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