

## YTTRANDEN

## EUROPEISKA DATATILLSYNSMANNEN

**Yttrande från Europeiska datatillsynsmannen om kommissionens förslag till Europaparlamentets och rådets förordning om administrativt samarbete genom informationssystemet för den inre marknaden (IMI)**

(2012/C 48/02)

EUROPEISKA DATATILLSYNSMANNEN HAR AVGETT DETTA YTTRANDE

med beaktande av fördraget om Europeiska unionens funktionsätt, 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 för sådana uppgifter <sup>(1)</sup>,

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 <sup>(2)</sup>,

med beaktande av begäran om yttrande i enlighet med artikel 28.2 i förordning (EG) nr 45/2001,

HÄRIGENOM FRAMFÖRS FÖLJANDE.

## 1. INLEDNING

### 1.1 Samråd med Europeiska datatillsynsmannen

1. Den 29 augusti 2011 antog kommissionen ett förslag till Europaparlamentets och rådets förordning (nedan kallat *förslaget* eller *förslaget till förordning*) om administrativt samarbete genom informationssystemet för den inre marknaden (IMI) <sup>(3)</sup>. Förslaget skickades samma dag till Europeiska datatillsynsmannen för samråd.

<sup>(1)</sup> EGT L 281, 23.11.1995, s. 31.

<sup>(2)</sup> EGT L 8, 12.1.2001, s. 1.

<sup>(3)</sup> KOM(2011) 522 slutlig.

2. Innan förslaget antogs gavs Europeiska datatillsynsmannen möjlighet att lämna informella kommentarer om förslaget, och innan dess om kommissionens meddelande "Bättre styrning av den inre marknaden genom utökat administrativt samarbete: En strategi för att utvidga och utveckla informationssystemet för den inre marknaden (IMI) (nedan kallat *meddelandet om IMI-strategin*) <sup>(4)</sup>", vilket föregick förslaget. Många av dessa kommentarer har beaktats i förslaget, och dataskyddsgarantierna i förslaget har förstärks till följd härav.

3. Europeiska datatillsynsmannen välkomnar att kommissionen rådfrågade honom och att en hänvisning till detta yttrande ingår i inledningen till förslaget.

### 1.2 Förslagets mål och omfattning

4. IMI är ett IT-verktyg med vilket behöriga myndigheter i medlemsstaterna kan utbyta information med varandra när de tillämpar lagstiftningen om den inre marknaden. IMI gör det möjligt för nationella, regionala och lokala myndigheter i EU-medlemsstaterna att kommunicera snabbt och enkelt med motsvarande myndigheter i andra länder i Europa. Här ingår också behandling av relevanta personuppgifter, inbegripet känsliga uppgifter.

5. IMI utformades först som ett kommunikationsverktyg för utbyte mellan två parter enligt direktivet om erkännande av yrkeskvalifikationer <sup>(5)</sup> och tjänstedirektivet <sup>(6)</sup>. IMI hjälper användarna att hitta rätt myndighet att kontakta i ett annat land och kommunicera med denna genom förhandsöversatta standardfrågor och standardsvar <sup>(7)</sup>.

<sup>(4)</sup> KOM(2011) 75.

<sup>(5)</sup> Europaparlamentets och rådets direktiv 2005/36/EG av den 7 september 2005 om erkännande av yrkeskvalifikationer (EUT L 255, 30.9.2005, s. 22).

<sup>(6)</sup> Europaparlamentets och rådets direktiv 2006/123/EG av den 12 december 2006 om tjänster på den inre marknaden (EUT L 376, 27.12.2006, s. 36).

<sup>(7)</sup> En typisk fråga som innehåller känsliga uppgifter är till exempel följande: "Kan den bifogade handlingen utgöra en rättslig grund för att den professionella verksamheten i fråga inte tillfälligt avbryts eller förbjuds på grund av allvarligt fel i yrkesutövningen eller en brottslig handling när det gäller [den som invandrat och utövar yrket]?"

6. IMI är emellertid utformat som ett flexibelt horisontellt system som kan stödja många områden av lagstiftningen om den inre marknaden. Det är tänkt att användningen successivt ska ökas och stödja ytterligare rättsliga områden i framtiden.

7. En utvidgning av funktionerna i IMI planeras också. Förutom utbyte av uppgifter mellan två parter finns det också andra funktioner som planeras eller redan har införts, såsom "anmälningsförfaranden, varningsmekanismer, arrangemang för ömsesidigt bistånd och problemlösning" <sup>(8)</sup> liksom "arkivering av uppgifter som framtida referens för IMI-aktörer" <sup>(9)</sup>. I många, men inte i alla dessa funktioner kan också behandlingen av personuppgifter ingå.

8. Enligt förslaget ska en tydlig rättslig grund och ett omfattande ramverk för uppgiftsskydd för IMI tillhandahållas.

### 1.3 Bakgrund till förslaget: ett stegvist tillvägagångssätt för att införa ett omfattande ramverk för uppgiftsskydd för IMI

9. Under våren 2007 begärde kommissionen ett yttrande från arbetsgruppen för skydd av uppgifter (nedan kallad *artikel 29-gruppen*) för att undersöka hur IMI påverkar uppgiftsskyddet. Artikel 29-gruppen avgav sitt yttrande den 20 september 2007 <sup>(10)</sup>. I yttrandet rekommenderades kommissionen att tillhandahålla en tydligare rättslig grund och särskilda riktlinjer för uppgiftsskydd vid utbyte av uppgifter inom IMI. Europeiska datatillsynsmannen deltog aktivt i arbetet i undergruppen för IMI och stödde slutsatserna i artikel 29-gruppens yttrande.

10. Europeiska datatillsynsmannen gav även fortsättningsvis ytterligare vägledning åt kommissionen om hur ett mer omfattande ramverk för uppgiftsskyddet för IMI skulle säkerställas steg för steg <sup>(11)</sup>. Inom ramen för detta samarbete och sedan Europeiska datatillsynsmannens yttrande om genomförandet av IMI <sup>(12)</sup> avgavs den 22 februari 2008 har denne konsekvent påpekat behovet av ett nytt rättsinstrument som antas genom det ordinarie lagstiftningsförfarandet för att inrätta ett mer omfattande ramverk för uppgiftsskyddet för IMI och skapa rättssäkerhet. Förslaget till ett sådant rättsinstrument har nu framlagts <sup>(13)</sup>.

## 2. ANALYS AV FÖRSLAGET

### 2.1 Europeiska datatillsynsmannens allmänna omdöme om förslaget och om de centrala utmaningar som gäller för IMI

11. Europeiska datatillsynsmannens allmänna omdöme om IMI är positivt. Europeiska datatillsynsmannen stöder kommissionens syften med att inrätta ett elektroniskt system för informationsutbyte och reglera dess dataskyddsaspekter. Ett sådant rationaliserat system kan inte bara effektivisera samarbetet utan också hjälpa till att säkerställa överensstämmelse med tillämplig dataskyddslagstiftning. Detta är möjligt genom att systemet tillhandahåller en tydlig ram för vilken typ av information som kan utbytas med vem och på vilka villkor.

12. Europeiska datatillsynsmannen välkomnar också att kommissionen föreslår ett horisontellt rättsinstrument för IMI i form av rådets och parlamentets förordning. Han välkomnar att de viktigaste uppgiftsskyddsfrågorna för IMI i stor utsträckning belyses i förslaget. Hans synpunkter ska läsas mot denna positiva bakgrund.

13. Europeiska datatillsynsmannen betonar icke desto mindre att införandet av ett enda centraliserat elektroniskt system för många områden av det administrativa samarbetet ger upphov till risker. Den viktigaste av dessa är att fler uppgifter kan lämnas ut mer allmänt än vad som är strikt nödvändigt för ett effektivt samarbete och att uppgifter, däribland potentiellt föräldrade och felaktiga, kan kvarstå i systemet längre än nödvändigt. Säkerheten hos en databas som är åtkomlig för 27 medlemsstater är också en känslig fråga, eftersom hela systemet bara är lika säkert som den svagaste länken i nätet.

#### Väsentliga utmaningar

14. Beträffande det rättsliga ramverk för IMI som ska inrättas genom den föreslagna förordningen vill Europeiska datatillsynsmannen rikta uppmärksamheten på två centrala utmaningar:

— behovet av att säkerställa enhetlighet samtidigt som mångfalden respekteras, och

— behovet av att väga flexibilitet mot rättssäkerhet.

15. Dessa väsentliga utmaningar är viktiga referenspunkter, och de bestämmer till stor del Europeiska datatillsynsmannens inställning i detta yttrande.

Enhetlighet samtidigt som mångfald respekteras

16. För det första är IMI ett system som används i 27 medlemsstater. Med den nuvarande nivån i fråga om harmonisering av den europeiska lagstiftningen finns det

<sup>(8)</sup> Se skäl 10.

<sup>(9)</sup> Se artikel 13.2.

<sup>(10)</sup> Artikel 29-gruppens yttrande nr 7/2007 om dataskyddsfrågor i samband med informationssystemet för den inre marknaden (IMI), WP140. Finns tillgängligt på [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp140\\_sv.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp140_sv.pdf)

<sup>(11)</sup> Nyckeldokumentet om detta samarbete finns tillgängliga på kommissionens webbplats för IMI på [http://ec.europa.eu/internal\\_market/imi-net/data\\_protection\\_sv.html](http://ec.europa.eu/internal_market/imi-net/data_protection_sv.html) och på Europeiska datatillsynsmannens webbplats på <http://www.edps.europa.eu>

<sup>(12)</sup> Yttrande från Europeiska datatillsynsmannen om kommissionens beslut 2008/49/EG av den 12 december 2007 om genomförandet av informationssystemet för den inre marknaden (IMI) med avseende på skyddet av personuppgifter (EUT C 270, 25.10.2008, s. 1).

<sup>(13)</sup> Artikel 29-gruppen planerar också att lämna synpunkter på förslaget. Europeiska datatillsynsmannen har följt utvecklingen i den relevanta undergruppen i artikel 29-gruppen och lämnat synpunkter.

avsevärda skillnader mellan de nationella administrativa förfarandena och mellan de nationella bestämmelserna om uppgiftsskydd. IMI måste utformas på ett sådant sätt att användarna i var och en av dessa 27 medlemsstater kan följa sina nationella lagar, inbegripet bestämmelser om uppgiftsskydd, när de utbyter personuppgifter via IMI. Samtidigt måste de registrerade också försäkras om att deras uppgifter skyddas konsekvent, oberoende av att uppgifterna överförs via IMI till en annan medlemsstat. Att iakttäta enhetlighet samtidigt som mångfalden respekteras är en viktig utmaning när både den tekniska och den rättsliga infrastrukturen för IMI utformas. Onödigt komplexitet och uppsplittring bör undvikas. Uppgiftsbehandlingen inom IMI måste vara transparent, och ansvaret för att fatta beslut om utformningen av systemet, det dagliga underhållet och användningen av systemet, och även övervakningen av det, måste vara tydligt fördelat.

#### Avvägning mellan flexibilitet och rätts-säkerhet

17. För det andra är IMI, till skillnad från andra storskaliga IT-system som Schengens informationssystem, informationssystemet för viseringar, tullinformationssystemet och Eurodac, vilka alla är inriktade på samarbete inom särskilda, klart definierade områden, ett horisontellt verktyg för informationsutbyte som kan användas för att underlätta informationsutbytet inom många olika politikområden. Avsikten är också att IMI:s tillämpningsområde stegvis ska utökas till ytterligare politikområden, och funktionerna kan också komma att innefatta hittills inte angivna typer av administrativt samarbete. Dessa utmärkande drag hos IMI gör det svårare att klart definiera systemets funktioner och det utbyte av uppgifter som kan äga rum i systemet. Det är därför också en större utmaning att klart definiera lämpliga säkerhetsåtgärder för uppgiftsskydd.
18. Europeiska datatillsynsmannen medger att det behövs flexibilitet och tar notis om kommissionens önskan att göra förordningen "framtidssäker". Detta får emellertid inte leda till bristande tydlighet eller rättsäkerhet i fråga om systemets funktioner och de säkerhetsåtgärder för uppgiftsskydd som ska införas. Förslaget bör därför alltid när det är möjligt göras mer specifikt, och inte bara vara en upprepning av de viktigaste principerna för uppgiftsskydd som anges i direktiv 95/46/EG och förordning (EG) nr 45/2001<sup>(14)</sup>.

## 2.2 IMI:s tillämpningsområde och dess förväntade utvidgning (artiklarna 3 och 4)

### 2.2.1 Inledning

19. Europeiska datatillsynsmannen välkomnar förslaget tydliga definition av IMI:s nuvarande tillämpningsområde, med bilaga I där den tillämpliga unionsrätt enligt vilken uppgifter kan utbytas anges. Här ingår samarbete enligt de

särskilda bestämmelserna i direktivet om erkännande av yrkeskvalifikationer och direktivet om tillämpningen av patienters rättigheter vid gränsöverskridande hälso- och sjukvård<sup>(15)</sup>.

20. Eftersom det förväntas att tillämpningsområdet för IMI kommer att utvidgas anges potentiella områden för utvidgning i bilaga II. Punkter i bilaga II kan flyttas till bilaga I genom en delegerad akt som antas av kommissionen efter en konsekvensbedömning<sup>(16)</sup>.
21. Europeiska datatillsynsmannen välkomnar denna metod eftersom den i) tydligt avgränsar IMI:s tillämpningsområde och ii) säkerställer insyn och iii) samtidigt ger flexibilitet i de fall då IMI används för ytterligare informationsutbyte i framtiden. Den säkerställer också att inget informationsutbyte kan genomföras genom IMI i) utan att det finns en lämplig rättslig grund i särskild lagstiftning om den inre marknaden som tillåter eller föreskriver informationsutbyte<sup>(17)</sup> och ii) utan att en hänvisning till denna rättsliga grund införs i bilaga I till förordningen.
22. I detta sammanhang råder det fortfarande osäkerhet beträffande IMI:s tillämpningsområde när det gäller de politikområden som IMI kan utvidgas till och beträffande de funktioner som ingår eller kan ingå i IMI.
23. För det första kan det inte uteslutas att IMI:s tillämpningsområde kan utvidgas mer än till att omfatta de politikområden som anges i bilagorna I och II. Detta kan inträffa om användningen av IMI för vissa typer av informationsutbyte inte föreskrivs av kommissionen i en delegerad akt utan i en akt som har antagits av parlamentet och rådet i ett fall där detta inte förutsetts i bilaga II<sup>(18)</sup>.

<sup>(15)</sup> Europaparlamentets och rådets direktiv 2011/24/EU av den 9 mars 2011 om tillämpningen av patienträttigheter vid gränsöverskridande hälso- och sjukvård (EUT L 88, 4.4.2011, s. 45).

<sup>(16)</sup> I själva utkastet till förordning anges inte någon konsekvensbedömning. På sidan 7 i motiveringen till förslaget förklaras det att kommissionen kommer att få befogenheter att flytta punkter från bilaga II till bilaga I genom att anta en delegerad akt och "efter en bedömning av teknisk genomförbarhet, kostnadseffektivitet, användarvänlighet och totala verkningar på systemet samt resultaten från en tänkbar testningsfas".

<sup>(17)</sup> Med undantag för Solvit (se bilaga II, I.1) där bara "mjuk lagstiftning", kommissionens rekommendation, finns tillgänglig. Från uppgiftsskyddssynpunkt kan enligt Europeiska datatillsynsmannen i det speciella fallet med Solvit den rättsliga grunden för behandlingen vara de registrerades "medgivande".

<sup>(18)</sup> Detta kan ske på initiativ av kommissionen, men det kan inte heller uteslutas att idén att använda IMI inom ett speciellt politikområde kan uppkomma senare i lagstiftningsprocessen och föreslås av parlamentet och rådet. Detta har redan tidigare skett beträffande direktivet om patienters rättigheter vid gränsöverskridande hälso- och sjukvård. Det skulle behövas mer klarhet i ett sådant fall när det gäller "förfarandet" för utvidgning, vilket bara tycks ha varit inriktat på fallet med utvidgning genom delegerade akter (se bestämmelserna om konsekvensbedömning, delegerade akter, och uppdatering av bilaga I).

<sup>(14)</sup> Se också våra synpunkter i avsnitt 2.2 beträffande den förutsedda utvidgningen av IMI i detta avseende.

24. För det andra, medan en utvidgning av tillämpningsområdet till nya politikområden i vissa fall bara kräver en liten eller ingen ändring av systemets befintliga funktioner<sup>(19)</sup>, kan andra utvidgningar kräva nya och annorlunda funktioner eller viktiga ändringar i befintliga funktioner:

— Även om det i förslaget hänvisas till olika befintliga eller planerade funktioner är hänvisningarna ofta inte tillräckligt tydliga eller tillräckligt preciserade. Detta gäller i varierande grad för hänvisningar till varningar, externa aktörer, arkivering, arrangemang för ömsesidigt bistånd och problemlösning<sup>(20)</sup>. Ordet "varning", som avser en befintlig central funktion, nämns till exempel bara en enda gång, i skäl 10.

— Enligt förslaget till förordning är det möjligt att anta nya typer av funktioner som inte alls nämns i förslaget.

— IMI har hittills beskrivits som ett IT-verktyg för informationsutbyte, med andra ord ett kommunikationsverktyg (se till exempel artikel 3 i förslaget). Vissa av de funktioner som anges i förslaget, inbegripet funktionen "arkivering av information" tycks emellertid sträcka sig längre. Den föreslagna förlängningen av arkiveringstiden till fem år tyder också på en förskjutning i riktning mot en "databas". En sådan utveckling skulle förändra IMI:s karaktär i grunden<sup>(21)</sup>.

### 2.2.2 Rekommendationer

25. För att ta itu med dessa osäkra punkter rekommenderar Europeiska datatillsynsmannen ett tvådelat tillvägagångssätt. Han föreslår för det första att funktioner som redan kan förutses ska klarläggas och tas upp mer specifikt, och för det andra att lämpliga förfarandemässiga skyddsåtgärder ska vidtas för att säkerställa att uppgiftsskyddet också nog övervägs under den framtida utvecklingen av IMI.

Klarläggande av funktioner som redan är tillgängliga eller förutsebara (t.ex. utbyte mellan två parter, varningar, arkivering, problemlösning och externa aktörer)

26. Europeiska datatillsynsmannen rekommenderar att förordningen görs mera specifik när det gäller funktioner där dessa redan är kända, som i fråga om det informationsutbyte som anges i bilagorna I och II.

<sup>(19)</sup> Informationsutbyte mellan två parter enligt direktivet om erkännande av yrkeskvalifikationer och direktivet om patienters rättigheter vid gränsöverskridande hälso- och sjukvård följer till exempel i huvudsak samma system och kan anpassas med hjälp av liknande funktioner som omfattas av liknande säkerhetsåtgärder för uppgiftsskydd.

<sup>(20)</sup> Se skälen 2, 10, 12, 13 och 15 och artiklarna 5 b, 5 i, 10.7 och 13.2.

<sup>(21)</sup> Om avsikten är att låta IMI ersätta eller komplettera den befintliga ärendehantering och arkiveringssystemen och/eller använda IMI som databas bör detta framgå tydligare i artikel 3.

27. Mer specifika och tydliga åtgärder skulle till exempel kunna anges för integreringen av Solvit<sup>(22)</sup> i IMI (bestämmelser för "externa aktörer" och "problemlösning") och för adresskatalogerna med yrkesverksamma och tillhandahållare av tjänster (bestämmelser om "arkivering").

28. Ytterligare klarlägganden bör också göras beträffande "varningar", vilka redan används enligt tjänstedirektivet och också kan införas inom ytterligare politikområden. I synnerhet bör "varning" som funktion definieras tydligare i artikel 5 (tillsammans med andra funktioner, som informationsutbyte mellan två parter och arkivering). Tillträdesrättigheter och lagringstider för varningar bör också klarläggas<sup>(23)</sup>.

Förfarandemässiga skyddsåtgärder (konsekvensbedömning av uppgiftsskydd och samråd med datatillsynsmyndigheter)

29. Om avsikten är att förordningen ska vara "framtidssäker" i fråga om ytterligare funktioner som kan bli nödvändiga på längre sikt och att således ytterligare funktioner ska tillåtas som ännu inte är definierade i förordningen bör detta åtföljas av lämpliga förfarandemässiga skyddsåtgärder för att säkerställa att lämpliga åtgärder vidtas för att införa de nödvändiga åtgärderna för uppgiftsskydd innan den nya funktionen tas i bruk. Detsamma bör gälla för utvidgningar till nya politikområden där detta påverkar uppgiftsskyddet.

30. Europeiska datatillsynsmannen rekommenderar en tydlig mekanism som säkerställer att uppgiftsskyddsfrågor nog utvärderas före varje utvidgning av funktionerna eller utsträckning till nya politikområden och att ytterligare skyddsåtgärder eller tekniska åtgärder införs i IMI:s arkitektur om det är nödvändigt. I synnerhet

— bör den konsekvensbedömning som anges på sidan 7 i motiveringen krävas speciellt i själva förordningen och även innefatta konsekvensbedömning av uppgiftsskydd som ska inriktas speciellt på vilka eventuella ändringar i utformningen av IMI som är nödvändiga för att säkerställa att förordningen fortsättningsvis innehåller lämpliga åtgärder för uppgiftsskydd som också omfattar de nya politikområdena och/eller funktionerna,

— bör det specifikt anges i förordningen att samråd med Europeiska datatillsynsmannen och nationella datatillsynsmyndigheter krävs före varje utvidgning av IMI. Samrådet kan äga rum genom mekanismen för samordnad övervakning i artikel 20.

<sup>(22)</sup> Se bilaga II, I.1.

<sup>(23)</sup> Se avsnitten 2.4 och 2.5.5 nedan.

31. Dessa förfarandemässiga skyddsåtgärder (konsekvensbedömning av uppgiftsskydd och samråd) bör gälla både för utvidgning genom en delegerad akt från kommissionen (flyttning av en post från bilaga II till bilaga I) och genom parlamentets och rådets förordning med införande av en post som ännu inte har angetts i bilaga II.
32. Slutligen rekommenderar Europeiska datatillsynsmannen att man i förordningen klarlägger huruvida tillämpningsområdet för de delegerade akter som kommissionen kommer att få befogenheter att anta enligt artikel 23 ska innefatta andra punkter utöver flyttning av poster från bilaga II till bilaga I: Om det är möjligt bör kommissionen ges befogenheter i förordningen att anta speciella genomförandeakter eller delegerade akter för att närmare definiera ytterligare funktioner i systemet eller ta upp uppgiftsskyddsfrågor som kan uppkomma i framtiden.

### 2.3 Roller, behörighet och ansvarsområden (artiklarna 7–9)

33. Europeiska datatillsynsmannen välkomnar att ett helt kapitel (kapitel II) ägnas åt att klarlägga de funktioner och ansvarsområden som de olika aktörer som är involverade i IMI har. Bestämmelserna skulle kunna stärkas ytterligare enligt följande.
34. I artikel 9 beskrivs de ansvarsområden som följer av kommissionens roll som kontrollerande institution. Europeiska datatillsynsmannen rekommenderar dessutom att ytterligare en bestämmelse införs med uppgift om kommissionens roll för att säkerställa att systemet är utformat med tillämpning av principerna om "inbyggt integritetsskydd" och dess roll som samordnare när det gäller uppgiftsskyddsfrågor.
35. Europeiska datatillsynsmannen välkomnar att det i IMI-samordnarnas uppgifter som anges i artikel 7 nu särskilt ingår samordningsuppgifter i fråga om uppgiftsskydd, inbegripet att fungera som kontaktperson för kommissionen. Han rekommenderar att det dessutom klargörs att kontakter med de nationella datatillsynsmyndigheterna också ingår i dessa samordningsuppgifter.

### 2.4 Tillträdesrättigheter (artikel 10)

36. I artikel 10 anges skyddsåtgärder i samband med tillträdesrättigheter. Europeiska datatillsynsmannen välkomnar att dessa bestämmelser har stärkts avsevärt efter det att han lämnat synpunkter.
37. Med tanke på IMI:s horisontella och expansiva karaktär är det viktigt att säkerställa att systemet garanterar att "kinesiska murar" tillämpas som begränsar den information som behandlas inom ett politikområde till enbart detta politikområde. Användarna av IMI bör i) bara få tillgång till information under förutsättning att informationen behövs, och ii) informationen ska begränsas till ett enda politikområde.
38. Om det är oundvikligt att en användare av IMI får rätt att få tillgång till information för flera politikområden (vilket kan vara fallet till exempel i lokal förvaltning) ska syste-

met åtminstone inte tillåta att information som kommer från olika politikområden slås samman. Undantag bör om det är nödvändigt anges i genomförandebestämmelser eller i en unionsrättsakt med strikt iakttagande av principen om ändamålsbegränsning.

39. Dessa principer anges nu i förordningstexten, men de kan stärkas och operationaliseras ytterligare.
40. När det gäller kommissionens tillträdesrättigheter välkomnar Europeiska datatillsynsmannen att det i förslaget artiklar 9.2, 9.4 och 10.6 sammantagna anges att kommissionen inte ska ha tillgång till de personuppgifter som utbyts mellan medlemsstater utom i de fall där kommissionen anges som deltagare i ett förfarande för administrativt samarbete.
41. Externa aktörers tillträdesrättigheter och tillträdesrätt till varningar bör också specificeras ytterligare<sup>(24)</sup>. Beträffande varningar rekommenderar Europeiska datatillsynsmannen att det i förordningen föreskrivs att varningar inte som standard ska skickas till alla behöriga myndigheter i fråga i alla medlemsstater, utan bara till dem som är berörda, under förutsättning att informationen behövs. Detta utesluter inte att varningar skickas till alla medlemsstater i speciella fall eller inom speciella politikområden om alla är berörda. Likaledes är en bedömning från fall till fall nödvändig för att avgöra huruvida kommissionen ska ha tillgång till varningar.

### 2.5 Bevarande av personuppgifter (artiklarna 13 och 14)

#### 2.5.1 Inledning

42. Genom artikel 13 i förslaget förlängs lagringstiden för uppgifter i IMI från för närvarande sex månader (räknat från det att ärendet avslutats) till fem år, varvid uppgifterna "blockeras" efter 18 månader. Under den period då uppgifterna "blockeras" är de bara tillgängliga efter ett speciellt förfarande för inhämtning som bara kan inledas på begäran av den registrerade personen eller om uppgifterna behövs "för att bevisa att informationsutbyte förekommit genom IMI".
43. I själva verket lagras uppgifterna i IMI således under tre olika perioder:
- från det att de lämnats och till dess att ärendet avslutats,
  - från det att ärendet avslutats för en period om 18 månader<sup>(25)</sup>,
  - i blockerad form i ytterligare tre år och sex månader från det att de 18 månaderna har löpt ut (med andra ord tills det har gått fem år sedan ärendet avslutades).

<sup>(24)</sup> Se även avsnitt 2.2.2.

<sup>(25)</sup> I artikel 13.1 föreslås att 18 månader ska vara "maximitid", och följaktligen kan även en kortare period fastställas. Detta skulle emellertid inte påverka den sammanlagda lagringstiden, som i vart fall skulle vara tills det har gått fem år sedan ärendet avslutades.

44. Utöver dessa allmänna regler är enligt artikel 13.2 "arkivering av uppgifter" tillåten så länge som det krävs för detta ändamål, med medgivande från den registrerade eller när "det är nödvändigt för att efterleva en unionsakt". I artikel 14 föreskrivs vidare en liknande blockeringsmekanism för bevarande av personuppgifter som gäller IMI-användare i fem år efter det att de upphört att vara IMI-användare.

45. Det finns inga andra speciella bestämmelser. Därför är förmodligen de allmänna reglerna avsedda att tillämpas inte bara på utbyte mellan två parter utan också på varningar, problemlösning (som i Solvit<sup>(26)</sup>) och på alla andra funktioner där personuppgifter behandlas.

46. Mot bakgrund av artikel 6.1 e i direktiv 95/46/EG och artikel 4.1 e i förordning (EG) nr 45/2001, vilka båda kräver att personuppgifter inte lagras under en längre tid än vad som är nödvändigt för de ändamål för vilka de samlades in eller för vilka de senare behandlas, ställer sig Europeiska datatillsynsmannen tveksam i flera avseenden när det gäller lagringstiderna.

#### 2.5.2 Från överföring till avslutning av ärendet: behovet av avslutning av ärendet i rätt tid

47. När det gäller den första perioden, från överföringen av information och till dess att ärendet avslutas, ställer sig Europeiska datatillsynsmannen tveksam eftersom det finns risk för att vissa ärenden kanske aldrig avslutas eller avslutas efter orimligt lång tid. Det kan leda till att vissa personuppgifter finns kvar längre i databasen än som är nödvändigt eller till och med för obestämd tid.

48. Europeiska datatillsynsmannen inser att kommissionen har gjort framsteg på det praktiska planet för att minska eftersläpningen i IMI, och det finns ett system för utbyte mellan två parter för att kontrollera att ärenden avslutas i rätt tid och för att påminna dem som ligger efter. Dessutom gör en ny ändring i systemets funktioner enligt principerna om "inbyggt integritetsskydd" det möjligt att med en enda knapptryckning acceptera ett svar och samtidigt avsluta ärendet. Tidigare har det krävts två olika steg för detta, vilket kan ha varit orsaken till en del av de vilande fall som har stannat kvar i systemet.

49. Europeiska datatillsynsmannen välkomnar dessa insatser på det praktiska planet. Han rekommenderar emellertid att det i själva förordningstexten ges garantier för att ärendena avslutas i rätt tid i IMI och att vilande ärenden (ärenden utan aktivitet på senare tid) tas bort ur databasen.

#### 2.5.3 Från avslutning av ärendet till 18 månader: är en förlängning av sexmånadersperioden befogad?

50. Europeiska datatillsynsmannen uppmanar parterna att på nytt överväga huruvida det är tillräckligt befogad att för-

länga den nuvarande sexmånadersperioden till 18 månader efter det att ärendet har avslutats och, om så är fallet, huruvida detta gäller bara för informationsutbyte mellan två parter eller också för andra typer av funktioner. IMI har nu funnits i flera år, och de praktiska erfarenheter som gjorts i detta avseende bör utnyttjas.

51. Om IMI fortsätter att vara ett verktyg för informationsutbyte (till skillnad från ett system för ärendehantering, en databas eller ett arkiveringssystem) och dessutom förutsatt att de behöriga myndigheterna ges verktyg för att från systemet hämta den information som de har tagit emot (antingen på elektronisk väg eller i pappersform, och åtminstone på ett sådant sätt att de kan använda den hämtade informationen som bevis<sup>(27)</sup>) tycks det inte finnas något större behov av att överhuvudtaget bevara uppgifterna i IMI efter det att ärendet har avslutats.

52. Vid utbyte av information mellan två parter kan det finnas behov av att ställa uppföljningsfrågor också efter det att ett svar har mottagits, och ett ärende således har avslutats, vilket kan motivera en (rimligt kort) lagringsperiod efter det att ärendet har avslutats. Den nuvarande sexmånadersperioden verkar vid första anblicken vara tillräckligt väl tilltagen för detta ändamål.

#### 2.5.4 Från 18 månader till fem år: "blockerade" uppgifter

53. Europeiska datatillsynsmannen anser att kommissionen inte heller har lämnat någon tillräcklig motivering till att det skulle vara nödvändigt och proportionerligt att lagra "blockerade uppgifter" i upp till fem år.

54. I motiveringen på sidan 8 hänvisas det till domstolens dom i målet *Rijkeboer*<sup>(28)</sup>. Europeiska datatillsynsmannen rekommenderar att kommissionen på nytt överväger hur detta ärende påverkar lagring av uppgifter i IMI. Han anser att domen i målet *Rijkeboer* inte medför att IMI måste konfigureras för att lagra uppgifter i fem år efter det att ärendet har avslutats.

55. Europeiska datatillsynsmannen anser inte att en hänvisning till domen i målet *Rijkeboer* eller till registrerades rätt att få tillgång till sina uppgifter är en tillräcklig och lämplig motivering för att lagra uppgifter i IMI i fem år efter det att ärendet har avslutats. Att lagra enbart "loggdata" (exakt definierade för att utesluta allt innehåll, bland annat bilagor och känsliga uppgifter) kan vara ett mindre inkräktande alternativ, vilket kanske förtjänar att övervägas ytterligare. På detta stadium är Europeiska datatillsynsmannen emellertid inte övertygad om att ens detta skulle vara vare sig nödvändigt eller proportionerligt.

<sup>(26)</sup> Se bilaga II, I.1.

<sup>(27)</sup> Vi förstår att insatser har gjorts för att säkerställa detta på det praktiska planet.

<sup>(28)</sup> C-553/07, *Rijkeboer* [2009], REG s. I-3889.

56. Dessutom är oklarheten om vem som ska få tillgång till de "blockerade uppgifterna" och för vilket syfte också problematisk. Att bara hänvisa till användning "när det gäller bevis på informationsutbyte" (som i artikel 13.3) är inte tillräckligt. Om man behåller bestämmelsen om "blockering" bör det i vart fall bättre anges vem som kan be om bevis på informationsutbyte och i vilket sammanhang. Skulle andra ha rätt att begära tillträde, förutom den registrerade personen? Om så var fallet, skulle det bara vara de behöriga myndigheterna, och bara för att bevisa att ett speciellt informationsutbyte med speciellt innehåll har ägt rum (om ett sådant utbyte har bestridits av de behöriga myndigheter som skickade eller tog emot meddelandet)? Förutses annan möjlig användning "för att bevisa att ett informationsutbyte har ägt rum" <sup>(29)</sup>?

### 2.5.5 Varningar

57. Europeiska datatillsynsmannen rekommenderar att det görs en tydligare åtskillnad mellan varningar och arkivering av information. Det är en sak att använda en varning som kommunikationsverktyg för att varna behöriga myndigheter om en speciell förseelse eller misstanke och en helt annan sak att lagra varningen i en databas under en lång eller till och med obestämd tid. Lagring av varningsinformation skulle leda till ytterligare betänkligheter och kräva särskilda regler och ytterligare skyddsåtgärder.

58. Europeiska datatillsynsmannen rekommenderar därför att det i förordningen föreskrivs som en generell regel i) att sex månaders lagring ska gälla för varningar om inget annat anges i vertikal lagstiftning och förutsatt att det finns andra tillräckliga skyddsmekanismer och, vilket är viktigt, ii) att denna period ska räknas från det att varningen skickas ut.

59. Som alternativ rekommenderar Europeiska datatillsynsmannen att detaljerade skyddsåtgärder anges speciellt i förslaget till förordning när det gäller varningar. Europeiska datatillsynsmannen är beredd att bistå kommissionen och lagstiftarna med ytterligare råd i detta avseende, om detta andra tillvägagångssätt tillämpas.

### 2.6 Specialkategorier av uppgifter (artikel 15)

60. Europeiska datatillsynsmannen välkomnar den åtskillnad som görs mellan sådana personuppgifter som anges i artikel 8.1 i direktiv 95/46/EG och sådana som nämns i artikel 8.5. Han välkomnar också att det i förordningen tydligt anges att hantering av specialkategorier av uppgifter endast ska tillåtas med hänvisning till ett särskilt skäl som anges i artikel 8 i direktiv 95/46/EG.

61. I detta hänseende förstår Europeiska datatillsynsmannen att IMI kommer att hantera en avsevärd mängd känsliga uppgifter som omfattas av artikel 8.2 i direktiv 95/46/EG. Från första början, när IMI först togs i bruk för att stödja

det administrativa samarbetet enligt tjänstedirektivet och direktivet om erkännande av yrkeskvalifikationer, utformades det faktiskt för att hantera sådana uppgifter, särskilt uppgifter i samband med protokoll över brott och administrativa förseelser som kan påverka en yrkesutövares eller tjänsteleverantörs rätt att utföra arbete/tjänster i en annan medlemsstat.

62. Dessutom ska förmodligen en avsevärd mängd känsliga uppgifter som omfattas av artikel 8.1 (huvudsakligen hälsorelaterade uppgifter) hanteras i IMI när IMI utvidgas till att innefatta en modul för Solvit <sup>(30)</sup>. Slutligen kan det inte uteslutas att ytterligare känsliga uppgifter i framtiden också kan samlas in genom IMI på *ad hoc*-basis eller systematiskt.

### 2.7 Säkerhet (artikel 16 och skäl 16)

63. Europeiska datatillsynsmannen välkomnar att det i artikel 16 särskilt anges att kommissionen är skyldig att följa sina egna interna bestämmelser som den har antagit enligt artikel 22 i förordning (EG) nr 45/2001 och att anta en säkerhetsplan för IMI och hålla denna uppdaterad.

64. För att ytterligare stärka dessa bestämmelser rekommenderar Europeiska datatillsynsmannen att förordningen ska kräva en riskbedömning och en översyn av säkerhetsplanen varje gång IMI ska utvidgas till ett nytt politikområde och innan en ny funktion som påverkar personuppgifter läggs till <sup>(31)</sup>.

65. Europeiska datatillsynsmannen har dessutom också konstaterat att endast kommissionens skyldigheter och Europeiska datatillsynsmannens roll som övervakare anges i artikel 16 och skäl 16. Detta kan vara missvisande. Det är visserligen sant att kommissionen är systemoperatör och som sådan har ansvar för en övervägande del av upprätthållandet av säkerheten i IMI, men de behöriga myndigheterna har också skyldigheter som i sin tur övervakas av nationella datatillsynsmyndigheter. I artikel 16 och skäl 16 bör därför också de skyldigheter beträffande säkerhet som gäller för resten av aktörerna inom IMI enligt direktiv 95/46/EG och för de nationella datatillsynsmyndigheternas tillsynsbefogenheter anges.

### 2.8 Information till de registrerade samt insyn (artikel 17)

#### 2.8.1 Information som lämnas i medlemsstater

66. Beträffande artikel 17.1 rekommenderar Europeiska datatillsynsmannen mer specifika bestämmelser i förordningen för att säkerställa att de registrerade ges fullständig information om sina uppgifter i IMI. Med tanke på att IMI används av många behöriga myndigheter, inbegripet många små lokala förvaltningar utan tillräckliga resurser, rekommenderas det eftertryckligen att lämnandet av meddelanden samordnas på nationell nivå.

<sup>(29)</sup> Även om lagring av personuppgifter innebär jämförelsevis små risker i fråga om den personliga integriteten anser Europeiska datatillsynsmannen ändå att lagring av IMI-användarnas personuppgifter i mer än fem år när de inte längre har tillträde till IMI inte har motiverats tillräckligt.

<sup>(30)</sup> Se bilaga II, I.1.

<sup>(31)</sup> Se även avsnitt 12 om rekommendationer beträffande granskningar.

### 2.8.2 Information som lämnas av kommissionen

67. Enligt artikel 17.2 a ska kommissionen lämna ett integritetsmeddelande beträffande sina egen behandling av uppgifter enligt artiklarna 10 och 11 i förordning (EG) nr 45/2001. Dessutom ska kommissionen enligt artikel 17.2 b också lämna information om "dataskyddsaspekterna i samband med förfaranden för administrativt samarbete i IMI, enligt artikel 12". Slutligen ska kommissionen enligt artikel 17.2 c lämna information om "undantag från eller begränsningar av de registrerades rättigheter, enligt artikel 19".
68. Europeiska datatillsynsmannen välkomnar dessa bestämmelser som bidrar till insyn i uppgiftsbehandlingen inom IMI. Såsom konstaterats i avsnitt 2.1 ovan har det avgörande betydelse att enhetlighet säkerställs i fråga om användningen av systemet, de skyddsåtgärder som tillämpas och den information som lämnas till de registrerade<sup>(32)</sup>.
69. Bestämmelserna i artikel 17.2 bör ändå stärkas ytterligare. Kommissionen i dess egenskap av systemoperatör har bäst förutsättningar för att inta en proaktiv hållning när en första "del" av meddelanden om skydd av personuppgifter och annan relevant information till de registrerade lämnas på dess flerspråkiga webbplats, också för behöriga myndigheters räkning, det vill säga sådan information som krävs enligt artiklarna 10 eller 11 i direktiv 95/46/EG. För meddelanden som lämnas av behöriga myndigheter i medlemsstater skulle det då ofta vara tillräckligt att helt enkelt hänvisa till det meddelande som kommissionen lämnat och bara göra nödvändiga kompletteringar, så att de följer eventuell ytterligare speciell information som krävs speciellt enligt nationell lagstiftning.
70. I artikel 17.2 b bör det också klargöras att information som lämnas av kommissionen ska omfatta alla politikområden, alla typer av förfaranden för administrativt samarbete och alla funktioner i IMI som helhet och också särskilt de kategorier av uppgifter som kan komma att behandlas. Dessutom bör de frågeserier som används vid samarbete mellan två parter också publiceras på IMI:s webbplats, vilket redan sker i praktiken.

### 2.9 Rätt till tillträde, korrigerig och radering (artikel 18)

71. Europeiska datatillsynsmannen vill åter hänvisa till att det, vilket konstaterats i avsnitt 2.1 ovan, har avgörande betydelse att enhetlighet säkerställs när det gäller driften av systemet och de skyddsåtgärder som tillämpas. Europeiska datatillsynsmannen skulle därför vilja se en ytterligare specificering av bestämmelserna om rätt till tillträde, korrigerig och radering.
72. I artikel 18 bör det anges vem de registrerade ska vända sig till för att begära tillträde. Detta bör vara tydligt när det gäller tillgång till uppgifter under olika tidsperioder:

- innan ärendet avslutas,
  - efter det att ärendet avslutats, men innan den 18 månader långa lagringstiden har löpt ut,
  - och slutligen under den tid då uppgifter är "blockerade".
73. Förordningen bör också kräva att de behöriga myndigheterna vid behov samarbetar när det gäller begäran om tillträde. Korrigerig och radering bör utföras "så snart som möjligt och senast inom 60 dagar" och inte "inom 60 dagar". En hänvisning bör också göras till möjligheten att bygga upp dataskyddsmoduler och utforma lösningar där registren utformas med "integritetsfrämjande teknik" och där myndigheterna samarbetar kring "den registrerades rätt att ta del av uppgifter", till exempel genom att ge dem direkt tillgång till uppgifterna när detta är tillämpligt och genomförbart.

### 2.10 Övervakning (artikel 20)

74. Under de senaste åren har modellen med "samordnad övervakning" utvecklats. Denna modell för övervakning som nu används i Eurodac och delar av tullinformations-systemet har också införts för informationssystemet för viseringar (VIS) och andra generationen av Schengens informationssystem (SIS II).
75. Modellen består av tre delar:
- Övervakning på nationell nivå säkerställs av nationella datatillsynsmyndigheter.
  - Övervakning på EU-nivå säkerställs av Europeiska datatillsynsmannen.
  - Samordningen tryggas genom regelbundna möten och andra samordnade aktiviteter som stöds av Europeiska datatillsynsmannen, vilken fungerar som sekretariat för samordningsmekanismen.
76. Modellen har visat sig vara framgångsrik och effektiv och bör i framtiden planeras för andra informationssystem.
77. Europeiska datatillsynsmannen välkomnar att det i artikel 20 i förslaget föreskrivs att de nationella datatillsynsmyndigheterna och Europeiska datatillsynsmannen ska samordna övervakningen enligt den modell som fastställs i VIS- och SIS II-förordningarna<sup>(33)</sup>.

<sup>(32)</sup> När detta tillvägagångssätt för att säkerställa enhetlighet tillämpas ska naturligtvis vederbörlig hänsyn tas till nationella skillnader när detta är nödvändigt och motiverat.

<sup>(33)</sup> Se Europaparlamentets och rådets förordning (EG) nr 1987/2006 av den 20 december 2006 om inrättande, drift och användning av andra generationen av Schengens informationssystem (SIS II) (EUT L 381, 28.12.2006, s. 4) Europaparlamentets och rådets förordning (EG) nr 767/2008 av den 9 juli 2008 om informationssystemet för viseringar (VIS) och utbytet mellan medlemsstaterna av uppgifter om viseringar för kortare vistelse (VIS-förordningen) (EUT L 218, 13.8.2008, s. 60).



78. Europeiska datatillsynsmannen skulle vilja stärka bestämmelserna om samordnad övervakning på vissa punkter och skulle därför förorda bestämmelser liknande dem som till exempel finns i samband med informationssystemet för viseringar (artiklarna 41–43 i VIS-förordningen), Schengen II (artiklarna 44–46 i SIS II-förordningen) och planeras för Eurodac<sup>(34)</sup>. Europeiska datatillsynsmannen rekommenderar i synnerhet

— att det i artikel 20.1 och 20.2 i förordningen görs en beskrivning och en tydligare definition av de nationella datatillsynsmyndigheternas och Europeiska datatillsynsmannens respektive övervakningsuppgifter<sup>(35)</sup>,

— att det i artikel 20.3 anges att de nationella datatillsynsmyndigheterna och Europeiska datatillsynsmannen inom ramen för sina befogenheter "ska samarbeta aktivt" och "trygga en samordnad övervakning av IMI" (och att man inte enbart hänvisar till samordnad övervakning utan att nämna aktivt samarbete)<sup>(36)</sup>, och

— att man mer i detalj anger vad som ska ingå i samarbetet, till exempel genom att föreskriva att de nationella datatillsynsmyndigheterna och Europeiska datatillsynsmannen, "inom ramen för sina respektive befogenheter, ska utbyta relevant information, bistå varandra vid granskningar och inspektioner, utreda svårigheter med tolkningen eller tillämpningen av IMI-förordningen, undersöka problem i samband med utövandet av oberoende tillsyn eller den registrerades rättigheter, utarbeta harmoniserade förslag till gemensamma lösningar på eventuella problem och främja medvetenheten om rättigheterna i fråga om uppgiftsskydd"<sup>(37)</sup>.

79. Europeiska datatillsynsmannen är ändå medveten om att de uppgifter som behandlas för närvarande är mindre omfattande och av en annan karaktär och att IMI utvecklas. Han medger därför att mer flexibilitet kan vara tillrädligt när det gäller mötes- och granskningsfrekvens. Europeiska datatillsynsmannen rekommenderar kort sagt att förordningen ska innehålla nödvändiga minimiregler för att trygga ett effektivt samarbete och inte skapa onödiga administrativa bördor.

80. I artikel 20.3 i förslaget föreskrivs inga regelbundna möten, utan bara att Europeiska datatillsynsmannen "vid behov [kan] kalla till ett möte med de nationella tillsynsmyndigheterna". Europeiska datatillsynsmannen välkomnar att de berörda parterna själva kan bestämma hur ofta och på vilket sätt mötena ska genomföras och om andra förfarandemässiga detaljer i fråga om samarbetet. Detta kan avtalas i de förfaranderegler som redan har nämnts i förslaget.

<sup>(34)</sup> Rådets förordning (EG) nr 2725/2000 av den 11 december 2000 om inrättande av Eurodac för jämförelse av fingeravtryck för en effektiv tillämpning av Dublinkonventionen (EGT L 316, 15.12.2000, s. 1), som håller på att revideras. I detta sammanhang planeras bestämmelser liknande dem i VIS- och SIS II-förordningarna.

<sup>(35)</sup> Se till exempel artiklarna 41 och 42 i VIS-förordningen.

<sup>(36)</sup> Se till exempel artikel 43.1 i VIS-förordningen.

<sup>(37)</sup> Se till exempel artikel 43.2 i VIS-förordningen.

81. Vad beträffar regelbundna granskningar kan det också vara mera effektivt att överlåta åt de samarbetande myndigheterna att i sina förfaranderegler bestämma när och hur ofta sådana granskningar ska genomföras. Detta kan vara beroende av ett antal faktorer och kanske också ändra sig med tiden. Europeiska datatillsynsmannen stöder därför kommissionens tillvägagångssätt, som tillåter mer flexibilitet också i detta avseende.

### 2.11 Nationell användning av IMI

82. Europeiska datatillsynsmannen välkomnar att förslaget tillhandahåller en tydlig rättslig grund för den nationella användningen av IMI och att sådan användning omfattas av flera villkor, samt att den nationella datatillsynsmyndigheten ska underrättas och att användningen måste följa den nationella lagstiftningen.

### 2.12 Informationsutbyte med tredjeländer (artikel 22)

83. Europeiska datatillsynsmannen välkomnar de krav som fastställs i artikel 22.1 för informationsutbyte och att artikel 22.3 säkerställer insyn i utvidgningen genom att en uppdaterad förteckning över de tredjeländer som använder IMI ska offentliggöras i *Europeiska unionens officiella tidning* (artikel 22.3).

84. Vidare rekommenderar Europeiska datatillsynsmannen att kommissionen kortar ner hänvisningen till undantagen enligt artikel 26 i direktiv 95/46/EG så att bara artikel 26.2 innefattas. Med andra ord: behöriga myndigheter eller andra externa aktörer i ett tredjeland utan tillräcklig skyddsnivå ska inte kunna få direkt tillträde till IMI såvida det inte stipuleras i lämpliga avtalsklausuler. Dessa klausuler bör förhandlas fram på EU-nivå.

85. Europeiska datatillsynsmannen vill betona att andra undantag som "överföringen är nödvändig eller följer av lag på grund av viktiga allmänna intressen, eller för att kunna fastställa, göra gällande eller försvara rättsliga anspråk" inte bör användas för att motivera överföring av uppgifter till tredjeländer genom direkt tillträde till IMI<sup>(38)</sup>.

### 2.13 Ansvarsskyldighet (artikel 26)

86. I linje med de förväntade förbättringarna av systemet för ansvarsskyldighet under översynen av EU:s ram för uppgiftsskydd<sup>(39)</sup> rekommenderar Europeiska datatillsynsmannen att det i förordningen fastställs en tydlig ram för tillräckliga interna kontrollmekanismer som säkerställer och styrker efterlevnaden av uppgiftsskyddet och som innehåller åtminstone de delar som anges nedan.

<sup>(38)</sup> Ett liknande tillvägagångssätt har tillämpats i artikel 22.2 för kommissionens som IMI-aktör.

<sup>(39)</sup> Se avsnitt 2.2.4 i yttrandet 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", KOM(2010) 609 slutlig. Se även avsnitt 7 i Europeiska datatillsynsmannens yttrande som avgavs den 14 januari 2011 om detta meddelande från kommissionen.

87. Europeiska datatillsynsmannen välkomnar i detta sammanhang kravet i artikel 26.2 i förordningen att kommissionen vart tredje år ska lämna en rapport till Europeiska datatillsynsmannen om aspekter som hör samman med skyddet av personuppgifter, inbegripet datasäkerhet. Det bör klargöras i förordningen att Europeiska datatillsynsmannen i sin tur ska överlämna kommissionens rapport till de nationella datatillsynsmyndigheterna inom ramen för den samordnade övervakning som anges i artikel 20. Det bör också klargöras att rapporten, med hänsyn till varje politikområde och varje funktion, bör ta upp hur de centrala principerna för uppgiftsskydd och uppgiftsskyddsproblem (till exempel information till de registrerade, tillträdesrättigheter och säkerhet) har hanterats i praktiken.

88. I förordningen bör dessutom klargöras att ramen för interna kontrollmekanismer också ska innefatta integritetsbedömningar (inbegripet analys av säkerhetsrisker), en uppgiftsskyddspolicy (inbegripet en säkerhetsplan) som antas på grundval av resultaten av dessa samt periodiskt återkommande översyn och granskning.

#### 2.14 Inbyggda säkerhetsmekanismer

89. Europeiska datatillsynsmannen välkomnar hänvisningen till denna princip i skäl 6 i förordningen<sup>(40)</sup>. Han rekommenderar att förordningen förutom denna hänvisning också inför speciella säkerhetsmekanismer såsom

- en uppgiftsskyddsmodul som gör det möjligt för de registrerade att utöva sina rättigheter på ett mer effektivt sätt<sup>(41)</sup>,
- tydlig åtskillnad av de olika politikområdena i IMI ("kinesiska murar")<sup>(42)</sup>,
- speciella tekniska lösningar som begränsar sökmöjligheterna i kataloger, varningsinformation med mera, för att säkerställa ändamålsbegränsning,
- speciella åtgärder för att säkerställa att ärenden utan aktivitet avslutas<sup>(43)</sup>,
- tillräckliga förfarandemässiga säkerhetsåtgärder i samband med framtida utveckling<sup>(44)</sup>.

### 3. SLUTSATSER

90. Europeiska datatillsynsmannens allmänna omdöme om IMI är positivt. Europeiska datatillsynsmannen stöder kommissionens syften med att inrätta ett elektroniskt system för informationsutbyte och reglera dess dataskyddsaspekter. Europeiska datatillsynsmannen välkomnar också att kommissionen föreslår ett horisontellt rättsinstrument för IMI i form av rådets och parlamentets förordning. Han

välkomnar att de viktigaste uppgiftsskyddsfrågorna för IMI i stor utsträckning belyses i förslaget.

91. Beträffande det rättsliga ramverk för IMI som ska inrättas genom den föreslagna förordningen vill Europeiska datatillsynsmannen rikta uppmärksamheten på två centrala utmaningar:

- Behovet av att säkerställa enhetlighet samtidigt som mångfalden respekteras.
- Behovet av att väga flexibilitet mot rättssäkerhet.

92. Funktioner i IMI som redan kan förutses bör klargöras och tas upp mer specifikt.

93. Lämpliga förfarandemässiga skyddsåtgärder bör tillämpas för att säkerställa att uppgiftsskyddet noga övervägs under den framtida utvecklingen av IMI. Här bör ingå en konsekvensbedömning och samråd med Europeiska datatillsynsmannen och nationella datatillsynsmyndigheter varje gång IMI:s tillämpningsområde ska utvidgas till ett nytt politikområde och/eller nya funktioner.

94. Externa aktörers tillträdesrättigheter och tillträdesrätt till varningar bör specificeras ytterligare.

95. När det gäller lagringstider

- bör det i förordningen ges garantier för att ärendena avslutas i IMI i rätt tid och att vilande ärenden (ärenden utan aktivitet på senare tid) tas bort ur databasen,
- bör det på nytt övervägas huruvida det är tillräckligt befogat att förlänga den nuvarande sexmånadersperioden till 18 månader efter det att ärendet har avslutats,
- har kommissionen inte lämnat någon tillräcklig motivering till att det skulle vara nödvändigt och proportionerligt att bevara "blockerade uppgifter" i upp till fem år, och detta förslag bör därför övervägas på nytt,
- bör det göras en tydligare åtskillnad mellan varningar och arkivering av information; förordningen bör det som en generell regel föreskrivas i) att sex månaders lagring ska gälla för varningar om inget annat anges i vertikal lagstiftning och förutsatt att det finns andra tillräckliga skyddsmekanismer och ii) att denna period ska räknas från det att varningen skickats ut.

96. Förordningen ska kräva en riskbedömning och en översyn av säkerhetsplanen varje gång IMI ska utvidgas till ett nytt politikområde och innan en ny funktion som påverkar personuppgifter läggs till.

97. Bestämmelserna om information till de registrerade och tillträdesrättigheter bör stärkas och främja ett mera enhetligt tillvägagångssätt.

<sup>(40)</sup> Se föregående fotnot.

<sup>(41)</sup> Se avsnitt 2.9 ovan.

<sup>(42)</sup> Se avsnitt 2.4 ovan.

<sup>(43)</sup> Se avsnitt 2.5.2 ovan.

<sup>(44)</sup> Se avsnitt 2.2.2 ovan.

98. Europeiska datatillsynsmannen skulle vilja stärka bestämmelserna om samordnad övervakning på vissa punkter och skulle därför förorda bestämmelser liknande dem som till exempel finns i samband med informationssystemet för viseringar och Schengen II och planeras för Eurodac. När det gäller mötes- och granskningsfrekvens stöder Europeiska datatillsynsmannen förslaget flexibla tillvägagångssätt för att säkerställa att förordningen tillhandahåller nödvändiga minimiregler för att trygga ett effektivt samarbete utan att skapa onödiga administrativa bördor.
99. Förordningen ska säkerställa att behöriga myndigheter eller andra externa aktörer i ett tredjeland utan tillräcklig skyddsnivå inte ska kunna få direkt tillträde till IMI såvida det inte stipuleras i lämpliga avtalsklausuler. Dessa klausuler bör förhandlas fram på EU-nivå.

100. Förordningen bör fastställa en tydlig ram för interna kontrollmekanismer som säkerställer och styrker efterlevnaden av uppgiftsskyddet, innefattande integritetsbedömningar (inbegripet analys av säkerhetsrisker), en uppgiftsskyddspolicy (inbegripet en säkerhetsplan) som antas på grundval av resultaten av dessa samt periodiskt återkommande översyn och granskning.
101. Särskilda säkerhetsmekanismer bör också införas genom förordningen.

Utfärdat i Bryssel den 22 november 2011.

Giovanni BUTTARELLI  
*Biträdande Europeisk datatillsynsman*

---