

UDTALELSER

DEN EUROPÆISKE TILSYNSFØRENDE FOR
DATABESKYTTELSE

Udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse om Kommissionens forslag til Europa-Parlamentets og Rådets forordning om administrativt samarbejde i informationssystemet for det indre marked (IMI-forordningen)

(2012/C 48/02)

DEN EUROPÆISKE TILSYNSFØRENDE FOR DATABESKYTTELSE HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 16,

under henvisning til Den Europæiske Unions charter om grundlæggende rettigheder, særlig artikel 7 og 8,

under henvisning til Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger ⁽¹⁾,

under henvisning til Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i fællesskabsinstitutionerne og -organerne og om fri udveksling af sådanne oplysninger ⁽²⁾,

under henvisning til anmodningen om en udtalelse i overensstemmelse med artikel 28 i forordning (EF) nr. 45/2001, —

VEDTAGET FØLGENDE UDTALELSE:

1. INDLEDNING

1.1. Høring af den tilsynsførende

1. Den 29. august 2011 vedtog Kommissionen et forslag til Europa-Parlamentets og Rådets forordning om administrativt samarbejde i informationssystemet for det indre marked (IMI-forordningen) (herefter benævnt »forslaget« eller »forslaget til forordning«) ⁽³⁾. Forslaget blev sendt til høring hos den tilsynsførende samme dag.
2. Den tilsynsførende fik allerede før vedtagelsen af forslaget mulighed for at fremsætte uformelle bemærkninger til

forslaget, og inden dette til Kommissionens meddelelse »Bedre styring af det indre marked gennem øget administrativt samarbejde: En strategi for at udbygge og udvikle informationssystemet for det indre marked (IMI)« (»meddelelsen om IMI-strategi«) ⁽⁴⁾, som blev fremsat forud for forslaget. Der er i forslaget taget hensyn til mange af disse bemærkninger, hvilket betyder, at garantierne til beskyttelse af personoplysninger er blevet styrket i forslaget.

3. Den tilsynsførende bifalder, at han formelt blev hørt af Kommissionen, samt at der er i præambelen til forslaget henvises til denne udtalelse.

1.2. Begrundelse og forslag

4. IMI er et informationsteknologiredskab, som giver de kompetente myndigheder mulighed for at udveksle oplysninger med hinanden, når de anvender lovgivningen om det indre marked. IMI giver de nationale, regionale og lokale myndigheder i EU-medlemsstaterne mulighed for hurtigt og nemt at kommunikere med deres modparter i andre europæiske lande. Dette omfatter også behandling af relevante personoplysninger, herunder følsomme oplysninger.
5. IMI er oprindeligt udformet som et kommunikationsværktøj for én til én-informationsudveksling under direktivet om erhvervmæssige kvalifikationer ⁽⁵⁾ og tjenesteydelsesdirektivet ⁽⁶⁾. IMI hjælper sine brugere med at finde den rette myndighed at kontakte i et andet land og kommunikere med dem ved hjælp af forud oversatte standardspørgsmål og -svar ⁽⁷⁾.

⁽⁴⁾ KOM(2011) 75.

⁽⁵⁾ Europa-Parlamentets og Rådets direktiv 2005/36/EF af 7. september 2005 om anerkendelse af erhvervmæssige kvalifikationer (EUT L 255 af 30.9.2005, s. 22).

⁽⁶⁾ Europa-Parlamentets og Rådets direktiv 2006/123/EF af 12. december 2006 om tjenesteydelser i det indre marked (EUT L 376 af 27.12.2006, s. 36).

⁽⁷⁾ Som eksempel kunne et typisk spørgsmål indeholdende følsomme oplysninger være: »Fremgår det af vedlagte dokument, at (den migrerende erhvervsudøver) ikke har fået suspenderet eller frataget retten til udøvelse af det relevante erhverv som følge af grov forsømmelse eller overtrædelse af straffeloven?»

⁽¹⁾ EFT L 281 af 23.11.1995, s. 31.

⁽²⁾ EFT L 8 af 12.1.2001, s. 1.

⁽³⁾ KOM(2011) 522 endelig.

6. IMI er imidlertid tænkt som et fleksibelt, horisontalt system, der kan understøtte flere forskellige områder af lovgivningen i det indre marked. IMI skal gradvist udvides til at omfatte yderligere politikområder.
7. Systemets funktioner forventes også at blive udvidet. Ud over én til én-udvekslinger mellem to medlemsstater er der ligeledes planlagt eller allerede gennemført andre funktioner, som f.eks. »notifikationsprocedurer, alarmmekanismer, ordninger om gensidig bistand og problemløsning«⁽⁸⁾, samt etablering af en »database for senere anvendelse af IMI-aktører«⁽⁹⁾. Mange, men ikke alle, af disse funktioner kan også omfatte behandling af personoplysninger.
8. Målet med forslaget er at skabe et klart retsgrundlag og en omfattende databeskyttelsesramme for IMI.

1.3. Baggrund for forslaget: en trinvis fremgangsmåde til etablering af en omfattende databeskyttelsesramme for IMI

9. I foråret 2007 anmodede Kommissionen om en udtalelse fra artikel 29-gruppen vedrørende databeskyttelse (herefter »artikel 29-gruppen«) med henblik på at vurdere IMI's betydning for databeskyttelsen. Artikel 29-gruppen afgav sin udtalelse den 20. september 2007⁽¹⁰⁾. Kommissionen blev i udtalelsen anbefalet at etablere et klarere retsgrundlag og fastsætte specifikke garantier til databeskyttelse i forbindelse med udveksling af data inden for rammerne af IMI. Den tilsynsførende deltog aktivt i undergruppens arbejde vedrørende IMI og støttede konklusionerne i udtalelsen fra artikel 29-gruppen.
10. Den tilsynsførende fortsatte efterfølgende med at vejlede Kommissionen om, hvordan der kan indføres en trinvis fremgangsmåde til etablering af en omfattende databeskyttelsesramme for IMI⁽¹¹⁾. Den tilsynsførende har i forbindelse med dette samarbejde og efter afgivelsen af sin udtalelse af 22. februar 2008 om gennemførelsen af IMI⁽¹²⁾ gjort opmærksom på behovet for en ny retsakt under den almindelige lovgivningsprocedure, som vil gøre det muligt at etablere en mere omfattende databeskyttelsesramme for IMI og skabe retssikkerhed. Der er nu fremsat forslag om en sådan retsakt⁽¹³⁾.

⁽⁸⁾ Se betragtning 10.

⁽⁹⁾ Se artikel 13, stk. 2.

⁽¹⁰⁾ Artikel 29-arbejdsgruppen vedrørende databeskyttelse, udtalelse nr. 7/2007 om databeskyttelsesspørgsmål i forbindelse med Informationssystemet for det indre marked (IMI), WP140. Findes på http://ec.europa.eu/justice/policies/privacy/docs/wpdocs2007/wp140_da.pdf

⁽¹¹⁾ De væsentligste dokumenter vedrørende dette samarbejde kan ses på Kommissionens websted om IMI på http://ec.europa.eu/internal_market/imi-net/data_protection_da.html samt på den tilsynsførendes websted <http://www.edps.europa.eu>

⁽¹²⁾ Udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse (EDPS) om Kommissionens beslutning 2008/49/EF af 12. december 2007 om gennemførelse af informationssystemet for det indre marked (IMI) hvad angår beskyttelse af personoplysninger (EUT C 270 af 25.10.2008, s. 1).

⁽¹³⁾ Artikel 29-gruppen agter også at fremsætte bemærkninger til forslaget. Den tilsynsførende har fulgt dette arbejde i den relevante undergruppe og har bidraget med bemærkninger.

2. ANALYSE AF FORSLAGET

2.1. Den tilsynsførendes generelle holdning til forslaget og til de største udfordringer i forbindelse med retsgrundlaget for IMI

11. Den tilsynsførende stiller sig generelt positivt til IMI. Den tilsynsførende støtter de mål, Kommissionen søger at nå med indførelsen af et elektronisk informationsudvekslingssystem og med regler for dets databeskyttelsesaspekter. Et sådant strømnet system vil ikke blot kunne gøre samarbejdet mere effektivt, men også hjælpe med til at sikre, at de gældende databeskyttelseslove overholdes. Dette kan ske ved hjælp af en klar ramme for, hvilke oplysninger der kan udveksles, med hvem og under hvilke betingelser.
12. Den tilsynsførende bifalder endvidere Kommissionens forslag om en horisontal retsakt for IMI i form af en forordning fra Rådet og Europa-Parlamentet. Han glæder sig over, at forslaget har omfattende fokus på de mest relevante databeskyttelsesspørgsmål i forbindelse med IMI. Hans bemærkninger skal læses på denne positive baggrund.
13. Den tilsynsførende advarer ikke desto mindre om, at indførelsen af et centralt elektronisk system også frembyder visse risici. De vigtigste risici er, at flere oplysninger vil kunne videregives og mere bredt end strengt nødvendigt for et effektivt samarbejde, og at oplysninger, herunder potentielt forældede og ukorrekte oplysninger, eventuelt opbevares i det elektroniske system længere end nødvendigt. Sikkerheden af en database, der er tilgængelig i 27 medlemsstater, er også et følsomt spørgsmål, da systemet kun er så sikkert som det svageste led i kæden.

De største udfordringer

14. Hvad angår det retsgrundlag for IMI, som fremsættes i forslaget til forordning, gør Den tilsynsførende opmærksom på to store udfordringer:

— behovet for at sikre en ensartet anvendelse, samtidig med at forskelligheden respekteres, og

— behovet for at skabe balance mellem fleksibilitet og retssikkerhed.

15. Disse store udfordringer er vigtige referencepunkter, som i vid udstrækning ligger til grund for den fremgangsmåde, som den tilsynsførende anbefaler i denne udtalelse.

Ensartet anvendelse med respekt for forskelligheden

16. IMI-systemet anvendes i 27 medlemsstater. Den nuværende grad af harmonisering af den europæiske lovgivning har først og fremmest skabt store forskelle mellem de nationale administrative procedurer og de nationale databeskyttelseslovgivninger. IMI skal udformes således, at

brugere i alle disse 27 medlemsstater kan overholde deres nationale lovgivning, herunder de nationale databeskyttelseslovgivninger, når de udveksler personoplysninger via IMI. Samtidig skal de registrerede have vished for, at deres oplysninger er omfattet af en ensartet beskyttelse, også selv om de overføres via IMI til en anden medlemsstat. Denne ensartede beskyttelse med respekt for forskellighederne er en stor udfordring i forbindelse med etableringen af både IMI's tekniske og retlige infrastruktur. Unødvendige komplikationer og opsplitting bør undgås. Behandlingen af oplysninger i IMI skal være gennemsigtig, og det skal klart fastlægges, hvem der har ansvar for at træffe beslutninger vedrørende systemets udformning, dets daglige vedligeholdelse og anvendelse samt tilsynet med systemet.

Balance mellem fleksibilitet og retssikkerhed

17. For det andet er IMI, i modsætning til andre store it-systemer såsom Schengen-informationssystemet, visainformationssystemet, toldinformationssystemet eller Eurodac, som alle har fokus på samarbejde inden for specifikke, klart definerede områder, et horisontalt værktøj til udveksling af oplysninger, og kan anvendes til at fremme informationsudvekslingen inden for mange forskellige politikområder. Det forventes også, at IMI's anvendelsesområde gradvist vil blive udvidet til at omfatte yderligere politikområder, og at dets funktioner kan blive ændret, så det kommer til at omfatte hidtil uspecificerede former for administrativt samarbejde. Disse særlige kendetegn for IMI gør det vanskeligere at fastlægge klart definerede funktioner for systemet og for de dataudvekslinger, som det kan anvendes til. Det stiller dermed også større udfordringer med hensyn til at definere de relevante databeskyttelsesgarantier.
18. Den tilsynsførende erkender, at der er behov for fleksibilitet og noterer sig Kommissionens ønske om at »fremtidssikre« forordningen. Dette bør imidlertid ikke medføre uklarhed eller retsikkerhed i forbindelse med systemets funktioner og de databeskyttelsesgarantier, der skal gennemføres. Forslaget bør derfor gøres mere specifikt og ikke blot nøjes med at genfremsætte de vigtigste bestemmelser vedrørende beskyttelse af personoplysninger, som er fastsat i direktiv 95/46/EF og forordning (EF) nr. 45/2001⁽¹⁴⁾.

2.2. IMI-systemets anvendelsesområde og den forventede udvidelse af anvendelsesområdet (artikel 3 og 4)

2.2.1. Indledning

19. Den tilsynsførende bifalder forslaget tydelige definition af IMI's nuværende anvendelsesområde samt listen i bilag I over de relevante EU-retsakter, som udgør retsgrundlaget for udvekslingen af oplysninger. Dette omfatter samarbejde under de specifikke bestemmelser i direktivet om anerkendelse af erhvervsmæssige kvalifikationer, tjene-

stedelsesdirektivet og direktivet om patientrettigheder i forbindelse med grænseoverskridende sundhedsydelse⁽¹⁵⁾.

20. Da anvendelsesområdet for IMI forventes at blive udvidet, er de potentielle områder, som systemet kan udvides til, opført i bilag II. Punkter fra bilag II kan flyttes til bilag I ved hjælp af en delegeret retsakt, som skal vedtages af Kommissionen, når der er foretaget en konsekvensanalyse⁽¹⁶⁾.
21. Den tilsynsførende hilser denne teknik velkommen, da den i) klart afgrænser IMI's anvendelsesområde) og ii) sikrer gennemsigtighed, samtidig med at den iii) er fleksibel for det tilfælde, at IMI skal bruges til yderligere informationsudvekslinger i fremtiden. Den sikrer også, at der ikke kan finde nogen informationsudveksling sted via IMI, i) uden at der findes et passende retsgrundlag i specifik lovgivning om det indre marked, der tillader eller bemyndiger til informationsudveksling⁽¹⁷⁾, og ii) uden at der henvises til dette retsgrundlag i bilag I til forordningen.
22. Der hersker dog fortsat en vis usikkerhed med hensyn til IMI's anvendelsesområde, for så vidt angår de politikområder, som IMI kan udvides til at omfatte, samt de funktioner, som eventuelt vil blive tilføjet til IMI.
23. Det kan for det første ikke udelukkes, at IMI's anvendelsesområde vil blive udvidet til at omfatte andre områder end de politikområder, der er opført i bilag I og II. Det vil kunne ske, hvis anvendelsen af IMI i forbindelse med visse former for informationsudvekslinger ikke fastsættes i en delegeret retsakt fra Kommissionen, men i en retsakt, som vedtages af Europa-Parlamentet og Rådet for et område, der ikke er taget højde for i bilag II⁽¹⁸⁾.

⁽¹⁵⁾ Europa-Parlamentets og Rådets direktiv 2011/24/EU af 9. marts 2011 om patientrettigheder i forbindelse med grænseoverskridende sundhedsydelse (EUT L 88 af 4.4.2011, s. 45).

⁽¹⁶⁾ Forslaget til forordning indeholder ingen henvisning til en konsekvensanalyse. På side 7 i begrundelsen til forslaget, anføres det imidlertid, at Kommissionen vil få beføjelse til at flytte punkter fra bilag II til bilag I ved at vedtage en delegeret retsakt og »efter en vurdering af systemets tekniske gennemførlighed, omkostnings-effektivitet, brugervenlighed og overordnede virkning samt af resultaterne af en eventuel testfase«.

⁽¹⁷⁾ Undtaget herfra er SOLVIT (se bilag II, punkt I, stk. 1), ifølge hvilken der kun kan anvendes »blød« lovgivning i form af en henstilling fra Kommissionen. Hvad angår databeskyttelse, mener den tilsynsførende, at retsgrundlaget for behandling af personoplysninger i forbindelse med SOLVIT kan være de registreredes »samtykke«.

⁽¹⁸⁾ Dette kan eventuelt ske på Kommissionens initiativ, men det kan ikke udelukkes, at Europa-Parlamentet og Rådet på et senere tidspunkt i lovgivningsprocessen fremsætter forslag om at anvende IMI inden for et specifikt politikområde. Det er allerede sket tidligere vedrørende direktivet om patientrettigheder i forbindelse med grænseoverskridende sundhedsydelse. I et sådant tilfælde er der brug for større klarhed omkring udvidelsesproceduren, som ser ud til udelukkende at have haft fokus på udvidelse ved hjælp af delegerede retsakter (jf. bestemmelserne om konsekvensanalyse, delegerede retsakter, ajourføring af bilag I).

⁽¹⁴⁾ I den forbindelse henvises desuden til vores bemærkninger i afsnit 2.2. vedrørende den planlagte udvidelse af IMI's anvendelsesområde IMI.

24. Mens udvidelsen af anvendelsesområdet til at omfatte nye politikområder i visse tilfælde kun vil kræve få eller ingen ændringer af systemets nuværende funktioner⁽¹⁹⁾, kan andre udvidelser for det andet kræve nye og forskellige funktioner eller væsentlige ændringer af de nuværende funktioner:

- Selvom forslaget henviser til adskillige eksisterende eller planlagte funktioner, er disse henvisninger ikke tilstrækkeligt klare eller tilstrækkeligt detaljerede. Dette gælder, i varierende omfang, for henvisninger til alarmmekanismer, eksterne aktører, databaser, ordninger om gensidig bistand samt problemløsning⁽²⁰⁾. Som eksempel herpå er ordet »alarmmekanismer«, som henviser til en væsentlig eksisterende funktion, kun nævnt en enkelt gang, nemlig i betragtning (10)
- Det er i henhold til den foreslåede forordning muligt at vedtage to nye funktioner, som ikke er nævnt i forordningen
- IMI er hidtil blevet beskrevet som et værktøj til udveksling af oplysninger. Denne ordlyd er taget fra artikel 3, stk. 1, i Kommissionens forslag. Nogle af de funktioner, der henvises til i forslaget, herunder funktionen som »database«, forekommer imidlertid at række ud over denne rene udvekslingsfunktion. Den foreslåede udvidelse af dataforvaringsperioden til fem år peger også i retning af en funktion som »database«. Denne udvikling vil medføre en grundlæggende ændring af IMI⁽²¹⁾.

2.2.2. Henstillinger

25. For at afhjælpe disse usikkerheder henstiller den tilsynsførende til, at der anvendes en tostrengt fremgangsmåde. Han foreslår for det første, at de funktioner, som allerede er planlagt, bør præciseres yderligere og beskrives mere specifikt, samt for det andet, at der bør anvendes passende retssikkerhedsgarantier for at sikre, at der også tages de fornødne hensyn til databeskyttelse i forbindelse med den videre udvikling af IMI.

Præcisering af funktioner, som allerede er tilgængelige, eller som forventes indført (f.eks. én til én-udvekslinger, alarmmekanismer, problemløsning og eksterne aktører)

26. Den tilsynsførende henstiller til, at forordningen gøres mere specifik med hensyn til allerede kendte funktioner, som f.eks. de informationsudvekslinger, der er anført i bilag I og II.

⁽¹⁹⁾ Én til én-informationsudvekslinger under direktivet om erhvervs-mæssige kvalifikationer og direktivet om patientrettigheder i forbindelse med grænseoverskridende sundhedsydelse har f.eks. i det væsentlige samme struktur og kan tilpasses ved anvendelse af de samme funktioner under ensartede databeskyttelsesgarantier.

⁽²⁰⁾ Se betragtning 2), 10), 12), 13) og 15) samt artikel 5, litra b), artikel 5, litra i), artikel 10, stk. 7, og artikel 13, stk. 2).

⁽²¹⁾ Såfremt man ønsker, at IMI skal erstatte/supplere de eksisterende systemer til dokumenthåndtering og -arkivering og/eller at anvende IMI som en database, bør dette præciseres i artikel 3.

27. Der kan f.eks. fastlægges mere specifikke og tydelige foranstaltninger vedrørende integrationen af SOLVIT⁽²²⁾ i IMI (bestemmelser vedrørende »eksterne aktører« og »problemløsning«) samt for registre over fagfolk og tjenesteudbydere (bestemmelser vedrørende »databaser«).

28. Der bør også foretages yderligere præciseringer med hensyn til »alarmmekanismer«, som allerede anvendes under tjenesteydelsesdirektivet, og som eventuelt også vil blive indført i forbindelse med yderligere politikområder. »Alarmmekanismer« bør navnlig defineres tydeligt i artikel 5 (sammen med en række andre funktioner, som f.eks. én til én-informationsudvekslinger og databaser). Retten til indsigt i oplysninger og dataforvaringsperioder bør også præciseres⁽²³⁾.

Retssikkerhedsgarantier (konsekvensanalyse af databeskyttelse og høring af databeskyttelsesmyndigheder)

29. Hvis hensigten er at »fremtidssikre« forordningen med hensyn til nye funktioner, som det kan blive nødvendigt at indføre på længere sigt, og dermed tillade indførelsen af yderligere funktioner, som endnu ikke er defineret i forordningen, bør dette følges op af passende retssikkerhedsgarantier for at sikre vedtagelse af passende bestemmelser med henblik på at gennemføre de nødvendige databeskyttelsesgarantier, inden en ny funktion indføres. Det samme bør gøre sig gældende for udvidelse til nye politikområder, når en sådan udvidelse har betydning for databeskyttelsen.

30. Den tilsynsførende henstiller til, at der indføres en tydelig mekanisme, som kan sikre en grundig evaluering af databeskyttelsesaspekterne, inden der foretages udvidelser af de enkelte funktioner eller til nye politikområder, samt til at der om nødvendigt indføres yderligere garantier eller tekniske foranstaltninger i IMI's struktur. Det drejer sig navnlig om følgende:

- Den konsekvensanalyse, som der henvises til på side 7 i begrundelsen, bør også være et specifikt krav i selve forordningen og omfatte en konsekvensanalyse af databeskyttelsen, hvori det bør anføres, hvilke — om nogle — ændringer af systemets udformning, der er nødvendige for at sikre, at det fortsat indeholder passende databeskyttelsesgarantier, som også dækker nye politikområder og/eller funktioner.

- Forordningen bør især indeholde en bestemmelse om, at den tilsynsførende og databeskyttelsesmyndighederne skal høres forud for enhver udvidelse af IMI's anvendelsesområde. Denne høring kan gennemføres ved hjælp af den mekanisme, der er fastsat i artikel 20 for koordineret tilsyn.

⁽²²⁾ Se bilag II, punkt I, stk.1).

⁽²³⁾ Se afsnit 2.4. og 2.5.5. nedenfor.

31. Disse retssikkerhedsgarantier (konsekvensanalyse af databeskyttelsen og høring) bør være gældende for udvidelser via en retsakt fra Kommissionen (hvor et punkt flyttes fra bilag II til bilag I) og via en forordning fra Europa-Parlamentet og Rådet, inklusive et punkt, som ikke er opført i bilag II.
32. Endelig henstiller den tilsynsførende til, at det i forordningen præciseres, hvorvidt anvendelsesområdet for de delegerede retsakter, som Kommissionen i henhold til artikel 23 vil få beføjelse til at vedtage, også omfatter andre aspekter end at flytte punkter fra bilag II til bilag I. Hvis det er muligt, bør forordningen give Kommissionen beføjelse til at vedtage specifikke gennemførelsesbestemmelser eller delegerede retsakter med henblik på at definere enhver ny funktion i systemet eller behandle eventuelle fremtidige problemer vedrørende databeskyttelse.

2.3. Roller, kompetencer og ansvarsområder (artikel 7-9)

33. Den tilsynsførende glæder sig over, at der er afsat et helt kapitel (kapitel II) til at præcisere de forskellige aktørers funktioner og ansvarsområder. Disse bestemmelser kan dog styrkes yderligere, som det vil fremgå af det nedenstående.
34. I artikel 9 beskrives Kommissionens ansvarsområder i forbindelse med dens rolle som registeransvarlig. Den tilsynsførende henstiller endvidere til, at der tilføjes en ny bestemmelse vedrørende Kommissionens rolle i forbindelse med at sikre, at systemet udformes under hensyntagen til princippet om »indbygget databeskyttelse« samt dens koordinerende rolle, hvad angår spørgsmål om databeskyttelse.
35. Den tilsynsførende bifalder, at IMI-koordinatorernes opgaver, som er anført i artikel 7, nu også omfatter koordinerende opgaver i forbindelse med databeskyttelse, herunder at optræde som kontaktperson for Kommissionen. Han henstiller til, at det endvidere præciseres, at disse koordinerende opgaver også omfatter kontakt til de nationale databeskyttelsesmyndigheder.

2.4. Adgangsrettigheder (artikel 10)

36. Artikel 10 indeholder garantier vedrørende adgangsrettigheder. Den tilsynsførende er tilfreds med, at disse bestemmelser er blevet betydeligt styrket, efter at han fremsatte sine bemærkninger.
37. I betragtning af IMI's horisontale karakter og udvidelsespotentialer er det vigtigt at sikre, at systemet garanterer anvendelse af informationsbarrierer (»kinesiske mure«), som sikrer, at oplysninger, der behandles inden for et bestemt politikområde, holdes inden for dette politikområde. IMI-brugere bør i) kun få adgang til oplysninger ud fra »need-to-know«-princippet og ii) kun inden for et enkelt politikområde.

38. Hvis det ikke kan undgås, at en IMI-bruger har ret til at få indsigt i oplysninger om flere politikområder (hvilket f.eks. kan være tilfældet i visse lokale regeringskontorer), bør systemet som minimum ikke give mulighed for at kombinere oplysninger om forskellige politikområder. Hvis det er nødvendigt at gøre undtagelser, bør disse anføres i gennemførelseslovgivningen eller i en EU-retsakt, under streng overholdelse af princippet om formålsbegrænsning.
39. Disse principper er nu knæsat i forordningsteksten, men kan styrkes yderligere og operationaliseres.
40. Hvad angår Kommissionens adgangsrettigheder, bifalder den tilsynsførende, at det i artikel 9, stk. 2 og 4 og artikel 10, stk. 6, i forslaget, anføres, at Kommissionen ikke har adgang til personoplysninger, som udveksles mellem medlemsstaterne, undtagen i tilfælde hvor Kommissionen er udpeget til at deltage i en administrativ samarbejdsprocedure.
41. Også eksterne aktørers adgangsrettigheder og adgangsrettigheder til alarmmekanismer bør anføres nærmere⁽²⁴⁾. Hvad angår alarmmekanismer, henstiller den tilsynsførende til, at det i forordningen bør anføres, at advarsler ikke pr. automatik bør sendes til alle relevante kompetente myndigheder i alle medlemsstater, men kun til de myndigheder, der er berørt, ud fra »need-to-know«-princippet. Dette udelukker ikke, at der i særlige tilfælde eller inden for særlige politikområder kan sendes advarsler til alle medlemsstater, hvis de alle er berørte. Det er endvidere nødvendigt, at spørgsmålet om, hvorvidt Kommissionen bør have adgang til advarsler, vurderes fra sag til sag.

2.5. Forvaring af personoplysninger (artikel 13 og 14)

2.5.1. Indledning

42. I forslagets artikel 13 forlænges datalagringsperioden i IMI fra de nuværende seks måneder (at regne fra sagens afslutning) til fem år, og oplysningerne »blokeres« efter 18 måneder. Under denne »blokering« er der kun adgang til at søge i oplysningerne efter en specifik procedure, som kun kan indledes på anmodning fra den registrerede, eller hvis oplysningerne er nødvendige »som dokumentation for en informationsudveksling via IMI«.
43. Det betyder således, at oplysninger opbevares i IMI i tre forskellige perioder:
- fra oplysningerne uploades, til sagen afsluttes
 - i en periode på 18 måneder fra sagens afslutning⁽²⁵⁾
 - fra afslutningen af blokeringsperioden i 18 måneder i en periode på yderligere tre år og seks måneder (dvs. indtil sagens afslutning efter fem år).

⁽²⁴⁾ Se også afsnit 2.2.2.

⁽²⁵⁾ Det anføres i artikel 13, stk. 1, at 18 måneder er en »maksimal« tidsfrist, hvilket betyder, at der også kan fastsættes en kortere periode. Dette vil dog ikke påvirke den samlede forvaringsperiode, som under alle omstændigheder er fem år, dvs. indtil sagens afslutning.

44. Ud over disse generelle bestemmelser gives der i artikel 13, stk. 2, mulighed for at forvare oplysninger i en »database«, så længe det er nødvendigt til dette formål, med den registreredes samtykke eller »hvis det foreskrives i en EU-retsakt«. I forslaget artikel 14 anføres en tilsvarende blokeringsmekanisme for opbevaringen af IMI-brugeres personoplysninger for en periode på fem år, efter de er ophørt med at være IMI-brugere.

45. Der er ikke andre specifikke bestemmelser. De generelle bestemmelser må derfor antages ikke blot at skulle gælde for én til én-udvekslinger, men også for advarsler, problemløsning (som i SOLVIT⁽²⁶⁾) og for alle andre funktioner, som anvendes til behandling af personoplysninger.

46. Den tilsynsførende har i lyset af artikel 6, stk. 1, litra d), i direktiv 95/46/EF og artikel 14, stk. 1, litra e), i forordning (EF) nr. 45/2001, flere betænkeligheder vedrørende forvaringsperioderne, som begge indeholder krav om, at personoplysninger ikke må opbevares længere, end det er nødvendigt til det formål, som de er indsamlet til, eller hvis de skal behandles yderligere.

2.5.2. Fra uploading til sagens afslutning: behovet for at afslutte sagen rettidigt

47. Hvad angår den første periode, fra oplysningerne uploades, til sagen afsluttes, er den tilsynsførende bekymret over risikoen for, at visse sager aldrig vil blive afsluttet, eller først afsluttes efter en uforholdsmæssig lang periode. Dette kan betyde, at visse personoplysninger forbliver i databasen længere, end det er nødvendigt, eller på ubestemt tid.

48. Den tilsynsførende anerkender, at Kommissionen på det praktiske plan har gjort fremskridt med hensyn til at reducere ulemperne ved IMI, og der er indført et system for én til én-udvekslinger til at føre tilsyn med, at sager afsluttes rettidigt, og til periodisk at sende påmindelser, når sager ikke afsluttes til tiden. Derudover giver en ny ændring af systemets funktioner, som bygger på princippet om »indbygget databeskyttelse«, mulighed for med et enkelt tryk på en knap at acceptere et svar og samtidig afslutte sagen. Dette har tidligere skullet gøres via to forskellige trin, hvilket måske har været årsag til, at nogle sager er blevet hængende i systemet.

49. Den tilsynsførende bifalder disse praktiske bestræbelser. Han henstiller dog til, at der i forordningen bør indføres garantier for, at sager vil blive afsluttet rettidigt i IMI, og at »sovende« sager (sager, hvor der igennem længere tid ikke har været aktivitet) vil blive slettet fra databasen.

2.5.3. Fra sagens afslutning til 18 måneder: er forlængelsen af seks-måneders-perioden begrundet?

50. Den tilsynsførende opfordrer til, at det nok engang overvejes, om der er en passende begrundelse for at forlænge den nuværende seksmåneders periode til 18 måneder efter sagens afslutning, og om denne begrundelse i givet fald kun er gældende for én til én-udvekslinger, eller om den også gælder andre former for funktioner. IMI har nu været i brug i en del år, og de erfaringer, der er gjort i årenes løb, bør udnyttes.

51. Hvis IMI fortsat skal fungere som et værktøj til informationsudveksling (i modsætning til et filhåndterings-system, en database eller et arkiveringssystem), samt forudsat, at de kompetente myndigheder har mulighed for at indhente de oplysninger, de har modtaget, i systemet (enten elektronisk eller i papirform, men under alle omstændigheder således, at de kan anvende de indhentede oplysninger som dokumentation⁽²⁷⁾), er der ikke umiddelbart behov for at opbevare oplysningerne i IMI, efter at sagen er afsluttet.

52. Ved én til én-udvekslinger af oplysninger kan det eventuelle behov for at stille opfølgende spørgsmål, efter at et svar er blevet accepteret, og sagen dermed er afsluttet, eventuelt begrunde en (forholdsvis kort) forvaringsperiode efter sagens afslutning. Den nuværende seksmåneders periode synes umiddelbart at være lang nok til dette formål.

2.5.4. Fra 18 måneder til fem år: »blokerede« oplysninger

53. Den tilsynsførende mener heller ikke, at Kommissionen i tilstrækkelig grad har begrundet behovet for og rimeligheden af at opbevare »blokerede oplysninger« i op til fem år.

54. Der henvises i begrundelsen på side 8 til Domstolens dom i sagen *Rijkeboer*⁽²⁸⁾. Den tilsynsførende henstiller til, at Kommissionen overvejer denne sags betydning for dataforvaring i IMI. Den tilsynsførende mener ikke, at *Rijkeboer*-dommen stiller krav om, at IMI skal konfigureres til at forvare oplysninger i op til fem år efter sagens afslutning.

55. Det er ikke den tilsynsførendes opfattelse, at en henvisning til *Rijkeboer*-dommen eller til den registreredes ret til indsigt i deres oplysninger er en tilstrækkelig og passende begrundelse for at forvare oplysninger i IMI i fem år efter sagens afslutning. Forvaring af rene »journaldata« (strengt begrænset til at udelukke f.eks. vedlagte dokumenter eller følsomme oplysninger) kunne være en mindre radikal løsning, som kunne overvejes nærmere. Den tilsynsførende er imidlertid ikke overbevist om, at dette på nuværende tidspunkt vil være hverken nødvendigt eller rimeligt.

⁽²⁶⁾ Se bilag II, punkt I, stk.1.

⁽²⁷⁾ Vi er klar over, at der på det praktiske plan er gjort bestræbelser på at sikre dette.

⁽²⁸⁾ C-553/07 *Rijkeboer*, Sml. 2009 I, s. 3889.

56. Det er endvidere problematisk, at det ikke tydeligt er defineret, hvem der har adgang til de »blokerede oplysninger« og til hvilke formål. Det er ikke tilstrækkeligt blot at henvise til anvendelse som »dokumentation for en informationsudveksling« (som i artikel 3, stk. 3). Hvis bestemmelsen vedrørende »blokering« bevares, bør det under alle omstændigheder præciseres nærmere, hvem der kan bede om at se dokumentation for en informationsudveksling og i hvilken sammenhæng. Har andre end den registrerede ret til indsigt i oplysningerne? Hvis ja, er det så udelukkende de kompetente myndigheder og kun med det formål at dokumentere eksistensen af en bestemt informationsudveksling med en privatperson (i tilfælde af at denne udveksling anfægtes af de kompetente myndigheder, som sendte eller modtog beskeden)? Er der taget højde for andre anvendelser end at »tjene som dokumentation for informationsudveksling«⁽²⁹⁾?

2.5.5. Advarsler/Alarmmekanismer

57. Den tilsynsførende henstiller til, at der foretages en tydeligere sondring mellem alarmmekanismer og databaser. Der er stor forskel på at anvende en alarmmekanisme som et kommunikationsværktøj til at advare kompetente myndigheder om en særlig overtrædelse eller mistanke og på at opbevare denne advarsel i en database i en forlænget eller endog ubegrænset periode. Opbevaring af oplysninger om en advarsel er betænkelig og kræver særlige regler og flere databeskyttelsesgarantier.

58. Den tilsynsførende henstiller derfor til, at forordningen som standard bør anføre i) en seks måneders forvaringsperiode for advarsler, medmindre der er angivet andet i den vertikale lovgivning, og forudsat at der er indført tilstrækkelige supplerende garantier, samt ii) at denne periode bør gælde fra det tidspunkt, hvor advarslen sendes.

59. Alternativt henstiller den tilsynsførende til, at der i forslaget til forordning fastsættes specifikke og detaljerede foranstaltninger vedrørende advarsler. Hvis denne alternative fremgangsmåde vælges, er den tilsynsførende klar til at bistå Kommissionen og lovgiverne med yderligere rådgivning.

2.6. Særlige kategorier af oplysninger (artikel 15)

60. Den tilsynsførende bifalder, at der skelnes mellem personoplysninger i den i artikel 8, stk. 1, i direktiv 95/46/EF anførte betydning og personoplysninger som defineret i samme direktivs artikel 8, stk. 5. Han bifalder endvidere, at det i forordningen tydeligt anføres, at behandlingen af særlige kategorier af oplysninger kun er tilladt på et særligt grundlag som omhandlet i artikel 8 i direktiv 95/46/EF.

61. Den tilsynsførende er i den forbindelse af den opfattelse, at IMI vil behandle et stort antal følsomme oplysninger, som henhører under artikel 8, stk. 2, i direktiv 95/46/EF.

IMI var fra starten, hvor det blev lanceret for at støtte det administrative samarbejde under tjenesteydelsesdirektivet og direktivet om erhvervs-mæssige kvalifikationer, udformet til at behandle følsomme oplysninger, navnlig oplysninger vedrørende registrering af kriminelle og administrative overtrædelser, som kan påvirke en erhvervsdrivendes eller tjenesteyders ret til at udøve sit erhverv/udbyde sin tjeneste i en anden medlemsstat.

62. Derudover vil der med stor sandsynlighed også blive behandlet et stort antal følsomme oplysninger under artikel 8, stk. 1, (hovedsageligt sundhedsrelaterede oplysninger) i IMI, så snart systemet er udvidet til også at omfatte et modul for SOLVIT⁽³⁰⁾. Endelig kan det ikke udelukkes, at der i fremtiden vil blive indsamlet yderligere følsomme oplysninger gennem IMI enten *ad hoc* eller systematisk.

2.7. Sikkerhed (artikel 16 og betragtning 16)

63. Den tilsynsførende glæder sig over, at der i artikel 16 henvises specifikt til Kommissionens forpligtelse til at følge dens egne interne regler, som er vedtaget i overensstemmelse med artikel 22 i forordning (EF) nr. 45/2001, samt til at vedtage og ajourføre en sikkerhedsplan for IMI.

64. For at styrke disse bestemmelser yderligere henstiller den tilsynsførende til, at der til forordningen tilføjes et krav om en risikovurdering og en revision af sikkerhedsplanen for hver gang, IMI udvides til at omfatte et nyt politikområde, eller inden der tilføjes en ny funktion, der har betydning for behandlingen af personoplysninger⁽³¹⁾.

65. Den tilsynsførende bemærker endvidere, at artikel 16 og betragtning 16 kun henviser til Kommissionens forpligtelser og til hans tilsynsfunktion. Denne henvisning kan være vildledende. Det er korrekt, at Kommissionen er operatør af systemet og som sådan er hovedansvarlig for at vedligeholde sikkerheden i IMI, men de kompetente myndigheder har også forpligtelser, som igen er underlagt de nationale databeskyttelsesmyndigheders tilsyn. Artikel 16 og betragtning 16 bør derfor også indeholde en henvisning til de øvrige IMI-aktørers sikkerhedsforpligtelser i henhold til direktiv 95/46/EF og til de nationale databeskyttelsesmyndigheders tilsynsbeføjelser.

2.8. Information til registrerede og gennemsigtighed (artikel 17)

2.8.1. Information i medlemsstaterne

66. Hvad angår artikel 17, stk. 1, henstiller den tilsynsførende til, at der indføres mere specifikke bestemmelser i forordningen for at sikre, at registrerede bliver fuldt informeret om behandlingen af deres oplysninger i IMI. I betragtning af at IMI anvendes af mange kompetente myndigheder, inklusive mange små lokale regeringskontorer uden tilstrækkelige ressourcer, anbefales det på det kraftigste, at udsendelsen af meddelelser koordineres på nationalt plan.

⁽²⁹⁾ Selv om forvaring af personoplysninger udgør en forholdsvis mindre risiko for beskyttelsen af privatlivets fred, mener den tilsynsførende ikke desto mindre, at heller ikke forvaring af IMI-brugeres personoplysninger i en periode på fem år, efter at brugerne ikke længere har adgang til IMI, er tilstrækkelig begrundet.

⁽³⁰⁾ Se bilag II, punkt I, stk.1.

⁽³¹⁾ Se endvidere afsnit 12 om henstillinger vedrørende revisioner.

2.8.2. Information fra Kommissionen

67. I henhold til artikel 17, stk. 2, skal Kommissionen offentliggøre en meddelelse om beskyttelse af personoplysninger vedrørende IMI i henhold til artikel 10 og 11 i forordning (EF) nr. 45/2001. Derudover kræves det i artikel 17, stk. 2, litra b), at Kommissionen skal offentliggøre oplysninger om »databeskyttelsesaspekter i forbindelse med de administrative samarbejdsprocedurer i IMI som omhandlet i artikel 12«. Endelig fastsættes det i artikel 17, stk. 2, litra c), at Kommissionen skal offentliggøre oplysninger om »undtagelser fra eller begrænsninger af de registreredes rettigheder som omhandlet i artikel 19«.
68. Den tilsynsførende glæder sig over disse bestemmelser, som bidrager til at sikre gennemsigtighed i forbindelse med behandlingen af oplysninger i IMI. Som anført i afsnit 2.1 ovenfor er det i forbindelse med et it-system, der anvendes i 27 forskellige medlemsstater, vigtigt at sikre sammenhæng, for så vidt angår systemets anvendelse, de anvendte databeskyttelsesgarantier og de oplysninger, der videregives til registrerede ⁽³²⁾.
69. Bestemmelserne i artikel 17, stk. 2, bør dog styrkes yderligere. Kommissionen kan som operatør af systemet naturligt indtage en proaktiv rolle ved at give meddelelse og andre oplysninger til de registrerede på sit websted også »på vegne af« kompetente myndigheder, dvs. oplysninger henhørende under artikel 10 og 11 i direktiv 95/46/EF. De kompetente myndigheder i medlemsstaterne vil således ofte kunne nøjes med at henvise til Kommissionens meddelelse om beskyttelse af personoplysninger og vil kun være nødt til at supplere denne meddelelse med de oplysninger, som er nødvendige for at overholde eventuelle nationale krav om videregivelse af specifikke oplysninger.
70. Derudover bør det i artikel 17, stk. 2, litra b), præciseres, at oplysninger fra Kommissionen vil dække alle politikområder, alle former for administrative samarbejdsprocedurer og alle funktioner i IMI, samt at de specifikt vil omfatte de kategorier af oplysninger, der kan behandles. Dette bør også omfatte offentliggørelse af de spørgsmål, der indgår i én til én-samarbejde på IMI's websted, som det for indværende er praksis.

2.9. Ret til indsigt i, berigtigelse og sletning af oplysninger (artikel 18)

71. Som anført i afsnit 2.1 ovenfor gør den tilsynsførende nok engang opmærksom på, at det er vigtigt at sikre sammenhæng, for så vidt angår systemets anvendelse og de anvendte databeskyttelsesgarantier. Den tilsynsførende vil derfor yderligere specificere bestemmelserne om ret til indsigt, berigtigelse og sletning.

⁽³²⁾ Denne fremgangsmåde for at sikre sammenhæng bør naturligvis tage højde for eventuelle nationale uoverensstemmelser, når dette er nødvendigt og begrundet.

72. Det bør i artikel 18 præciseres, hvem de registrerede skal rette deres anmodning om indsigt til. Dette bør være tydeligt i forbindelse med adgang til oplysninger i de forskellige perioder:
- inden sagens afslutning
 - efter sagens afslutning, men inden for forvaringsperioden på 18 måneder
 - og endelig i den periode, hvor oplysninger er »blokerede«.
73. Forordningen bør også indeholde krav om, at de kompetente myndigheder skal samarbejde om anmodninger om indsigt, hvis det er nødvendigt. Berigtigelse og sletning bør foretages »hurtigst muligt og inden for en frist på højst 60 dage« frem for »inden for en frist på 60 dage«. Der bør også henvises til muligheden for at skabe et databeskyttelsesmodul og muligheden for indbyggede databeskyttelsesløsninger i forbindelse med samarbejde mellem myndigheder med hensyn til adgangsrettigheder samt »bemyndigelse af de registrerede«, hvor det er relevant og muligt.

2.10. Tilsyn (artikel 20)

74. De seneste år er modellen for »koordineret tilsyn« blevet udviklet. Denne tilsynsmodel, som nu er taget i anvendelse i Eurodac og dele af toldinformationssystemet, er også blevet vedtaget for visainformationssystemet (VIS) og anden generation af Schengen-informationssystemet (SIS-II).
75. Denne model består af tre lag:
- de nationale databeskyttelsesmyndigheder sikrer tilsyn på nationalt plan
 - den tilsynsførende sikrer tilsyn på EU-plan
 - koordinering sikres ved hjælp af regelmæssige møder og andre koordinerede aktiviteter, som støttes af den tilsynsførende, der fungerer som sekretariat for denne koordineringsmekanisme.
76. Denne model har vist sig at være vellykket og effektiv og bør fremadrettet også anvendes for andre informationssystemer.
77. Den tilsynsførende bifalder, at artikel 20 indeholder et specifikt krav om koordineret tilsyn mellem de nationale databeskyttelsesmyndigheder og den tilsynsførende, og at dette tilsyn i store træk følger den model, der er fastsat i VIS- og SIS II-forordningerne ⁽³³⁾.

⁽³³⁾ Se Europa-Parlamentets og Rådets forordning (EF) nr. 1987/2006 af 20. december 2006 om oprettelse, drift og brug af anden generation af Schengen-informationssystemet (SIS II) (EUT L 381 af 28.12.2006, s. 4) og Europa-Parlamentets og Rådets forordning (EF) nr. 767/2008 af 9. juli 2008 om visuminformationssystemet (VIS) og udveksling af oplysninger mellem medlemsstaterne om visa til kortvarigt ophold (VIS-forordningen) (EUT L 218 af 13.8.2008, s. 60).

78. Den tilsynsførende ønsker at styrke visse dele af bestemmelserne om koordineret tilsyn og vil til det formål støtte bestemmelser, som svarer til de bestemmelser, der f.eks. er gældende for visainformationssystemet (artikel 41-43 i VIS-forordningen), Schengen II (artikel 44-46 i SIS II-forordningen), og som forventes indført for Eurodac⁽³⁴⁾. Det vil især være hensigtsmæssigt, hvis forordningen ændres på følgende punkter:

— fastsættelse og tydelig opdeling i artikel 20, stk. 1, og 2, af henholdsvis de nationale databeskyttelsesmyndigheders tilsynsopgaver og den tilsynsførendes tilsynsopgaver⁽³⁵⁾

— angivelse i artikel 20, stk. 3, af, at de nationale databeskyttelsesmyndigheder og den tilsynsførende, der hver især handler inden for deres respektive beføjelser, »samarbejder aktivt« og »sikrer et samordnet tilsyn« (frem for blot at henføre til koordineret tilsyn uden at nævne aktivt samarbejde)⁽³⁶⁾, og

— en mere detaljeret angivelse af, hvad dette samarbejde kan omfatte, f.eks. med et krav om, at de nationale databeskyttelsesmyndigheder og den tilsynsførende, idet »de hver især handler inden for deres respektive beføjelser, udveksler de relevante oplysninger, bistår hinanden med at gennemføre revisioner og inspektioner, undersøger vanskeligheder med fortolkningen eller anvendelsen af IMI-forordningen, undersøger problemer med udøvelsen af uafhængigt tilsyn eller i forbindelse med udøvelsen af den registreredes rettigheder, udarbejder harmoniserede forslag til fælles løsninger på eventuelle problemer og fremmer bevidstheden om databeskyttelsesrettigheder alt efter behov«⁽³⁷⁾.

79. Den tilsynsførende er dog opmærksom på, at IMI på nuværende tidspunkt er mindre, behandler anderledes oplysninger og er under konstant udvikling. Han erkender derfor, at det kan være hensigtsmæssigt med større fleksibilitet i forbindelse med hyppigheden af møder og revisioner. Den tilsynsførende henstiller til, at forordningen indeholder de nødvendige minimumsregler til at sikre et effektivt samarbejde, uden at skabe unødvendige administrative byrder.

80. Artikel 20, stk. 3, i forslaget indeholder ikke krav om regelmæssige møder, men fastsætter blot, at den tilsynsførende kan »... efter behov indkalde de nationale tilsynsmyndigheder til møde« Den tilsynsførende bifalder, at disse bestemmelser lader det være op til de berørte parter at fastsætte hyppigheden og retningslinjerne for møderne og andre proceduremæssige detaljer vedrørende deres samarbejde. Dette kan vedtages i forretningsordenen, som allerede er nævnt i forslaget.

⁽³⁴⁾ Rådets forordning (EF) nr. 2725/2000 af 11. december 2000 om oprettelse af »Eurodac« til sammenligning af fingeraftryk med henblik på en effektiv anvendelse af Dublin-konventionen (EFT L 316 af 15.12.2000, s. 1), der på nuværende tidspunkt er under revision. I den forbindelse overvejes der indført bestemmelser, som svarer til bestemmelserne i VIS- og SIS II-forordningerne.

⁽³⁵⁾ Se f.eks. artikel 41 og 42 i VIS-forordningen.

⁽³⁶⁾ Se f.eks. artikel 43, stk. 1, i VIS-forordningen.

⁽³⁷⁾ Se f.eks. artikel 43, stk. 2, i VIS-forordningen.

81. Hvad angår regelmæssige revisioner, kan det også øge effektiviteten at lade det være op til de samarbejdende myndigheder i deres forretningsorden at fastsætte, hvornår og hvor hyppigt disse revisioner skal foretages. Dette kan afhænge af en række faktorer, og behovet kan ændre sig med tiden. Den tilsynsførende støtter derfor Kommissionens fremgangsmåde, som giver øget fleksibilitet også på dette område.

2.11. National anvendelse af IMI

82. Den tilsynsførende er tilfreds med, at forslaget angiver et tydeligt retsgrundlag for den nationale anvendelse af IMI, og at denne anvendelse er underlagt adskillige betingelser, herunder at de nationale databeskyttelsesmyndigheder skal høres, og at anvendelsen skal være i overensstemmelse med national lovgivning.

2.12. Informationsudveksling med tredjelande (artikel 22)

83. Den tilsynsførende bifalder de krav, der fastsættes i artikel 22, stk. 1, vedrørende informationsudveksling, samt at artikel 22, stk. 3, sikrer gennemsigtighed i forbindelse med udvidelsen, idet Kommissionen i Den Europæiske Unions Tidende skal offentliggøre en ajourført liste over tredjelande, der anvender IMI (artikel 22, stk. 3).

84. Den tilsynsførende henstiller endvidere til, at Kommissionen indsnævrer henvisningen til undtagelser under artikel 26 i direktiv 95/46/EF til kun at omfatte artikel 26, stk. 2. Det vil med andre ord sige, at de kompetente myndigheder eller andre eksterne aktører i et tredjeland, som ikke yder tilstrækkelig beskyttelse, ikke skal have direkte adgang til IMI, medmindre der er indført passende kontraktbestemmelser. Disse bestemmelser bør forhandles på EU-plan.

85. Den tilsynsførende understreger, at andre undtagelser som den, hvor »videregivelsen er nødvendig eller følger af lov eller bestemmelser fastsat med hjemmel i lov for at beskytte en vigtig samfundsinteresse eller for, at et retskrav kan fastlægges, gøres gældende eller forsvares«, ikke bør anvendes til at begrunde dataoverførsler til tredjelande via direkte adgang til IMI⁽³⁸⁾.

2.13. Ansvarlighed (artikel 26)

86. Den tilsynsførende henstiller, i overensstemmelse med den forventede styrkelse af ordningerne til sikring af større ansvarlighed i forbindelse med revisionen af EU's regler for databeskyttelse⁽³⁹⁾, at der i forordningen fastsættes en klar ramme for passende interne mekanismer og kontrolsystemer for at sikre overholdelse af databeskyttelse og fremlæggelse af bevis herfor, der som minimum indeholder ovennævnte elementer.

⁽³⁸⁾ Samme fremgangsmåde er fastsat i artikel 22, stk. 2, for Kommissionen som IMI-aktør.

⁽³⁹⁾ Se afsnit 2.2.4. i meddelelse fra Kommissionen til Europa-Parlamentet, Rådet, Det Økonomiske og Sociale Udvalg og Regionsudvalget — En global metode til beskyttelse af personoplysninger i Den Europæiske Union, KOM(2010) 609 endelig. Se også afsnit 7 i Udtalelse fra Den Europæiske Tilsynsførende vedrørende denne meddelelse fra Kommissionen, af 14. januar 2011.

87. Den tilsynsførende bifalder i den forbindelse kravet i forordningens artikel 26, stk. 2, om, at Kommissionen hvert tredje år aflægger rapport til den tilsynsførende om aspekter vedrørende beskyttelse af personoplysninger, herunder datasikkerhed. Det vil være hensigtsmæssigt, hvis det i forordningen præciseres, at den tilsynsførende til gengæld lader de nationale databeskyttelsesmyndigheder få adgang til Kommissionens rapport inden for rammerne af det koordinerede tilsyn, som der henvises til i artikel 20. Det vil endvidere være nyttigt at præcisere, at det i rapporten skal undersøges, hvordan de vigtigste databeskyttelsesprincipper (f.eks. information til registrerede, adgangsrettigheder, sikkerhed) er blevet overholdt i praksis, for så vidt angår de enkelte politikområder og funktioner.
88. Det bør endvidere præciseres i forordningen, at reglerne for interne kontrolmekanismer også omfatter vurderinger vedrørende beskyttelse af privatlivets fred (inklusive en sikkerhedsanalyse) samt en databeskyttelsespolitik (inklusive en sikkerhedsplan), som er vedtaget på grundlag af disse regler, samt periodiske revisioner og kontroller.

2.14. Indbygget databeskyttelse

89. Den tilsynsførende bifalder henvisningen til dette princip i betragtning 6 i forordningen⁽⁴⁰⁾. Han henstiller til, at forordningen udover denne henvisning også tilføjes specifikke krav til beskyttelse af privatlivets fred, som f.eks.:
- et databeskyttelsesmodul, der giver registrerede mulighed for mere effektivt at udøve deres rettigheder⁽⁴¹⁾
 - tydelig opdeling af de forskellige politikområder, som hører under IMI (»kinesiske mure«)⁽⁴²⁾
 - specifikke tekniske løsninger til at indsnævre søgemulighederne i registre, alarminformationer og andet for at sikre formålsbegrænsning
 - specifikke foranstaltninger til at sikre, at sager, hvor der ikke foregår aktivitet, afsluttes⁽⁴³⁾
 - passende retssikkerhedsgarantier i forbindelse med den fremtidige udvikling af systemet⁽⁴⁴⁾.

3. KONKLUSIONER

90. Den tilsynsførendes generelle holdning til IMI er positiv. Den tilsynsførende støtter de mål, som Kommissionen søger at nå med indførelsen af et elektronisk informationsudvekslingssystem og med regler for dets databeskyttelsesaspekter. Den tilsynsførende er endvidere tilfreds med Kommissionens forslag om en horisontal retsakt for IMI i form af en forordning fra Rådet og Europa-Parlamentet. Han er positiv over for, at forslaget har omfattende fokus på de mest relevante databeskyttelses-spørgsmål i forbindelse med IMI.

91. Hvad angår det retsgrundlag for IMI, som fremsættes i forslaget til forordning, gør den tilsynsførende opmærksom på to store udfordringer:

- behovet for at sikre en ensartet anvendelse, samtidig med at forskelligheden respekteres, og
- behovet for at skabe balance mellem fleksibilitet og retssikkerhed.

92. Det bør præciseres, hvilke funktioner der allerede er planlagt indført i IMI, og de bør beskrives nærmere.

93. Der bør anvendes passende retssikkerhedsgarantier for at sikre, at der i forbindelse med den fremtidige udvikling af IMI vil blive taget nøje hensyn til databeskyttelsen. Forordningen bør især indeholde en bestemmelse om, at den tilsynsførende og databeskyttelsesmyndighederne skal høres forud for enhver udvidelse af IMI's anvendelsesområde.

94. Eksterne aktørers adgangsrettigheder og adgangsrettigheder til advarselsmeddelelser bør også præciseres.

95. Hvad angår dataforvaringsperioder:

- bør der i forordningen indføres garantier for, at sager vil blive afsluttet rettidigt i IMI, og at »sovende« sager (sager, hvor der igennem længere tid ikke har været aktivitet) vil blive slettet fra databasen
- bør det genovervejes, om der foreligger en passende begrundelse for at udvide den nuværende seks måneders periode til 18 måneder efter sagens afslutning
- har Kommissionen ikke i tilstrækkelig grad begrundet behovet for og rimeligheden af at opbevare »blokerede oplysninger« i op til fem år, og dette forslag bør derfor tages op til fornyet overvejelse

- bør der foretages en tydeligere sondring mellem alarmmekanismer og databaser. Den tilsynsførende henstiller derfor til, at forordningen som standard bør anføre i) en seks måneders forvaringsperiode for advarselsmeddelelser, medmindre der er angivet andet i den vertikale lovgivning og forudsat, at der er indført tilstrækkelige supplerende garantier, samt ii) at denne periode bør gælde fra det tidspunkt, hvor meddelelsen sendes.

96. forordningen bør indeholde krav om en risikoanalyse og en revision af sikkerhedsplanen for hver gang, IMI udvides til at omfatte et nyt politikområde, eller inden der tilføjes en ny funktion, der har betydning for behandlingen af personoplysninger.

97. Bestemmelserne om information til registrerede og adgangsrettigheder bør styrkes og bør fremme en mere ensartet fremgangsmåde.

⁽⁴⁰⁾ Idem.

⁽⁴¹⁾ Se afsnit 2.9. ovenfor.

⁽⁴²⁾ Se afsnit 2.4. ovenfor.

⁽⁴³⁾ Se afsnit 2.5.2. ovenfor.

⁽⁴⁴⁾ Se afsnit 2.2.2. ovenfor.

98. Den tilsynsførende ønsker at styrke visse dele af bestemmelserne om koordineret tilsyn og vil til det formål støtte bestemmelser, som svarer til de bestemmelser, der f.eks. er gældende for visainformationssystemet, Schengen II, og som forventes indført for Eurodac. Den tilsynsførende henstiller til, at forordningen indeholder de nødvendige minimumsregler til at sikre et effektivt samarbejde, men ikke skaber unødvendige administrative byrder.
99. Forordningen bør sikre, at de kompetente myndigheder eller andre eksterne aktører i et tredjeland, som ikke yder tilstrækkelig beskyttelse, ikke skal have direkte adgang til IMI, medmindre der er indført passende kontraktbestemmelser. Disse kontraktbestemmelser bør forhandles på EU-plan.
100. Det bør endvidere præciseres i forordningen, at reglerne for interne kontrolmekanismer også omfatter vurderinger vedrørende beskyttelse af privatlivets fred (herunder en sikkerhedsanalyse) samt en databeskyttelsespolitik (herunder en sikkerhedsplan), som er vedtaget på grundlag af disse regler, samt periodiske vurderinger og revision.
101. Der bør også til forordningen tilføjes specifikke regler for indbygget databeskyttelse.

Udfærdiget i Bruxelles, den 22. november 2011.

Giovanni BUTTARELLI
*Europæisk assisterende tilsynsførende for
databeskyttelse*
