I

(Resolutioner, rekommendationer och yttranden)

YTTRANDEN

EUROPEISKA DATATILLSYNSMANNEN

Yttrande från Europeiska datatillsynsmannen om kommissionens meddelande till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén och Regionkommittén – ”Ett samlat grepp på skyddet av personuppgifter i Europeiska unionen”

(2011/C 181/01)

EUROPEISKA DATATILLSYNSMANNEN HAR ANTAGIT DETTA YTTRANDE

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 16,

med beaktande av Europeiska unionens stadga om de grundläggande rättigheterna, särskilt artiklarna 7 och 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.

A. ALLMÄNT

1. Inledning

1.1 *En första och allmän bedömning*

1. Den 4 november 2010 antog kommissionen ett meddelande med titeln ”Ett samlat grepp på skyddet av personuppgifter i Europeiska unionen” (”meddelandet”) ([3]). Meddelandet sändes till Europeiska datatillsynsmannen för samråd. Datatillsynsmannen välkomnar att kommissionen samrått med honom i enlighet med artikel 41 i förordning (EG) nr 45/2001. Han fick möjlighet att lämna informella kommentarer redan innan meddelandet antogs och vissa av dessa kommentarer har beaktats i slutversionen av dokumentet.

2. I meddelandet beskrivs hur kommissionen ska hantera översynen av EU:s rättsliga ram för skyddet av personuppgifter på alla EU:s verksamhetsområden, med särskild hänsyn till de utmaningar som globaliseringen och den nya tekniken medför ([4]).

3. Europeiska datatillsynsmannen välkomnar meddelandet rent allmänt, eftersom han är övertygad om att en översyn av den nuvarande rättsliga ramen för skydd av personuppgifter inom EU är nödvändig för att säkra ett effektivt skydd för informationssamhällets fortsatta utveckling. Redan i sitt yttrande av den 25 juli 2007 om genomförande av dataskyddsdirektivet ([5]) drog han slutsatsen att förändringar av direktiv 95/46/EG förefaller oundvikliga på längre sikt.

4. Meddelandet utgör ett viktigt steg i riktning mot en sådan ändring av lagen som i sin tur skulle vara den viktigaste utvecklingen när det gäller uppgiftsskydd inom EU sedan direktiv 95/46/EG antogs, vilket i allmänhet betraktas som den viktigaste hörnstenen för dataskydd inom Europeiska unionen (och i ett vidare begrepp inom Europeiska ekonomiska samarbetsområdet).

5. Meddelandet erbjuder rätt ram för en målinriktad översyn, även på grund av att det rent allmänt identifierar huvudfrågor och utmaningar. Datatillsynsmannen instämmer i kommissionens uppfattning att ett starkt system för dataskydd kommer att behövas även i framtiden, baserat på principen att befintliga allmänna principer för dataskydd fortfarande är giltiga i ett samhälle som genomgår grundläggande förändringar på grund av snabb teknisk utveckling och globalisering. Detta kräver att befintliga lagstiftningslösningar ses över.

([1]) EGT L 281, 23.11.1995, s. 31.
([2]) EGT L 8, 12.1.2001, s. 1.
([3]) KOM(2010) 609 slutlig.
([4]) Se s. 5 i meddelandet, första stycket.
([5]) Yttrande från Europeiska datatillsynsmannen av den 25 juli 2007 om meddelandet från kommissionen till Europaparlamentet och rådet om uppföljningen av arbetsprogrammet för ett bättre genomförande av dataskyddsdirektivet, (EUT C 255, 27.10.2007, s. 1).

6. I meddelandet betonas med rätta att utmaningarna är enorma. Datatillsynsmannen instämmer i yttrandet och betonar att de föreslagna lösningarna bör vara lika ambitiösa och göra skyddet effektivare.

1.2 *Syftet med yttrandet*

7. I detta yttrande bedöms de lösningar som föreslås i meddelandet på grundval av följande två kriterier: ambition och effektivitet. Perspektivet är på det hela taget positivt. Datatillsynsmannen stöder meddelandet men är samtidigt kritisk till aspekter där enligt hans uppfattning större ambitioner skulle leda till ett effektivare system.

8. Datatillsynsmannen hoppas med detta yttrande kunna bidra till att den rättsliga ramen för dataskydd utvecklas ytterligare. Han ser fram emot kommissionens förslag som förväntas under mitten av 2011 och hoppas att hans idéer kommer att beaktas i förslaget. Han noterar också att man i meddelandet förefaller utesluta vissa områden, exempelvis behandling av uppgifter inom EU:s institutioner och organ, från det allmänna instrumentet. Om kommissionen verkligen skulle besluta sig för att utelämna vissa områden på detta stadium – något som datatillsynsmannen skulle beklaga – vädjar han till kommissionen att åta sig att ta fram en heltäckande utformning inom en kort och angiven tidsram.

1.3 *Yttrandets beståndsdelar*

9. Det här yttrandet är inte fristående. Det bygger på tidigare ståndpunkter från datatillsynsmannen och Europeiska dataskyddsmyndigheter vid olika tillfällen. Det bör framför allt betonas att i det tidigare nämnda yttrandet från datatillsynsmannen av den 25 juli 2007 fastställdes och utvecklades några viktiga beståndsdelar i framtida ändringar ([6]). Yttrandet bygger också på diskussioner med andra aktörer på området integritet och dataskydd. Deras bidrag utgjorde en mycket användbar bakgrund för både meddelandet och detta yttrande. Man kan därför dra slutsatsen att det finns synergier när det gäller hur dataskyddet kan effektiviseras.

10. En annan viktig komponent i detta yttrande är dokumentet ”Integritetens framtid”, det gemensamma bidraget från artikel 29-arbetsgruppen och arbetsgruppen om polis och rättsväsende som inleddes av kommissionen 2009 (”arbetsgruppens dokument om integritetens framtid”) ([7]).

11. Vid en presskonferens den 15 november 2010 lämnade datatillsynsmannen också sina första reaktioner på det aktuella meddelandet. I detta yttrande utvecklas närmare de mer allmänna uppfattningar som framfördes under presskonferensen ([8]).

12. Avslutningsvis utnyttjas i detta yttrande ett antal tidigare yttranden från datatillsynsmannen samt handlingar från artikel 29-arbetsgruppen. Hänvisningar till dessa yttranden och handlingar görs på olika platser i detta yttrande när det är relevant.

2. **Bakgrund**

13. Översynen av reglerna för dataskydd genomförs vid en historiskt avgörande tidpunkt. I meddelandet beskrivs bakgrunden på ett omfattande och övertygande sätt. Baserat på den beskrivningen identifierar datatillsynsmannen de fyra huvudfaktorer som avgör den miljö där översynsprocessen äger rum.

14. Den första faktorn är teknisk utveckling. Dagens teknik är inte densamma som när direktiv 95/46/EG utformades och antogs. Tekniska företeelser som datormoln, beteendestyrd annonsering, sociala nätverk, vägtullar och gps-system förändrade på djupet hur uppgifter behandlas och innebär enorma utmaningar för dataskyddet. I en översyn av reglerna för europeiskt dataskydd måste dessa utmaningar tas upp på ett effektivt sätt.

15. Den andra faktorn är globaliseringen. Det successiva avskaffandet av handelshinder har gjort affärsverksamheten allt mer internationell. Gränsöverskridande hantering av

([6]) Se särskilt (punkt 77 i yttrandet): Inget behov av att ändra befintliga principer men ett klart behov av andra administrativa lösningar, dataskyddslagstiftningens breda tillämpning på all användning av personuppgifter bör inte förändras, dataskyddslagstiftningen bör möjliggöra ett balanserat tillvägagångssätt i konkreta fall och bör också göra det möjligt för dataskyddsmyndigheterna att fastställa prioriteringar; systemet bör gälla fullt ut för användningen av personuppgifter vid brottsbekämpning, men det kan krävas ytterligare lämpliga åtgärder för att hantera särskilda problem på detta område.

([7]) Arbetsgruppens dokument 168 (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf). Dess huvudbudskap är att en lagändring är ett bra tillfälle att klargöra vissa huvudregler och principer (exempelvis samtycke, öppenhet), införa några nya principer (exempelvis inbyggda skyddsmekanismer, ansvarighet), öka effektiviteten genom att modernisera lösningarna (exempelvis genom att begränsa befintliga anmälningskrav) och samla allt i ett heltäckande regelverk (inbegripet polisiärt och rättsligt samarbete).

([8]) Presskonferensens talepunkter finns på datatillsynsmannens webbplats: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-11-15_Press_conf_speaking_points_PHBG_EN.pdf

uppgifter internationella överföringar har ökat enormt de senaste åren. Dessutom har behandling av uppgifter blivit allestädes närvarande på grund av informations- och kommunikationsteknik: Internet och datormoln gjorde det möjligt att utlokalisera hanteringen av stora mängder uppgifter över hela världen. Under det senaste årtiondet har vi också sett en ökning av internationella polisiära och rättsliga åtgärder för att bekämpa terrorism och andra former av internationell organiserad brottslighet, med stöd av ett enormt utbyte av information. Allt detta kräver noggranna överväganden om hur skydd av personuppgifter kan tryggas effektivt i en globaliserad värld, utan att internationella databehandlingsåtgärder hindras alltför mycket.

16. Den tredje faktorn är Lissabonfördraget. Lissabonfördragets ikraftträdande innebär en ny era för uppgiftsskyddet. Artikel 16 i fördraget om Europeiska unionens funktionssätt innehåller inte bara en individuell rätt för den som berörs av uppgifterna utan även en direkt rättslig grund för en stark lag i hela EU om uppgiftsskydd. I och med att pelarstrukturen avskaffats blir Europaparlamentet och rådet dessutom skyldiga att tillhandahålla uppgiftsskydd inom alla områden i EU:s lagstiftning. Med andra ord möjliggör det en omfattande rättslig ram för uppgiftsskydd som kan tillämpas på den privata sektorn, den offentliga sektorn i medlemsstaterna och EU:s institutioner och organ. I Stockholmsprogrammet ([9]) fastställs genomgående i detta hänseende att unionen behöver säkerställa en omfattande strategi för att skydda uppgifter inom EU och sina förbindelser med andra länder.

17. Den fjärde faktorn utgörs av parallella utvecklingar som äger rum inom internationella organisationer. Olika pågående debatter fokuserar på modernisering av de nuvarande rättsliga instrumenten för uppgiftsskydd. Det är viktigt att i detta sammanhang nämna de aktuella reflektioner som gjorts om den kommande översynen av Europarådets konvention 108 ([10]) och av OECD:s riktlinjer för privatlivet ([11]). En annan viktig utveckling gäller antagandet av internationella normer för skydd av personuppgifter och integritet, som eventuellt kan leda till att ett bindande övergripande instrument om dataskydd antas. Samtliga dessa initiativ förtjänar att stödjas i sin helhet. Deras gemensamma mål bör vara att säkra ett effektivt och konsekvent skydd i en teknikdriven och globaliserad miljö.

3. **Huvudperspektiv**

3.1 *Dataskydd främjar tillit och måste stödja andra (offentliga) intressen*

18. En stark ram för dataskydd är den nödvändiga konsekvensen av den betydelse som dataskydd fått enligt Lissabonfördraget, särskilt artikel 8 i unionens stadga om de grundläggande rättigheterna och artikel 16 i fördraget om Europeiska unionens funktionssätt, liksom den starka kopplingen till artikel 7 i stadgan ([12]).

19. En stark ram för dataskydd gynnar emellertid också större offentliga och privata intressen i ett informationssamhälle där behandling av uppgifter förekommer överallt. Dataskydd främjar förtroende som är ett grundläggande inslag i ett väl fungerande samhälle. Det är avgörande att lösningar för dataskydd tolkas på ett sätt så att de – så långt det är möjligt – aktivt stödjer snarare än hindrar andra berättigade rättigheter och intressen.

20. Viktiga exempel på andra berättigade intressen är en stark europeisk ekonomi, enskildas säkerhet liksom regeringars ansvarighet.

21. Ekonomisk utveckling inom EU går hand i hand med införande och marknadsföring av ny teknik och nya tjänster. I informationssamhället är framväxt och framgångsrik utveckling av informations- och kommunikationsteknik och tjänster beroende av förtroende. Om människor inte litar på informations- och kommunikationstekniken riskerar tekniken att misslyckas ([13]). Och människor kommer endast att lita på informations- och kommunikationstekniken om deras uppgifter skyddas effektivt. Dataskydd bör därför vara en integrerad del av teknik och tjänster. En stark ram för dataskydd främjar den europeiska ekonomin, under förutsättning att detta ramverk inte bara är starkt utan även utformat på rätt sätt. Ytterligare harmonisering inom EU och minimering av administrativa bördor är i detta sammanhang grundläggande (se kapitel 5 i yttrandet).

22. Mycket har de senaste åren sagts om behovet av balans mellan integritet och säkerhet, särskilt i förhållande till instrument för behandling och utbyte av data på området polissamarbete och rättsligt samarbete ([14]). Dataskydd beskrevs ganska ofta felaktigt som ett hinder för att fullt ut skydda enskildas fysiska säkerhet ([15]), eller åtminstone som ett oundvikligt villkor som skulle respekteras av brottsbekämpande myndigheter. Det är emellertid inte hela sanningen. En stark ram för dataskydd kan vässa och stärka säkerheten. På grundval av principerna om dataskydd ska registeransvariga – när principerna fungerar väl – se till att informationen är korrekt och uppdaterad och att överflödiga personuppgifter som inte krävs för brottsbekämpning raderas i systemen. Man kan även peka på skyldigheter att genomföra tekniska och

([9]) Stockholmsprogrammet Ett öppet och säkert EU som tjänar och skyddar sina medborgare, (EUT C 115, 4.5.2010, s. 1), på s. 10.

([10]) Europarådets konvention 108 om skydd för enskilda vid automatisk behandling av personuppgifter, ETS Nr 108, 28 januari 1981.

([11]) OECD:s riktlinjer för integritetsskydd och gränsöverskridande flöden av personuppgifter, publicerade på http://www.oecd.org

([12]) Denna betydelse av dataskydd och kopplingen till integritet i stadgan betonades av EG-domstolen i dess dom av den 9 november 2010, gemensamma målen C-92/09 och C-93/09, *Schecke*, ännu ej publicerad i rättsfallssamlingen.

([13]) Se Europeiska datatillsynsmannens yttrande av den 18 mars 2010 om att främja förtroendet för informationssamhället genom data- och integritetsskydd, (EUT C 280, 16.10.2010, s. 1), punkt 113.

([14]) Se exempelvis datatillsynsmannens yttrande av den 10 juli 2009 om kommissionens meddelande till Europaparlamentet och rådet om ett område med frihet, säkerhet och rättvisa i allmänhetens tjänst, (EUT C 276, 17.9.2009, s. 8).

([15]) Säkerhet är ett vidare begrepp än fysisk säkerhet, men som en illustration av de argument som det handlar om här används det här i den mer begränsade betydelsen.

åorganisatoriska åtgärder för att trygga säkerheten i system, exempelvis system som skyddar mot otillåten spridning eller tillträde och som har utvecklats inom dataskyddsområdet.

23. Om principerna för skydd av uppgifter följs kan det ytterligare bidra till att de brottsbekämpande myndigheterna följer rättsstatens regler vilket leder till förtroende för deras uppträdande och i en vidare mening främjar förtroendet för våra samhällen. Den rättspraxis som utvecklas i artikel 8 i den europeiska konventionen om skydd för de mänskliga rättigheterna tryggar att polis- och rättsväsende kan behandla alla uppgifter som är relevanta för deras arbete men inte på ett obegränsat sätt. Dataskydd kräver kontroller och balanser (se kapitel 9 i yttrandet om polis- och rättsväsende).

24. I demokratiska samhällen är regeringar ansvariga för alla sina åtgärder, vilket även innefattar användning av personuppgifter för olika offentliga intressen. Detta sträcker sig från offentliggörande av uppgifter på Internet av öppenhetsskäl, till användning av uppgifter som ett stöd till politik inom områden som folkhälsa, transport eller beskattning, eller övervakning av enskilda i brottsbekämpande syfte. Med hjälp av ett starkt ramverk för dataskydd kan regeringar ta sitt ansvar och vara ansvariga som en del av en god förvaltning.

3.2 *Konsekvenser för den rättsliga ramen för dataskydd*

3.2.1 Ytterligare harmonisering krävs

25. I meddelandet slogs med rätta fast att en av den nuvarande ramens största brister är att medlemsstaterna i alltför stor utsträckning själva kan bestämma om införlivandet av EU:s bestämmelser i nationell lag. Bristande harmonisering får ett antal negativa konsekvenser i ett informationssamhälle där de fysiska gränserna mellan medlemsstaterna blir allt mindre relevanta (se kapitel 5 i yttrandet).

3.2.2 Allmänna principer för dataskydd är fortfarande giltiga

26. Ett första och mer formellt skäl till att de allmänna principerna för dataskydd varken bör eller kan ändras är av rättsligt slag. Dessa principer slås fast i Europarådets konvention 108 som är bindande för alla medlemsstater. Konventionen ligger till grund för dataskyddet inom EU. Några av huvudprinciperna nämns dessutom uttryckligen i artikel 8 i stadgan om de grundläggande rättigheterna i unionen. Om dessa principer ändras skulle alltså fördragen behöva ändras.

27. Det är emellertid inte hela sanningen. Det finns också avsevärda skäl till att inte ändra de allmänna principerna. Datatillsynsmannen anser att ett informationssamhälle inte kan eller bör fungera utan lämpligt skydd av enskildas privatliv och personuppgifter. När mer information hanteras behövs också ett bättre skydd. Ett informationssamhälle där ett överflöd av information om alla behandlas behöver bygga på begreppet med den enskildas kontroll, så att han eller hon kan agera som enskild och använda sina friheter i ett demokratiskt samhälle, exempelvis yttrandefriheten.

28. Det är dessutom svårt att tänka sig kontroll av den enskilda utan att de ansvariga är skyldiga att begränsa behandlingen enligt principerna om nödvändighet, proportionalitet och begränsning av syfte. Det är också svårt att tänka sig kontroll av den enskilda om det inte finns några erkända rättigheter för registrerade, exempelvis rätten till tillträde, ändring, radering eller blockering av uppgifter.

3.2.3 Perspektivet med grundläggande rättigheter

29. Datatillsynsmannen betonar att dataskydd erkänns som en grundläggande rättighet. Det innebär inte att dataskydd alltid ska ha företräde före andra viktiga rättigheter och intressen i ett demokratiskt samhälle, men det får konsekvenser för form och omfattning av det skydd som måste erbjudas enligt en rättslig ram inom EU, så att kraven när det gäller dataskydd alltid beaktas på lämpligt sätt.

30. Dessa huvudsakliga konsekvenser kan definieras på följande sätt:

— Skyddet måste vara effektivt. En rättslig ram måste tillhandahålla instrument som gör att enskilda kan utöva sina rättigheter i praktiken.

— Ramen måste vara stabil under en lång period.

— Skydd måste erbjudas under alla omständigheter och får inte bero på politiska preferenser inom en viss tidsram.

— Utövandet av rätten kan behöva begränsas, men det måste utgöra ett undantag, motiveras på lämpligt sätt och aldrig påverka de grundläggande beståndsdelarna i själva rättigheten ([16]).

Datatillsynsmannen rekommenderar att kommissionen tar hänsyn till dessa konsekvenser när lagstiftningsförslag föreslås.

3.2.4 Nya lagstiftningsförslag behövs

31. Meddelandet koncentreras med rätta på behovet av att stärka lagstiftningslösningar för dataskydd. I detta sammanhang är det lämpligt att erinra om att i arbetsgruppens dokument om integritetens framtid ([17]) betonade dataskyddsmyndigheterna behovet av starkare roller för

([16]) Se även Europeiska datatillsynsmannens yttrande av den 25 juli 2007 om kommissionens meddelande till Europaparlamentet och rådet om uppföljningen av arbetsprogrammet för ett bättre genomförande av dataskyddsdirektivet, punkt 17, som bygger på rättspraxis från Europadomstolen och EG-domstolen.

([17]) Se fotnot 7.

dataskyddsområdets olika aktörer, framför allt registrerade personer, registeransvariga och de övervakande myndigheterna själva.

32. Intressenterna förefaller ha en bred samsyn om att starkare lagstiftningslösningar – som tar hänsyn till teknisk utveckling och globalisering – är nyckeln till ett ambitiöst och effektivt dataskydd även i framtiden. Såsom redan angivits i punkt 7 är detta datatillsynsmannens kriterier för bedömning av alla föreslagna lösningar.

3.2.5 Allsidighet som en nödvändig förutsättning

33. Såsom erinras om i meddelandet gäller direktiv 95/46/EG all verksamhet rörande behandling av personuppgifter i medlemsstaterna inom både offentlig och privat sektor, med undantag för åtgärder som inte omfattas av tidigare gemenskapslagstiftning ([18]). Detta undantag behövdes enligt det tidigare fördraget men är inte längre nödvändigt efter att Lissabonfördraget trätt i kraft. Dessutom strider undantaget mot – texten och i vilket fall som helst andan i – artikel 16 i fördraget om Europeiska unionens funktionssätt.

34. Enligt datatillsynsmannen måste ett omfattande lagstiftningsinstrument för dataskydd inbegripet polisiärt och rättsligt samarbete i brottmål ses som en av de viktigaste förbättringar som en ny rättslig ram kan åstadkomma. Det är en nödvändig förutsättning för ett effektivt dataskydd i framtiden.

35. Datatillsynsmannen betonar följande argument som stöd för detta uttalande:

— Distinktionen mellan åtgärder inom den privata sektorn och sektorn för brottsbekämpning är oklar. Enheter inom den privata sektorn kan behandla uppgifter som sedan används brottsförebyggande (exempelvis: passageraruppgifter ([19])), medan de i andra fall måste behålla uppgifterna i brottsförebyggande syfte (exempelvis: direktivet om lagring av uppgifter ([20])).

— Det finns ingen grundläggande skillnad mellan polisiära och rättsliga myndigheter och andra brottsbekämpande myndigheter (skattemyndigheter, tull, bedrägeribekämpning, immigrationsmyndigheter) när det gäller direktiv 95/46/EG.

— I meddelandet anges helt korrekt att de rättsliga instrument för dataskydd som för närvarande är tillämpliga på polisiära och rättsliga myndigheter (rambeslut 2008/977/RIF ([21])) är otillräckliga.

— Flertalet medlemsstater har införlivat direktiv 95/46/EG och konvention 108 i sin nationella lagstiftning och därmed gjort dem tillämpliga för de polisiära och rättsliga myndigheterna.

36. Att låta polis och rättsliga myndigheter omfattas av det allmänna rättsliga instrumentet skulle inte bara innebära större garantier för medborgarna utan också göra polismyndigheternas uppgift enklare. Att behöva tillämpa olika uppsättningar regler är besvärligt, onödigt tidsödande och hindrar internationellt samarbete (se vidare kapitel 9 i yttrandet). Detta talar också för att även behandling vid nationella säkerhetstjänster bör ingå, under förutsättning att det är möjligt enligt nuvarande EU-lagstiftning.

3.2.6 Teknisk neutralitet

37. Tiden sedan direktiv 95/46/EG antogs 1995 kan beskrivas som tekniskt turbulent. Den tekniska utvecklingen går framåt och nya hjälpmedel införs hela tiden. I många fall har detta lett till grundläggande förändringar av hur enskildas personuppgifter hanteras. Informationssamhället kan inte längre betraktas som en parallell miljö där enskilda frivilligt kan delta utan har blivit en integrerad del av vårt dagliga liv. Bara som ett exempel upprättar sakernas Internet ([22]) förbindelser mellan fysiska objekt och information på nätet som handlar om dem.

38. Tekniken kommer att utvecklas ytterligare. Detta får konsekvenser för den nya rättsliga ramen. Den måste fungera under ett stort antal år, och samtidigt inte hindra ytterligare teknisk utveckling. Det kräver tekniskt neutrala lagstiftningslösningar. Ramen måste emellertid också skapa större rättssäkerhet för företag och enskilda. De måste förstå vad som förväntas av dem och kunna utöva sina rättigheter. Lagstiftningslösningarna måste därför vara exakta.

39. Enligt datatillsynsmannen måste ett allmänt instrument för skydd av uppgifter så långt det är möjligt utformas på ett tekniskt neutralt sätt. Det innebär att rättigheter och skyldigheter för olika aktörer måste formuleras på ett allmänt och neutralt sätt så att de i princip förblir giltiga och verkställbara oavsett vilken teknik som väljs för att behandla personuppgifterna. Det finns inget annat val, med tanke på hur snabbt tekniken nu utvecklas. Datatillsynsmannen föreslår att nya ”tekniskt neutrala” rättigheter

([18]) Detta yttrande kommer huvudsakligen att inriktas på den tidigare tredje pelaren (polisiärt och rättsligt samarbete i brottmål), eftersom den tidigare andra pelaren inte bara är ett mer komplicerat område av EU:s lagstiftning (vilket också erkänns i artikel 16 i fördraget om Europeiska unionens funktionssätt och artikel 39 i fördraget om Europeiska unionen), men också i mindre utsträckning relevant för behandling av uppgifter.

([19]) Se exempelvis kommissionens meddelande om en övergripande strategi när det gäller överföring av passageraruppgifter (PNR-uppgifter) till tredjeländer, KOM(2010) 492 slutlig.

([20]) Europaparlamentets och rådets direktiv 2006/24/EG av den 15 mars 2006 om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät, och om ändring av direktiv 2002/58/EG (EUT L 105, 13.4.2006, s. 54).

([21]) Rådets rambeslut 2008/977/RIF av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete (EUT L 350, 30.12.2008, s. 60).

([22]) Enligt definitionen i ”Sakernas Internet – en handlingsplan för Europa”, KOM(2009) 278 slutlig.

ska införas utöver befintliga principer för dataskydd, något som skulle kunna få särskild betydelse i en snabbt förändlig elektronisk miljö (se huvudsakligen kapitel 6 och 7).

3.2.7 Långsiktigt: Rättssäkerhet under längre tid

40. Direktiv 95/46/EG har varit det huvudsakliga dokumentet när det gäller dataskydd inom EU under de senaste 15 åren. Det införlivades i medlemsstaternas lagstiftning och tillämpades av olika aktörer. Under åren har man utnyttjat praktiska erfarenheter och ytterligare rådgivning från kommissionen, dataskyddsmyndigheter (på nationell nivå och inom ramen för artikel 29-arbetsgruppen) samt nationella och europeiska domstolar.

41. Det är bra att betona att denna utveckling kräver tid och – särskilt eftersom vi har att göra med en allmän ram som påverkar en grundläggande rättighet – att denna tid behövs för att skapa rättssäkerhet och stabilitet. Ett nytt allmänt rättsligt instrument behöver utarbetas med ambitionen att det ska kunna skapa rättssäkerhet och stabilitet under en längre period, och med tanke på att det är mycket svårt att förutsäga hur teknik och globalisering kommer att utvecklas ytterligare. I vilket fall som helst stöder datatillsynsmannen målet att skapa rättssäkerhet under en längre tid, jämfört med perspektivet i direktiv 95/46/EG. När tekniken utvecklas snabbt måste lagen vara stabil.

3.2.8 Kortsiktigt: Bättre utnyttjande av befintliga instrument

42. På kort sikt är det avgörande att befintliga lagstiftningslösningar är effektiva, i första hand genom att koncentreras på verkställighet, på nationell nivå och EU-nivå (se kapitel 11 i detta yttrande).

B. **BESTÅNDSDELAR I EN NY RAM**

4. **Övergripande strategi**

43. Datatillsynsmannen stöder helt det samlade greppet på skyddet av uppgifter som inte bara är titeln utan också utgångspunkten för meddelandet och nödvändigtvis innefattar en utvidgning av de allmänna reglerna för dataskydd till polissamarbete och straffrättsligt samarbete ([23]).

44. Datatillsynsmannen noterar emellertid också att kommissionen inte har för avsikt att ta med all behandling av uppgifter i detta allmänna rättsliga instrument. Behandling av uppgifter inom EU:s institutioner, organ, kontor och byråer kommer framför allt inte att omfattas. Kommissionen slår endast fast att den ”kommer att bedöma behovet av att anpassa andra rättsliga instrument till den nya allmänna ramen för dataskydd”.

([23]) Se s. 14 i meddelandet och avsnitt 3.2.5 i detta yttrande.

45. Europeiska datatillsynsmannen föredrar absolut att behandling på EU-nivå ska ingå i den allmänna rättsliga ramen. Han erinrar om att detta var den ursprungliga avsikten i den tidigare artikel 286 EG där dataskydd för första gången nämndes i fördraget. Artikel 286 EG innebar helt enkelt att rättsliga instrument för behandling av personuppgifter även skulle gälla för institutionerna. Vad som är ännu viktigare är att en lagtext innebär att risken för bristande överensstämmelse mellan bestämmelser undviks och den skulle vara bäst lämpad för utbyte av uppgifter mellan EU och offentliga och privata enheter i medlemsstaterna. Det skulle också innebära att man undviker risken att det efter ändring av direktiv 95/46/EG inte längre finns något politiskt intresse av att ändra förordning (EG) nr 45/2001 eller ge denna ändring tillräcklig prioritet för att undvika bristande överensstämmelse när det gäller datum för ikraftträdande.

46. Datatillsynsmannen vädjar till kommissionen – i det fall den skulle dra slutsatsen att det inte skulle vara möjligt att införliva behandling på EU-nivå i det allmänna rättsliga instrumentet – att föreslå en anpassning av förordning (EG) nr 45/2001 (inte ”bedöma behovet”) så snart som möjligt och helst före slutet av 2011.

47. Det är lika viktigt att kommissionen ser till att andra områden inte hamnar på efterkälken, framför allt följande:

— Dataskydd i den gemensamma utrikes- och säkerhetspolitiken, på grundval av artikel 39 i fördraget om Europeiska unionens funktionssätt ([24]).

— Sektorspecifika system för dataskydd för EU:s organ, exempelvis Europol, Eurojust och för storskaliga informationssystem, i den mån de behöver anpassas till det nya rättsliga instrumentet.

— Direktivet om integritet och elektronisk kommunikation 2002/58 i den mån det behöver anpassas till det nya rättsliga instrumentet.

48. Avslutningsvis kan och sannolikt bör ett allmänt rättsligt instrument för dataskydd kompletteras med ytterligare sektorsvisa och specifika förordningar, exempelvis för polissamarbete och rättsligt samarbete, men även inom andra områden ([25]). Vid behov och för att vara förenliga med subsidiaritetsprincipen bör dessa ytterligare förordningar antas på EU-nivå. Medlemsstaterna kan utarbeta ytterligare regler inom särskilda områden när detta är befogat (se 5.2).

([24]) Se även Europeiska datatillsynsmannens yttrande av den 24 november 2010 om kommissionens meddelande till Europaparlamentet och rådet – EU:s strategi för terrorismbekämpning: Viktiga framsteg och kommande utmaningar, punkt 31.

([25]) Se även arbetsgruppens dokument om integritetens framtid (fotnot 7), punkterna 18–21.

5. Ytterligare harmonisering och förenkling

5.1 *Behovet av harmonisering*

49. Harmonisering är av största betydelse för EU:s lagstiftning om dataskydd. I meddelandet betonas med rätta att dataskydd har en stark koppling till den inre marknaden eftersom det måste säkra fritt flöde av personuppgifter mellan medlemsstaterna på den inre marknaden. Harmoniseringsnivån enligt det nuvarande direktivet har emellertid bedömts som allt annat än tillfredsställande. I meddelandet erkänns att detta är ett av de vanligaste återkommande orosmomenten bland intressenter. Intressenterna betonar framför allt behovet av att förbättra rättssäkerheten, minska den administrativa bördan och se till att de ekonomiska aktörerna har samma villkor. Såsom kommissionen med rätta noterar gäller detta särskilt för registeransvariga som är etablerade i flera medlemsstater och som måste uppfylla (sannolikt olika) krav i nationell lagstiftning om dataskydd ([26]).

50. Harmonisering är inte enbart viktigt för den inre marknaden utan även för att säkra lämpligt dataskydd. Enligt artikel 16 i fördraget om Europeiska unionens funktionssätt har ”alla” rätt till skydd av personuppgifter som gäller dem. För att denna rättighet verkligen ska respekteras måste samma skyddsnivå garanteras i hela EU. I arbetsgruppens dokument om integritetens framtid betonades att flera bestämmelser om de registrerades ställning inte har införlivats eller tolkats enhetligt i alla medlemsstater ([27]). I en globaliserad och sammanlänkad värld kan dessa skillnader underminera eller begränsa enskildas skydd.

51. Datatillsynsmannen anser att ytterligare och bättre harmonisering är en av huvudmålsättningarna med översynsförfarandet. Han välkomnar kommissionens avsikt att granska möjligheterna att uppnå ytterligare harmonisering av dataskydd på EU-nivå. Han noterar dock med viss förvåning att meddelandet på detta stadium inte innehåller några konkreta förslag. Han anger därför själv ett antal områden där det snarast krävs större enhetlighet (se 5.3). Ytterligare harmonisering inom dessa områden bör inte enbart uppnås genom att manöverutrymmet för nationell lag minskas utan även förebygga felaktigt införlivande i medlemsstaterna (se även kapitel 11) och säkra ett mer enhetligt och samordnat verkställande (se även kapitel 10).

5.2 *Minskning av manöverutrymmet vid direktivets införlivande*

52. Direktivet innehåller ett antal brett utformade bestämmelser som lämnar stort utrymme för olika införlivanden. I skäl 9 i direktivet bekräftas uttryckligen att medlemsstaterna har fått ett visst manöverutrymme och att skillnader inom denna marginal kan uppstå vid direktivets införlivande. Flera bestämmelser har införlivats på olika sätt av medlemsstaterna, inbegripet några avgörande bestämmelser ([28]). Situationen är inte tillfredsställande och större enhetlighet borde eftersträvas.

53. Det innebär inte att mångfald bör uteslutas utan vidare. Inom vissa områden kan flexibilitet behövas för att behålla motiverade särdrag, viktiga offentliga intressen eller institutionell självständighet i medlemsstaterna. Enligt datatillsynsmannen bör utrymmet för skillnader mellan medlemsstaterna framför allt begränsas till följande specifika situationer:

— Yttrandefrihet: Enligt den nuvarande ramen (artikel 9) kan medlemsstaterna bevilja undantag och avvikelser när det gäller behandling av uppgifter i journalistiskt syfte eller i konstnärliga eller litterära sammanhang. Denna flexibilitet förefaller väl lämpad, naturligtvis med förbehåll för gränser i stadgan och den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna, med tanke på olika traditioner och kulturella skillnader som kan finnas inom detta område i de olika medlemsstaterna. Det skulle emellertid inte hindra att nuvarande artikel 9 uppdateras mot bakgrund av Internets utveckling.

— Särskilda offentliga intressen: Enligt den nuvarande ramen (artikel 13) kan medlemsstaterna anta lagstiftningsåtgärder för att begränsa omfattningen av skyldigheter och rättigheter när en sådan begränsning utgör en nödvändig åtgärd för att skydda viktiga offentliga intressen såsom nationell säkerhet, försvar, offentlig säkerhet, etc. En sådan behörighet för medlemsstaterna är fortfarande motiverad. När så är möjligt bör emellertid tolkningen av undantagen harmoniseras ytterligare (se avsnitt 9.1). Dessutom förefaller den nuvarande omfattningen av undantag från artikel 6.1 onödigt omfattande.

— Rättsmedel, sanktioner och administrativa förfaranden: Ett europeiskt ramverk skulle fastställa huvudvillkoren, men enligt EU-lagstiftningens nuvarande utformning måste fastställande av sanktioner, rättsmedel, förfaranderegler och villkoren för inspektioner som är tillämpliga på nationell nivå ligga hos medlemsstaterna.

([26]) Meddelandet s. 10.

([27]) Se arbetsgruppens dokument om integritetens framtid (fotnot 7), punkt 70. Dokumenten hänvisar framför allt till bestämmelser om ansvar och möjligheten att yrka på immateriella skador.

([28]) Vissa motstridiga synsätt föreligger också när det gäller manuella uppgifter.

5.3 *Områden som kan harmoniseras ytterligare*

54. *Definitioner* (artikel 2 i direktiv 95/46/EG). Definitionerna är rättssystemets hörnsten och bör tolkas enhetligt i alla medlemsstater, utan någon marginal när det gäller införlivande. Skillnader har uppstått inom den nuvarande ramen, exempelvis när det gäller begreppet registeransvarig ([29]). Datatillsynsmannen föreslår att ytterligare punkter ska läggas till den nuvarande förteckningen i artikel 2 för att åstadkomma större rättssäkerhet, exempelvis anonyma uppgifter, pseudonymförsedda uppgifter, rättsliga uppgifter, överföring av uppgifter och uppgiftsskyddsombud.

55. *Bestämmelser om när uppgifter får behandlas (artikel 5)*. Det nya rättsliga instrumentet bör vara så exakt som möjligt när det gäller huvudbeståndsdelarna för att fastställa när uppgifter får behandlas. Artikel 5 i direktivet (liksom skäl 9) som ger medlemsstaterna rätt att mer exakt fastställa villkoren för hur uppgifter får behandlas, kanske därför inte kommer att behövas i en framtida ram.

56. *Grunder för behandling av uppgifter* (artikel 7 och 8). Att fastställa villkoren för behandling av uppgifter är en grundläggande beståndsdel i all lagstiftning om dataskydd. Medlemsstaterna ska inte ha rätt att införa ytterligare eller ändrade grunder för behandling eller utesluta några. Möjligheten till undantag bör uteslutas eller begränsas (särskilt när det gäller känsliga uppgifter ([30])). I ett nytt rättsligt instrument bör grunderna för hantering av uppgifter formuleras tydligt och på så sätt minska marginalen för bedömning vid införlivande eller verkställande. Begreppet samtycke kan framför allt behöva specificeras ytterligare (se avsnitt 6.5). Grunderna baserade på berättigade intressen för den registeransvariga (artikel 7 f), ger dessutom utrymme för högst olika tolkningar på grund av sin flexibla utformning. Det behövs därför ytterligare specificering. En annan bestämmelse som sannolikt behöver specificeras är artikel 8.2 b, som tillåter behandling av känsliga uppgifter som är nödvändiga för att fullgöra de skyldigheter och särskilda rättigheter som åligger den registeransvarige inom arbetsrätten ([31]).

57. *Rättigheter för registrerade personer* (artiklarna 10–15). Detta är ett av de områden där inte alla delar av direktivet har införlivats och tolkats konsekvent av medlemsstaterna. Rättigheter för registrerade är en viktig del av ett effektivt dataskydd. Manöverutrymmet bör därför minskas avsevärt. Datatillsynsmannen rekommenderar att information som lämnas till registrerade personer bör vara enhetlig inom hela EU.

58. *Internationella överföringar* (artiklarna 25–26). Detta är ett område som har gett upphov till omfattande kritik på grund av bristen på enhetlig praxis i hela EU. Intressenter kritiserade att kommissionens beslut om lämplighet tolkas och införlivas mycket olika av medlemsstaterna. Bindande regler för företag är ett annat område där datatillsynsmannen rekommenderar ytterligare harmonisering (se kapitel 9).

59. *Nationella dataskyddsmyndigheter* (artikel 28). Nationella dataskyddsmyndigheter omfattas av högst olika regler i de 27 medlemsstaterna, särskilt när det gäller deras ställning, resurser och befogenheter. Artikel 28 har delvis bidragit till denna skillnad på grund av bristande precision ([32]) och bör därför specificeras ytterligare, i enlighet med EG-domstolens dom i mål C-518/07 ([33]) (se närmare kapitel 10).

5.4 *Förenkling av anmälningssystemet*

60. Kraven på anmälan (artiklarna 18–21 i direktiv 95/46/EG) är ett annat område där medlemsstaterna hittills har haft stor frihet. I meddelandet erkänns med rätta att ett harmoniserat system skulle minska kostnaderna liksom den administrativa bördan för registeransvariga ([34]).

61. Detta är ett område där förenkling bör vara huvudmålsättningen. Översynen av ramen för uppgiftsskydd är en unik möjlighet att ytterligare förenkla och/eller minska omfattningen av de nuvarande kraven på anmälan. I meddelandet erkänns också att det finns en allmän samsyn bland intressenterna om att det nuvarande systemet för anmälan är relativt besvärligt och i sig självt inte tillför något mervärde när det gäller skydd av enskildas personuppgifter ([35]). Europeiska datatillsynsmannen välkomnar därför kommissionens satsning på att undersöka olika möjligheter att förenkla det nuvarande anmälningssystemet.

62. Enligt datatillsynsmannen borde utgångspunkten för denna förenkling vara en övergång från ett system där anmälan är regel, om den inte tillhandahålls på annat sätt (dvs. ”undantagssystem”), till ett mer inriktat system. Undantagssystemet har visat sig ineffektivt eftersom det genomfördes på ett inkonsekvent sätt i medlemsstaterna ([36]). Europeiska datatillsynsmannen föreslår att följande alternativ ska övervägas:

([29]) Se artikel 29-arbetsgruppens yttrande 1/2010 om begreppen ”registeransvarig” och ”registerförare” (arbetsgruppen 169).

([30]) Artikel 8.4 och 8.5 tillåter för närvarande medlemsstaterna att enligt vissa villkor medge ytterligare undantag för känsliga uppgifter.

([31]) Se i detta hänseende kommissionens första rapport om införlivandet av dataskyddsdirektivet som citeras ovan, s. 14.

([32]) Arbetsgruppens dokument om Integritetens framtid, punkt 87.

([33]) Mål C-518/07, *Kommissionen mot Tyskland,* ännu ej offentliggjord i rättsfallssamlingen.

([34]) Se fotnot 26.

([35]) Se fotnot 26.

([36]) Artikel 29-arbetsgruppens rapport om skyldigheten med anmälan till de nationella tillsynsmyndigheterna, den bästa användningen av undantag och förenklingar och rollen för uppgiftsskyddsombud inom Europeiska unionen, WP 106, 2005, s. 7.

— Begränsa anmälningsskyldigheten till specifika slag av behandlingar som innebär specifika risker (dessa anmälningar kan medföra ytterligare steg såsom tidigare undersökning av behandlingen).

— En enkel registreringsskyldighet som innebär att registeransvariga måste registrera sig (i motsats till omfattande registrering av alla åtgärder inom behandling av uppgifter).

En standardiserad alleuropeisk anmälningsblankett skulle dessutom kunna införas för att åstadkomma harmoniserade synsätt när det gäller den information som begärs.

63. Översynen av det nuvarande systemet för anmälan bör inte påverka förbättringen av skyldigheten till kontroll i förväg för vissa skyldigheter när det gäller behandling som kan innebära specifika risker (exempelvis storskaliga informationssystem). Datatillsynsmannen skulle förorda att en ofullständig förteckning över fall där sådan kontroll i förväg krävs införs i det nya rättsliga instrumentet. Förordning (EG) nr 45/2001 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter innehåller en användbar modell för detta ([37]).

5.5 *En förordning, inte ett direktiv*

64. Avslutningsvis anser datatillsynsmannen att processen med översyn också är ett tillfälle att överväga vilken typ av rättsligt instrument som lämpar sig för uppgiftsskydd. En förordning, ett enda instrument som är direkt tillämpligt i medlemsstaterna är det mest effektiva sättet att skydda de grundläggande rättigheterna till skydd av uppgifter och skapa en verklig inre marknad där personuppgifter kan överföras fritt och där skyddsnivån är densamma oavsett land eller sektor där uppgifterna behandlas.

65. En förordning skulle minska utrymmet för motstridiga tolkningar och för omotiverade skillnader när lagen ska införas och tillämpas. Det skulle också minska betydelsen av att fastställa vilken lag som är tillämplig på behandling av åtgärder inom EU, vilket är en av de mest kontroversiella aspekterna av det nuvarande systemet (se kapitel 9).

66. Inom området dataskydd är en förordning desto mer motiverad eftersom

— artikel 16 i fördraget om Europeiska unionens funktionssätt innehåller en uppgradering av rätten till skydd av personuppgifter till fördragsnivå och förbereder för – eller till och med förordar – en enhetlig skyddsnivå för enskilda i hela EU,

— behandling av uppgifter sker i en elektronisk miljö där de inre gränserna mellan medlemsländerna har blivit mindre viktiga.

67. Valet av en förordning som ett allmänt instrument gör det möjligt att vid behov inrätta bestämmelser som är direkt riktade till medlemsstater där flexibilitet krävs. Det påverkar inte heller medlemsstaternas behörighet att vid behov anta ytterligare regler för dataskydd, i enlighet med EU:s lagstiftning.

6. **Stärka enskildas rättigheter**

6.1 *Behovet av att stärka rättigheter*

68. Datatillsynsmannen stöder helt meddelandets förslag att stärka enskildas rättigheter eftersom befintliga rättsliga instrument inte fullt ut ger det effektiva skydd som behövs i en allt mer komplex och digitaliserad värld.

69. Å ena sidan innebär utvecklingen av en digitaliserad värld en stark ökning av insamling, användning och ytterligare överföring av personuppgifter på ett extremt komplext och icke öppet sätt. Enskilda är ofta inte medvetna om eller förstår inte hur detta sker, vem som samlar in deras uppgifter eller hur de kan utöva kontroll. En illustration av denna företeelse är annonsnätverksleverantörers övervakning av enskildas webbläsningsaktiviteter med hjälp av cookies eller liknande hjälpmedel, i syfte att inrikta reklamen på vissa målgrupper. När användarna besöker webbplatser förväntar de sig inte att en osynlig tredje part registrerar sådana besök och skapar användarregister, baserade på information som avslöjar deras livsstil eller vad de tycker om eller inte tycker om.

70. Å andra sidan stimulerar utvecklingen enskilda personer som aktivt delar med sig av sin personliga information, exempelvis på sociala nätverk. Unga människor ingår i allt större utsträckning i ett socialt nätverk och samverkar med likasinnade. Det är tveksamt om (unga) människor är medvetna om i vilken omfattning informationen sprids och om de långsiktiga effekterna av deras åtgärder.

6.2 *Öka insynen*

71. Öppenhet är av stor betydelse i alla system för uppgiftsskydd, inte enbart på grund av det inneboende värdet utan också för att det gör det möjligt att tillämpa andra principer för uppgiftsskydd. Det är först när de enskilda känner till hur uppgifterna behandlas som de kan utöva sina rättigheter.

72. Flera bestämmelser i direktiv 95/46/EG handlar om öppenhet. Artikel 10 och 11 innehåller en skyldighet att informera enskilda om insamling av deras personuppgifter. I artikel 12 erkänns dessutom rätten att erhålla en kopia av de egna personuppgifterna i en begriplig form (rätt till tillträde). I artikel 15 erkänns rätten att ha tillträde till den logik där automatiska beslut som ger rättsliga effekter fattas. Sist men inte minst innehåller artikel 6.1 a, där det krävs att hanteringen också ska vara rättvis, ett krav på öppenhet. Personuppgifter kan inte behandlas av dolda eller hemliga skäl.

([37]) Se artikel 27 i förordningen, (EGT L 8, 12.1.2001, s. 1).

73. I meddelandet föreslås att en allmän princip om öppenhet ska läggas till. Som en reaktion på detta förslag betonar datatillsynsmannen att begreppet öppenhet också är en fullständig del av den nuvarande rättsliga ramen om uppgiftsskydd, om än på ett implicit sätt. Denna slutsats kan dras från de olika bestämmelserna om öppenhet vilket också nämns i föregående stycke. Enligt datatillsynsmannen kunde det ha tillfört värde att ta med en *explicit* princip om öppenhet, eventuellt kopplad till den befintliga bestämmelsen om rättvis behandling. Det skulle öka rättssäkerheten och även bekräfta att en registeransvarig under alla förhållanden bör hantera personuppgifter på ett öppet sätt, inte bara på begäran eller när en särskild rättslig bestämmelse kräver att så sker.

74. Det är emellertid kanske viktigare att förstärka befintliga bestämmelser om öppenhet, exempelvis de befintliga artiklarna 10 och 11 i direktiv 95/46/EG. Där anges vilken information som måste tillhandahållas, utan att de exakta villkoren anges. Mer konkret föreslår datatillsynsmannen att befintliga bestämmelser ska stärkas enligt följande:

— Krav för en registeransvarig att tillhandahålla information om behandling av uppgifter på ett sätt som är lättillgängligt och lätt att förstå, på ett tydligt och lättfattligt språk ([38]). Informationen ska vara tydlig, synlig och framträdande. Bestämmelsen kan också innefatta skyldigheten att se till att informationen är lätt att förstå. Denna skyldighet skulle innebära att integritetspolicyer som är dunkla eller svårförståeliga blir olagliga.

— Ett krav på att lämna informationen enkelt och direkt till de personer som berörs av uppgifterna. Informationen ska också alltid vara tillgänglig och inte försvinna från ett elektroniskt medium efter kort tid. Detta skulle hjälpa användarna att lagra och reproducera informationen i framtiden och möjliggöra ytterligare tillgång.

6.3 *Stöd till en skyldighet att rapportera säkerhetsöverträdelser*

75. Datatillsynsmannen stöder införandet i det allmänna instrumentet av en bestämmelse om anmälan av överträdelse när det gäller personuppgifter, vilket utvidgar skyldigheten som införlivades i det reviderade direktivet om integritet och elektronisk kommunikation för vissa leverantörer till alla registeransvariga, enligt förslaget i meddelandet. Enligt det reviderade direktivet om integritet och elektronisk kommunikation gäller skyldigheten enbart tjänsteleverantörer inom elektronisk kommunikation (leverantörer av telefoni [inbegripet VoIP] och Internetleverantörer). Andra registeransvariga omfattas inte av skyldigheten. Skälen som motiverar skyldigheten gäller fullt ut för andra registeransvariga än tjänsteleverantörer inom elektronisk kommunikation.

76. Anmälan om säkerhetsöverträdelser har olika syften och mål. Det mest uppenbara som också betonas av kommissionen är att fungera som ett informationsverktyg för att göra enskilda medvetna om riskerna de löper när deras personuppgifter äventyras. Det hjälper dem att vidta nödvändiga åtgärder för att mildra dessa risker. När enskilda varnas om överträdelser som påverkar deras finansiella information kan de exempelvis ändra sina lösenord eller säga upp sina konton. Anmälan om säkerhetsöverträdelse bidrar också till en effektiv tillämpning av andra principer och skyldigheter i direktivet. Krav när det gäller anmälan om säkerhetsöverträdelser sporrar exempelvis registeransvariga att införa omfattande säkerhetsåtgärder för att förebygga överträdelser. Säkerhetsöverträdelser är också ett verktyg för att stärka ansvaret för registeransvariga och i ännu större utsträckning att öka ansvarigheten (se kapitel 7). Avslutningsvis fungerar det som ett verktyg för dataskyddsmyndigheters verkställande. En anmälan om överträdelse till dataskyddsmyndigheter kan leda till att en registeransvarigs hela verksamhet undersöks.

77. De särskilda reglerna om säkerhetsöverträdelser i det ändrade direktivet om integritet och elektronisk kommunikation diskuterades omfattande under den parlamentariska fasen av lagstiftningsramen som föregick antagandet av direktivet. I denna debatt beaktades uppfattningarna från artikel 29-arbetsgruppen och från datatillsynsmannen tillsammans med synpunkter från andra intressenter. Reglerna återspeglar olika intressenters synpunkter. De utgör en balans av intressen: samtidigt som kriterierna för skyldigheten att anmäla i princip är lämpliga för att skydda enskilda gör de det utan att ställa alltför besvärliga och oanvändbara krav.

6.4 *Förstärkt samtycke*

78. I artikel 7 i direktivet om uppgiftsskydd anges sex rättsliga grunder för att hantera personuppgifter. Samtycke från den enskilda är en av dem. En registeransvarig har rätt att behandla personuppgifter i den utsträckning som enskilda har lämnat ett informerat medgivande till att få sina uppgifter insamlade och ytterligare behandlade.

79. I praktiken har användare ofta begränsad kontroll över sina uppgifter, särskilt i tekniska miljöer. En metod som ibland används är underförstått samtycke, vilket innebär att samtycke har antytts. Man kan dra den slutsatsen från en handling som den enskilda har utfört (exempelvis betraktas en handling som består i att använda en webbplats som samtycke till att registrera användaruppgifter för

([38]) Se meddelandet, s. 6.

marknadsföringssyfte). Det kan också underförstås genom tystnad eller overksamhet (att inte kryssa av en ifylld ruta betraktas som samtycke).

80. För att samtycket ska vara giltigt måste det enligt direktivet vara informerat, frivilligt lämnat och specifikt. Det måste vara en informerad indikation på den enskildas önskemål genom vilket han ger sitt samtycke till att personuppgifter som gäller honom får behandlas. Sättet som samtycket lämnas på måste vara otvetydigt.

81. Samtycke som har antytts genom en handling och framför allt genom tystnad eller overksamhet är ofta inte ett otvetydigt samtycke. Det är emellertid inte alltid tydligt vad som utgör ett verkligt otvetydigt samtycke. Vissa registeransvariga utnyttjar denna osäkerhet genom att förlita sig på metoder som inte är lämpliga för att lämna ett verkligt otvetydigt samtycke.

82. Mot bakgrund av ovanstående stöder datatillsynsmannen kommissionens uppfattning att gränserna för samtycke behöver klargöras och att man behöver se till att endast samtycke som förklaras på ett omsorgsfullt sätt betraktas som sådant. Datatillsynsmannen föreslår därför följande åtgärder ([39]):

— Man skulle kunna överväga att bredda de situationer där uttryckligt samtycke krävs, vilket för närvarande är begränsat till känsliga uppgifter.

— Anta ytterligare regler för samtycke på nätet.

— Anta ytterligare regler för samtycke till att behandla uppgifter för underordnade syften (dvs. behandlingen är underordnad huvudbehandlingen eller är inte en uppenbar sådan).

— I ett ytterligare lagstiftningsinstrument oavsett om det antas av kommissionen enligt artikel 290 i fördraget om Europeiska unionens funktionssätt fastställs den typ av samtycke som krävs, exempelvis för att specificera nivån av samtycke när det gäller behandling av uppgifter från RFID-taggar på konsumentprodukter eller annan specifik teknik.

6.5 *Portabilitet av uppgifter och rätt till radering*

83. Portabilitet av uppgifter och rätt till radering är två sammanhängande begrepp som läggs fram i meddelandet för att stärka registrerade personers rättigheter. De kompletterar de principer som redan nämnts i direktivet, och ger registrerade personer rätt att motsätta sig ytterligare behandling av sina personuppgifter, och en skyldighet för den registeransvariga att radera information så snart den inte längre är nödvändig för behandlingen.

84. Dessa två nya begrepp har huvudsakligen tillfört värde i informationssamhället där fler och fler uppgifter lagras automatiskt och behålls under obestämd tid. Det har i praktiken visat sig att även om uppgifterna laddas upp av den registrerade personen själv är den personens faktiska kontroll över sina personuppgifter mycket begränsad. Det är desto mer sant mot bakgrund av det gigantiska minne som Internet i dag utgör. Ur ett ekonomiskt perspektiv är det dessutom dyrare för den registeransvariga att radera uppgifter än att fortsätta att lagra dem. Enskildas utövande av sina rättigheter strider därför mot den naturliga ekonomiska trenden.

85. Både uppgifters portabilitet och rätten till radering kan bidra till att ändra balansen till förmån för registrerade personer. Målsättningen för uppgifters portabilitet skulle vara att ge den enskilda större kontroll över informationen, medan rätten till radering skulle trygga att informationen automatiskt försvinner efter en viss tidsperiod, även om den registrerade personen inte vidtar någon åtgärd eller ens är medveten om att uppgifterna överhuvudtaget lagrades.

86. Mer specifikt innebär uppgifters portabilitet en möjlighet för användaren att ändra preferens när det gäller behandling av deras uppgifter, framför allt i anslutning till tjänster inom ny teknik. Detta gäller i allt större utsträckning tjänster som medför lagring av information, inbegripet personuppgifter, såsom mobiltelefoni och tjänster som lagrar bilder, e-post och annan information, och som ibland använder datormoln.

87. Enskilda personer måste enkelt och fritt kunna byta leverantör och överföra sina personuppgifter till en annan tjänsteleverantör. Datatillsynsmannen anser att de nuvarande rättigheter som anges i direktiv 95/46/EG kan förstärkas genom en rätt till portabilitet särskilt rörande informationssamhällets tjänster, för att bistå enskilda när det gäller att trygga att leverantörer och andra relevanta registeransvariga ger dem tillgång till deras personliga uppgifter samtidigt som det säkras att de tidigare leverantörerna eller andra registeransvariga raderar den informationen, även om de skulle vilja behålla den för egna berättigade syften.

88. En nyligen kodifierad ”rätt till radering” skulle trygga radering av personuppgifter eller förbud mot att använda dem ytterligare utan att den registrerade personen ska vara tvungen vidta åtgärder, men under förutsättning att dessa uppgifter redan har lagrats för en viss tid. Uppgifterna skulle med andra ord förses med något slags utgångsdatum. Principen har redan bekräftats i nationella domstolsfall eller tillämpats inom specifika sektorer, exempelvis polisakter, brottsregister eller disciplinära akter: enligt

([39]) Artikel 29-arbetsgruppen arbetar för närvarande med ett yttrande om ”samtycke”. Detta yttrande kan leda till ytterligare förslag.

viss nationell lagstiftning ska information om enskilda automatiskt raderas eller inte användas eller spridas ytterligare, särskilt efter en fastställd tidsperiod, utan att detta först behöver analyseras från fall till fall.

89. I den meningen borde en ny ”rätt till radering” kombineras med portabilitet av uppgifter. Det mervärde detta skulle tillföra är att den registrerade personen inte skulle behöva anstränga sig eller yrka på att uppgifterna ska raderas, eftersom detta skulle ske objektivt och automatiskt. Endast under mycket specifika omständigheter, när det kan fastställas att det finns ett specifikt behov av att behålla uppgifterna under längre tid, kan en registreringsansvarig få rätt att behålla uppgifterna. Denna ”rätt till radering” skulle därmed överföra bevisbördan från den enskilda till den registeransvariga och utgöra en ”förvald inställning för sekretess” vid behandling av personuppgifter.

90. Datatillsynsmannen anser att rätten till radering kan visa sig särskilt användbar i samband med informationssamhällets tjänster. En skyldighet att radera eller att inte ytterligare sprida information efter en bestämd tidsperiod är rimlig, särskilt i media eller på Internet, och framför allt i sociala nätverk. Det skulle också vara användbart när det gäller terminalutrustning: uppgifter som lagras på mobila enheter eller datorer skulle automatiskt raderas eller blockeras efter en bestämd tidsperiod när de inte längre innehas av den enskilda. I den betydelsen kan rätten till radering omsättas till en skyldighet till ”inbyggda skyddsmekanismer”.

91. Sammanfattningsvis anser datatillsynsmannen att uppgifters portabilitet och rätten till radering båda är användbara koncept. Det skulle kunna vara användbart att införliva dem i det rättsliga instrumentet, men sannolikt begränsat till den elektroniska miljön.

6.6 Hantering av personuppgifter som rör barn

92. Enligt direktiv 95/46/EG finns det inga särskilda regler för behandling av personuppgifter som rör barn. Det innebär att behovet av ett särskilt skydd för barn under specifika omständigheter, på grund av deras sårbarhet, inte erkänns eftersom det orsakar rättslig osäkerhet, särskilt inom följande områden:

— Insamling av uppgifter om barn och hur de måste informeras om insamlingen.

— Hur barnens medgivande erhålls. Eftersom det inte finns några särskilda regler för hur barns medgivande ska erhållas eller för hur länge barnen ska betraktas som barn, hanteras dessa frågor i nationell lagstiftning, vilket skiljer sig från medlemsstat till medlemsstat ([40]).

— Hur barn eller deras juridiska företrädare kan utöva sina rättigheter enligt direktivet.

93. Datatillsynsmannen anser att barns särskilda intressen bättre skulle skyddas om det nya rättsliga instrumentet innehöll ytterligare bestämmelser, som särskilt gäller insamling och ytterligare behandling av barns uppgifter. Dessa specifika bestämmelser skulle också bidra till rättssäkerheten inom detta specifika område och de skulle gynna registeransvariga som för närvarande utsätts för olika rättsliga krav.

94. Datatillsynsmannen föreslår att följande bestämmelser införs i det rättsliga instrumentet:

— Ett krav på att information ska anpassas till barn i den mån som detta skulle göra det enklare för barn att förstå vad det innebär när uppgifter samlas in från dem.

— Andra informationskrav anpassade till barn, om hur informationen måste lämnas och sannolikt också om innehållet.

— En särskild bestämmelse som skyddar barn mot beteendestyrd annonsering.

— Principen om att begränsa syftet bör förstärkas när det gäller barns uppgifter.

— Vissa kategorier av uppgifter bör aldrig samlas in från barn.

— En åldergräns. Under denna åldersgräns bör generellt information från barn samlas in endast med uttryckligt och kontrollerbart medgivande från föräldrar.

— Om det krävs medgivande från en förälder skulle det vara nödvändigt att fastställa regler för hur man verifierar ett barns ålder, med andra ord hur man vet att barnet är minderårigt hur man kontrollerar

([40]) Samtycke är vanligtvis kopplat till den ålder då barn kan träffa avtal. Det är en ålder då barn förväntas ha uppnått en viss mognadsnivå. Exempelvis kräver spansk lag föräldrarnas medgivande för att samla in uppgifter om barn när barnen är under 14 år. Om barnen är äldre anses de kunna ge sitt medgivande. I Storbritannien hänvisar Data protection act inte till någon särskild ålder eller gräns. Storbritanniens myndighet för uppgiftsskydd har emellertid ansett att barn över 12 år kan ge sitt medgivande. Omvänt kan barn under 12 år inte ge sitt medgivande och för att kunna erhålla sina personuppgifter krävs det först tillstånd från en förälder eller en vårdnadshavare.

föräldrarnas medgivande. Detta är ett område där EU kan få inspiration från andra länder, exempelvis Förenta staterna ([41]).

6.7 *Kollektiva mekanismer för upprättelse*

95. Att stärka innehållet i enskildas rättigheter skulle vara meningslöst om det inte finns några effektiva mekanismer för att verkställa dessa rättigheter. Datatillsynsmannen rekommenderar därför att det i EU:s lagstiftning införs kollektiva mekanismer för upprättelse om reglerna för uppgiftsskydd överträds. Kollektiva mekanismer för upprättelse som ger grupper av medborgare möjligheter att samla sina krav i en gemensam åtgärd utgör ett mycket kraftfullt verktyg för att underlätta tillämpningen av reglerna för uppgiftsskydd ([42]). Denna innovation stöds också av dataskyddsmyndigheterna i artikel 29-dokumentet om integritetens framtid.

96. I fall med mindre inflytande är det osannolikt att offren för en överträdelse av regler om uppgiftsskydd skulle genomföra enskilda åtgärder mot de registeransvariga, med tanke på kostnader, förseningar, osäkerhet, risker och bördor de skulle utsättas för. Dessa svårigheter skulle kunna överbryggas eller avsevärt minskas om ett system med kollektiv upprättelse fanns, som skulle göra det möjligt för dem som utsätts för överträdelser att samla sina enskilda krav i en gemensam åtgärd. Datatillsynsmannen skulle också förespråka möjligheten för kvalificerade enheter, såsom konsumentsammanslutningar eller offentliga organ, att vidta åtgärder när registrerade personer drabbas av skador på grund av att uppgiftsskyddet har överträtts. Dessa åtgärder skulle inte påverka rätten för registrerade personer att vidta enskilda åtgärder.

97. Kollektiva åtgärder är inte bara viktiga för att säkra full kompensation eller andra åtgärder, de har också indirekt en avskräckande funktion. Risken att drabbas av dyrbara kollektiva skadeståndskrav vid sådana åtgärder skulle öka de registeransvarigas incitament att effektivt se till att kraven uppfylls. I detta hänseende skulle förbättrat privat genomförande med hjälp av kollektiva mekanismer för upprättelse komplettera det offentliga genomförandet.

98. Meddelandet innehåller ingen ståndpunkt i den här frågan. Datatillsynsmannen är medveten om den debatt som pågår inom EU om att införa kollektiva konsumentmekanismer för upprättelse. Han är också medveten om risken för överdrifter som dessa mekanismer kan medföra på grundval av erfarenheterna från andra rättsliga system. Dessa faktorer utgör emellertid inte enligt hans uppfattning tillräckliga argument för att avvisa eller skjuta upp deras införande i lagstiftningen om uppgiftsskydd, med tanke på de fördelar de skulle innebära ([43]).

7. **Stärkning av organisationers/registeransvarigas roll**

7.1 *Allmänt*

99. Datatillsynsmannen anser att utöver att förstärka enskildas rättigheter måste ett modernt rättsligt system för uppgiftsskydd innehålla nödvändiga verktyg som ökar de registeransvarigas ansvar. Ramen måste i synnerhet innehålla incitament för registeransvariga inom den privata eller offentliga sektorn att aktivt införliva åtgärder för uppgiftsskydd i sina affärsprocesser. Dessa verktyg skulle till att börja med vara till nytta eftersom, vilket också nämnts tidigare, teknisk utveckling leder till en stark ökning av insamling, användning och ytterligare överföring av personuppgifter vilket ökar risken för integriteten och skyddet av personuppgifter för enskilda, vilket i sin tur borde kompenseras på ett effektivt sätt. För det andra saknar den nuvarande ramen – med undantag för ett fåtal, väldefinierade bestämmelser (se nedan) – sådana verktyg och registeransvariga kan inta ett *reaktivt* synsätt på uppgiftsskydd och privatliv och endast agera efter att ett problem har uppstått. Detta synsätt återspeglas i statistik som visar att bristande tillämpningar när det gäller överensstämmelse och förlust av uppgifter är återkommande problem.

100. Enligt datatillsynsmannen är den befintliga ramen inte tillräcklig för att skydda personuppgifter effektivt enligt nuvarande och kommande villkor. Ju högre risken är, desto större är behovet av att införliva konkreta åtgärder som skyddar information på en praktisk nivå och ger ett effektivt skydd. Om dessa aktiva åtgärder *de facto* inte införs kommer sannolikt misstag, missöden och försumlighet att fortsätta inträffa och enskildas privatliv att utsättas för fara i det alltmer digitala samhället. Därför föreslår datatillsynsmannen följande åtgärder.

7.2 *Förstärkning av de registeransvarigas ansvarighet*

101. Datatillsynsmannen rekommenderar att en ny bestämmelse förs in i det rättsliga instrumentet som innebär att registeransvariga ska genomföra lämpliga och effektiva åtgärder för att verkställa det rättsliga instrumentets principer och skyldigheter och visa detta på begäran.

([41]) I USA kräver COPPA (Childrens Online Privacy Protection Act Rule) att de som har en kommersiell webbplats eller onlinetjänster som vänder sig till barn under 13 år måste ha föräldrarnas medgivande innan de samlar in personuppgifter, och de som driver kommersiella webbplatser för allmänheten måste ha faktisk kunskap om att vissa besökare är barn.

([42]) Se även Europeiska datatillsynsmannens yttrande av den 25 juli 2007 om kommissionens meddelande till Europaparlamentet och rådet om uppföljningen av arbetsprogrammet för ett bättre genomförande av dataskyddsdirektivet, (EUT C 255, 27.10.2007, s. 10).

([43]) Vissa nationella lagar innehåller redan liknande mekanismer.

102. Denna typ av bestämmelse är inte helt ny. I artikel 6.2 i direktiv 95/46/EG hänvisas till principerna om uppgiftskvalitet och det sägs att ”det är den registeransvariga som ska se till att punkt 1 uppfylls”. I artikel 17.1 krävs också att registeransvariga ska genomföra åtgärder, både tekniska och organisatoriska. Dessa bestämmelser har emellertid en begränsad omfattning. Att införa en allmän bestämmelse om ansvarighet skulle stimulera de registeransvariga att införa aktiva åtgärder för att kunna uppfylla alla delar i lagen om uppgiftsskydd.

103. En bestämmelse om ansvarighet skulle leda till att registeransvariga måste införa interna mekanismer och kontrollsystem som ser till att ramverkets principer och skyldigheter följs. Det skulle exempelvis innebära att man måste involvera den högsta ledningen när det gäller politiken för uppgiftsskydd, kartläggningsförfaranden för att säkra korrekt identifiering av alla åtgärder för uppgiftsskydd, ha en bindande policy för uppgiftsskydd vilken också skulle ses över och uppdateras kontinuerligt för att täcka nya åtgärder inom uppgiftshantering som överensstämmer med principerna om uppgiftskvalitet, anmälan, säkerhet, tillträde etc. Det skulle också kräva att de registeransvariga behåller bevis för att på begäran från myndigheterna kunna visa att reglerna följs. Att visa för den stora allmänheten att reglerna följs bör i vissa fall också bli obligatoriskt. Det kan exempelvis ske genom att kräva att de registeransvariga ska införliva uppgiftsskydd i offentliga (års)rapporter, när sådana rapporter är obligatoriska av andra skäl.

104. De olika interna och externa åtgärder som bör genomföras måste naturligtvis vara lämpliga och beror på fakta och omständigheter i varje enskilt fall. Det är skillnad om en registeransvarig hanterar några hundra kundregister som huvudsakligen består av namn och adresser eller om det handlar om register över miljontals patienter och deras medicinska historia. Detsamma gäller de specifika sätt som åtgärdernas effektivitet måste bedömas på. Det finns ett behov av skalanpassning.

105. I det allmänna övergripande rättsliga instrumentet för uppgiftsskydd bör inte de specifika kraven på ansvarighet slås fast utan enbart de grundläggande beståndsdelarna. I meddelandet planeras vissa beståndsdelar för att förstärka ansvaret för registeransvariga, vilket är mycket välkommet. Datatillsynsmannen stöder i synnerhet att uppgiftsskyddsombud och bedömningar av inverkan på privatlivet görs obligatoriska, inom vissa fastställda gränser.

106. Datatillsynsmannen rekommenderar dessutom att befogenheter delegeras till kommissionen enligt artikel 290 i fördraget om Europeiska unionens funktionssätt för att komplettera baskraven för att uppfylla ansvarighetsnormerna. Om de registeransvariga använder dessa befogenheter skulle det öka deras rättssäkerhet och harmonisera överensstämmelsen inom hela EU. Vid utveckling av sådana specifika instrument bör artikel 29-arbetsgruppen och Europeiska datatillsynsmannen konsulteras.

107. Avslutningsvis kan också de konkreta ansvarighetsåtgärder som genomförs av registeransvariga krävas av dataskyddsmyndigheter i anslutning till deras tillsynsbefogenheter. Dataskyddsmyndigheterna bör därför få nya befogenheter så att de kan införa åtgärder eller sanktioner. Exemplen bör innefatta inrättande av interna program för att uppfylla reglerna, för att genomföra inbyggda skyddsmekanismer för vissa produkter och tjänster, etc. Åtgärderna ska endast införas om de är lämpliga, proportionella och effektiva för att säkra överensstämmelse med tillämpliga och verkställbara rättsliga normer.

7.3 Inbyggda skyddsmekanismer

108. Inbyggda skyddsmekanismer innebär att uppgiftsskydd och integritet införlivas redan vid framtagningen av nya produkter, tjänster och förfaranden som omfattar behandling av personuppgifter. Enligt datatillsynsmannen är inbyggda skyddsmekanismer en del av ansvarigheten. Registeransvariga skulle därför också uppmanas att visa att de hade genomfört inbyggda skyddsmekanismer när så är lämpligt. Den 32:e internationella konferensen för ombudsmännen för dataskydd och integritet utfärdade en resolution där man slår fast att inbyggda skyddsmekanismer är en mycket viktig beståndsdel i grundläggande integritetsskydd ([44]).

109. Direktiv 95/46/EG innehåller ett antal bestämmelser som uppmuntrar inbyggda skyddsmekanismer ([45]), men erkänner inte en sådan skyldighet explicit. Europeiska datatillsynsmannen är nöjd med att man i meddelandet stöder inbyggda skyddsmekanismer som ett verktyg för att säkra överensstämmelse med reglerna för uppgiftsskydd. Han föreslår att en bindande bestämmelse om skyldighet till ”inbyggda skyddsmekanismer”, ska införas vilken kan bygga på lydelsen i skäl 46 i direktiv 95/46/EG. Mer specifikt åskulle bestämmelsen uttryckligen kräva att registeransvariga genomför tekniska och organisatoriska åtgärder, både i samband med utformningen av

([44]) Resolution om inbyggda skyddsmekanismer, antagen av den 32:a internationella konferensen för ombudsmännen för dataskydd och integritet, Jerusalem 27–29 oktober 2010.

([45]) Direktivet innehåller bestämmelser som indirekt i olika situationer kräver att inbyggda skyddsmekanismer införlivas. Framför allt i artikel 17 krävs att registeransvariga genomför lämpliga tekniska och organisatoriska åtgärder för att förhindra olovlig behandling av uppgifter. Direktivet om integritet och elektronisk kommunikation är mer explicit. I artikel 14.3 står att ”När så krävs får åtgärder vidtas för att säkerställa att terminalutrustning är konstruerad så att den är förenlig med användarnas rätt till skydd och kontroll av sina personuppgifter i enlighet med direktiv 1999/5/EG och rådets beslut 87/95/EEG av den 22 december 1986 om standardisering inom området informationsteknologi och telekommunikation)”.

förfarandesystemet och vid själva förfarandet, särskilt i syfte att säkra skyddet av personuppgifter och förebygga otillåten behandling ([46]).

110. På grundval av en sådan bestämmelse skulle registeransvariga vara tvungna att – bland annat – se till att system för databehandling är utformade för att behandla så få personuppgifter som möjligt, för att genomföra inbyggda skyddsmekanismer, exempelvis i sociala nätverk, för att hålla enskildas profiler automatiskt åtskilda från andras och införa verktyg som gör det lättare för användarna att skydda sina personuppgifter (exempelvis tillträdeskontroll och kryptering).

111. Fördelarna med en mer explicit hänvisning till inbyggda skyddsmekanismer kan sammanfattas enligt följande:

— Det skulle betona betydelsen av principen i sig, som ett verktyg för att säkra att förfaranden, produkter och tjänster redan från början är utformade med tanke på integritet.

— Det skulle minska missbruk av integritet och minimera onödig insamling av uppgifter samt göra det möjligt för enskilda att göra verkliga val när det gäller deras personuppgifter.

— Det skulle också förhindra att man blir tvungen att senare ”lägga förband på” för att försöka lösa problem som kan vara svåra eller till och med omöjliga att reparera.

— Det skulle också göra det enklare för dataskyddsmyndigheter att effektivt tillämpa och verkställa principen.

112. Den kombinerade effekten av denna skyldighet skulle leda till större efterfrågan på produkter och tjänster inom inbyggda skyddsmekanismer, vilket i sin tur skulle ge näringslivet större incitament att möta en sådan efterfrågan. Man bör dessutom överväga att skapa en separat skyldighet som vänder sig till designers och tillverkare av nya produkter och tjänster som kan tänkas påverka dataskydd och integritet. Datatillsynsmannen föreslår att en sådan separat skyldighet ska införlivas som i ännu större utsträckning skulle kunna göra det möjligt för registeransvariga att uppfylla sina egna skyldigheter.

113. Kodifieringen av inbyggda skyddsmekanismer kan kompletteras av en bestämmelse om allmänna krav när det gäller inbyggda skyddsmekanismer som är tillämpliga inom olika sektorer, produkter och tjänster, exempelvis att säkerställa användarnas åtgärder för egenmakt som ska antas enligt principen.

114. Datatillsynsmannen rekommenderar dessutom att befogenheter delegeras till kommissionen enligt artikel 290 i fördraget om Europeiska unionen – när så är lämpligt – för att komplettera grundkraven för inbyggda skyddsmekanismer för utvalda produkter och tjänster. Om registeransvariga använder dessa befogenheter skulle det öka deras rättssäkerhet och harmonisera överensstämmelsen inom hela EU. Vid utveckling av sådana specifika instrument bör artikel 29-arbetsgruppen och Europeiska datatillsynsmannen konsulteras (se även punkt 106 om ansvarighet).

115. Avslutningsvis bör dataskyddsmyndigheterna få befogenheter att införa åtgärder eller sanktioner, enligt liknande restriktiva villkor som redan nämnts i punkt 107, när de registeransvariga tydligt har misslyckats med att vidta konkreta åtgärder i fall där detta skulle krävas.

7.4 *Certifieringstjänster*

116. I meddelandet erkänns behovet av att undersöka inrättandet av certifieringssystem inom EU för produkter och tjänster som garanterar skydd av privatlivet. Datatillsynsmannen stöder fullt ut detta mål och föreslår att en bestämmelse ska införas som tillgodoser deras inrättande och möjliga effekter i hela EU, vilket kan utvecklas ytterligare i senare lagstiftning. Bestämmelsen ska komplettera bestämmelserna om ansvarighet och inbyggda skyddsmekanismer.

117. Frivilliga certifieringssystem skulle göra det möjligt att kontrollera att en registeransvarig har infört åtgärder för att uppfylla det rättsliga instrumentet. Registeransvariga – eller till och med produkter eller tjänster – som har förmånen att vara certifierade kommer dessutom sannolikt att ha en konkurrensfördel framför andra. Sådana system skulle också hjälpa dataskyddsmyndigheter i deras övervakande och verkställande roll.

8. **Globalisering och tillämplig lag**

8.1 *Ett tydligt behov av mer konsekvent skydd*

118. Såsom nämnts i kapitel 2 har överföring av personuppgifter utanför EU:s gränser ökat exponentiellt som en konsekvens av utvecklingen av ny teknik, multinationella företags roll och regeringars ökade påverkan när det gäller behandling och spridning av personuppgifter på internationell nivå. Detta är ett av huvudskälen till att den nuvarande rättsliga ramen bör ses över. Detta är därmed ett av de områden där datatillsynsmannen kräver ambition och effektivitet, eftersom det finns ett tydligt behov av mer konsekvent skydd när uppgifter behandlas utanför EU.

([46]) Enligt den nuvarande ramen uppmuntras i skäl 46 registeransvariga som inför sådana åtgärder, men ett skäl har självfallet ingen bindande kraft.

8.2 *Investeringar i internationella regler*

119. Enligt datatillsynsmannen behövs mer satsningar på att utveckla internationella regler. Större harmonisering av skyddsnivån för personuppgifter i hela världen skulle avsevärt klargöra innehållet i de principer som bör uppfyllas och villkoren för överföring av uppgifter. Dessa övergripande regler skulle behöva kombinera kraven på en hög standard när det gäller uppgiftsskydd – inbegripet de viktigaste beståndsdelarna i uppgiftsskyddet i EU – med regionala särdrag.

120. Europeiska datatillsynsmannen stöder det ambitiösa arbete som hittills utförts inom ramen för den internationella konferensen för ombudsmän för dataskydd och integritet för att utveckla och sprida de så kallade ”Madridnormerna”, i syfte att integrera dem i ett bindande instrument och sannolikt initiera en mellanstatlig konferens ([47]). Han uppmanar kommissionen att ta nödvändiga initiativ för att underlätta genomförandet av denna målsättning.

121. Enligt datatillsynsmannen är det också viktigt att se till att detta initiativ är förenligt med internationella normer, den nuvarande översynen av EU:s ram för uppgiftsskydd och annan utveckling, exempelvis den nuvarande översynen av OECD:s riktlinjer för integritet samt konvention 108 från Europarådet som är öppen för undertecknande av tredje länder (se även punkt 17). Datatillsynsmannen anser att kommissionen kan spela en specifik roll här, genom att specificera hur den kommer att främja denna konsekvens i förhandlingarna i OECD och Europarådet.

8.3 *Klargörande av tillämpliga lagkriterier*

122. Eftersom det inte är enkelt att uppnå fullständig konsekvens kommer det – åtminstone inom den närmaste tiden – att kvarstå vissa skillnader mellan lagarna inom EU och de utanför EU:s gränser. Datatillsynsmannen anser att ett nytt rättsligt instrument behöver klargöra kriterierna som fastställer tillämplig lag, och säkerställa rationella system för uppgiftsflöden liksom ansvarighet för aktörer som är involverade i uppgiftsflöden.

123. Till att börja med bör det rättsliga instrumentet säkra att EU:s lagstiftning är tillämplig när personuppgifter behandlas utanför EU:s gränser, men där det finns ett motiverat krav på att tillämpa EU:s lagstiftning. Exemplet med icke europeiska molnbaserade datortjänster som är inriktade på EU-medborgare illustrerar varför detta är nödvändigt. I en miljö där uppgifter inte fysiskt lagras och hanteras på en fast plats, där tjänsteleverantörer och användare i olika länder har avgörande påverkan på uppgifter är det mycket svårt att identifiera vem som är ansvarig för att uppfylla principerna för uppgiftsskydd. Ledning ges, särskilt av dataskyddsmyndigheter, om hur direktiv 95/46/EG ska tolkas och tillämpas i sådana fall, men enbart ledning är inte tillräckligt för att trygga rättssäkerheten i denna nya miljö.

124. Inom EU:s territorium har behovet av större precision inom den rättsliga ramen och ett förenklat kriterium för att fastställa den lag som ska tillämpas betonats av artikel 29-arbetsgruppen i ett yttrande nyligen ([48]).

125. Enligt datatillsynsmannen skulle den bästa lösningen vara att slå fast det rättsliga instrumentet i en förordning som skulle leda till identiska regler som är tillämpliga i alla medlemsstater. En förordning skulle göra behovet av att fastställa tillämplig lag mindre viktigt. Detta är ett av skälen till att datatillsynsmannen starkt förordar en förordning. Även en förordning kan emellertid medge visst manöverutrymme för medlemsstaterna. Om visst betydande manöverutrymme behålls i det nya instrumentet skulle datatillsynsmannen stödja arbetsgruppens förslag om en övergång från en distributiv tillämpning av olika nationella lagar till en centraliserad tillämpning av en enda lagstiftning i alla medlemsstater där en registeransvarig har anläggningar. Han vädjar också om större samarbete och samordning mellan dataskyddsmyndigheter vid gränsöverskridande mål, fall och klagomål (se kapitel 10).

8.4 *Rationella system för uppgiftsflöden*

126. Behovet av enhetlighet och höga normer måste beaktas inte enbart med tanke på övergripande principer för uppgiftsskydd utan även när det gäller internationella överföringar. Datatillsynsmannen stöder fullständigt kommissionens målsättning att rationalisera nuvarande förfaranden för internationella överföringar av uppgifter och trygga ett mer enhetligt och sammanhängande synsätt gentemot tredje länder och internationella organisationer.

127. Mekanismer för uppgiftsflöden innefattar både överföringar inom den privata sektorn, särskilt via kontraktsklausuler eller bindande företagsregler, och överföringar mellan offentliga myndigheter. Bindande företagsregler är en av de beståndsdelar där ett mer enhetligt och rationellt synsätt skulle vara önskvärt. Datatillsynsmannen rekommenderar att villkoren för bindande företagsregler tas upp på ett explicit sätt i det nya rättsliga instrumentet ([49]), genom att

— uttryckligen erkänna bindande företagsregler som ett verktyg som tillhandahåller lämpliga säkerheter,

— se till att huvudbeståndsdelarna/villkoren för att anta bindande företagsregler finns,

([47]) Enligt förslaget i resolutionen om internationella normer, antagen av den 32:a internationella konferensen för ombudsmän för data-

([48]) Artikel 29-arbetsgruppens yttrande 8/2010 om tillämplig lag, arbetsgrupp 179.

([49]) Beträffande internationella överföringar, se även kapitel 8 i yttrandet.

— införa samarbetsförfaranden för antagande av bindande företagsregler inbegripet kriterier för att välja ut en ledande myndighet för övervakning (en enda kontaktpunkt).

9. **Polis och rättsväsende**

9.1 *Allmänt instrument*

128. Kommissionen har vid upprepade tillfällen betonat betydelsen av att stärka dataskyddet när det gäller upprätthållande av lag och ordning och brottsförebyggande där utbytet och användningen av personuppgifter intensifierats avsevärt. Även i Stockholmsprogrammet, som godkänts av Europeiska rådet, hänvisas till ett system för starkt uppgiftsskydd som en huvudsaklig förutsättning för EU:s strategi för informationshantering på detta område ([50]).

129. Översynen av den allmänna ramen för dataskydd är ett perfekt tillfälle att göra framsteg på området, särskilt som rambeslut 2008/977 i meddelandet med rätta beskrivs som bristfälligt ([51]).

130. Datatillsynsmannen pläderade i avsnitt 3.2.5 i detta yttrande för varför området med polisärt och rättsligt samarbete skulle ingå i det allmänna instrumentet. Det finns ett antal fördelar med att införliva polis och rättsväsende i instrumentet. Det innebär att reglerna inte längre enbart kommer att gälla för utbyte av uppgifter över gränserna ([52]), utan även för behandling inom länderna. Lämpligt skydd vid utbyte av personuppgifter med tredje land kommer att garanteras bättre, även när det gäller internationella avtal. Myndigheter som hanterar personuppgifter kommer dessutom att ha samma omfattande och harmoniserade befogenheter gentemot polis och rättsliga myndigheter som gentemot andra registeransvariga. Avslutningsvis måste den nuvarande artikel 13, som innebär att medlemsstaterna är berättigade att anta särskild lagstiftning för att begränsa skyldigheter och rättigheter enligt det allmänna instrumentet för särskilda offentliga intressen, tillämpas på samma restriktiva sätt som den tillämpas på andra områden. De särskilda garantier som erhålls enligt det allmänna instrumentet inom detta område måste framför allt respekteras även inom nationell lagstiftning som antas på området polisiärt och rättsligt samarbete.

9.2 *Ytterligare särskilda regler för polis och rättsväsende*

131. Detta införlivande utesluter emellertid inte särskilda regler och undantag, vilka vederbörligen tar hänsyn till särdragen inom denna sektor, i linje med förklaring 21 till Lissabonfördraget. Begränsningar av rättigheter för personer som berörs av uppgifterna kan ingå, men de måste vara nödvändiga och proportionella och får inte ändra själva rättighetens grundläggande beståndsdelar. Det bör i detta sammanhang betonas att direktiv 95/46/EG, inklusive artikel 13 i detta, för närvarande gäller för brottsbekämpning inom olika områden (exempelvis beskattning, tull, bedrägeribekämpning) som inte i grunden skiljer sig från många verksamheter inom det polisiära och rättsliga området.

132. Särskilda garantier behöver dessutom införas för att kompensera registrerade personer genom att ge dem extra skydd inom ett område där hantering av personuppgifter kan vara mer påträngande.

133. Mot bakgrund av ovanstående anser datatillsynsmannen att den nya ramen bör innefatta minst följande beståndsdelar, i linje med konvention 108 och rekommendation nr R (87) 15:

— En distinktion mellan olika kategorier av uppgifter och register i enlighet med hur korrekta och tillförlitliga de är, och stöd till principen att uppgifter baserade på fakta bör skiljas från uppgifter baserade på uppfattningar eller personliga bedömningar.

— En distinktion mellan olika kategorier av personer som berörs av uppgifterna (brottsmisstänkta, offer, vittnen, etc.) och register (tillfälliga och permanenta register samt underrättelseregister). Särskilda villkor och garantier behövs för hantering av uppgifter om personer som inte är misstänkta.

— Mekanismer för att trygga periodisk kontroll och rättelse för att garantera kvaliteten på de uppgifter som hanteras.

— Särskilda bestämmelser och/eller garantier kan införas för (den allt mer relevanta) behandlingen av biometriska och genetiska uppgifter på det brottsförebyggande området. Användningen av dem bör begränsas endast till fall där inga mindre inkräktande möjligheter är tillgängliga som kan garantera samma effekt ([53]).

— Villkor för överföring av personuppgifter till icke behöriga myndigheter och privata aktörer liksom för tillträde och ytterligare användning inom brottsbekämpande myndigheter av personuppgifter som samlats in av privata parter.

([50]) Se Europeiska datatillsynsmannens yttrande av den 30 september 2010 om kommissionens meddelande till Europaparlamentet och rådet – ”Översikt av informationshanteringen inom området för frihet, säkerhet och rättvisa”, punkterna 9–19.

([51]) Se avsnitt 3.2.5 ovan.

([52]) Detta är för närvarande den begränsade omfattningen av rambeslut 2008/977.

([53]) Se arbetsgruppens dokument om Integritetens framtid, punkt 112.

9.3 *Sektorspecifika system för dataskydd*

134. I meddelandet slås fast att ”inte heller rambeslutet ersätter de olika rättsakter om polisiärt och straffrättsligt samarbete som antagits inom EU, särskilt inte dem som styr funktionssätten för Europol, Eurojust, Schengens informationssystem (SIS) och tullinformationssystem (CIS) vilka antingen innehåller särskilda bestämmelser om uppgiftsskydd eller vanligen hänvisar till Europarådets rättsakter om uppgiftsskydd”.

135. Enligt datatillsynsmannen bör en ny rättslig ram så långt det är möjligt vara tydlig, enkel och konsekvent. När olika system sprids som gäller för exempelvis Europol, Eurojust, SIS och Prüm måste de fortfarande överensstämma med reglerna eller blir till och med ännu mer komplicerade. Det är ett av skälen till att datatillsynsmannen förespråkar en övergripande rättsakt för alla sektorer.

136. Datatillsynsmannen inser emellertid att anpassningen av de olika systemens regler kommer att kräva avsevärt arbete, vilket måste genomföras mycket noggrant. Han anser att ett gradvis synsätt som nämns i meddelandet förefaller rimligt så länge satsningen på att hålla en hög nivå på uppgiftsskyddet på ett konsekvent och effektivt sätt fortfarande är tydlig och synlig. För att vara mer konkret:

— I ett första skede bör den allmänna rättsakten för uppgiftsskydd gälla all hantering inom det polisiära och rättsliga samarbetet, och innefatta anpassningar till polis och rättsväsende (enligt betydelsen i 9.2).

— I ett andra steg bör de sektorsspecifika systemen för uppgiftsskydd anpassas till detta allmänna instrument. Kommissionen bör anta förslag för detta andra steg, inom en kort och specificerad tidsram.

10. **Dataskyddsmyndigheter och samarbete mellan dessa myndigheter**

10.1 *Förstärkt roll för dataskyddsmyndigheterna*

137. Datatillsynsmannen stöder fullständigt kommissionens målsättning att ta upp frågan om dataskyddsmyndigheternas ställning och mer explicit stärka deras oberoende, resurser och befogenheter när det gäller verkställighet.

138. Datatillsynsmannen betonar också behovet av att i det nya rättsliga instrumentet klargöra det grundläggande begreppet med oberoende för dessa myndigheter. EG-domstolen har nyligen fattat ett beslut i frågan i mål C-518/07 ([54]), där domstolen betonar att oberoende innebär avsaknad av all extern påverkan. En dataskyddsmyndighet får inte efterfråga eller ta instruktioner från någon. Datatillsynsmannen föreslår uttryckligen att dessa inslag av oberoende ska kodifieras i lagen.

139. För att utföra sina uppgifter måste dessa myndigheter få tillräckliga resurser när det gäller personal och finanser. Datatillsynsmannen föreslår att detta krav ska införlivas i lagen ([55]). Han betonar slutligen behovet av att se till att myndigheterna har fullt harmoniserade befogenheter när det gäller undersökning och införande av tillräckligt avskräckande åtgärder och sanktioner. Detta skulle öka rättssäkerheten för både registrerade personer och för registeransvariga.

140. Ökat oberoende, resurser och befogenheter för dataskyddsmyndigheter bör införas tillsammans med förstärkt samarbete på multilateral nivå, särskilt mot bakgrund av det växande antalet frågor om uppgiftsskydd på europeisk nivå. Den huvudsakliga infrastruktur som bör användas för detta samarbete är helt uppenbart artikel 29-arbetsgruppen.

10.2 *Stärkt roll för arbetsgruppen*

141. Historien har visat att sedan gruppen startade 1997 och fram till i dag har gruppens funktion utvecklats. Den har blivit mer oberoende och kan kanske inte längre i praktiken betraktas som en enkel rådgivande arbetsgrupp till kommissionen. Datatillsynsmannen föreslår ytterligare förbättringar av arbetsgruppens funktionssätt, även vad gäller dess infrastruktur och oberoende.

142. Datatillsynsmannen anser att gruppens inneboende styrka är kopplad till medlemmarnas oberoende och befogenheter. Arbetsgruppens autonomi bör tryggas i den nya rättsliga ramen i enlighet med kriterierna för dataskyddsmyndigheters fullständiga oberoende som utarbetats av EG-domstolen i mål C-518/07. Datatillsynsmannen anser att arbetsgruppen också bör få tillräckliga resurser och budget och ett förstärkt sekretariat för att stödja dess bidrag.

143. När det gäller arbetsgruppens sekretariat uppskattar datatillsynsmannen det faktum att det ingår i enheten för dataskydd vid GD Rättvisa, frihet och säkerhet vilket har fördelen att arbetsgruppen själv kan dra nytta av effektiva och flexibla kontakter och uppdaterad information om utvecklingen när det gäller dataskydd. Å andra sidan ifrågasätter han det faktum att kommissionen (och mer specifikt enheten) samtidigt är medlem, sekretariat för och mottagare av arbetsgruppens yttranden. Det skulle motivera ett större oberoende för sekretariatet. Datatillsynsmannen uppmuntrar kommissionen att – i nära samarbete med intressenter – bedöma hur detta oberoende bäst kan åstadkommas.

([54]) Mål C-518/07, *Kommissionen* mot *Tyskland*, ännu ej offentliggjort i REG.

([55]) Se exempelvis artikel 43.2 i förordning (EG) nr 45/2001, som innehåller sådana krav för Europeiska datatillsynsmannen.

144. En förstärkning av dataskyddsmyndigheternas inflytande kräver också starka befogenheter för arbetsgruppen inklusive bättre regler och garantier samt större öppenhet. Detta kommer att utvecklas dels för arbetsgruppens rådgivande, dels för dess verkställande roll.

10.3 *Arbetsgruppens rådgivande roll*

145. Arbetsgruppens ståndpunkt måste införlivas effektivt när det gäller dess rådgivande roll gentemot kommissionen, särskilt i förhållande till tolkningen och tillämpningen av principerna i direktivet och andra instrument för uppgiftsskydd, med andra ord för att trygga en officiell utformning av arbetsgruppens ståndpunkter. Ytterligare diskussioner behövs bland dataskyddsmyndigheter för att fastställa hur detta kan införlivas i det rättsliga instrumentet.

146. Datatillsynsmannen rekommenderar lösningar som skulle göra yttranden från arbetsgruppen mer officiella utan att deras funktionssätt ändras avsevärt. Datatillsynsmannen föreslår att en skyldighet ska införas för dataskyddsmyndigheter och kommissionen att ta största hänsyn till yttranden och gemensamma ståndpunkter som antagits av arbetsgruppen, baserat på den modell som antagits för ståndpunkterna från organet för europeiska regleringsmyndigheter för elektronisk kommunikation (Berec) ([56]). Den nya rättsakten kan dessutom ge arbetsgruppen den uttryckliga uppgiften att anta ”förklarande rekommendationer”. Dessa alternativa lösningar skulle ge arbetsgruppens ståndpunkter en starkare roll, även inför domstolarna.

10.4 *Samordnat verkställande av arbetsgruppen*

147. Enligt den nuvarande ramen lämnas verkställandet av dataskyddslagstiftning i medlemsstaterna till 27 olika dataskyddsmyndigheter med liten samordning när det gäller hantering av särskilda fall. När det handlar om fall som omfattar mer än en medlemsstat eller har en tydlig global dimension mångfaldigas kostnaderna för företag, vilka måste ha kontakt med olika offentliga myndigheter för samma aktivitet, och det ökar risken för inkonsekvent tillämpning: I undantagsfall kan samma behandlingsåtgärd betraktas som laglig av en dataskyddsmyndighet och förbjuden av en annan.

148. Vissa fall är av strategisk betydelse och bör tas upp på ett centraliserat sätt. Artikel 29-arbetsgruppen underlättar samordning och verkställande av åtgärder mellan olika dataskyddsmyndigheter ([57]) i stora frågor om uppgiftsskydd med dessa internationella effekter. Detta var fallet med sociala nätverk och sökmotorer ([58]), liksom när det gäller samordnade inspektioner i olika medlemsstater om telekommunikation och hälsoförsäkringsfrågor.

149. Det finns emellertid gränser för vilka verkställandeåtgärder som arbetsgruppen kan vidta enligt det nuvarande ramverket. Gemensamma ståndpunkter kan intas av arbetsgruppen men det finns inget instrument för att se till att dessa faktiskt genomförs i praktiken.

150. Datatillsynsmannen föreslår att det rättsliga instrumentet ska innehålla ytterligare bestämmelser som kan stödja ett samordnat verkställande, framför allt följande:

— En skyldighet att se till att dataskyddsmyndigheter och kommissionen tar den största hänsyn till yttranden och gemensamma ståndpunkter som antagits av artikel 29-arbetsgruppen ([59]).

— En skyldighet för dataskyddsmyndigheter att trovärdigt samarbeta med varandra och med kommissionen och artikel 29-arbetsgruppen ([60]). Som en praktisk illustration av ett trovärdigt samarbete kan ett förfarande inrättas där dataskyddsmyndigheter informerar kommissionen eller arbetsgruppen vid nationella åtgärder för verkställande som har ett gränsöverskridande inslag, i analogi med förfarandet i den nuvarande ramen vad gäller beslut om nationell lämplighet.

— Specificering av röstningsreglerna för att öka dataskyddsmyndigheters satsning på att genomföra arbetsgruppens beslut. Arbetsgruppen skulle kunna planera

([56]) Europaparlamentets och rådets förordning (EG) nr 1211/2009 av den 25 november 2009 om inrättande av organet för europeiska regleringsmyndigheter för elektronisk kommunikation (Berec) och byrån, (EUT L 337, 18.12.2009, s. 1).

([57]) Utöver artikel 29-arbetsgruppen har den europeiska konferensen för ombudsmän för dataskydd för cirka tio år sedan inrättat en permanent workshop som ska hantera gränsöverskridande klagomål på ett samordnat sätt. Även om denna workshop obestridligt tillför mervärde när det gäller utbyte mellan personal vid dataskyddsmyndigheter och erbjuder ett tillförlitligt nätverk av kontaktpunkter, kan det inte betraktas som en samordnad mekanism för beslutsfattande.

([58]) Se skrivelser från artikel 29-arbetsgruppen av den 12 maj 2010 och den 26 maj 2010, offentliggjorda på artikel 29-arbetsgruppens webbplats (http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010-others_en.htm).

([59]) Såsom angivits ovan fastställs en liknande skyldighet i förordning (EG) nr 1211/2009 där rollen för organet för europeiska regleringsmyndigheter för elektronisk kommunikation (Berec) specificeras.

([60]) Se i detta hänseende artikel 3 i förordning (EG) nr 1211/2009, som citeras ovan.

för att fatta beslut på grundval av en samsyn och när samsyn inte kan uppnås verkställs beslutet enbart med kvalificerad majoritet. Utöver detta kan det i ett skäl anges att de dataskyddsmyndigheter som röstar för ett dokument är skyldiga eller åtar sig att genomföra det på nationell nivå.

151. Datatillsynsmannen vill protestera mot införandet av starkare åtgärder såsom att ge artikel 29-arbetsgruppens ståndpunkter bindande kraft. Det skulle underminera datatillsynsmyndigheters oberoende ställning som medlemsstaterna enligt nationell lag måste garantera. Om arbetsgruppens beslut direkt skulle inverka på tredje part såsom registeransvariga skulle nya förfaranden behövas, inklusive garantier som öppenhet och upprättelse, samt möjlighet till överklagande vid EG-domstolen.

10.5 *Samarbete mellan datatillsynsmannen och arbetsgruppen*

152. Datatillsynsmannens och arbetsgruppens samarbete kan också förbättras ytterligare. Datatillsynsmannen är medlem i arbetsgruppen och bidrar till ståndpunkter om de viktigaste strategiska utvecklingarna inom EU, samtidigt som han säkerställer att dessa är förenliga med hans egna ståndpunkter. Datatillsynsmannen noterar det ökande antalet privata frågor, både inom den privata och den offentliga sektorn, vilket får effekter på nationell nivå i flera medlemsstater, och där kan arbetsgruppen spela en specifik roll.

153. Datatillsynsmannen har en kompletterande uppgift att ge råd om utvecklingen inom EU och den bör bibehållas. I sin egenskap av europeiskt organ utövar han denna rådgivande befogenhet gentemot EU:s institutioner på samma sätt som nationella dataskyddsmyndigheter ger råd till sina regeringar.

154. Datatillsynsmannen och arbetsgruppen arbetar ur olika men kompletterande perspektiv. Det finns därför ett behov av att bevara och kanske förbättra samordningen mellan arbetsgruppen och datatillsynsmannen, så att de samarbetar om de viktigaste frågorna kring uppgiftsskydd, exempelvis genom att samordna agendor regelbundet ([61]), och genom att säkra öppenhet i frågor som har en mer nationell eller specifik EU-aspekt.

155. Samordning nämns inte i det nuvarande direktivet av det enkla skälet att datatillsynsmannen inte fanns när direktivet antogs, men efter sex års existens är det uppenbart att datatillsynsmannen och arbetsgruppen kompletterar varandra och detta kan erkännas formellt. Datatillsynsmannen erinrar om att enligt förordning (EG) nr 45/2001 är han skyldig att samarbeta med nationella dataskyddsmyndigheter och delta i arbetsgruppens verksamhet. Datatillsynsmannen rekommenderar att samarbete uttryckligen ska nämnas i det nya rättsliga instrumentet och struktureras vid behov, exempelvis genom att fastställa ett förfarande för samarbete.

10.6 *Samarbete mellan Europeiska datatillsynsmannen och dataskyddsmyndigheter vid övervakning av EU:s system*

156. Dessa beaktanden gäller även områden där övervakandet måste samordnas mellan europeisk och nationell nivå. Det gäller exempelvis EU-organ som hanterar betydande mängder uppgifter från nationella myndigheter eller för storskaliga informationssystem som är såväl europeiska som nationella.

157. Befintliga system för några EU-organ och storskaliga informationssystem – exempelvis Europol, Eurojust och den första generationen Schengens informationssystem (SIS) har gemensamma tillsynsorgan med företrädare för nationella dataskyddsmyndigheter – är en kvarleva från mellanstatligt samarbete från tiden före Lissabon och följer inte EU:s institutionella struktur som Europol och Eurojust nu är en fullständig del av och där ”Schengenregelverket” nu också har införlivats ([62]).

158. I meddelandet aviseras att kommissionen under 2011 kommer att inleda ett samråd med intressenter om översynen av dessa övervakningssystem. Datatillsynsmannen uppmanar kommissionen att så snart som möjligt (inom en kort och specificerad tidsram, se ovan) inta en ståndpunkt i den pågående diskussionen om övervakning. Han kommer att i denna diskussion inta följande ståndpunkt.

159. Utgångsläget bör vara att se till att alla övervakande organ uppfyller det nödvändiga kriteriet med oberoende, resurser och verkställande befogenheter. Det bör dessutom säkerställas att de perspektiv och de expertkunskaper som finns på EU-nivå beaktas. Det innebär att nationella myndigheter bör samarbeta sinsemellan men även med europeiska datatillsynsmyndigheter (för närvarande Europeiska datatillsynsmannen). Datatillsynsmannen anser det nödvändigt att följa en modell som uppfyller dessa krav ([63]).

160. Under de senaste åren har modellen med ”samordnad övervakning” utvecklats. Denna övervakningsmodell är nu operativ inom Eurodac och delar av tullinformationssystemet och kommer snart att utvidgas till Informationssystemet för viseringar (VIS) och den andra generationen av Schengens informationssystem (SIS II). Modellen har tre nivåer: (1) övervakning på nationell nivå sköts av dataskyddsmyndigheter, (2) övervakning inom EU sköts av

([61]) Exempelvis på grundval av förteckningen över lagstiftningsåtgärder som offentliggörs varje år och uppdateras regelbundet och som är tillgänglig på Europeiska datatillsynsmannens webbplats.

([62]) Enligt förordning (EG) nr 45/2001 är Europeiska datatillsynsmannen skyldig att samarbeta med dessa organ.

([63]) För Eurojust bör modellen också ta hänsyn till att övervakningen av dataskyddet respekterar domstolarnas oberoende, när Eurojust hanterar uppgifter i samband med brottmål.

Europeiska datatillsynsmannen och (3) samordning säkerställs genom regelbundna möten som datatillsynsmannen kallar till när han fungerar som sekretariat för denna samordningsmekanism. Modellen har visat sig framgångsrik och effektiv och bör användas i framtiden för andra informationssystem.

C. **HUR KAN TILLÄMPNINGEN AV DEN NUVARANDE RAMEN FÖRBÄTTRAS?**

11. **På kort sikt**

161. Eftersom översynsprocessen pågår bör ansträngningar göras för att de nuvarande reglerna verkligen ska införlivas fullständigt och effektivt. Dessa regler kommer att vara tillämpliga till dess att det kommande ramverket antas och kommer sedan att införlivas i nationell lag i medlemsstaterna. I det sammanhanget finns flera möjliga åtgärder.

162. För det första bör kommissionen fortsätta att övervaka att medlemsstaterna efterlever direktiv 95/46/EG och vid behov använder sina befogenheter enligt artikel 258 i Fördraget om Europeiska unionens funktionssätt. Nyligen har förfaranden om överträdelser inletts på grund av underlåtenhet att korrekt införliva artikel 28 i direktivet vad gäller kravet på oberoende för dataskyddsmyndigheter ([64]). Även inom andra områden behöver man övervaka att reglerna följs och verkställs i sin helhet ([65]). Datatillsynsmannen välkomnar därför och stöder fullständigt kommissionens satsning i meddelandet på att fortsätta sin aktiva politik när det gäller överträdelser. Kommissionen bör även fortsätta den strukturella dialogen med medlemsstaterna om införlivande ([66]).

163. För det andra måste verkställande på nationell nivå uppmuntras så att regler för uppgiftsskydd, inbegripet när det gäller nya tekniska företeelser och globala aktörer verkligen tillämpas praktiskt. Dataskyddsmyndigheter bör fullt ut utnyttja sina befogenheter när det gäller undersökning och sanktioner. Det är också viktigt att befintliga rättigheter för registrerade personer, särskilt rätten till tillträde, genomförs praktiskt i sin helhet.

164. För det tredje förefaller större samordning när det gäller verkställande nödvändigt på kort sikt. Artikel 29-arbetsgruppens roll och dess tolkande dokument är i detta hänseende avgörande men även dataskyddsmyndigheter bör göra sitt bästa för att omsätta dem i praktiken. Olika resultat inom EU eller globalt behöver undvikas och gemensamma synsätt kan och bör uppnås inom arbetsgruppen. Samordnade undersökningar inom hela EU under överinseende av arbetsgruppen kan också tillföra betydande mervärde.

165. För det fjärde bör principer för uppgiftsskydd ”byggas in” aktivt i nya förordningar som direkt eller indirekt kan påverka uppgiftsskyddet. Inom EU gör datatillsynsmannen avsevärda ansträngningar för att bidra till en bättre EU-lagstiftning och dessa satsningar måste också genomföras på nationell nivå. Dataskyddsmyndigheter bör därför fullt ut utnyttja sina rådgivande befogenheter för att säkra ett sådant aktivt synsätt. Dataskyddsmyndigheter, inbegripet Europeiska datatillsynsmannen, kan också spela en aktiv roll när det gäller att övervaka teknisk utveckling. Övervakning är viktigt för att på ett tidigt stadium identifiera framväxande trender, understryka möjliga konsekvenser när det gäller uppgiftsskydd, stödja lösningar som gynnar uppgiftsskydd och öka intressenternas medvetenhet.

166. Avslutningsvis behöver samarbetet mellan olika aktörer på internationell nivå aktivt fortsätta. Det är därför viktigt att förstärka det internationella samarbetsinstrumentet. Initiativ som Madridnormerna och det pågående arbetet inom Europarådet och OECD förtjänar fullt stöd. Det är därför mycket positivt att även US Federal Trade Commission nu också ingår i gruppen av ombudsmän för dataskydd och integritet inom ramen för deras internationella konferens.

D. **SLUTSATSER**

ALLMÄNNA KOMMENTARER

167. Datatillsynsmannen välkomnar meddelandet rent allmänt, eftersom han är övertygad om att översynen av den nuvarande rättsliga ramen för skydd av personuppgifter är nödvändig för att säkra ett effektivt skydd i ett alltmer utvecklat och globaliserat informationssamhälle.

168. I meddelandet identifieras huvudfrågor och utmaningar. Datatillsynsmannen instämmer i kommissionens uppfattning att ett starkt system för uppgiftsskydd kommer att behövas även i framtiden, baserat på principen att befintliga allmänna principer för uppgiftsskydd fortfarande är giltiga i ett samhälle som genomgår grundläggande förändringar. Datatillsynsmannen instämmer också i meddelandets yttrande om att utmaningarna är enorma och betonar att de föreslagna lösningarna bör vara lika ambitiösa och göra skyddet effektivare. Han efterlyser därför ett mer ambitiöst synsätt på en rad punkter.

169. Europeiska datatillsynsmannen stöder helt den övergripande strategin för uppgiftsskydd. Han beklagar emellertid att meddelandet utesluter vissa områden, exempelvis uppgiftshantering inom EU:s institutioner och organ, från det allmänna instrumentet. Om kommissionen skulle besluta

([64]) Se mål C-518/07 som nämns ovan och kommissionens pressmeddelande av den 28 oktober 2010 (IP/10/1430).

([65]) Kommissionen har inlett ett överträdelseförfarande mot Storbritannien för en påstådd överträdelse av olika bestämmelser om uppgiftsskydd, inbegripet krav på konfidentialitet inom elektronisk kommunikation när det gäller beteendestyrd annonsering. Se kommissionens pressmeddelande av den 9 april 2009 (IP/09/570).

([66]) Se kommissionens första rapport om införlivande av dataskyddsdirektivet som nämns i punkt 22 och följande ovan.

att utelämna dessa områden vädjar datatillsynsmannen till kommissionen om att snarast anta ett förslag på EU-nivå, företrädesvis före slutet av 2011.

HUVUDPERSPEKTIV

170. Utgångspunkterna för översynsförfarandet för datatillsynsmannen är följande:

— Lösningar för uppgiftsskydd måste så långt det är möjligt aktivt stödja snarare än hindra andra berättigade intressen (såsom europeisk ekonomi, enskildas säkerhet och regeringars ansvarighet).

— Den allmänna principen för uppgiftsskydd varken bör eller kan ändras.

— Ytterligare harmonisering bör vara en av huvudmålsättningarna för översynen.

— Perspektivet med grundläggande rättigheter bör stå i centrum för översynsförfarandet. En grundläggande rätt syftar till att skydda medborgare under alla förhållanden.

— Det nya rättsliga instrumentet måste innefatta den polisiära och rättsliga sektorn.

— Det nya rättsliga instrumentet måste så långt det är möjligt utformas på ett tekniskt neutralt sätt och syfta till att skapa rättssäkerhet på längre sikt.

BESTÅNDSDELAR I EN NY RAM

Harmonisering och förenkling

171. Datatillsynsmannen välkomnar kommissionens satsning på att granska möjligheterna att uppnå ytterligare harmonisering av uppgiftsskyddet på EU-nivå. Enligt datatillsynsmannen finns det områden där ytterligare och bättre harmonisering snarast behövs: definitioner, grunder för behandling av uppgifter, rättigheter för registrerade personer, internationella överföringar och dataskyddsmyndigheter.

172. Europeiska datatillsynsmannen föreslår att följande alternativ ska övervägas för att underlätta och/eller minska omfattningen av kraven på anmälan:

— Begränsa anmälningsskyldigheten till specifika slag av behandlingsåtgärder som medför specifika risker.

— En enkel registreringsskyldighet som innebär att registeransvariga måste registrera sig (i motsats till omfattande registrering av alla åtgärder inom databehandling).

— Införande av en standardiserad alleuropeisk anmälningsblankett.

173. Enligt datatillsynsmannen är en förordning, ett instrument som är direkt tillämpligt i medlemsstaterna, det mest effektiva sättet att skydda de grundläggande rättigheterna till skydd av uppgifter och uppnå ytterligare enhetlighet på den inre marknaden.

Stärka enskildas rättigheter

174. Datatillsynsmannen stöder meddelandets förslag att stärka enskilda rättigheter. Han lämnar följande förslag:

— En öppenhetsprincip kan införlivas i lagen. Det är emellertid viktigare att förstärka befintliga bestämmelser om öppenhet (såsom befintliga artiklar 10 och 11 i direktiv 95/46/EG).

— En bestämmelse om anmälan av överträdelse som utvidgar skyldigheten i det reviderade direktivet om integritet och elektronisk kommunikation från vissa leverantörer till alla registeransvariga bör införas i det allmänna instrumentet.

— Gränserna för medgivande bör klargöras. Att bredda de fall där uttryckligt medgivande krävs bör övervägas liksom att anta ytterligare regler för miljön på nätet.

— Ytterligare rättigheter bör införas såsom uppgifters portabilitet och rätten till radering, särskilt tjänster inom informationssamhället på Internet.

— Barns intressen bör skyddas bättre med ytterligare ett antal bestämmelser som särskilt gäller insamling och vidare behandling av barns uppgifter.

— Mekanismer för kollektiv upprättelse vid överträdelse av regler för uppgiftsskydd bör införas i EU:s lagstiftning för att ge kvalificerade enheter möjlighet att vidta åtgärder för grupper av enskilda.

Stärkning av organisationers/registeransvarigas skyldigheter

175. Den nya ramen måste innehålla incitament för registeransvariga att aktivt införliva åtgärder för dataskydd i sin affärsverksamhet. Datatillsynsmannen föreslår att allmänna bestämmelser om ansvarighet och inbyggda skyddsmekanismer ska införas. En bestämmelse om system för sekretesscertifiering bör också införas.

Globalisering och tillämplig lag

176. Datatillsynsmannen stöder det ambitiösa arbetet inom ramen för den internationella konferensen för ombudsmän för dataskydd och integritet för att utveckla de så kallade ”Madridnormerna” i syfte att införliva dem i ett bindande instrument och sannolikt initiera en mellanstatlig konferens. Datatillsynsmannen uppmanar kommissionen att vidta konkreta steg i denna riktning i nära samarbete med OECD och Europarådet.

177. Ett nytt rättsligt instrument måste klargöra kriterierna som fastställer tillämplig lag. Det bör säkerställas att uppgifter som behandlas utanför EU:s gränser ändå omfattas av EU:s jurisdiktion när det finns ett motiverat krav på att EU-lagstiftning ska tillämpas. Om den rättsliga ramen skulle ha formen av en förordning skulle reglerna vara identiska i alla medlemsstater och det skulle vara mindre relevant att fastställa tillämplig lag (inom EU).

178. Datatillsynsmannen stöder helt målsättningen att säkerställa ett mer enhetligt och sammanhängande synsätt gentemot tredje länder och internationella organisationer. Bindande företagsregler bör ingå i det rättsliga instrumentet.

Polis och rättsväsende

179. Ett övergripande instrument som innefattar polis och rättsväsende kan möjliggöra särskilda regler som vederbörligen tar hänsyn till särdragen inom denna sektor, i linje med förklaring 21 till Lissabonfördraget. Särskilda garantier behöver införas för att kompensera registrerade personer genom att ge dem extra skydd inom ett område där hantering av personuppgifter är mer påträngande.

180. Den nya rättsliga ramen bör så långt det är möjligt vara tydlig, enkel och konsekvent. En spridning av olika system som exempelvis gäller för Europol, Eurojust, SIS och Prüm bör undvikas. Datatillsynsmannen inser att de olika systemens regler måste anpassas noggrant och successivt.

Dataskyddsmyndigheter och samarbete mellan dessa myndigheter

181. Datatillsynsmannen stöder fullständigt kommissionens målsättning att ta upp frågan om dataskyddsmyndigheternas ställning och stärka deras oberoende, resurser och befogenheter när det gäller verkställighet. Han rekommenderar följande:

— Kodifiera i det nya rättsliga instrumentet det grundläggande begreppet med oberoende för dataskyddsmyndigheter, enligt specifikationen från EG-domstolen.

— Slå fast i lagen att dataskyddsmyndigheterna måste få tillräckliga resurser.

— Ge myndigheter harmoniserade befogenheter för undersökning och sanktionering.

182. Datatillsynsmannen föreslår ytterligare förbättringar av artikel 29-arbetsgruppens funktionssätt, inbegripet av dess oberoende och infrastruktur. Arbetsgruppen bör också få tillräckliga resurser och ett förstärkt sekretariat.

183. Datatillsynsmannen föreslår att den rådgivande rollen för arbetsgruppen ska förstärkas genom att man inför en skyldighet för dataskyddsmyndigheter och kommissionen att ta den största hänsyn till yttranden och gemensamma ståndpunkter som antagits av arbetsgruppen. Datatillsynsmannen är inte positiv till att ge bindande kraft åt arbetsgruppens ståndpunkter, särskilt på grund av enskilda dataskyddsmyndigheters oberoende ställning. Datatillsynsmannen rekommenderar att kommissionen inför särskilda bestämmelser för att öka samarbetet med Europeiska datatillsynsmannen i det nya rättsliga instrumentet.

184. Datatillsynsmannen vädjar till kommissionen att så snart som möjligt inta en ståndpunkt i frågan om kontroll av EU:s organ och storskaliga informationssystem, med tanke på att alla övervakande organ bör uppfylla det nödvändiga kriteriet med oberoende, tillräckliga resurser och verkställande befogenheter och att man ser till att EU:s perspektiv är väl representerat. Datatillsynsmannen stöder modellen med ”samordnad övervakning”.

Förbättringar inom det nuvarande systemet:

185. Datatillsynsmannen uppmuntrar kommissionen att

— fortsätta att övervaka att medlemsstaterna efterlever direktiv 95/46/EG och vid behov använda sina befogenheter enligt artikel 258 i fördraget om Europeiska unionens funktionssätt,

— uppmuntra verkställande på nationell nivå liksom samordning av verkställande,

— aktivt bygga in principer för uppgiftsskydd i nya förordningar som direkt eller indirekt kan påverka uppgiftsskyddet,

— aktivt fortsätta ytterligare samarbete mellan olika aktörer på internationell nivå.

Utfärdat i Bryssel den 14 januari 2011.

Peter HUSTINX

Europeiska datatillsynsmannen