, och b) fastställa de viktigaste områdena för vidareutveckling, dvs. harmonisering av säkerheten och införlivande av integritet i e-hälsa. För dessa frågor kan det fastställas särskilda bestämmelser (i den föreslagna artikeln), såsom anges i stegen 3 och 4 nedan.

Steg 3 – Särskilda bestämmelser om harmonisering av säkerheten

45. Efter ändringen i steg 2 rekommenderar datatillsynsmannen att kommissionen antar en mekanism för fastställande av en allmänt godtagbar skyddsnivå för hälsouppgifter på nationell nivå, med beaktande av befintliga tekniska standarder på området. Detta bör återspeglas i förslaget. Ett tänkbart genomförande skulle kunna vara att utnyttja kommittéförfarandet eftersom detta redan anges i artikel 19 och gäller för andra delar av förslaget. Även kompletterande instrument skulle kunna användas för att utarbeta relevanta riktlinjer där alla berörda aktörer deltar, t.ex. arbetsgruppen för skydd av enskilda med avseende på behandlingen av personuppgifter och datatillsynsmannen.

Steg 4 – Införlivande av integritet i modellen för e-recept

46. I artikel 14 om erkännande av recept som utfärdas i en annan medlemsstat föreskrivs det att en EU-modell för recept ska utvecklas för att främja att e-recept blir kompatibla. Denna åtgärd ska antas genom kommittéförfarande eftersom detta fastställs i artikel 19.2 i förslaget.

47. Datatillsynsmannen rekommenderar att den föreslagna EU-modellen för recept ska inbegripa integritet och säkerhet, även i den mycket grundläggande semantiska definitionen av modellen. Detta bör uttryckligen anges i artikel 14.2 a. Återigen är medverkan av alla berörda aktörer av stor betydelse. I detta avseende vill datatillsynsmannen bli informerad om och delta i ytterligare åtgärder när det gäller denna fråga genom det föreslagna kommittéförfarandet.

Steg 5 – Senare användning av hälsouppgifter för statistik- och övervakningsändamål

48. För att undvika missförstånd önskar datatillsynsmannen att begreppet ”andra kompletterande uppgifter” i artikel 18.1 klargörs. Artikeln ska dessutom ändras så att den mer uttryckligen hänvisar till kraven när det gäller senare användning av hälsouppgifter i enlighet med artikel 8.4 i direktiv 95/46/EG. Skyldigheten i andra stycket att överföra alla uppgifter till kommissionen bör dessutom underställas en bedömning av behovet av sådana överföringar för lagliga ändamål som vederbörligen anges i förväg.

IV. **SLUTSATSER**

49. Datatillsynsmannen uttrycker sitt stöd för initiativen för att förbättra villkoren för gränsöverskridande hälso- och sjukvård, men är emellertid bekymrad över att initiativ kopplade till hälso- och sjukvård i gemenskapen inte alltid är väl samordnade när det gäller användning av informations- och kommunikationsteknik, integritet och säkerhet, vilket hindrar att man inför en enhetlig strategi för dataskydd inom hälso- och sjukvård.

50. Datatillsynsmannen välkomnar hänvisningen till integritet i det föreliggande förslaget. Det krävs emellertid ett antal ändringar vilka förklaras i avsnitt III i detta yttrande i syfte att fastställa tydliga krav, såväl för den behandlande medlemsstaten som för medlemsstaten där patienten är försäkrad, samt att man på lämpligt sätt behandlar frågan om dataskydd i samband med gränsöverskridande vård.

— Det bör i artikel 4 införas en definition av hälsouppgifter, vilken omfattar alla personuppgifter som har ett tydligt och nära samband med beskrivningen av personens hälsotillstånd. Detta bör i princip inbegripa medicinska uppgifter samt administrativa och finansiella uppgifter som rör hälsa.

— Införandet av en särskild artikel om dataskydd rekommenderas starkt. Denna artikel bör ge en tydlig och övergripande bild och beskriva ansvaret för den medlemsstat där patienten är försäkrad respektive ansvaret för den behandlande medlemsstaten samt fastställa de viktigaste områdena för vidareutveckling, dvs. harmonisering av säkerhet och införlivande av integritet, särskilt när det gäller tillämpningar för e-hälsa.

— Kommissionen rekommenderas att inom ramen för detta förslag anta en mekanism för fastställande av en allmänt godtagbar skyddsnivå för hälsouppgifter på nationell nivå, med beaktande av befintliga tekniska standarder på området. Ytterligare och/eller kompletterande initiativ med deltagande av alla berörda aktörer, arbetsgruppen för skydd av enskilda med avseende på behandlingen av personuppgifter och datatillsynsmannen, bör även främjas.

— Det rekommenderas att begreppet ”inbyggda skyddsmekanismer” införs i förslaget om en EU-modell för e-recept (även på semantisk nivå). Detta bör uttryckligen anges i artikel 14.2 a. Datatillsynsmannen vill bli informerad om och delta i ytterligare åtgärder när det gäller denna fråga genom det föreslagna kommittéförfarandet.

— Det rekommenderas att formuleringen preciseras i artikel 18 och att det görs en mer uttrycklig hänvisning till de särskilda krav som gäller för senare användning av uppgifter som rör hälsa i enlighet med artikel 8.4 i direktiv 95/46/EG.

Utfärdat i Bryssel den 2 december 2008.

Peter HUSTINX

Europeiska datatillsynsmannen

Andra yttrandet från Europeiska datatillsynsmannen om översynen av direktiv 2002/58/EG om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktivet om integritet och elektronisk kommunikation).

(2009/C 128/04)

EUROPEISKA DATATILLSYNSMANNEN HAR ANTAGIT DETTA YTTRANDE

med beaktande av fördraget om upprättandet av Europeiska gemenskapen, särskilt artikel 286,

med beaktande av Europeiska unionens stadga om de grundläggande rättigheterna, särskilt artikel 8,

med beaktande av Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter,

med beaktande av Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation,

med beaktande av Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter, särskilt artikel 41.

HÄRIGENOM FRAMFÖRS FÖLJANDE.

I. INLEDNING

Bakgrund

1. Den 13 november 2007 antog Europeiska kommissionen ett förslag om ändring av bland annat direktivet om integritet och elektronisk kommunikation [1] (nedan kallat *förslaget* eller *kommissionens förslag*). Den 10 april 2008 antog Europeiska datatillsynsmannen ett yttrande om kommissionens förslag i vilket han lade fram rekommendationer för att förbättra förslaget i ett försök att bidra till att säkerställa att de föreslagna ändringarna leder till bästa möjliga skydd för enskildas integritet och personuppgifter (*datatillsynsmannens första yttrande*) [2].

2. Europeiska datatillsynsmannen välkomnade det föreslagna inrättandet av ett system för obligatoriska anmälningar av säkerhetsöverträdelser enligt vilket företag är skyldiga att meddela enskilda personer när deras personuppgifter har äventyrats. Vidare lovordade han även den nya bestämmelse som ska göra det möjligt för juridiska personer (t.ex. konsumentorganisationer och Internetleverantörer) att vidta åtgärder mot personer som ägnar sig åt att skicka elektronisk skräppost och ytterligare komplettera de befintliga verktygen för att bekämpa skräppost.

3. Under de parlamentsdiskussioner som föregick Europaparlamentets första behandling tillhandahöll datatillsynsmannen ytterligare råd genom att kommentera utvalda frågor som hade kommit upp i rapporterna från de av Europaparlamentets utskott som är behöriga när det gäller översynen av direktivet om samhällsomfattande tjänster [3] och direktivet om integritet och elektronisk kommunikation (*kommentarer*) [4]. Dessa kommentarer tog i första hand upp frågor I samband med behandling av trafikuppgifter och skydd av immateriella rättigheter.

4. Den 24 september 2008 antog Europaparlamentet (*parlamentet*) en lagstiftningsresolution om direktivet om integritet och elektronisk kommunikation (*första behandlingen*) [5]. Datatillsynsmannen såg positivt på flera av parlamentets ändringsförslag som antogs efter datatillsynsmannens ovan nämnda yttrande och kommentarer. Bland de viktiga ändringarna återfanns införandet av

[1] Översynen av direktivet om integritet och elektronisk kommunikation utgör en del av en vidare översynsprocess vars syfte är att inrätta en europeisk telekommyndighet, att se över direktiven 2002/21/EG, 2002/19/EG, 2002/20/EG, 2002/22/EG och 2002/58/EG samt förordning (EG) nr 2006/2004 (nedan tillsammans kallade *översynen av telekompaketet*).

[2] Yttrande av den 10 april 2008 om förslaget till direktiv om ändring av bland annat direktiv 2002/58/EG om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation), EUT C 181, 18.7.2008, s. 1.

[3] Direktiv 2002/22/EG om samhällsomfattande tjänster och användares rättigheter avseende elektroniska kommunikationsnät och kommunikationstjänster (direktivet om samhällsomfattande tjänster), EGT L 108, 24.4.2002 s. 51.

[4] Datatillsynsmannens kommentarer om valda frågor som kommit upp i rapporten från IMCO-utskottet om översynen av direktiv 2002/22/EG (direktivet om samhällsomfattande tjänster) och direktiv 2002/58/EG (direktivet om integritet och elektronisk kommunikation), den 2 september 2008. Återfinns på följande webbplats: www.edps.europa.eu

[5] Europaparlamentets lagstiftningsresolution av den 24 september 2008 om förslaget till Europaparlamentets och rådets direktiv om ändring av direktiv 2002/22/EG om samhällsomfattande tjänster och användares rättigheter avseende elektroniska kommunikationsnät och kommunikationstjänster, direktiv 2002/58/EG om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation och förordning (EG) nr 2006/2004 om konsumentskyddssamarbete (KOM(2007) 698 – C6-0420/2007 – 2007/0248(COD).

leverantörer av informationssamhällets tjänster (dvs. företag som tillhandahåller tjänster till konsumenter på Internet) i tillämpningsområdet för skyldigheten att anmäla säkerhetsöverträdelse. Datatillsynsmannen välkomnade även den ändring som gör det möjligt för juridiska och fysiska personer att vidta rättsliga åtgärder mot överträdelser av alla bestämmelser i direktivet om integritet och elektronisk kommunikation (och inte bara för överträdelse av bestämmelser om skräppost vilket ursprungligen föreslogs i kommissionens förslag). Efter parlamentets första behandling antog kommissionen sitt ändrade förslag till direktiv om integritet och elektronisk kommunikation (nedan kallat *det ändrade förslaget*) ([6]).

5. Den 27 november 2008 nådde rådet en politisk överenskommelse om en översyn av bestämmelserna i telekompaketet, inbegripet direktivet om integritet och elektronisk kommunikation, vilket kommer att utgöra rådets gemensamma ståndpunkt (*den gemensamma ståndpunkten*) ([7]). Den gemensamma ståndpunkten kommer att delges parlamentet i enlighet med artikel 251.2 i fördraget om upprättandet av Europeiska gemenskapen, vilket kan medföra ändringsförslag från parlamentet.

Allmänna kommentarer om rådets ståndpunkt

6. Rådet ändrade väsentliga delar i förslaget och godkände inte många av de ändringar som hade antagits av parlamentet. Även om den gemensamma ståndpunkten visserligen innehåller positiva inslag är datatillsynsmannen överlag bekymrad över dess innehåll, särskilt eftersom den gemensamma ståndpunkten inte inbegriper några av de positiva ändringar som föreslagits av parlamentet, i det ändrade förslaget, i datatillsynsmannens yttranden eller av de europeiska dataskyddsmyndigheterna inom artikel 29-gruppen ([8]).

7. I stället har bestämmelser i det ändrade förslaget och parlamentets ändringar som ger skydd åt medborgarna i ganska många fall strukits eller väsentligen urvattnats. Detta leder till att den skyddsnivå som tillförsäkras enskilda personer i den gemensamma ståndpunkten i hög grad har luckrats upp. Därför utfärdar datatillsynsmannen nu ett andra yttrande i förhoppningen att nya ändringar kommer att antas som återställer garantierna för uppgiftsskydd när direktivet om integritet och elektronisk kommunikation passerar genom lagstiftningsförfarandet.

8. I detta andra yttrande ligger tyngdpunkten på några väsentliga farhågor och alla punkter i datatillsynsmannens första yttrande upprepas inte, men alla är fortsatt giltiga. I detta yttrande tas följande punkter upp till diskussion:

— Bestämmelserna om anmälan av säkerhetsöverträdelser.

— Tillämpningsområdet för direktivet om integritet och elektronisk kommunikation när det gäller privata nät och allmänt tillgängliga privata nät.

— Behandlingen av trafikuppgifter för säkerhetsändamål.

— Möjligheten för juridiska personer att vidta åtgärder mot överträdelse av direktivet om integritet och elektronisk kommunikation.

9. Genom att ta upp de ovan nämnda frågorna analyserar datatillsynsmannen i detta yttrande rådets gemensamma ståndpunkt och jämför den med parlamentets första behandling och kommissionens ändrade förslag. I yttrandet ingår rekommendationer i syfte att göra bestämmelserna i direktivet om integritet och elektronisk kommunikation enklare och att säkerställa att direktivet även i fortsättningen skyddar enskilda personers privatliv och personuppgifter.

II. BESTÄMMELSERNA OM ANMÄLAN AV SÄKERHETSÖVERTRÄDELSER

10. Datatillsynsmannen stöder ett antagande av ett system för anmälan av säkerhetsöverträdelser enligt vilket myndigheter och enskilda personer kommer att informeras när deras personuppgifter har äventyrats ([9]). Anmälningar av säkerhetsöverträdelser kan hjälpa enskilda personer att vidta de åtgärder som behövs för att mildra eventuell skada till följd av detta äventyrande. Skyldigheten att skicka meddelanden om säkerhetsöverträdelser kommer att uppmuntra företagen att förbättra sin datasäkerhet och förstärka deras ansvarighet när det gäller de personuppgifter de ansvarar för.

11. Kommissionens ändrade förslag, Europaparlamentets första behandling och rådets gemensamma ståndpunkt utgör tre olika förhållningssätt till den anmälning av säkerhetsöverträdelser som för närvarande behandlas. Vart och ett av de tre förhållningssätten har sina positiva aspekter. Datatillsynsmannen anser dock att det finns utrymme för förbättringar när det gäller vart och ett av förhållningssätten och förordar att man beaktar de rekommendationer som beskrivs nedan när man överväger de avslutande stegen inför antagandet av ett system för anmälan av säkerhetsöverträdelser.

([6]) Ändrat förslag till Europaparlamentets och rådets direktiv om ändring av direktiv 2002/22/EG om samhällsomfattande tjänster och användares rättigheter avseende elektroniska kommunikationsnät och kommunikationstjänster, direktiv 2002/58/EG om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation och förordning (EG) nr 2006/2004 om konsumentskyddssamarbete, Bryssel, 6.11.2008 KOM(2008) 723 slutlig.

([7]) Återfinns på rådets offentliga webbplats.

([8]) Yttrande 2/2008 om översynen av direktiv 2002/58/EG om integritet och elektronisk kommunikation (direktivet om integritet och elektronisk kommunikation) som är tillgängligt på artikel 29-gruppens webbplats.

([9]) I detta yttrande används ordet *äventyrats* för att beteckna varje personuppgiftsöverträdelse som har inträffat till följd av en oavsiktlig eller olaglig förstörelse, förlust, ändring eller ett inte auktoriserat avslöjande av eller tillgång till personuppgifter som överförts, lagrats eller på annat sätt behandlats.

12. Vid analysen av de tre systemen för anmälan av säkerhetsöverträdelser finns det fem kritiska punkter som måste övervägas: *i)* definitionen av säkerhetsöverträdelse, *ii)* de enheter som ska omfattas av skyldigheten att göra anmälan (*omfattade enheter*), *iii)* den norm som utlöser skyldigheten att göra anmälan, *iv)* identifieringen av den enhet som ansvarar för fastställandet av huruvida en säkerhetsöverträdelse uppfyller denna norm eller inte, samt *v)* mottagarna av anmälan.

Översikt över kommissionens, rådets och Europaparlamentets synsätt

13. Europaparlamentet, kommissionen och rådet har alla intagit olika synsätt till anmälningar av säkerhetsöverträdelser. I parlamentets första behandling ändrades det ursprungliga systemet för anmälan av säkerhetsöverträdelser som hade lagts fram i kommissionens förslag ([10]). Enligt parlamentets synsätt ska skyldigheten att göra anmälan inte endast gälla leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster utan även leverantörer av informationssamhällets tjänster. Enligt detta synsätt måste dessutom alla personuppgiftsöverträdelser meddelas den nationella regleringsmyndigheten eller de behöriga myndigheterna (tillsammans *myndigheterna*). Om myndigheterna skulle komma fram till att överträdelsen är *allvarlig* skulle de kräva att leverantörerna av allmänt tillgängliga elektroniska kommunikationstjänster och leverantörerna av informationssamhällets tjänster utan dröjsmål underrättar den berörda personen. Vid överträdelser som innebär ett överhängande och direkt hot skulle leverantörerna av allmänt tillgängliga elektroniska kommunikationstjänster och leverantörerna av informationssamhällets tjänster underrätta personerna innan de meddelar myndigheterna och inte invänta något rättsligt avgörande. Ett undantag från skyldigheten att meddela konsumenter gäller sådana enheter som kan bevisa för myndigheterna att *"lämpliga tekniska skyddsåtgärder har tillämpats"* som gör uppgifterna oläsbara för alla personer som inte är behöriga att få tillgång till dessa.

14. Enligt rådets synsätt måste även anmälan lämnas både till abonnenterna och myndigheterna, men endast när *den enhet som omfattas* bedömer att överträdelsen utgör en *allvarlig risk* för intrång i abonnentens privatliv (*dvs.* identitetsstöld eller identitetsbedrägeri, personskada, betydande förnedring eller skadat rykte).

15. I kommissionens ändrade förslag bibehålls parlamentets skyldighet att meddela myndigheterna alla överträdelser. I motsats till parlamentets synsätt ingår det emellertid ett undantag från anmälningsskyldigheten i det ändrade förslaget när det gäller de berörda personerna där leverantörer av offentliga elektroniska kommunikationstjänster visar den behöriga myndigheten att, i) ingen skada (dvs. ekonomisk förlust eller social skada eller identitetsstöld) *sannolikt kommer att uppstå* på grund av överträdelsen eller att, *ii) lämpliga tekniska skyddsåtgärder* har tillämpats på de uppgifter som berörts av säkerhetsöverträdelsen. I kommissionens synsätt ingår sålunda en skadebaserad analys i samband med enskilda anmälningar.

([10]) Särskilt i parlamentets ändringar 187, 124127 samt 27, 21 och 32 behandlas denna fråga.

16. Det är viktigt att notera att det enligt parlamentets ([11]) och kommissionens synsätt är *myndigheterna* som i sista hand har ansvar för att avgöra huruvida överträdelsen är allvarlig eller rimligen kan komma att förorsaka skada. Däremot ska beslutet enligt rådets synsätt överlåtas åt de *berörda enheterna*.

17. Både rådets och kommissionens upplägg gäller enbart leverantörer av offentliga elektroniska kommunikationstjänster och inte leverantörer av informationssamhällets tjänster, vilket är fallet i parlamentets synsätt.

Definitionen av en säkerhetsöverträdelse

18. Datatillsynsmannen konstaterar med tillfredsställelse att de tre lagförslagen innehåller samma definition av anmälan av säkerhetsöverträdelse, vilken beskrivs som *"säkerhetsöverträdelse som leder till en oavsiktlig eller olaglig förstörelse, förlust, ändring eller ett inte auktoriserat avslöjande av eller tillgång till personuppgifter som överförts, lagrats eller på annat sätt behandlats [...]"* ([12]).

19. Som framgår av beskrivningen nedan är denna definition välkommen eftersom den är tillräckligt bred för att inbegripa de flesta relevanta situationer där anmälningar av säkerhetsöverträdelser eventuellt är motiverade.

20. För det första omfattas situationer när en *inte auktoriserad tillgång* till personuppgifter av tredje part har ägt rum, till exempel ett intrång i en server som innehåller personuppgifter och inhämtning av sådana uppgifter.

21. För det andra skulle denna definition även inbegripa situationer där en förlust eller ett avslöjande av personuppgifter har ägt rum, medan en inte auktoriserad tillgång ännu inte har kunnat påvisas. Detta skulle inbegripa situationer där personuppgifterna eventuellt har förlorats (t.ex. cd-romskivor, USB-minnen eller andra bärbara anordningar) eller gjorts allmänt tillgängliga av vanliga användare (en datafil om anställda som av misstag och tillfälligt gjorts tillgänglig på ett allmänt tillgängligt område via Internet). Eftersom det ofta inte finns något som talar för eller emot att sådana uppgifter vid en viss tidpunkt kan vara tillgängliga för eller användas av icke-auktoriserade tredje parter verkar det lämpligt att inbegripa dessa instanser så att de omfattas av definitionen. Europeiska datatillsynsmannen rekommenderar därför att man bibehåller denna definition. Datatillsynsmannen rekommenderar även ett införlivande av definitionen av säkerhetsöverträdelse i artikel 2 i direktivet om integritet och elektronisk kommunikation, eftersom detta skulle stämma bättre överens med direktivets allmänna struktur och ge större klarhet.

([11]) Utom för överträdelser som innebär ett överhängande och direkt hot då de enheter som omfattas först måste underrätta konsumenterna.

([12]) Artikel 2 i) i den gemensamma ståndpunkten och det ändrade förslaget och artikel 3.3 i parlamentets första behandling.

Enheter som bör omfattas av skyldigheten att göra anmälan

22. Skyldigheten att göra anmälan enligt parlamentets upplägg gäller både leverantörerna av allmänt tillgängliga elektroniska kommunikationstjänster och leverantörerna av informationssamhällets tjänster. Enligt rådets och kommissionens system kommer endast leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster, t.ex. telekommunikationsföretag och Internetleverantörer vara skyldiga att meddela enskilda personer när de utsatts för säkerhetsöverträdelser som leder till att deras personuppgifter äventyras. Övriga verksamhetssektorer, till exempel Internetbanker, onlineåterförsäljare, leverantörer av hälso- och sjukvård via Internet och andra är inte bundna av denna skyldighet. Av de skäl som närmare anges nedan anser datatillsynsmannen att det av allmänna policyskäl är av central betydelse att se till att informationssamhällets tjänster, vilka omfattar Internetbanker, Internetföretag, leverantörer av hälso- och sjukvård via Internet osv. även omfattas av skyldigheten att göra anmälan.

23. För det första noterar datatillsynsmannen att även om telekomföretag definitivt utgör mål för säkerhetsöverträdelser som motiverar en anmälningsskyldighet gäller detta även för andra former av företag/leverantörer. Det är lika sannolikt att onlineåterförsäljare, Internetbanker och Internetapotek utsätts för säkerhetsöverträdelser som telekomföretag, om inte i ännu högre grad. Riskbedömningar talar därför inte för en begränsning av tillämpningsområdet för kravet på anmälningar av säkerhetsöverträdelser till leverantörer av offentliga elektroniska kommunikationstjänster. Behovet av en bredare strategi har visats av erfarenheter i andra länder. Till exempel i Förenta staterna har nästan alla stater (mer än 40 för tillfället) antagit lagar om anmälan av säkerhetsöverträdelser som har ett bredare tillämpningsområde, vilket inte bara inbegriper leverantörer av offentliga elektroniska kommunikationstjänster utan även alla enheter som förfogar över de personuppgifter som krävs.

24. För det andra, även om de slag av personuppgifter som regelbundet behandlas av leverantörer av offentliga elektroniska kommunikationstjänster klart kan påverka den enskildes personliga integritet gäller detta även, om inte i ännu högre grad, för de slag av personuppgifter som behandlas av leverantörer av informationssamhällets tjänster. Banker och andra finansinstitut kan definitivt förfoga över synnerligen förtrolig information (t.ex. detaljer om bankkonton), som om den avslöjas kan användas för identitetsstöld. Likaså kan avslöjandet av ytterst känsliga uppgifter i samband med hälso- och sjukvård av hälso- och sjukvårdsföretag via Internet vara särskilt negativa för enskilda personer. De olika slag av personuppgifter som kan äventyras motiverar därför en bredare tillämpning av anmälningar av säkerhetsöverträdelser som åtminstone skulle inbegripa leverantörer av informationssamhällets tjänster.

25. Vissa rättsliga frågor har tagits upp som talar emot ett utvidgat tillämpningsområde, dvs. de enheter som ska omfattas av detta krav. Särskilt det faktum att det övergripande tillämpningsområdet för direktivet om integritet och elektronisk kommunikation endast gäller leverantörer av offentliga elektroniska kommunikationstjänster har framförts som ett hinder för att utvidga anmälningsskyldigheten även till leverantörer av informationssamhällets tjänster.

26. I detta sammanhang önskar datatillsynsmannen påminna om följande *i)* Det finns inga som helst rättsliga hinder för ett införande av andra aktörer än leverantörer av offentliga elektroniska kommunikationstjänster i tillämpningsområdet för vissa bestämmelser i direktivet. Gemenskapslagstiftaren har ensam behörighet att besluta i detta avseende. *ii)* Det finns andra prejudikat i det befintliga direktivet om integritet och elektronisk kommunikation när det gäller tillämpning på andra enheter än leverantörer av offentliga elektroniska kommunikationstjänster.

27. Till exempel gäller artikel 13 inte endast leverantörer av offentliga elektroniska kommunikationstjänster utan alla företag som skickar icke-begärda kommunikationer för vilka föregående samtycke om frivilligt deltagande krävs. Dessutom är artikel 5.3 i direktivet om integritet och elektronisk kommunikation som bland annat förbjuder lagring av information som t.ex. kakor i användarnas terminalutrustning, bindande inte endast för leverantörer av offentliga elektroniska kommunikationstjänster utan för vem som helst som försöker lagra information eller få tillgång till uppgifter som är lagrade i enskilda personers terminalutrustning. I det aktuella lagstiftningsförfarandet har dessutom kommissionen t.o.m. föreslagit att tillämpningsområdet för artikel 5.3 ska utvidgas när liknande teknik (kakor/spionvara) inte bara tillhandahålls genom elektroniska kommunikationssystem utan även genom någon annan tänkbar metod (distribution via nedladdningar från Internet eller via externa datalagringsmedier, som t.ex. cd-romskivor, USB-minnen, flash-drivar etc.). Alla dessa element är välkomna och bör bibehållas, men bör även utgöra prejudikat för den aktuella diskussionen om tillämpningsområde.

28. I det aktuella lagstiftningsförfarandet har dessutom kommissionen och parlamentet samt förmodligen rådet föreslagit en ny artikel 6.6a som diskuteras nedan som kommer att gälla andra enheter än leverantörer av offentliga elektroniska kommunikationstjänster.

29. Slutligen, med tanke på de övergripande positiva inslag som uppstår genom skyldigheten att anmäla säkerhetsöverträdelser kommer medborgarna mycket sannolikt att förvänta sig dessa fördelar inte bara när deras personuppgifter har äventyrats av leverantörer av offentliga elektroniska kommunikationstjänster utan även av leverantörer av informationssamhällets tjänster. Medborgarnas förväntningar kan eventuellt inte uppfyllas om de till exempel inte meddelas när en Internetbank har förlorat uppgifter om deras bankkonton.

30. Sammanfattningsvis är datatillsynsmannen övertygad om att de fulla fördelarna av anmälningar av säkerhetsöverträdelser endast kan uppnås om tillämpningsområdet omfattar både leverantörer av offentliga elektroniska kommunikationstjänster och leverantörer av informationssamhällets tjänster.

Den norm som utlöser anmälan

31. När det gäller den utlösande faktorn för en anmälan, vilken förklaras mer ingående nedan, anser datatillsynsmannen att den norm som anges i det ändrade förslaget *"sannolikt kommer att förorsaka skada"* är den lämpligaste av de tre föreslagna normerna. Det är dock viktigt att se till att "skada" är tillräckligt omfattande för att täcka alla relevanta situationer med negativa följder för enskilda personers integritet eller andra legitima intressen. Annars är det bättre att skapa en ny norm enligt vilken anmälan är obligatorisk *"om överträdelsen rimligen kan komma att förorsaka negativa effekter för enskilda personer"*.

32. I enlighet med det föregående avsnittet varierar villkoren enligt vilka underrättelser till enskilda måste lämnas (även kallade *utlösaren* eller *normen*) i parlamentets, kommissionens och rådets upplägg. Den mängd meddelanden som enskilda personer kommer att få beror i hög grad på vilken utlösare eller norm som kommer att fastställas för anmälan.

33. I enlighet med rådets och kommissionens system måste anmälan lämnas om överträdelsen innebär ett *"allvarligt intrång i abonnentens privatliv"* (rådet) och om *"skada för konsumenternas intressen sannolikt kommer att uppstå på grund av överträdelsen"* (kommissionen). I enlighet med parlamentets system utgörs utlösaren för underrättelser till enskilda av *"allvaret i överträdelsen"* (dvs. anmälan till enskilda personer krävs om överträdelsen betraktas som *"allvarlig"*). Anmälan är inte nödvändig under denna tröskel ([13]).

34. Om personuppgifter äventyrats, inser Europeiska datatillsynsmannen att det kan hävdas att de privatpersoner som uppgifterna tillhör under alla omständigheter har rätt att få kännedom om det. Det är dock bara rimligt att fundera över om detta är en lämplig lösning med tanke på andra intressen och överväganden.

35. Man har föreslagit att en skyldighet att alltid skicka anmälan när personuppgifter äventyrats, dvs. utan begränsningar, kan leda till för många anmälningar och "att man tröttnar på anmälningarna", vilket kan leda till avtrubbning. Så som närmare kommer att framgå tar datatillsynsmannen fasta på detta argument. Samtidigt vill han dock framhålla sin oro över att förekomsten av för många anmälningar kan vara ett tecken på ett omfattande misslyckande med praxisen för informationssäkerhet.

36. Såsom redan nämnts ser Europeiska datatillsynsmannen de möjliga negativa konsekvenserna av för många anmälningar och skulle vilja bidra till att se till att det den rättsliga ram som antas för anmälan av säkerhetsöverträdelser inte får sådana konsekvenser. Om privatpersoner ofta får anmälningar om överträdelser, även i de situationer där det saknas negativa konsekvenser, skada eller obehag, kan resultatet bli att ett av de viktigaste målen med anmälningarna äventyras, eftersom privatpersoner ironiskt nog kan bortse från anmälningar i fall där de faktiskt behöver vidta åtgärder för att skydda sig. Det är således viktigt att meningsfulla anmälningar lämnas på ett välavvägt sätt, eftersom anmälningssystemens effektivitet minskar kraftigt om personerna inte reagerar på de anmälningar som de får.

37. För att välja en standard som inte leder till för många anmälningar måste inte bara utlösningsmekanismen för anmälningar diskuteras utan även andra faktorer, framför allt definitionen av säkerhetsöverträdelse och den information som anmälningsskyldigheten ska omfatta. Datatillsynsmannen noterar i detta avseende att enligt de tre föreslagna strategierna kan antalet anmälningar bli stort med tanke på den breda definition av säkerhetsöverträdelser som diskuterats ovan. Denna oro över att anmälningarna ska bli för många förstärks ytterligare av att definitionen av säkerhetsöverträdelse omfattar alla typer av personuppgifter. Datatillsynsmannen anser visserligen att detta är den rätta strategin (att inte begränsa anmälan till vissa typer av personuppgifter), till skillnad från andra lösningar som t.ex. USA:s lagstiftning, där kraven är inriktade på informationens känslighet, men det rör sig ändå om en faktor som måste beaktas.

38. Mot bakgrund av det ovannämnda och med hänsyn till de olika variablerna sammantaget anser Europeiska datatillsynsmannen att det är lämpligt att införa en tröskel eller norm under vilken det inte krävs någon anmälan.

39. Det föreslagna normerna, dvs. att en överträdelse ska utgöra en "allvarlig *risk för intrång i privatlivet*" eller *"sannolikt kommer att förorsaka skada"*, verkar båda omfatta t.ex. social skada, skadat rykte eller ekonomisk förlust. Dessa normer skulle exempelvis hantera fall när någon utsatts för identitetsstöld genom att icke-offentliga identifikationsuppgifter såsom passnummer lämnats ut, samt när information om en persons privatliv röjts. Europeiska datatillsynsmannen välkomnar detta synsätt. Han är övertygad om att fördelarna med anmälan av säkerhetsöverträdelser inte fullt ut nås om anmälningssystemet endast omfatta överträdelser som orsakar ekonomisk skada.

([13]) Se fotnot 11 om undantag från denna regel.

40. Av de båda föreslagna normerna föredrar Europeiska datatillsynsmannen kommissionens norm *"sannolikt kommer att förorsaka skada"*, eftersom den ger en lämpligare nivå av skydd för privatpersoner. Sannolikheten att överträdelser leder till anmälan är mycket större om dessa *"sannolikt kommer att förorsaka skada"* mot enskilda personers privatliv än om de måste utgöra en *"allvarlig risk"* för sådan skada. Om endast överträdelser som medför allvarlig risk för intrång i privatlivet ingår, minskar således antalet anmälningspliktiga överträdelser avsevärt. Om endast sådana överträdelser ingår, blir resultatet att leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster och leverantörer av informationssamhällets tjänster får för stort utrymme för egen bedömning av huruvida det krävs en anmälan, eftersom de skulle vara mycket enklare för dem att motivera slutsatsen att ingen *"allvarlig risk"* för skada föreligger än att ingen skada *"sannolikt kommer att förorsakas"*. Det måste absolut undvikas att anmälningarna blir för många, men på det hela taget bör principen om tvivelsmålets fördel gälla för skyddet av personers integritetsintressen, och personer bör skyddas åtminstone om det är sannolikt att en överträdelse förorsakar dem skada. Dessutom kommer begreppet *"sannolikt"* att vara effektivare i praktiken, både med avseende på de enheter som omfattas och de behöriga myndigheterna, efter som det förutsätter en objektiv bedömning av ärendet och relevanta omständigheter.

41. Om personuppgifter äventyras kan dessutom skador förorsakas som är svåra att kvantifiera och som kan variera från fall till fall. Röjandet av samma typer av uppgifter kan beroende på de specifika omständigheterna förorsaka en person betydande skada medan skadorna för en annan blir mindre. Det är inte lämpligt med en norm som kräver att skadan ska vara materiell, betydande eller allvarlig. Exempelvis ger rådets ansats, som kräver att överträdelsen *allvarligt* hotar en persons integritet, privatpersonerna otillräckligt skydd eftersom den normen kräver att konsekvenserna för privatlivet ska vara *"allvarliga"*. Det ger också möjlighet till subjektiv bedömning.

42 Medan formuleringen *"sannolikt kommer att förorsaka skada"* torde vara en lämplig norm för anmälan om säkerhetsöverträdelse, oroas datatillsynsmannen dock fortfarande över att den kanske inte omfattar alla situationer som motiverar en anmälan till personer, dvs. alla situationer med negativa följder för personers integritet eller andra legitima intressen. Man kan därför tänka sig en norm enligt vilken anmälan krävs *"om det är sannolikt att överträdelsen får negativa följder för personer"*.

43. Denna alternativa norm har den ytterligare fördelen att den är förenlig med EU:s dataskyddslagstiftning. I dataskyddsdirektivet hänvisas det faktiskt ofta till negativa följder för de registrerades rättigheter och friheter. I artikel 18 och skäl 49, som behandlar skyldigheten att registrera behandlingar av uppgifter hos dataskyddsmyndigheterna, ger medlemsstaterna exempelvis rätt att bevilja undantag från denna skyldighet om behandlingarna *"[sannolikt] inte kommer att kränka de registrerades fri- och rättigheter"*. En liknande formulering används i artikel 16.6 i den gemensamma ståndpunkten för att juridiska personer ska kunna väcka talan mot den som skickar elektronisk skräppost.

44. Med hänsyn till det ovanstående skulle man dessutom kunna förvänta sig att de enheter som omfattas – och framför allt myndigheter med behörighet att tillämpa dataskyddslagstiftningen – hade bättre kunskap om denna norm och således lättare kunde bedöma huruvida en viss överträdelse uppfyller kraven.

Enhet som ska fastställa om en säkerhetsöverträdelse uppfyller normen eller inte

45. Enligt Europaparlamentets ansats (utom i fall av överhängande fara) och kommissionens ändrade förslag är det medlemsstaternas myndigheter som ska avgöra om en säkerhetsöverträdelse uppfyller den norm som medför skyldighet att underrätta berörda personer.

46. Europeiska datatillsynsmannen anser att det är viktigt att en myndighet medverkar när det ska fastställas om normen uppfylls, eftersom en korrekt tillämpning av lagstiftningen därigenom i viss utsträckning garanteras. Ett sådant system kan hindra företag från att på ett olämpligt sätt uppfatta överträdelsen som icke skadlig/allvarlig och alltså avstå från anmälan, när en sådan anmälan i själva verket är nödvändig.

47. Europeiska datatillsynsmannen är å andra sidan orolig för att ett system som innebär att myndigheterna måste göra bedömningen kan vara opraktiskt och svårt att tillämpa eller i praktiken kan visa sig motverka sina syften. Det kan således till och med försämra personernas dataskyddsgarantier.

48. Med ett sådant synsätt är det sannolikt att dataskyddsmyndigheterna översvämmas av anmälningar om säkerhetsöverträdelser och får det mycket svårt att göra de bedömningar som krävs. Det är viktigt att komma ihåg att myndigheterna för att kunna bedöma om en överträdelse uppfyller normen måste få tillräckligt med bakgrundsinformation, som ofta är tekniskt komplicerad, som de sedan måste behandla mycket snabbt. Med tanke på att det är svårt att göra bedömningar och att vissa myndigheter har begränsade resurser, är Europeiska datatillsynsmannen orolig för att det kommer att bli mycket svårt för myndigheterna att fullgöra denna skyldighet och att resurser kommer att tas från andra viktiga prioriteringar. Ett sådant system kan dessutom innebära orimliga påfrestningar för myndigheterna: om de beslutar att överträdelsen inte är allvarlig och personer likväl lider skada, riskerar myndigheterna att hållas ansvariga.

49. Detta problem accentueras ytterligare om man tar hänsyn till att tiden är en viktig faktor när det gäller att minimera risker som härrör från säkerhetsöverträdelser. Om inte myndigheterna kan göra sin bedömning mycket snabbt, kan all den ytterligare tid som de behöver för dessa bedömningar förvärra de skador som de berörda personerna lider. Därför kan denna ytterligare åtgärd, som är tänkt att ge personer ökat skydd, ironiskt nog leda till minskat skydd jämfört med system som bygger på direkt anmälan.

50. Av ovanstående skäl anser Europeiska datatillsynsmannen att det skulle vara bättre med ett system som innebär att det är de berörda enheterna som ska göra bedömningen av om överträdelsen uppfyller normen eller inte, i enlighet med rådets ansats.

51. För att emellertid undvika riskerna för eventuellt missbruk, t.ex. om enheter avstår från anmälan när en sådan helt klart är påkallad, är det av största vikt att vissa av de dataskyddsgarantier som beskrivs nedan ingår.

52. För det första måste de berörda enheternas skyldighet att avgöra om de måste göra en anmälan naturligtvis åtföljas av en ytterligare en skyldighet: att alla överträdelser som uppfyller normen obligatoriskt måste anmälas till myndigheterna. De berörda enheterna bör i så fall vara skyldiga att informera myndigheterna om överträdelsen och skälen till deras beslut om anmälan samt i förekommande fall om innehållet i anmälan.

53. För det andra måste myndigheterna ges en reell tillsynsroll. När myndigheterna utövar denna roll, måste de få men inte behöva utreda omständigheterna kring överträdelsen och begära lämpliga motåtgärder ([14]). Detta bör inte bara omfatta anmälan till personer (om sådan ännu inte gjorts) utan även förmågan att föreskriva om en skyldighet om att vidta åtgärder för att förhindra fortsatta överträdelser. Myndigheterna bör beviljas faktiska befogenheter och resurser för detta, och myndigheterna måste ges tillräckligt utrymme för att kunna besluta när de ska reagera på en anmälan om säkerhetsöverträdelse. Myndigheterna skulle härigenom med andra ord kunna agera selektivt och utreda till exempel stora, verkligt skadliga säkerhetsöverträdelser och kontrollera och genomdriva att lagens villkor uppfylls.

([14]) I artikel 15a.3 erkänns dessa tillsynsbefogenheter genom att medlemsstaterna *"ska säkerställa att behöriga nationella myndigheter och, där det är relevant, andra nationella organ har alla nödvändiga undersökande befogenheter och resurser, inbegripet tillgång till all information de kan behöva, för att kunna övervaka de nationella bestämmelser som antagits i enlighet med detta direktiv och se till att de efterlevs"*.

54. För att åstadkomma det ovan nämnda rekommenderar Europeiska datatillsynsmannen, utöver de befogenheter som erkänns enligt direktivet om integritet och elektronisk kommunikation, t.ex. artikel 15a.3, och dataskyddsdirektivet, att följande text läggs till: *"Om den berörda abonnenten eller privatpersonen inte redan har erhållit anmälan, får den behöriga nationella myndigheten efter att ha tagit hänsyn till överträdelsens art kräva att leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster eller leverantörerna av informationssamhällets tjänster gör anmälan"*.

55. Datatillsynsmannen rekommenderar dessutom Europaparlamentet och rådet att bekräfta den skyldighet som Europaparlamentet föreslagit (ändring 122, artikel 4.1 a) för enheter att göra en riskbedömning och riskidentifiering om sina system och de personuppgifter de avser att behandla. På grundval av denna skyldighet ska enheterna fastställa en specialanpassad och exakt definition av de säkerhetsåtgärder som kommer att tillämpas i deras fall och som bör stå till myndigheternas förfogande. Om en säkerhetsöverträdelse inträffar kommer denna skyldighet att hjälpa de enheter som omfattas – och i slutänden även myndigheterna i deras tillsynsroll – att avgöra om äventyrandet av sådana uppgifter kan leda till negativa följder eller skada för privatpersonen.

56. För det tredje måste skyldigheten för de enheter som omfattas att avgöra huruvida de måste underrätta personer åtföljas av en skyldighet att ha en detaljerad och heltäckande intern verifieringskedja som beskriver överträdelser som gjorts och anmälningar av dem samt åtgärder som vidtagits för att undvika fortsatta överträdelser. Den interna verifieringskedjan måste ställas till myndigheternas förfogande för genomgång och eventuell utredning. Därigenom får myndigheterna möjlighet att utöva sin tillsyn. Detta kan åstadkommas genom följande formulering: *"Leverantörerna av offentliga elektroniska kommunikationstjänster och leverantörerna av informationssamhällets tjänster ska föra och bevara heltäckande register över alla säkerhetsöverträdelser som inträffat, relevanta tekniska uppgifter med anknytning därtill och motåtgärder som vidtagits. Registren ska även innehålla en hänvisning till alla anmälningar som gjorts till abonnenter eller berörda personer och till de behöriga nationella myndigheterna, inbegripet datum och innehåll. Registren ska på begäran överlämnas till den behöriga nationella myndigheten"*.

57. För att sörja för enhetlighet i genomförandet av denna norm och andra relevanta aspekter av ramen för säkerhetsöverträdelser, t.ex. format och förfaranden för anmälan, bör kommissionen naturligtvis anta tekniska tillämpningsbestämmelser efter att ha hört Europeiska datatillsynsmannen, artikel 29-gruppen och berörda parter.

Mottagare av anmälan

58. När det gäller mottagare av anmälningar föredrar Europeiska datatillsynsmannen Europaparlamentets och kommissionens terminologi framför rådets. EP har ersatt ordet ”abonnenter” med ”användare”. Kommissionen använder ”abonnenter” och ”den berörda privatpersonen”. I både Europaparlamentet och kommissionens text skulle inte enbart nuvarande abonnenter ingå som mottagare av anmälningar utan även f.d. abonnenter och tredjeparter, t.ex. användare som samverkar med en del berörda enheter utan att vara abonnenter. Datatillsynsmannen välkomnar denna ansats och uppmanar Europaparlamentet och rådet att hålla fast vid den.

59. Datatillsynsmannen noterar dock ett antal inkonsekvenser som bör åtgärdas, när det gäller terminologin vid Europaparlamentets första behandling, som bör fastställas. Så har till exempel ordet ”abonnenter” i de flesta fall, men inte alltid, ersatts med ”användare” och i andra fall med ”konsumenter”. Detta bör harmoniseras.

III. TILLÄMPNINGSOMRÅDET FÖR DIREKTIVET OM INTEGRITET OCH ELEKTRONISK KOMMUNIKATION: OFFENTLIGA OCH PRIVATA NÄT

60. I artikel 3.1 i direktivet om integritet och elektronisk kommunikation anges vilka enheter som i första hand berörs av direktivet,. dvs. enheter som behandlar uppgifter ”*i samband med*” tillhandahållande av offentliga elektroniska kommunikationstjänster i allmänna kommunikationsnät (ovan kallade *leverantörer av offentliga elektroniska kommunikationstjänster*) ([15]). I den verksamhet som utövas av leverantörer av offentliga elektroniska kommunikationstjänster ingår tillhandahållande av Internetanslutning, överföring av information via elektroniska nät, mobil- och telefonförbindelser m.m.

61. Europaparlamentet antog en ändring 121 om ändring av artikel 3 i kommissionens ursprungliga förslag, enligt vilket tillämpningsområdet för direktivet om integritet och elektronisk kommunikation breddas till att omfatta ”*behandling av personuppgifter i samband med att allmänt tillgängliga elektroniska kommunikationstjänster tillhandahålls i allmänna och privata kommunikationsnät samt för allmänheten tillgängliga privata nätverk inom gemenskapen, […]*” Artikel 3.1 i direktivet om integritet och elektronisk kommunikation). Tyvärr har det visat sig vara svårt för rådet och kommissionen att godta denna ändring och detta synsätt har därför inte kommit till uttryck i den gemensamma ståndpunkten och det ändrade förslaget.

Tillämpning av direktivet om integritet och elektronisk kommunikation på för allmänheten tillgängliga privata nät

62. Av nedan förklarade skäl, och för att främja samförstånd, manar Europeiska datatillsynsmannen till att behålla ändring 121 i väsentliga delar. Han föreslår dessutom en ändring som ska bidra till att ytterligare klargöra vilka typer av tjänster som ska omfattas av det utvidgade tillämpningsområdet.

63. Privata nät används ofta för att tillhandahålla elektroniska kommunikationstjänster, t.ex. Internetuppkoppling, till människor vars antal inte har fastställts men kan vara omfattande. Detta är fallet när det gäller till exempel Internetuppkoppling på Internetkaféer och i WiFi-zoner på hotell, restauranger, flygplatser, tåg och andra inrättningar som är öppna för allmänheten, där dessa tjänster ofta tillhandahålls som komplement till andra tjänster (drycker, inkvartering m.m.).

64. I alla dessa exempel ställs en kommunikationstjänst, t.ex. Internetuppkoppling, till allmänhetens förfogande, men inte genom ett allmänt nät utan snarare med vad som kan betraktas som ett privat nät, dvs. ett privat drivet nät. Trots att kommunikationstjänsten tillhandahålls allmänheten i de ovannämnda fallen, kunde man på grund av att nättypen är privat snarare än allmän *hävda* att direktivet om integritet och elektronisk kommunikation överhuvudtaget inte, eller endast i fråga om vissa artiklar, är tillämpligt på dessa tjänster ([16]). Resultatet blir att de rättigheter som personer garanteras genom direktivet om integritet och elektronisk kommunikation inte skyddas i dessa fall och att ett orättvist rättsligt läge skapas för användare som använder samma Internetuppkopplingstjänster via allmänt tillgängliga telekommunikationer jämfört med dem som använder dem via privata tjänster. Detta trots att hoten mot personers privatliv och personuppgifter i samtliga dessa fall är lika stora som när allmänt tillgängliga nät används för att förmedla tjänsten. Slutsatsen blir att det inte torde finnas något som med stöd av direktivet berättigar särbehandling av kommunikationstjänster som tillhandahålls via ett privat nät jämfört med tjänster som tillhandahålls via ett allmänt tillgängligt nät.

65. Därför önskar Europeiska datatillsynsmannen stödja en ändring som Europaparlamentets ändring 121 enligt vilken direktivet om integritet och elektronisk kommunikation även skulle vara tillämpligt på behandling av personuppgifter i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster i *privata* kommunikationsnät.

66. Europeiska datatillsynsmannen medger dock att formuleringen kan få oförutsedda och eventuellt oavsedda konsekvenser. Hänvisningen till privata nät kan som sådan

([15]) ”Detta direktiv skall tillämpas på behandling av personuppgifter i samband med att allmänt tillgängliga elektroniska kommunikationstjänster tillhandahålls i allmänna kommunikationsnät inom gemenskapen”.

([16]) Det kan å andra sidan hävdas att i och med att kommunikationstjänsten tillhandahålls allmänheten omfattas tillhandahållandet av dessa tjänster av den gällande rättsliga ramen, trots att nätet är privat. I t.ex. Frankrike har faktiskt arbetsgivare som ger sina anställda tillgång till Internet ansetts vara likvärdiga med Internetleverantörer som erbjuder anslutning till Internet på kommersiella villkor. Denna tolkning godtas endast i begränsad omfattning.

tolkas som att den omfattar situationer som helt klart inte är avsedda att falla inom ramen för direktivet. Det kan till exempel hävdas att en bokstavlig eller strikt tolkning av formuleringen kan göra att den som äger en WiFi-utrustad ([17]) bostad och som därigenom ger någon annan inom dess räckvidd (normalt bostaden) möjlighet till uppkoppling omfattas av direktivets tillämpningsområde, trots att detta inte är avsikten med ändring 121. För att förhindra dessa följder föreslår datatillsynsmannen att ändring 121 ändras så att *"behandling av personuppgifter i samband med att allmänt tillgängliga elektroniska kommunikationstjänster tillhandahålls i allmänna eller allmänt tillgängliga privata kommunikationsnät i gemenskapen, [...]"* omfattas av direktivet om integritet och elektronisk kommunikation.

67. Därigenom skulle det bli lättare att klargöra att endast privata nät som är allmänt tillgängliga omfattas av direktivet om integritet och elektronisk kommunikation. Genom att tillämpa bestämmelserna i direktivet om integritet och elektronisk kommunikation *endast* på *allmänt tillgängliga privata kommunikationsnät* (men inte samtliga privata nät) sätts en gräns, så att direktivet endast omfattar kommunikationstjänster som tillhandahålls i privata nät som avsiktligen görs *tillgängliga* för allmänheten. Denna formulering kommer att bidra till att ytterligare framhålla att det privata nätets *tillgänglighet för allmänheten* är avgörande när det gäller att fastställa om direktivet är tillämpligt (utöver bestämmelsen om allmänt tillgängliga privata kommunikationsnät). Om nätet avsiktligen gjorts tillgängligt för allmänheten för att tillhandahålla en allmänt tillgänglig kommunikationstjänst, till exempel Internetuppkoppling, omfattas denna typ av tjänst/nät med andra ord av direktivet om integritet och elektronisk kommunikation, oavsett om nätet är allmänt tillgängligt eller privat, också om denna tjänst kompletterar en annan (t.ex. hotellinkvartering).

68. Europeiska datatillsynsmannen noterar att denna ovan förordade metod, som innebär att bestämmelserna i direktivet om integritet och elektronisk kommunikation är tillämpliga på *allmänt tillgängliga privata kommunikationsnät*, är förenlig med de metoder som valts i flera medlemsstater, där myndigheterna redan ansett denna typ av tjänster och tjänster som tillhandahålls i rent privata nät falla inom tillämpningsområdet för de nationella bestämmelser varigenom direktivet om integritet och elektronisk kommunikation genomförs ([18]).

69. För att främja rättsäkerheten när det gäller de enheter som omfattas av det nya tillämpningsområdet, kan det vara lämpligt att införa en ändring med en definition av *allmänt tillgängliga privata nät* i direktivet om integritet och elektronisk kommunikation, som kan ha följande lydelse: *"allmänt tillgängligt privat nät: ett privatdrivet nät till vilket allmänheten normalt har obegränsad tillgång, oavsett om det förutsätter betalning eller ej eller samband med andra tjänster eller erbjudanden, under förutsättning att tillämpliga villkor godtagits."*

70. I praktiken skulle denna metod betyda att privata nät på hotell och andra inrättningar som allmänheten tillgång Internet via ett privat nät skulle ingå. Motsatt gäller att tillhandahållandet av kommunikationstjänster i rent privata nätverk inte ingår, om tjänsten begränsas till en begränsad grupp av identifierbara personer. Därför skulle till exempel virtuella privata nät och konsumenters bostäder, när de är utrustade med WiFi, inte omfattas av direktivet. Inte heller tjänster som tillhandahålls av rena företagsnät skulle ingå.

Privata när som omfattas av tillämpningsområdet för direktivet om integritet och elektronisk kommunikation

71. Att utesluta privata nätverk som sådana enligt ovanstående förslag bör ses som en tillfällig åtgärd som bör diskuteras ytterligare. Lösningen kan behöva omprövas i framtiden med tanke på dels de följder som ett uteslutande av privata nät får som sådant för privatlivet, dels att ett stort antal människor som normalt kopplar upp sig till Internet i företagsnät kommer att påverkas. Därför, och för att främja debatten i denna fråga, rekommenderar Europeiska datatillsynsmannen införande av ett skäl i direktivet om integritet och elektronisk kommunikation enligt vilket kommissionen kommer att hålla offentligt samråd om tillämpningen av det direktivet på alla privata nät, med synpunkter från datatillsynsmannen, dataskyddsmyndigheter och andra relevanta intressenter. Det kan dessutom anges i skälet att kommissionen som ett resultat av det offentliga samrådet bör lägga fram lämpliga förslag om att öka eller begränsa antalet typer av enheter som bör omfattas av direktivet om integritet och elektronisk kommunikation.

72. Dessutom bör artiklarna i direktivet om integritet och elektronisk kommunikation ändras på motsvarande sätt så att alla bestämmelser i artikeldelen uttryckligen avser inte bara allmänt tillgängliga nät utan även för allmänheten tillgängliga privata nät.

IV. **BEHANDLING AV TRAFIKUPPGIFTER FÖR SÄKERHETSÄNDAMÅL**

73. Under lagstiftningsprocessen i samband med översynen av direktivet om integritet och elektronisk kommunikation, hävdade företag som tillhandahåller säkerhetstjänster att det var nödvändigt att införa en bestämmelse som berättigar insamling av trafikuppgifter för att garantera faktisk online-säkerhet.

([17]) Vanligtvis trådlösa lokala nät (LAN).
([18]) Se fotnot 16.

74. Som ett resultat införde Europaparlamentet ändring 181, enligt vilken en ny artikel 6.6a införs. så att behandling av trafikuppgifter för säkerhetsändamål uttryckligen tillåts: *"Utan att det påverkar tillämpningen av andra bestämmelser än artikel 7 i direktiv 95/46/EG och artikel 5 i detta direktiv får trafikuppgifter behandlas om den dataregisteransvarige har ett legitimt intresse att genomföra tekniska åtgärder för att säkerställa den nät- och informationssäkerhet som definieras i artikel 4 c i Europaparlamentets och rådets förordning (EG) nr 460/2004 av den 10 mars 2004 om inrättandet av den europeiska byrån för nät- och informationssäkerhet, med avseende på en offentlig elektronisk kommunikationstjänst, ett offentligt eller privat elektroniskt kommunikationsnät, en tjänst inom informationssamhället eller tillhörande terminalutrustning och elektronisk kommunikationsutrustning, utom då sådana intressen åsidosätts av intressena för den registrerades grundläggande rättigheter och friheter. Denna behandling måste begränsas till vad som är absolut nödvändigt för denna säkerhetsverksamhet."*

75. I kommissionens ändrade förslag godtogs denna ändring i princip, men man strök en viktig klausul som var avsedd att se till att de övriga bestämmelserna i direktivet skulle följas när *"Utan att det påverkar tillämpningen [...] detta direktiv"* ströks. Rådet antog en omarbetad version, där man gick ännu längre med att försvaga viktiga skyddsinslag och intresseavvägningar som ingick i ändring 181 och antog följande formulering: *"Trafikuppgifter får behandlas i den utsträckning som är absolut nödvändig för att säkerställa den nät- och informationssäkerhet som definieras i artikel 4 c i Europaparlamentets och rådets förordning (EG) nr 460/2004 av den 10 mars 2004 om inrättandet av den europeiska byrån för nät- och informationssäkerhet."*

76. Såsom förklaras mer i detalj nedan är artikel 6.6a onödig och riskerar att missbrukas, särskilt om den antas i en form som saknar de viktiga garantierna, bestämmelser om att övriga bestämmelser i direktivet ska gälla och en avvägning mellan olika intressen. Europeiska datatillsynsmannen rekommenderar därför att denna artikel avvisas eller en sådan artikel i denna fråga omfattar de typer av garantier som fanns i den av parlamentet antagna ändring 181.

Rättsliga grunder för behandling av trafikuppgifter avseende elektroniska kommunikationstjänster och andra dataregisteransvariga enligt gällande dataskyddslagstiftning

77. Tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster får lagligt behandla trafikuppgifter i en omfattning som fastställs i artikel 6 i direktivet om integritet och elektronisk kommunikation som innebär att behandlingen av trafikuppgifter begränsas till ett visst antal ändamål, t.ex. fakturering, samtrafik och marknadsföring. Behandlingen får äga rum endast om vissa villkor är uppfyllda, t.ex. att privatpersoner uttryckt sitt samtycke i fråga om marknadsföring. Dessutom får andra dataregisteransvariga, t.ex. leverantörer av informationssamhällets tjänster, behandla trafikuppgifter med stöd av artikel 7 i dataskyddsdirektivet, där det fastställs att dataregisteransvariga får behandla personuppgifter i enlighet med minst ett av de rättsliga underlag som räknas upp i en förteckning och som även kallas rättsliga grunder.

78. Ett exempel på sådan rättslig grund är artikel 7 a i dataskyddsdirektivet, enligt vilken den registrerades samtycke krävs. En återförsäljare på nätet som vill behandla trafikuppgifter för att skicka reklam eller marknadsföringsmaterial måste till exempel inhämta personens samtycke. Enligt en annan rättslig grund som fastställs i artikel 7 kan under vissa omständigheter till exempel säkerhetsföretag som erbjuder säkerhetstjänster tillåtas att behandla trafikuppgifter i säkerhetssyfte. Detta grundas på artikel 7 f enligt vilken dataregisteransvariga får behandla personuppgifter om behandlingen är *"nödvändig för ändamål som rör berättigade intressen hos den registeransvarige eller hos den eller de tredje män till vilka uppgifterna har lämnats ut, utom när sådana intressen uppvägs av den registrerades intressen eller dennes grundläggande fri- och rättigheter [...]."* Det anges inte i dataskyddsdirektivet under vilka omständigheter behandling av personuppgifter skulle motsvara detta krav. I stället avgörs frågan från fall till fall av dataregisteransvariga, ofta med godkännande från nationella dataskyddsmyndigheter och andra myndigheter.

79. Samspelet mellan artikel 7 i dataskyddsdirektivet och artikel 6.6a i direktivet om integritet och elektronisk kommunikation bör beaktas. Den föreslagna artikel 6.6a är en specificering av de omständigheter under vilka kraven i den ovan beskrivna artikel 7 f är uppfyllda. Genom att tillåta behandling av trafikuppgifter för att bidra till att nät- och informationssäkerheten säkerställs möjliggör artikel 6.6a denna behandling för ändamål som rör berättigade intressen hos den registeransvarige.

80. Såsom närmare förklaras nedan anser Europeiska datatillsynsmannen att artikel 6.6a varken är nödvändig eller användbar. Ur rättslig synvinkel är det i princip onödigt att fastställa huruvida en viss typ av uppgiftsbehandling, i detta fall behandling av trafikuppgifter i säkerhetssyfte, uppfyller kraven i artikel 7 f i dataskyddsdirektivet eller ej, i vilket fall personens samtycke kan vara nödvändigt enligt artikel 7 a. Såsom konstaterats ovan, görs bedömningen ofta av de dataregisteransvariga, dvs. företag, på genomförandenivå i samråd med dataskyddsmyndigheter och, vid behov, domstolar. Europeiska datatillsynsmannen tror att berättigad behandling av trafikuppgifter i säkerhetssyfte, i specifika fall och om den utförs utan att den hotar personers grundläggande rättigheter och friheter, i allmänhet torde motsvara kraven i artikel 7 f i dataskyddsdirektivet och därför kan utföras. Det saknas för övrigt

något annat prejudikat i direktiven om dataskydd och om integritet och elektronisk kommunikation för att välja ut eller särbehandla sådana typer av behandling av uppgifter som motsvarar kraven i artikel 7 f och det har inte kunnat visas att det finns något behov av ett sådant undantag. Såsom konstaterats ovan torde denna typ av verksamhet däremot under många omständigheter bekvämt passa in i den nuvarande texten. Därför är det i princip onödigt med en rättslig bestämmelse där denna bedömning bekräftas.

Europaparlamentets, rådets och kommissionens versioner av artikel 6.6a

81. Såsom förklarats ovan är det viktigt, även om det inte är nödvändigt, att framhålla att ändring 181 i dess av Europaparlamentet antagna lydelse dock i viss grad utformades med beaktande av de skyddsprinciper som dataskyddslagstiftningen innehåller. Europaparlamentets ändring 181 kan dessutom behandla intresset av uppgifts- och integritetsskydd genom införande av orden ”i specifika fall” för att se till denna artikel tillämpas selektivt eller genom införande av en särskild lagringstid.

82. Ändring 181 innehåller vissa positiva inslag. Det bekräftas att behandlingen bör följa alla andra principer för skydd av uppgifter som är tillämpliga på behandling av personuppgifter (”*Utan att det påverkar tillämpningen av andra bestämmelser [...] i direktiv 95/46/EG och [...] i detta direktiv*”). Trots att behandling av trafikuppgifter i säkerhetssyfte tillåts enligt ändring 181, görs dessutom i ändringen en avvägning mellan den trafikuppgiftsbehandlande enhetens intressen och de intressen som de vars uppgifter behandlas har, så att denna uppgiftsbehandling kan äga rum endast om behovet att tillgodose att personers grundläggande rättigheter och friheter inte åsidosätts av den uppgiftsbehandlande enheten (”*utom då sådana intressen åsidosätts av intressena för den registrerades grundläggande rättigheter och friheter*”). Detta krav är väsentligt i och med att det kan medge behandling av trafikuppgifter i specifika fall. En enhet skulle emellertid inte få behandla trafikuppgifter utan urskiljning.

83. I rådets omarbetade version av ändringen finns lovvärda inslag, till exempel att orden ”*absolut nödvändigt*” fått stå kvar, vilket understryker denna artikels begränsade tillämpningsområde. I rådets version utgår emellertid de garantier för uppgifts- och integritetsskydd som nämns ovan. Även om de allmänna bestämmelserna om skydd av uppgifter i princip gäller, oavsett specifika hänvisningar i varje enskilt fall, kan rådets version av artikel 6.6a trots allt tolkas som att obegränsat utrymme för skönsmässig bedömning lämnas i fråga om behandling av trafikuppgifter, utan några av de garantier för uppgifts- och integritetsskydd som alltid när trafikuppgifter behandlas. Det kunde därför hävdas att trafikuppgifter får samlas in, lagras och fortsätta att användas, utan att uppgiftsskyddsprinciper och särskilda förpliktelser som annars gäller för de ansvariga behöver följas, t.ex. kvalitetsprincipen eller skyldigheten till korrekt och laglig behandling och skyldigheten att skydda uppgifternas konfidentialitet och säkerhet. Eftersom ingen hänvisning görs till tillämpliga uppgiftsskyddsprinciper som anger tidsgränser för lagring av information eller till särskilda tidsgränser i den artikeln, kan rådets version dessutom tolkas som att insamling och behandling av trafikuppgifter i säkerhetssyfte är tillåten under en icke närmare angiven tid.

84. Dessutom har rådet försvagat integritetsskyddet i vissa delar av texten genom att potentiellt bredda formuleringarna. Så har exempelvis hänvisningen till ”*den dataregisteransvariges legitima intresse*” utgått, vilket skapar osäkerhet om vilka typer av enheter som kan åberopa detta undantag. Det är ytterst viktigt att förhindra att användare eller rättsliga enheter kan dra fördel av denna ändring.

85. Erfarenheterna från Europaparlamentet och rådet på senare tid visar att det är svårt att i lag fastställa i vilken utsträckning och på vilka villkor behandling av uppgifter i säkerhetssyfte kan utföras lagligt. Det är osannolikt att någon befintlig eller framtida artikel skulle kunna undanröja risken för en alltför bred tillämpning av undantaget av andra skäl än de rent säkerhetsrelaterade eller av enheter som inte bör få dra nytta av undantaget. Det innebär inte att sådan behandling aldrig får äga rum. Det är emellertid bättre att bedömningen av om den får göras och i så fall i vilken omfattning görs på genomförandenivån. Enheter som vill börja med sådan behandling bör diskutera omfattningen och villkoren med dataskyddsmyndigheterna och eventuellt med artikel 29-gruppen. Alternativt kan direktivet om integritet och elektronisk kommunikation innehålla en artikel enligt vilken behandling av trafikuppgifter är tillåten, om tillstånd uttryckligen beviljats av dataskyddsmyndigheterna.

86. Med beaktande av å ena sidan de risker som artikel 6.6a innebär för den grundläggande rättigheten till skydd av privatpersoners uppgifter och integritet, och å andra sidan att denna artikel, såsom förklarats i detta yttrande, ur rättslig synvinkel är onödig, har Europeiska datatillsynsmannen dragit slutsatsen att det bästa vore om den föreslagna artikel 6.6a helt och hållet utgår.

87. Om en text motsvarande någon av de nuvarande versionerna av artikel 6.6a antas, trots datatillsynsmannens rekommendation, bör den i alla fall innehålla de dataskyddsgarantier som diskuterats ovan. Den bör också integreras på ett korrekt sätt i den nuvarande strukturen i artikel 6, helst som en ny punkt 2a.

V. **MÖJLIGHETEN FÖR JURIDISKA PERSONER ATT VIDTA ÅTGÄRDER MOT ÖVERTRÄDELSE AV DIREKTIVET OM INTEGRITET OCH ELEKTRONISK KOMMUNIKATION**

88. Europaparlamentet antog ändring 133 som ger Internetleverantörer och andra rättsliga enheter, t.ex. konsumentorganisationer, möjlighet att väcka talan vid överträdelse av bestämmelserna i direktivet om integritet och elektronisk kommunikation ([19]). Tyvärr har varken kommissionen eller rådet godtagit ändringen. Europeiska datatillsynsmannen anser denna ändring vara mycket positiv och rekommenderar att den får stå kvar.

89. För att förstå betydelsen av denna ändring måste man inse att i frågor som rör skyddet av uppgifter och privatlivet är den skada som en enskilt betraktad person lider normalt sätt inte tillräcklig för att han eller hon ska få väcka talan vid domstol. Privatpersoner går normalt inte på egen hand till domstol för att de erhållit skräppost eller för att deras namn av ogiltiga skäl tagits med i ett register. Denna ändring gör det möjligt för konsumentorganisationer och fackföreningar som företräder konsumenters intressen att väcka kollektiv talan inför domstol på dessa konsumenters vägnar. En ökad mångfald av verkställighetsmekanismer främjar sannolikt även ökad överensstämmelse och stöder därför en effektiv tillämpning av bestämmelserna i direktivet om integritet och elektronisk kommunikation.

90. Det finns rättsliga prejudikat i en del medlemsstaters rättsliga ramar som redan förutser möjligheten av grupptalan för att konsument- eller intressegrupper ska kunna begära ersättning av den part som orsakat skada.

91. I vissa medlemsstaters konkurrenslagstiftning ([20]) har vidare konsumenter, intressegrupper (utöver den *berörda konkurrenten*) rätt att väcka talan mot den enhet som begått överträdelsen. Skälen till denna lösning är att företag som bryter mot konkurrenslagstiftningen sannolikt tjänar på det, eftersom konsumenter som endast lider marginell skada generellt är tveksamma till att väcka talan. Detta skäl kan även tillämpas på integritets- och dataskydd.

92. Än viktigare är, såsom redan nämnts, att om rättsliga enheter som konsumentsammanslutningar och leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster ges rätt att väcka talan stärks konsumenternas ställning och främjas ett övergripande iakttagande av bestämmelserna i dataskyddslagstiftningen. Om företag som bryter mot bestämmelserna löper ökad risk att stämmas, är de mer benägna att investera mer i att följa bestämmelserna i dataskyddslagstiftningen, vilket i längden höjer integritets- och konsumentdataskyddet. Av alla dessa skäl uppmanar Europeiska datatillsynsmannen Europaparlamentet och rådet att anta en bestämmelse som för det möjligt för rättsliga enheter att väcka talan vid överträdelse av bestämmelserna i direktivet om integritet och elektronisk kommunikation.

([19]) Artikel 13.6 enligt Europaparlamentets första behandling.
([20]) Se till exempel § 8 i den tyska lagen om oskälig konkurrens (UWG).

VI. **SLUTSATSER**

93. Rådets gemensamma ståndpunkt, Europaparlamentets första behandling och kommissionens ändrade förslag innehåller i varierande grad positiva inslag som är ägnade att stärka skyddet av privatpersoners integritet och personuppgifter.

94. Europeiska datatillsynsmannen anser dock att det finns utrymme för förbättringar, särskilt när det gäller rådets gemensamma ståndpunkt, som tyvärr inte har behållit vissa av de parlamentsändringar som var avsedda att bidra till att säkerställa ett tillräckligt skydd av privatpersoners integritet och personuppgifter. Europeiska datatillsynsmannen vädjar till parlamentet och rådet om att de ska återinföra de integritetsgarantier som finns i texten från Europaparlamentets första behandling.

95. Datatillsynsmannen anser dessutom att vissa bestämmelser i direktivet bör effektiviseras. Dessa gäller i synnerhet bestämmelserna om säkerhetsöverträdelser, eftersom datatillsynsmannen anser att de fullständiga fördelarna med anmälningar av överträdelser bäst förverkligas om den rättsliga ramen fastställs redan från början. Han anser slutligen att vissa bestämmelser i direktivet bör formuleras bättre och klarare.

96. Mot bakgrund av det ovannämnda vädjar Europeiska datatillsynsmannen till Europaparlamentet och rådet om att de ska öka insatserna för att förbättra och förtydliga vissa bestämmelser i direktivet om integritet och elektronisk kommunikation och samtidigt återinföra de ändringar som Europaparlamentet antog vid första behandlingen i syfte att föreskriva ett lämpligt integritets- och dataskydd. I punkterna 97–100 sammanfattas därför de frågor som måste besvaras och presenteras vissa rekommendationer och förslag till utformning. Europeiska datatillsynsmannen uppmanar alla medverkande parter att beakta dessa på förslagets väg mot slutligt antagande.

Säkerhetsöverträdelser

97. Europaparlamentet, kommissionen och rådet har alla intagit olika inställningar till anmälningar av säkerhetsöverträdelser. Det finns skillnaderna mellan de tre modellerna när det gäller bland annat de enheter som omfattas av skyldigheten, normen eller utlösningsmekanismen för anmälan, de registrerade som har rätt att bli underrättade, m.m. Europaparlamentet och rådet måste göra sitt yttersta för att ta fram en robust rättslig ram för säkerhetsöverträdelser. Europaparlamentet och rådet bör därför göra följande:

— *Behålla* definitionen av säkerhetsöverträdelser i Europaparlamentets, rådets och kommissionens texter, eftersom den är tillräckligt bred för att inbegripa de flesta relevanta situationer där anmälningar av säkerhetsöverträdelser eventuellt är motiverade.

— När det gäller tillämpningsområdet för de enheter som ska omfattas av det föreslagna anmälningskravet: *inkludera* leverantörer av informationssamhällets tjänster. Risken för att onlineåterförsäljare, Internetbanker och Internetapotek utsätts för säkerhetsöverträdelser är lika stor som när det gäller telekomföretag, om inte ännu större. Medborgarna kommer att förvänta sig att få en anmälan inte endast när Internetleverantörer, utan i synnerhet även när Internetbanker och Internetapotek, drabbas av säkerhetsöverträdelser.

— När det gäller den utlösande faktorn för anmälan, är den norm som anges i det ändrade förslaget – *"sannolikt kommer att förorsaka skada"* – en lämplig norm som ger ett fungerande system. Det är dock viktigt att se till att "skada" är tillräckligt omfattande för att täcka alla relevanta situationer med negativa följder för enskilda personers integritet eller andra legitima intressen. Annars är det bättre att skapa en ny norm enligt vilken anmälan är obligatorisk *"om överträdelsen rimligen kan komma att förorsaka negativa effekter för enskilda personer"*. Rådets ansats, som kräver att överträdelsen *allvarligt* hotar en persons integritet, ger privatpersonerna otillräckligt skydd eftersom den normen kräver att konsekvenserna för privatlivet ska vara "allvarliga". Det ger också möjlighet till subjektiv bedömning.

— Att en myndighet medverkar till att avgöra om en berörd enhet är skyldig att göra en anmälan till privatpersoner ger förvisso positiva resultat, men det kan vara opraktiskt och svårt att tillämpa och kan leda bort resurser från andra viktiga prioriteringar. Datatillsynsmannen fruktar att ett sådant system, om myndigheterna inte kan reagera extremt snabbt, till och med kan minska privatpersoners skydd och innebära orimliga påfrestningar för myndigheterna. Således rekommenderar Europeiska datatillsynsmannen på det hela taget att ett system *inrättas* som innebär att det är de berörda enheternas sak att bedöma huruvida det krävs en anmälan.

— För att ge myndigheterna möjlighet att utöva tillsyn över de bedömningar som görs av de enheter som omfattas, när det gäller frågan om huruvida de ska göra en anmälan: *genomför* följande garantier:

  — *Se till* att sådana enheter är skyldiga att anmäla alla överträdelser som motsvarar normen till myndigheterna.

  — *Ge* myndigheterna en tillsynsroll som ger dem möjlighet att vara selektiva för att kunna vara effektiva. Införa följande formulering för att åstadkomma det ovannämnda: *"Om den berörda abonnenten eller personen inte redan har erhållit anmälan, får den behöriga nationella myndigheten efter att ha tagit hänsyn till överträdelsens art kräva att leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster eller leverantörerna av informationssamhällets tjänster gör anmälan"*.

  — *Anta* en ny bestämmelse om att enheterna måste ha en detaljerad och heltäckande intern verifieringskedja. Detta kan åstadkommas genom följande formulering: *"Leverantörerna av offentliga elektroniska kommunikationstjänster och leverantörerna av informationssamhällets tjänster ska föra och bevara heltäckande register över alla säkerhetsöverträdelser som inträffat, relevanta tekniska uppgifter med anknytning därtill och motåtgärder som vidtagits. Registren ska även innehålla en hänvisning till alla anmälningar som gjorts till abonnenter eller berörda personer och till de behöriga nationella myndigheterna, inbegripet datum och innehåll. Register ska på begäran överlämnas till den behöriga myndigheten."*

— För att sörja för ett enhetligt genomförande av ramen för säkerhetsöverträdelser: *ge* kommissionen möjlighet att anta tekniska tillämpningsföreskrifter efter föregående samråd med Europeiska datatillsynsmannen, artikel 29-gruppen och andra relevanta intressenter.

— När det gäller de personer som ska erhålla anmälan: *använd* kommissionens eller Europaparlamentets terminologi, dvs. "berörda privatpersoner" eller "berörda användare", eftersom den inbegriper alla de personer vars personuppgifter har äventyrats.

Allmänt tillgängliga privata nät

98. Det förekommer ofta att allmänheten tillhandahålls kommunikationstjänster genom nät som inte är allmänna utan privat drivna (t.ex. WiFi-zoner på hotell och flygplatser), och det kan hävdas att dessa nät inte omfattas av direktivet. Europaparlamentet antog ändring 121 (artikel 3) för att bredda direktivets tillämpningsområde till att omfatta allmänna och privata kommunikationsnät samt allmänt tillgängliga privata nät. I detta avseende bör Europaparlamentet och rådet göra följande:

— *Behålla* ändring 121 till sitt väsentliga innehåll, men *omformulera* den så att endast *"behandling av personuppgifter i samband med att allmänt tillgängliga elektroniska kommunikationstjänster tillhandahålls i allmänna eller allmänt tillgängliga privata kommunikationsnät i gemenskapen"* omfattas av tillämpningsområdet för direktivet om integritet och elektronisk kommunikation. Rent privat drivna när (i motsats till allmänt tillgängliga privata nät) skulle inte uttryckligen ingå.

— *Ändra* på samma sätt alla bestämmelser i artikeldelen så att de uttryckligen avser inte bara allmänna nät utan även allmänt tillgängliga privata nät.

— *Införa* en ändring med följande definition: *"allmänt tillgängligt privat nät: ett privatdrivet nät till vilket allmänheten normalt har obegränsad tillgång till, oavsett om det förutsätter betalning eller ej eller samband med andra tjänster eller erbjudanden, under förutsättning att tillämpliga villkor godtagits."* Det ger ökad rättsäkerhet när det gäller att veta vilka enheter som omfattas av det nya tillämpningsområdet.

— *Anta* ett nytt skäl enligt vilket kommissionen ska hålla offentligt samråd om tillämpningen av det direktivet om integritet och elektronisk kommunikation på alla privata nät, med synpunkter från datatillsynsmannen, artikel 29-gruppen och andra relevanta intressenter. Ange att kommissionen som ett resultat av det offentliga samrådet bör lägga fram lämpliga förslag om att öka eller begränsa antalet typer av enheter som bör omfattas av direktivet om integritet och elektronisk kommunikation.

Behandling av trafikuppgifter för säkerhetsändamål

99. Europaparlamentet antog vid första behandlingen ändring 181 (artikel 6.6a) varigenom behandling av trafikuppgifter för säkerhetsändamål tillåts. I rådets gemensamma ståndpunkt antogs en ny version, där vissa viktiga skyddsgarantier försvagas. I detta avseende rekommendera Europeiska datatillsynsmannen att Europaparlamentet och rådet

— *avvisar* denna artikel i dess helhet, eftersom den är onödig och kan äventyra privatpersoners uppgifts- och integritetsskydd om den missbrukas,

— eller, om någon variation på den nuvarande versionen av artikel 6.6a antas, *införlivar* de dataskyddsgarantier som diskuterats i detta yttrande (liknande dem i Europaparlamentets ändring).

Åtgärder vid åsidosättande av bestämmelserna i direktivet om integritet och elektronisk kommunikation

100. Parlamentet antog ändring 133 (artikel 13.6) enligt vilken rättsliga enheter ges möjlighet att väcka talan om överträdelse av direktivets bestämmelser. Tyvärr bibehöll rådet den inte. Rådet och Europaparlamentet bör

— *godkänna* den bestämmelse som ger rättsliga enheter, t.ex. konsument- och arbetstagarorganisationer, rätt att väcka talan vid överträdelse av bestämmelserna i direktivet (inte bara vid överträdelse av bestämmelserna om skräppost, vilket är den nuvarande inställningen i den gemensamma ståndpunkten och det ändrade förslaget). En ökad mångfald av verkställighetsmekanismer kommer att främja ökad överensstämmelse och effektivare tillämpning av bestämmelserna i direktivet om integritet och elektronisk kommunikation som helhet.

Att anta utmaningen

101. I alla de ovannämnda frågorna måste Europaparlamentet och rådet anta utmaningen att utforma korrekta regler och bestämmelser som är både praktiskt användbara och funktionella samt respekterar privatpersoners rätt till integritets- och uppgiftsskydd. Europeiska datatillsynsmannen hyser förhoppningar om att de berörda parterna kommer att göra sitt yttersta för anta denna utmaning och hoppas att detta yttrande kommer att vara till hjälp i det arbetet.

Utfärdat i Bryssel den 9 januari 2009

Peter HUSTINX
Europeisk datatillsynsman

Yttrande från Europeiska datatillsynsmannen om förslaget till rådets direktiv om en skyldighet för medlemsstaterna att inneha minimilager av råolja och/eller petroleumprodukter

(2009/C 128/05)

EUROPEISKA DATATILLSYNSMANNEN HAR ANTAGIT DETTA YTTRANDE

med beaktande av fördraget om upprättandet av Europeiska gemenskapen, särskilt artikel 286,

med beaktande av Europeiska unionens stadga om de grundläggande rättigheterna, särskilt artikel 8,

med beaktande av Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter ([1]),

med beaktande av Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter, särskilt artikel 41 ([2]),

med beaktande av den begäran om ett yttrande i enlighet med artikel 28.2 i förordning (EG) nr 45/2001 som översändes till datatillsynsmannen den 14 november 2008.

HÄRIGENOM FRAMFÖRS FÖLJANDE:

I. INLEDNING

1. Den 13 november 2008 antog kommissionen ett förslag till rådets direktiv om en skyldighet för medlemsstaterna att inneha minimilager av råolja och/eller petroleumprodukter (nedan kallat ”förslaget”) ([3]).

2. Förslaget syftar till att med hjälp av tillförlitliga och översiktliga mekanismer som är grundade på solidaritet mellan medlemsstaterna säkerställa en hög säkerhetsnivå för oljeförsörjningen i gemenskapen, hålla minimilager av olja och petroleumprodukter samt införa de förfaranden som krävs för att avhjälpa eventuella allvarliga brister.

3. Den 14 november 2008 översände kommissionen förslaget till datatillsynsmannen för samråd i enlighet med artikel 28.2 i förordning (EG) nr 45/2001. Datatillsynsmannen välkomnar kommissionens begäran om samråd i detta ärende och noterar att det hänvisas till detta samråd i förslagets ingress i enlighet med artikel 28 i förordning (EG) nr 45/2001.

4. Innan förslaget antogs samrådde kommissionen informellt med datatillsynsmannen om en särskild artikel i utkastet till förslag (nuvarande artikel 19). Datatillsynsmannen välkomnar detta informella samråd eftersom det gav honom möjlighet att lämna några förslag innan kommissionens antog förslaget.

II. ANALYS AV FÖRSLAGET

Allmän analys

5. Den aktuella frågan belyser väl det faktum att det bör finnas en ständig medvetenhet om bestämmelserna om uppgiftsskydd. I en situation som gäller medlemsstaterna och deras skyldighet att hålla beredskapslager av olja, vilka huvudsakligen ägs av juridiska personer, är behandling av personuppgifter inte helt självklar, men även om detta i sig inte har planerats kan det likväl förekomma. Man bör under alla omständigheter överväga sannolikheten för att personuppgifter behandlas och agera därefter.

6. I det nuvarande läget finns det i princip två verksamheter i direktivet som skulle kunna inbegripa behandling av personuppgifter. Den första gäller medlemsstaternas insamling av uppgifter om oljelager och den därpå följande överföringen av uppgifterna till kommissionen. Den andra verksamheten gäller kommissionens behörighet att utföra kontroller i medlemsstaterna. Insamlingen av uppgifter om oljelagrens ägare skulle kunna inbegripa personuppgifter, såsom namn och kontaktuppgifter för ledande befattningshavare i företagen. Denna insamling samt den senare överföringen till kommissionen skulle då utgöra behandling av personuppgifter och avgöra huruvida den nationella lagstiftningen för genomförande av bestämmelserna i direktiv 95/46/EG eller förordning (EG) nr 45/2001 är tillämplig, beroende på vem som faktiskt behandlar uppgifterna. Behörighet för kommissionen att utföra kontroller av beredskapslager i medlemsstaterna, vilket omfattar rätten att samla in uppgifter i allmänhet, skulle också kunna inbegripa insamling och således även behandling av personuppgifter.

([1]) EGT L 281, 23.11.1995, s. 31.
([2]) EGT L 8, 12.1.2001, s. 1.
([3]) KOM(2008) 775 slutlig.

7. Under det informella samrådet, som uteslutande gällde bestämmelsen om kommissionens undersökningsbehörighet, rekommenderade datatillsynsmannen kommissionen att fastställa huruvida behandlingen av personuppgifter inom ramen för kommissionens undersökning skulle vara helt tillfällig eller ske regelbundet och tjäna syftet med undersökningen. I förhållande till resultatet av bedömningen föreslogs två olika metoder.

8. Om behandling av personuppgifter inte hade planerats utan skulle vara av helt tillfällig art, rekommenderade datatillsynsmannen för det första att uttryckligen utesluta att behandlingen av personuppgifter tjänar syftet med kommissionens undersökning och, för det andra, att det ska anges att alla personuppgifter som kommissionen kommer i kontakt med under undersökningen varken kommer att samlas in eller beaktas och att de vid oavsiktligt insamling omedelbart ska förstöras. Som en allmän stödåtgärd föreslog datatillsynsmannen dessutom att det ska införas en bestämmelse där det anges att direktivet inte påverkar tillämpningen av de bestämmelser om uppgiftsskydd som fastställs i direktiv 95/46/EG och i förordning (EG) nr 45/2001.

9. Om det å andra sidan var tänkt att behandling av uppgifter regelbundet skulle ske inom ramen för kommissionens undersökning, rekommenderade datatillsynsmannen kommissionen att införa en text som återspeglar resultatet av en lämplig utvärdering av uppgiftsskyddet. Detta skulle kunna inbegripa följande inslag: I) Det faktiska syftet med databehandlingen, II) nödvändigheten av databehandlingen för att uppnå detta syfte och III) proportionaliteten i databehandlingen.

10. Även om datatillsynsmannens informella råd endast gällde kommissionens undersökningsbehörighet gällde hans synpunkter även den andra huvudsakliga verksamhet som beskrivs i förslaget till direktiv, nämligen insamling och överföring till kommissionen av uppgifter från medlemsstaterna.

11. Det framgår tydligt i det slutliga förslaget till direktiv att kommissionen har fastställt att någon behandling av personuppgifter inte planeras för att tjäna direktivets syfte. Datatillsynsmannen välkomnar att hans första förslag till tillvägagångssätt till fullo återspeglas i förslaget.

12. Datatillsynsmannen stöder därför det sätt på vilket kommissionen sörjer för att dataskyddsbestämmelserna iakttas i förslaget till direktiv. I återstoden av yttrandet görs endast några detaljerade rekommendationer.

Synpunkter på detaljer

13. Artikel 15 i förslaget till direktiv handlar om skyldigheten för medlemsstaterna att förelägga kommissionen statistiska sammanställningar varje vecka över nivåerna för de kommersiella lager som hålls inom det nationella territoriet. Sådan information innehåller vanligtvis få personuppgifter. Den kan dock innehålla information om fysiska personer som äger oljelager eller som arbetar för en juridisk person som äger lagret. För att hindra medlemsstaterna från att ge kommissionen sådana uppgifter anges i artikel 15.1 att om medlemsstaterna gör detta får ”ägarna till dessa lager [...] inte namnges”. Även om man bör vara medveten om att avlägsnandet av ett namn inte alltid resulterar i uppgifter som inte kan spåras till en fysisk person, förefaller det som om denna kompletterande mening i denna situation (statistiska sammanställningar av oljelagernivåerna) räcker för att säkerställa att personuppgifter inte kommer att överföras till kommissionen.

14. Kommissionens undersökningsbehörighet fastställs i artikel 19 i förslaget till direktiv. Det framgår tydligt av artikeln att kommissionen har följt det första tillvägagångssättet, vilket beskrivs i punkt 8 ovan. Det fastställs att insamling av personuppgifter inte får utgöra en del av de kontroller som genomförs av kommissionen. Och även om kommissionen kommer i kontakt med sådana uppgifter får de inte beaktas och måste förstöras vid oavsiktligt insamling. För att anpassa ordalydelsen till den lydelse som används i dataskyddslagstiftningen och för att undvika eventuella missförstånd rekommenderar datatillsynsmannen att ordet ”insamling” i punkt 2 första meningen ska ersättas av ordet ”behandling”.

15. Datatillsynsmannen välkomnar att det även har tagits med en allmän stödbestämmelse när det gäller relevant dataskyddslagstiftning i förslaget. I artikel 20 erinras medlemsstaterna, kommissionen och andra gemenskapsorgan tydligt om sina skyldigheter enligt direktiv 95/46/EG respektive förordning (EG) nr 45/2001. I artikeln framhålls dessutom de registrerades rättigheter enligt dessa bestämmelser, såsom rätten att motsätta sig att deras uppgifter behandlas, rätten till tillgång till sina uppgifter och rätten att få sina uppgifter rättade om de är oriktiga. Man kan eventuellt ha synpunkter på var i förslaget denna bestämmelse är placerad. Eftersom den är allmänt hållen är den inte enbart begränsad till kommissionens undersökningsbehörighet. Datatillsynsmannen rekommenderar därför att artikeln flyttas till den första delen av direktivet, efter artikel 2 exempelvis.

16. Även i skäl 25 hänvisas det till direktiv 95/46/EG och förordning (EG) nr 45/2001. Syftet med detta skäl är dock ganska oklart eftersom bara dataskyddslagstiftningen som sådan nämns, utan närmare precisering. Det bör i skälet klart framgå att bestämmelserna i direktivet inte påverkar tillämpningen av den nämnda lagstiftningen. Den sista meningen i skälet verkar dessutom innebära att dataskyddslagstiftningen uttryckligen kräver att de registeransvariga omedelbart ska förstöra uppgifter som av misstag samlats in. Även om detta skulle kunna vara konsekvensen av de fastställda bestämmelserna, finns det inte någon sådan skyldighet i den lagstiftningen. Det är en allmän dataskyddsprincip att personuppgifter inte får bevaras längre än nödvändigt för de ändamål för vilka de har

samlats in eller senare behandlas. Om den första delen av skälet anpassas på det sätt som här föreslagits blir den sista meningen överflödig. Datatillsynsmannen föreslår därför att den sista meningen i skäl 25 ska strykas.

III. **SLUTSATS**

17. Datatillsynsmannen stöder det sätt på vilket kommissionen sörjt för att dataskyddsbestämmelserna iakttas i förslaget till direktiv.

18. På detaljnivå rekommenderar datatillsynsmannen

— att ordet ”insamling” i den första meningen i artikel 19.2 ersätts med ordet ”behandling”,

— att artikel 20, som utgör den allmänna dataskyddsbestämmelsen, flyttas till den första delen av direktivet, närmare bestämt direkt efter artikel 2,

— att det i skäl 25 läggs till att bestämmelserna i direktivet inte påverkar tillämpningen av bestämmelserna i direktiv 95/46/EG och förordning (EG) nr 45/2001,

— att skäl 25 sista meningen stryks.

Utfärdat i Bryssel den 3 februari 2009.

Peter HUSTINX

Europeiska datatillsynsmannen

IV

(Upplysningar)

UPPLYSNINGAR FRÅN EUROPEISKA UNIONENS INSTITUTIONER OCH ORGAN

KOMMISSIONEN

Eurons växelkurs [1]

5 juni 2009

(2009/C 128/06)

1 euro =

	Valuta	Kurs		Valuta	Kurs
USD	US-dollar	1,4177	AUD	australisk dollar	1,7606
JPY	japansk yen	137,48	CAD	kanadensisk dollar	1,5657
DKK	dansk krona	7,4472	HKD	Hongkongdollar	10,9887
GBP	pund sterling	0,87920	NZD	nyzeeländsk dollar	2,2263
SEK	svensk krona	10,9250	SGD	singaporiansk dollar	2,0530
CHF	schweizisk franc	1,5191	KRW	sydkoreansk won	1 768,65
ISK	isländsk krona		ZAR	sydafrikansk rand	11,4189
NOK	norsk krona	8,9700	CNY	kinesisk yuan renminbi	9,6871
BGN	bulgarisk lev	1,9558	HRK	kroatisk kuna	7,3550
CZK	tjeckisk koruna	27,003	IDR	indonesisk rupiah	14 078,75
EEK	estnisk krona	15,6466	MYR	malaysisk ringgit	4,9556
HUF	ungersk forint	289,10	PHP	filippinsk peso	67,016
LTL	litauisk litas	3,4528	RUB	rysk rubel	43,5789
LVL	lettisk lats	0,7094	THB	thailändsk baht	48,464
PLN	polsk zloty	4,5420	BRL	brasiliansk real	2,7345
RON	rumänsk leu	4,2185	MXN	mexikansk peso	18,7066
TRY	turkisk lira	2,1834	INR	indisk rupie	66,7910

[1] *Källa*: Referensväxelkurs offentliggjord av Europeiska centralbanken.

RÄTTELSER

Rättelse till räntesats som Europeiska centralbanken tillämpar på sina huvudsakliga refinansieringstransaktioner

(Europeiska unionens officiella tidning C 124 av den 4 juni 2009)

(2009/C 128/07)

På sidan 1 och på omslaget ska det:

i stället för: ”1,00 % den 4 juni 2009”

vara: ”1,00 % den 1 juni 2009”.

PRENUMERATIONSPRISER 2009 (exkl. moms, inkl. frakt och porto)

Europeiska unionens officiella tidning, L- och C-serierna, endast pappersversion	22 officiella EU-språk	1 000 euro per år (*)
Europeiska unionens officiella tidning, L- och C-serierna, endast pappersversion	22 officiella EU-språk	100 euro per månad (*)
Europeiska unionens officiella tidning, L- och C-serierna, pappersversion + årsutgåva på cd-rom	22 officiella EU-språk	1 200 euro per år
Europeiska unionens officiella tidning, L-serien, endast pappersversion	22 officiella EU-språk	700 euro per år
Europeiska unionens officiella tidning, L-serien, endast pappersversion	22 officiella EU-språk	70 euro per månad
Europeiska unionens officiella tidning, C-serien, endast pappersversion	22 officiella EU-språk	400 euro per år
Europeiska unionens officiella tidning, C-serien, endast pappersversion	22 officiella EU-språk	40 euro per månad
Europeiska unionens officiella tidning, L- och C-serierna, månatlig (kumulativ) utgåva på cd-rom	22 officiella EU-språk	500 euro per år
Tillägg till *Europeiska unionens officiella tidning* (S-serien), meddelanden och offentliga kontrakt, cd-rom, 2 nummer per vecka	flerspråkig: 23 officiella EU-språk	360 euro per år (= 30 euro per månad)
Europeiska unionens officiella tidning, C-serien – allmänna uttagningsprov	Antal språk beroende på uttagningsprov	50 euro per år

(*) Lösnummerpris:

1–32 sidor:	6 euro
33–64 sidor:	12 euro
Mer än 64 sidor:	Priset varierar

Europeiska unionens officiella tidning (EUT) ges ut på EU:s officiella språk, och det går att prenumerera på den i 22 olika språkversioner. Den består av två serier: L (lagstiftning) och C (meddelanden och upplysningar).

Varje språkversion kräver en separat prenumeration.

Enligt rådets förordning (EG) nr 920/2005 som offentliggjordes i EUT L 156 av den 18 juni 2005 är Europeiska unionens institutioner under en övergångsperiod inte skyldiga att avfatta och offentliggöra alla rättsakter på iriska. Den iriska utgåvan av EUT säljs därför separat.

En prenumeration på tillägget till EUT (S-serien: meddelanden och offentliga kontrakt) omfattar en flerspråkig cd-rom med alla de 23 officiella språkversionerna.

Prenumeranter på EUT kan på begäran få de olika bilagorna till tidningen. När en bilaga ges ut meddelas prenumeranterna detta genom ett ”meddelande till läsarna” i *Europeiska unionens officiella tidning*.

Försäljning och prenumeration

Publikationsbyrån ger ut publikationer för försäljning som kan beställas från någon av våra kommersiella distributörer. En lista över dessa finns på följande Internetadress:

http://publications.europa.eu/others/agents/index_sv.htm

Via EUR-Lex (http://eur-lex.europa.eu) har du kostnadsfritt direkt tillgång till Europeiska unionens lagstiftning. På webbplatsen kan du söka i *Europeiska unionens officiella tidning* samt i fördrag, lagstiftning, rättspraxis och förberedande rättsakter.

Mer information om Europeiska unionen finns på http://europa.eu

Publikationsbyrån
Publications.europa.eu

BYRÅN FÖR EUROPEISKA GEMENSKAPERNAS OFFICIELLA PUBLIKATIONER
L-2985 LUXEMBURG

SV