

NL

NL

NL



EUROPESE COMMISSIE

Brussel, 22.4.2010
COM(2010)170 definitief

VERSLAG VAN DE COMMISSIE

**over de situatie op het gebied van gegevensbescherming
in het Informatiesysteem Interne markt**

VERSLAG VAN DE COMMISSIE

over de situatie op het gebied van gegevensbescherming in het Informatiesysteem Interne markt

1. SAMENVATTING

De Commissie is tevreden over de wijze waarop de rechten en vrijheden van personen met betrekking tot persoonsgegevens (hierna "gegevensbescherming") in het Informatiesysteem Interne markt (IMI) worden gewaarborgd. IMI is een op internet gebaseerd, beveiligd en meertalig systeem voor informatie-uitwisseling dat de lidstaten helpt bij het uitvoeren van hun taken op het gebied van administratieve samenwerking. De Commissie is ook tevreden over de tenuitvoerlegging van de aanbeveling inzake richtsnoeren betreffende gegevensbescherming voor IMI.

De lidstaten hebben geen gegevensbeschermingsproblemen gemeld. Dit rechtvaardigt de met de Europese Toezichthouder voor gegevensbescherming overeengekomen stapsgewijze aanpak voor het creëren van het rechtskader voor IMI in reactie op technische ontwikkelingen en de uitbreiding van het systeem naar andere terreinen van de internemarktwetgeving.

De Commissie zal in 2010 onderzoeken of het mogelijk is IMI uit te breiden naar andere terreinen van de interne markt en zij zal meer ervaring opdoen met de praktische toepassing van het systeem op het gebied van diensten. In het eerste kwartaal van 2011 zal zij een werkdocument publiceren over de werking en de ontwikkeling van IMI in 2010, dat ook zal handelen over gegevensbescherming.

2. ONDERWERP VAN DIT VERSLAG

In dit verslag, dat is aangekondigd in de aanbeveling van de Commissie inzake richtsnoeren betreffende gegevensbescherming voor het informatiesysteem voor de interne markt¹ ('de aanbeveling'), worden de tenuitvoerlegging van de aanbeveling door de lidstaten en de Commissie en de situatie op het gebied van gegevensbescherming in IMI beoordeeld. Ook wordt er ingegaan op nieuwe kwesties die in de aanbeveling niet zijn behandeld — met name de uitbreiding tot de nieuwe Dienstenrichtlijn.

Bij het opstellen van het verslag heeft de Commissie rekening gehouden met de feedback die de lidstaten hebben geleverd via een ad-hocraadpleging in november 2009² en via regelmatige contacten met IMI-coördinatoren en

¹ C(2009) 2041 definitief. PB L 100 van 18.4.2009, blz. 12–28.

² Zeventien lidstaten reageerden op de raadpleging, waarbij de volgende vragen werden gesteld:
- Heeft u contact opgenomen met uw nationale autoriteiten voor gegevensbescherming? Hebben deze opvattingen geuit over de nationale toepassing van de richtsnoeren?
- Heeft u een algemene verklaring inzake het privacybeleid voor alle IMI-gebruikers opgesteld of wordt dit plaatselijk door uw bevoegde autoriteiten geregeld?

vertegenwoordigers van de lidstaten tijdens vergaderingen van IMAC-IMI (Raadgevend Comité voor de interne markt - IMI).

3. DE ONTWIKKELING VAN IMI IN 2009

Het jaar 2009 was cruciaal voor de ontwikkeling van IMI. Het gebruik van IMI voor wetgeving inzake beroepskwalificaties werd uitgebreid tot 20 nieuwe beroepen en de meeste middelen werden aangewend voor de uitbreiding van IMI om de Dienstenrichtlijn³ te bestrijken.

De nationale IMI-coördinatoren namen deel aan het proefproject voor de uitwisseling van informatie in het kader van de Dienstenrichtlijn (op basis van werkelijke en fictieve zaken) en aan de opleidingssessies die plaatsvonden in Brussel⁴. De Commissie bracht een nieuwe versie van de software (1.7) uit om bevoegde autoriteiten de mogelijkheid van zelfregistratie te bieden. Aan het eind van het jaar bracht zij ook een tussenversie 2.0 uit met een afzonderlijke IT-applicatie voor het waarschuwingsmechanisme⁵. Deze nieuwe softwarerelease werd volledig operationeel in het eerste kwartaal van 2010.

Dankzij deze gezamenlijke inspanningen van de Commissie en de lidstaten waren eind januari 2010 4 508 bevoegde autoriteiten geregistreerd in IMI. 3 698 hiervan hadden toegang tot het nieuwe wetgevingsgebied 'diensten', maar dit aantal zal in de komende maanden naar verwachting aanzienlijk stijgen. Het gemiddelde aantal dagelijks ingelogde gebruikers is gestegen van 40 in januari 2009 naar 180 in december 2009.

- Hebben uw bevoegde autoriteiten problemen met gegevensbescherming ondervonden bij het verzenden of beantwoorden van verzoeken in IMI?

- Hebben uw bevoegde autoriteiten problemen met de behandeling van vragen over strafregisterinformatie gemeld?

- Hebben uw bevoegde autoriteiten verzoeken om toegang, verwijdering of rectificatie ontvangen van betrokkenen?

- Zijn uw bevoegde autoriteiten op de hoogte van de mogelijkheid om persoonsgegevens in het systeem in een vroeg stadium te verwijderen? Maken zij van deze mogelijkheid gebruik?

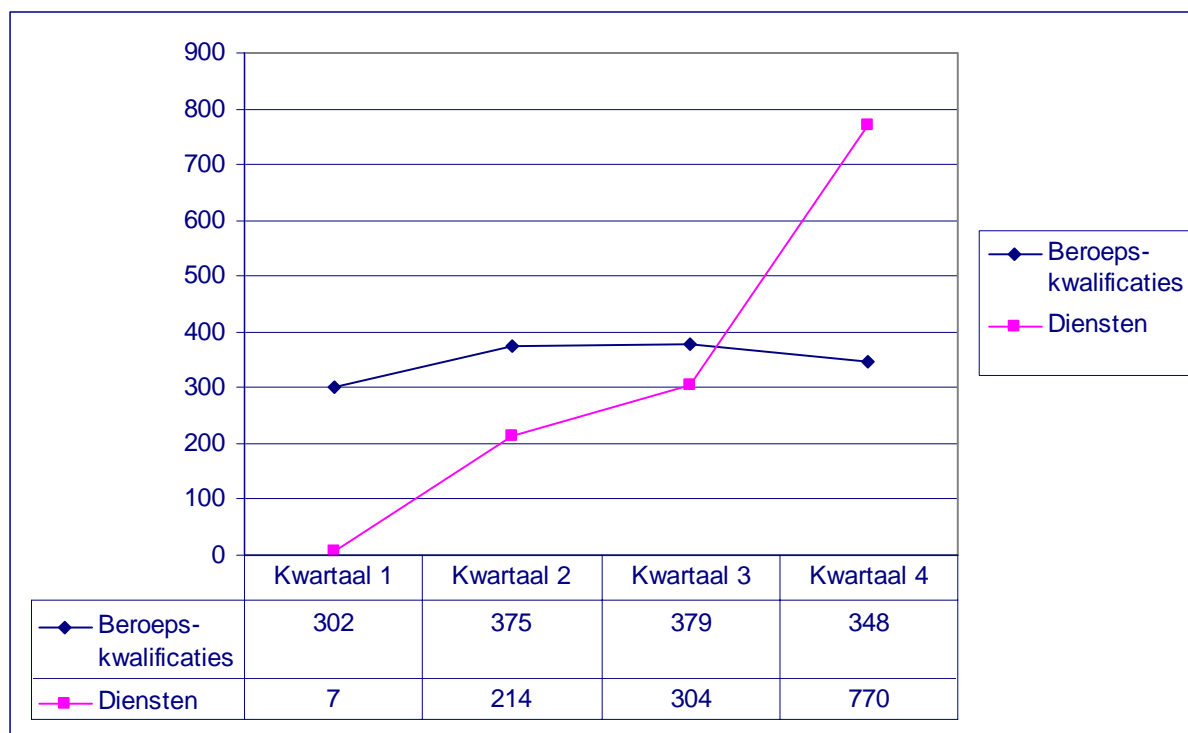
- Heeft u gegevensbescherming in uw opleidingssessies voor IMI opgenomen?

³ Richtlijn 2006/123/EG van het Europees Parlement en de Raad van 12 december 2006 betreffende diensten op de interne markt, PB 376 van 27.12.2006, blz. 36–68.

⁴ De Commissie heeft in 2009 in Brussel drie opleidingsdagen voor IMI-coördinatoren gehouden, waaraan telkens circa 60 personen deelnamen. In diezelfde periode hebben de lidstaten samen meer dan 100 opleidingsevenementen georganiseerd voor bevoegde autoriteiten op lokaal, regionaal en nationaal niveau.

⁵ Zie artikel 32 van de Dienstenrichtlijn.

Totaal aantal verzonden verzoeken per kwartaal en per wetgevingsgebied in 2009



Het systeem heeft op het gebied van beroepskwalificaties aan maturiteit gewonnen. Het duidelijke succes illustreert het potentieel van IMI als instrument voor administratieve samenwerking in de EU. Per kwartaal zijn er gemiddeld 350 verzoeken verzonden. Meer dan 90% van alle in 2009 verzonden verzoeken in verband met beroepskwalificaties was afkomstig uit de EU-15, de lidstaten die vóór 2004 zijn toetreden. Hieruit blijkt de richting van de arbeidsmigratie. Polen en Roemenië hebben 32% van alle verzoeken ontvangen.

Bij deze aantallen is het van belang te vermelden dat 56% van de verzoeken binnen een week werd beantwoord.

Benodigde tijd voor het afhandelen van een verzoek in het kader van de Richtlijn beroepskwalificaties in 2009

| | Aanvaarde verzoeken | Cumulatief % | Beantwoorde verzoeken | Cumulatief % |
|-----------------------|---------------------|--------------|-----------------------|--------------|
| Binnen 3 dagen | 741 | 57,0% | 518 | 43,0% |
| Binnen 1 week | 216 | 73,7% | 167 | 56,8% |
| Binnen 2 weken | 166 | 86,5% | 170 | 71,0% |
| Binnen 4 weken | 120 | 95,7% | 164 | 84,6% |
| Binnen 8 weken | 35 | 98,4% | 106 | 93,4% |

| | | | | |
|-------------------------|--------------|---------------|--------------|---------------|
| Meer dan 8 weken | 21 | 100,0% | 80 | 100,0% |
| Totaal: | 1 299 | | 1 205 | |

(* Het verschil tussen de aanvaarde en beantwoorde verzoeken is toe te schrijven aan verzoeken die eind december 2009 waren ingetrokken of nog in behandeling waren)

4. VERBETERING VAN GEGEVENSBESCHERMING IN IMI, EEN STAPSGEWIJZE AANPAK

IMI volgt de zogeheten ‘Privacy by Design’-aanpak waarbij gegevensbescherming van meet af aan een onderdeel is van het ontwerp van het informatiesysteem. Aan gegevensbeschermingsoverwegingen wordt ook aandacht besteed bij het dagelijkse gebruik van het systeem en in het opleidingsmateriaal. Het is een aanpak die verder reikt dan een formalistische of theoretische bescherming. Zij lijkt vruchten af te werpen, aangezien geen enkele lidstaat ook maar één gegevensbeschermingsincident in IMI heeft gemeld en er geen klachten van betrokkenen zijn ontvangen.

De Commissie is in de laatste twee jaar een dialoog aangegaan met de autoriteiten voor gegevensbescherming en de Europese Toezichthouder voor gegevensbescherming (EDPS). Het belangrijkste beginsel waarop de stapsgewijze aanpak stoelt, is dat het rechtskader voor IMI, aangezien het systeem een hoog niveau van technische en procedurele gegevensbescherming garandeert en de Commissie zich duidelijk ertoe heeft verbonden het voortdurend te verbeteren, de technische ontwikkelingen en de uitbreiding van het systeem naar andere terreinen van internemarktwetgeving moet volgen.

Dankzij de stapsgewijze aanpak is de Commissie, op basis van de eerste ervaring met het systeem, in staat geweest tegemoet te komen aan alle zorgen die de EDPS had geuit in een advies van 12 december 2007 en drie wetteksten vast te stellen die betrekking hebben op gegevensbescherming voor IMI:

- a) Beschikking van de Europese Commissie van 12 december 2007 inzake de bescherming van persoonsgegevens bij de invoering van het informatiesysteem interne markt (IMI)⁶;
- b) Aanbeveling van de Europese Commissie van 26 maart 2009 inzake richtsnoeren betreffende gegevensbescherming voor het informatiesysteem voor de interne markt (IMI)⁷;
- c) Beschikking van de Europese Commissie van 2 oktober 2009 tot vaststelling van de praktische regels voor de uitwisseling van informatie via elektronische middelen tussen de lidstaten uit hoofde van hoofdstuk VI van Richtlijn 2006/123/EG van het Europees Parlement en de Raad betreffende diensten op internet⁸.

⁶ C(2007) 6306, PB L 13 van 16.1.2008, blz. 13-23.

⁷ C(2009) 2041 definitief, PB L 100 van 18.4.2009, blz. 12-28.

⁸ C(2009) 7493, PB L 263 van 7.10.2009, blz. 32-34.

In hoofdstuk 6 van dit verslag zal worden ingegaan op overige kwesties zoals de inhoud en de adequate termijn voor toekomstige maatregelen, waaronder de mogelijke goedkeuring van een juridisch instrument.

5. DE TENUITVOERLEGGING VAN DE AANBEVELING VAN DE COMMISSIE

5.1. Verbeteringen door de lidstaten

5.1.1. Contacten met de autoriteiten voor gegevensbescherming

In de aanbeveling [heeft de Commissie aanbevolen dat de lidstaten] *‘IMI-coördinatoren ertoe aansporen contact te leggen met hun nationale autoriteiten voor gegevensbescherming zodat deze sturing en bijstand kunnen bieden voor de beste wijze van tenuitvoerlegging van deze richtsnoeren krachtens nationale wetgeving’*. De meeste lidstaten hebben in hun verslagen aan de Commissie aangegeven dat zij hun nationale autoriteiten voor gegevensbescherming hebben geraadpleegd. Dankzij deze raadplegingen weten IMI-gebruikers zich ervan verzekerd dat de uitwisseling van persoonsgegevens via IMI overeenkomstig de wetgeving op het gebied van gegevensbescherming gebeurt; de nationale regelgevingsinstanties zijn op hun beurt in staat gesteld om werkrelaties op te bouwen met vertegenwoordigers van overheidsdiensten die grote waarde hechten aan gegevensbescherming en zich ervoor inspannen dit werkelijk Europees project tot een succes te maken.

5.1.2. Privacyverklaringen

Op voorstel van de EDPS werden IMI-coördinatoren in de aanbeveling ook ertoe aangespoord de inhoud van privacyverklaringen met lokale autoriteiten voor gegevensbescherming te bespreken. De aanbeveling kon niet zeer specifiek zijn hierover, omdat de lidstaten over een beoordelingsbevoegdheid beschikken bij de tenuitvoerlegging van sommige bepalingen van de Richtlijn gegevensbescherming, hoewel deze geheel is geharmoniseerd. De verslagen van de lidstaten bevestigen dat er qua inhoud en opmaak van privacyverklaringen verschillende nationale praktijken zijn. Een kleine meerderheid van de lidstaten heeft het standpunt ingenomen dat de juiste opmaak en inhoud van de informatie die aan individuen moet worden verstrekt, plaatselijk door iedere bevoegde autoriteit moet worden vastgesteld in overeenstemming met de lokale wetgeving. In enkele lidstaten zijn daarentegen aanpasbare modellen voorgesteld voor de hele lidstaat⁹.

5.1.3. Bewustmaking en opleiding

Een van de belangrijkste verwezenlijkingen van de aanbeveling is dat zij de actoren en gebruikers van IMI meer bewust heeft gemaakt van gegevensbescherming. Zij zijn nu vertrouwd met algemene gegevensbeschermingsbeginselen en hebben ook praktische voorstellen gedaan om een hoog niveau van gegevensbescherming in IMI

⁹ Een goed voorbeeld van een nationaal model dat is opgesteld met technische bijstand van de nationale autoriteit voor gegevensbescherming, is de privacyverklaring (*cláusula de privacidad*) die door het Spaanse IMI-team beschikbaar is gemaakt:
http://www.mpt.es/documentacion/sistema_IMI/documentos/protex_datos/ClausulaIMI_ES/document_es/Clausula_IMI.pdf.

te waarborgen. Dankzij de aanbeveling zijn er ook verwijzingen naar de richtsnoeren betreffende gegevensbescherming opgenomen in het IMI-opleidingsmateriaal dat voor bevoegde autoriteiten is opgesteld.

5.2. Verbeteringen door de Commissie

5.2.1. Het beveiligingsplan voor IMI

De beveiliging en de vertrouwelijkheid van gegevens worden gereguleerd door het besluit van de Europese Commissie van 16 augustus 2006 betreffende de beveiliging van de door de Europese Commissie gebruikte informatiesystemen¹⁰. Het besluit is bijgewerkt met in 2009 vastgestelde uitvoeringsregels en recente richtsnoeren en normen die in het algemeen gelijk zijn aan internationale normen. De beveiligingsmaatregelen in IMI zijn herzien en dienovereenkomstig bijgewerkt en in 2009 is er een uitgebreid beveiligingsplan vastgesteld, dat in 2010 zal worden beoordeeld.

5.2.2. Technische verbeteringen

Wanneer de informatie-uitwisseling betrekking heeft op gevoelige gegevens, verschijnt er nu een herinnering op het scherm dat het om gevoelige gegevens gaat en dat de dossierbehandelaar die informatie alleen moet aanvragen indien het absoluut noodzakelijk is en de informatie rechtstreeks verband houdt met het uitoefenen van de beroepsactiviteit of het verlenen van een bepaalde dienst. In het ontwerp en de tenuitvoerlegging van het nieuwe waarschuwingsmechanisme is er ook ten volle rekening gehouden met gegevensbescherming (zie punt 5.2.3.2 hierna).

De IMI-website is ook verbeterd om deze meer intuïtief te maken voor gebruikers bij het zoeken naar de relevante documenten. Het gedeelte over gegevensbescherming¹¹ is bijgewerkt met alle relevante gegevensbeschermingswetgeving, correspondentie met de EDPS en in het systeem opgenomen vragenreeksen. Met het oog op de transparantie zijn er op aanraden van de Europese Toezichthouder vragen over gevoelige gegevens vastgesteld.

5.2.3. Het nieuwe wetgevingsgebied van de Dienstenrichtlijn

5.2.3.1. Het gebruik van IMI voor de Dienstenrichtlijn

In de Dienstenrichtlijn wordt niet specifiek verwezen naar IMI (maar slechts meer in het algemeen naar een elektronisch systeem voor de uitwisseling van informatie). Daarom was het nodig om formeel te bepalen dat IMI voor dat doel zou worden gebruikt. Dit gebeurde door middel van een beschikking¹² die door de Commissie is gegeven volgens de procedure waarin de Dienstenrichtlijn voorziet ("comitologiebeschikking").

¹⁰ C(2006) 3602.

¹¹ http://ec.europa.eu/internal_market/imi-net/data_protection_en.html.

¹² Beschikking van de Commissie van 2 oktober 2009 tot vaststelling van de praktische regels voor de uitwisseling van informatie via elektronische middelen tussen de lidstaten uit hoofde van hoofdstuk VI van Richtlijn 2006/123/EG van het Europees Parlement en de Raad betreffende diensten op de interne markt.

In deze comitologiebeschikking worden praktische regels gegeven voor de uitwisseling van informatie in het IMI-gedeelte voor ‘diensten’. De beschikking draagt bij aan het hoge gegevensbeschermingsniveau van het systeem en zorgt voor een grotere transparantie en nauwkeurigheid van de algemene regels die voortvloeien uit Beschikking 2008/49/EG en de richtsnoeren betreffende gegevensbescherming in de aanbeveling. Zij laat de mogelijkheid open dat er later aanvullende gegevensbeschermingsmaatregelen worden getroffen indien dit in het licht van de opgedane ervaring met het systeem nodig blijkt¹³.

5.2.3.2. Een gegevensbescherming bevorderend ontwerp voor het waarschuwingsmechanisme

Het waarschuwingsmechanisme is een alarmmechanisme dat is opgezet ingevolge artikel 29, lid 3, en artikel 32 van de Dienstenrichtlijn en dat het RAPEX-systeem voor producten aanvult. Het helpt de uit diensten voortvloeiende risico's voor ontvangers te voorkomen.

Het waarschuwingsmechanisme stelt de lidstaten in staat te voldoen aan een wettelijke verplichting tot de uitwisseling van informatie en is dus geheel rechtmatig in het licht van de gegevensbescherming. De Commissie is zich echter bewust van de gegevensbeschermingsimplicaties van een dergelijk systeem. Zij heeft daarom grote aandacht besteed aan het ontwerp van het systeem, ervoor zorgend dat het gegevensbescherming bevordert, en zij verzoekt de lidstaten, die verantwoordelijk zijn voor de gegevensbescherming wanneer zij waarschuwingen verzenden of ontvangen, met aandrang erop toe te zien dat de regels op correcte wijze worden toegepast.

Het waarschuwingsmechanisme bevat vele gegevensbeschermingsmaatregelen die algemene kenmerken van het IMI-systeem zijn, plus enkele specifieke beveiligingen die zorgen voor het volgende:

a) **De toegang tot de gegevens is beperkt tot specifieke bevoegde autoriteiten/gebruikers**

In overeenstemming met de algemene aanpak in IMI is de toegang tot informatie in het kader van het waarschuwingsmechanisme strikt beperkt op ‘need-to-know’-basis. Bevoegde autoriteiten en IMI-gebruikers hebben alleen toegang tot waarschuwingen indien hun door de lidstaten niet alleen tot IMI in het algemeen, maar ook tot de speciale applicatie voor waarschuwingen specifieke toegang is verleend. Bevoegde autoriteiten en IMI-gebruikers kunnen standaard geen waarschuwingen verzenden of ontvangen. Deze functie moet afzonderlijk worden geactiveerd.

b) **Er worden geen onnodige waarschuwingen verzonden**

Er kan geen waarschuwing worden verzonden zonder een checklijst in te vullen om ervoor te zorgen dat er aan de criteria wordt voldaan; bijvoorbeeld, dat er ernstige handelingen of omstandigheden zijn in verband met een dienstverrichting die tot ernstige schade zouden kunnen leiden. Indien de initiërende autoriteit niet alle

¹³ Zie hoofdstuk 13 van de aanbeveling, subdeel ‘Werk in uitvoering’, onder d).

relevante criteria afvinkt, gaat het systeem niet over tot het verzenden van een waarschuwing.

Bovendien wordt de waarschuwing niet onmiddellijk naar andere lidstaten verzonden; zij wordt eerst voorgelegd aan een waarschuwingscoördinator in dezelfde lidstaat. Deze waarschuwingscoördinator moet opnieuw bepalen of de waarschuwing al dan niet naar andere lidstaten moet worden doorgezonden.

c) **Waarschuwingen worden niet naar meer ontvangers verzonden dan noodzakelijk is om te voldoen aan de informatievereisten in de wetgeving**

Wanneer er waarschuwingen naar andere lidstaten worden doorgezonden, moeten de initiërende autoriteit en de waarschuwingscoördinator beoordelen welke lidstaten de waarschuwing moeten ontvangen. Indien de lidstaat waar een dienst wordt verleend een waarschuwing wil zenden, zullen standaard alleen de lidstaat waar de dienstverlener is gevestigd en de Commissie de waarschuwing ontvangen. Deze standaardinstelling zorgt ervoor dat er per geval wordt bepaald welke andere lidstaten, op ‘need-to-know’-basis, aan de lijst van ontvangers moeten worden toegevoegd.

Wanneer de waarschuwing naar andere lidstaten wordt doorgezonden, wordt deze bovendien niet naar alle bevoegde autoriteiten in de ontvangende lidstaten gezonden, maar alleen naar een mailbox voor waarschuwingen (gewoonlijk de nationale waarschuwingscoördinator). De ontvanger zal dan beslissen welke bevoegde autoriteiten in de lidstaat betrokken zijn en moeten worden ingelicht.

d) **De Commissie heeft geen toegang tot persoonsgegevens bij het ontvangen van waarschuwingen zoals geregeld in de Dienstenrichtlijn**

De Dienstenrichtlijn bepaalt dat alle waarschuwingen naar de Commissie worden verzonden; in tegenstelling tot de lidstaten hoeft de Commissie echter geen toegang te hebben tot persoonsgegevens. De Commissie ontvangt dus waarschuwingen zonder persoonsgegevens.

e) **Indien er ongegronde waarschuwingen worden verzonden, ondanks de voorzorgsmaatregelen, kunnen deze snel worden ingetrokken; verkeerde gegevens kunnen ook worden gerectificeerd of verwijderd**

In het IMI-systeem kan een bevoegde autoriteit die een ongegronde waarschuwing heeft verzonden, deze onmiddellijk intrekken en onzichtbaar maken voor alle IMI-gebruikers. Indien de waarschuwing gerechtvaardigd was, maar het nodig is bepaalde informatie te rectificeren, kan de initiërende bevoegde autoriteit dit te allen tijde doen. Daarnaast stelt het IMI-systeem andere bevoegde autoriteiten die de waarschuwing hebben ontvangen, in staat aan te geven dat bepaalde informatie in een waarschuwing onjuist is.

f) **De waarschuwingen worden beëindigd zodra er geen risico meer bestaat; de gegevens worden onmiddellijk onzichtbaar voor alle gebruikers en de persoonsgegevens worden zes maanden na de beëindiging verwijderd**

Zodra er een einde komt aan het risico dat aanleiding gaf tot de waarschuwing, moet de waarschuwing worden beëindigd. Het IMI-systeem stelt de lidstaat van vestiging

dus in staat de waarschuwing te beëindigen en de verantwoordelijke autoriteiten ontvangen herinneringen per e-mail. Zodra een waarschuwing is beëindigd, wordt deze onzichtbaar. Uiterlijk zes maanden na de beëindiging worden alle persoonsgegevens automatisch verwijderd, ook uit het systeem.

6. NADER TE OVERWEGEN KWESTIES

Hoewel de meeste lidstaten een positieve beoordeling over de gegevensbescherming in IMI hebben uitgesproken, hebben enkele lidstaten bepaalde kwesties naar voren gebracht die in dit deel van het verslag worden besproken.

6.1. Toepasselijke regels voor de beveiliging en de vertrouwelijkheid van gegevens

De verwerking van persoonsgegevens in IMI behelst een gezamenlijke verwerking (door de Commissie en de lidstaten), een gedeelde verantwoordelijkheid (tussen de verschillende gebruikers en actoren) en een gezamenlijk toezicht (door de nationale autoriteiten voor gegevensbescherming en de EDPS). In een dergelijk complex scenario is het niet altijd gemakkelijk verantwoordelijkheden toe te wijzen.

De Deense en Duitse autoriteiten voor gegevensbescherming hebben het volgende standpunt ingenomen: aangezien de bevoegde autoriteiten op hun grondgebied aan bepaalde nationale vereisten dienen te voldoen (bv. een sterker authenticatiemechanisme zoals vermeld in het volgende deel), zouden zij erop moeten aandringen dat IMI aan deze nationale vereisten voldoet of het systeem niet langer moeten gebruiken. De bevoegde autoriteiten hebben deze verzoeken voorgelegd aan de Commissie, die verantwoordelijk is voor de beveiliging van het systeem.

De Commissie meent dat IMI een beveiligd systeem is en dat een werkelijk Europees netwerk als IMI eenvoudigweg niet zou kunnen functioneren als iedere lidstaat zou eisen dat er aan zijn nationale beveiligingsnormen wordt voldaan. De vaststelling van de Richtlijn gegevensbescherming bijna twintig jaar geleden had als tweeledig doel, enerzijds, het fundamenteel recht op gegevensbescherming te beschermen en, anderzijds, het vrije verkeer van persoonsgegevens tussen lidstaten en tussen de lidstaten en de EU-instellingen te garanderen¹⁴.

Op grond hiervan dringt de Commissie erop aan dat nationale autoriteiten voor gegevensbescherming geen hindernissen opwerpen voor het gebruik van het systeem voor nationale bevoegde autoriteiten, gelet op het hoge niveau van garanties voor gegevensbescherming in het IMI-systeem en het beginsel van loyale samenwerking in artikel 4, lid 3), van het Verdrag betreffende de Europese Unie.

¹⁴ Dit beginsel wordt duidelijk uiteengezet in artikel 1, lid 2, van de Richtlijn gegevensbescherming en artikel 1, lid 1, en overweging 13 van de Verordening gegevensbescherming: 'Doel is zorg te dragen voor zowel doeltreffende naleving van de regels inzake de bescherming van de fundamentele rechten en vrijheden van natuurlijke personen als het vrije verkeer van persoonsgegevens tussen de lidstaten en de communautaire instellingen en organen of tussen die instellingen en organen onderling, voor met de uitoefening van hun respectieve bevoegdheden verband houdende doeleinden'.

6.2. Naar een sterkere vorm van authenticatie in IMI

Het authenticatiesysteem van IMI is een geavanceerde versie van één-factorauthenticatie, aangezien het een gebruikersnaam en wachtwoord met een PIN combineert. Wanneer de gebruiker toegang tot het systeem probeert te krijgen, wordt hem gevraagd een willekeurig gekozen combinatie van karakters van de PIN-code te verstrekken.

De Duitse en Deense autoriteiten voor gegevensbescherming hebben enige bezorgdheid geuit over het authenticatiesysteem van IMI. De Commissie meent dat het huidige authenticatiemechanisme adequaat is, rekening houdend met de stand van de techniek en de implementatiekosten, maar ze is het ermee eens dat een sterkere authenticatie op lange termijn wenselijk is. Daar de lidstaten verschillende authenticatiesystemen hebben geïntroduceerd die niet altijd interoperabel zijn, lijkt de voorkeursoplossing voor een sterkere authenticatie in IMI te bestaan in e-identiteiten die op lidstaatniveau worden beheerd en door middel van middleware interoperabel worden.

Een van de opties is het STORK-project. Dit wordt momenteel ontwikkeld door een consortium waaraan enkele lidstaten deelnemen en het wordt gefinancierd uit hoofde het kaderprogramma voor concurrentievermogen en innovatie – ICT-beleids ondersteuningsprogramma. De Commissie zal de vorderingen in de komende maanden nauwlettend volgen; deze zullen bepalend zijn voor de beslissing of het in IMI kan worden gebruikt.

Verdere informatie over gegevensbeveiliging wordt gegeven in punt 7.2.

6.3. Bewaren van gegevens

Het beleid inzake het bewaren van gegevens in IMI is zeer streng¹⁵ en sommige actoren en gebruikers hebben aangegeven dat het moet worden herzien. Het snel verwijderen van persoonsgegevens in het systeem is niet altijd in het belang van de betrokkene, die mogelijk de voorkeur eraan zou geven dat zijn of haar gegevens voor een langere periode in IMI worden bewaard, bijvoorbeeld in het geval van rechtszaken.

Het Europees Hof van Justitie heeft in een recente uitspraak¹⁶ verklaard dat er niet alleen voor het heden, maar ook voor het verleden een recht op toegang tot informatie geldt¹⁷. Daarom meent het Hof dat het beperken van de toegang door het verwijderen van de gegevens in strijd kan zijn met de wet, tenzij wordt aangetoond dat een langere bewaring van de informatie een buitensporige last zou inhouden voor de voor de verwerking verantwoordelijke. De Commissie vindt niet dat het bewaren van persoonsgegevens in IMI voor een langere periode een buitensporige last zou inhouden en daarom is zij voornemens na te denken over een langere bewaartijd, met eventueel een overgangsfase waarin de gegevens worden geblokkeerd en voor alle

¹⁵ Het in een vroeg stadium verwijderen van persoonsgegevens is met slechts enkele klikken mogelijk; alle persoonsgegevens worden in ieder geval zes maanden na de beëindiging van de informatieverzoeken automatisch verwijderd.

¹⁶ C-553/07, Rotterdam/Rijkeboer.

¹⁷ Zie artikel 12, onder a), van Richtlijn 95/46/EG.

gebruikers onzichtbaar worden gemaakt voordat ze uiteindelijk worden verwijderd. De mogelijke implicaties van het beleid inzake het blokkeren van gegevens, inclusief wie toegang zou mogen hebben tot de geblokkeerde gegevens en om welke redenen, zullen zorgvuldig worden geanalyseerd.

Dit is een goed voorbeeld van de noodzaak om zeer zorgvuldig na te denken alvorens een reeks regels voor de werking van IMI in een wettelijk bindend instrument vast te stellen. Het is van wezenlijk belang dat de Commissie en de lidstaten lessen kunnen trekken uit voldoende ervaring met het systeem om ondoeltreffende en zelfs averechtse regels voor gegevensbescherming te voorkomen, terwijl een goede gegevensbescherming en de betrokkenheid van de autoriteiten voor gegevensbescherming bij het proces worden gegarandeerd.

6.4. Nationaal gebruik van IMI

Bij de omzetting van de Dienstenrichtlijn in Nederland is bepaald dat IMI voor nationale doeleinden zal worden gebruikt, d.w.z. dat er ook informatie tussen Nederlandse overheidsdiensten zal worden uitgewisseld. De Europese Commissie prijst deze aanpak, die een illustratie is van het potentieel van IMI om tussen overheidsdiensten te worden gebruikt. Het nationale gebruik van IMI door de lidstaten moet evenwel aan drie voorwaarden voldoen:

- a) het verwerken van persoonsgegevens en het bewaren van informatie op servers van de Commissie worden naar nationaal recht rechtmatig geacht;
- b) het systeem wordt gebruikt zoals het is, met dezelfde vragenreeksen en functionaliteiten; en
- c) de lidstaten dragen de volledige verantwoordelijkheid voor kwesties (inzake gegevensbescherming of andere kwesties) die verband houden met het gebruik van het systeem voor nationale doeleinden.

Indien lidstaten geïnteresseerd zijn in het nationale gebruik van IMI, is het daarom raadzaam dat zij eerst hun nationale autoriteiten voor gegevensbescherming hierover raadplegen en zich ervan vergewissen dat dit geen problemen zal veroorzaken in het licht van de wetgeving op het gebied van gegevensbescherming.

6.5. Specifieke gegevensbeschermingsmaatregelen in wettelijk bindende communautaire wetgeving

In zijn advies van 12 december 2007 en correspondentie met de Commissie heeft de EDPS verzocht om specifieke, wettelijk bindende gegevensbeschermingsmaatregelen in EU-wetgeving vast te stellen naarmate het toepassingsgebied van IMI verder reikt dan de Dienstenrichtlijn en de Richtlijn beroepskwalificaties. De Duitse autoriteiten voor gegevensbescherming hebben soortgelijke opvattingen geuit.

In 2010 zal de nieuwe Commissie zich met hernieuwde aandacht buigen over de functionering van de interne markt en over de mogelijkheid tot het vergroten van de bijdrage van IMI aan de verbetering van de tenuitvoerlegging van de internemarktwetgeving door de lidstaten. Zij zal dus overwegen welke andere beleidsterreinen baat zouden kunnen hebben van het gebruik van IMI.

Er is reeds een solide pakket gegevensbeschermingsmaatregelen ingevoerd en de ontvangen feedback van de lidstaten was positief. Daarom meent de Commissie dat het onverstandig zou zijn tot een wetsvoorstel over te gaan voordat het toepassingsgebied van IMI is gedefinieerd en voordat er lessen kunnen worden getrokken uit de praktijkervaring met het gebruik van het systeem voor 'diensten'. Alle toekomstige voorstellen moeten goed zijn afgestemd op deze ontwikkelingen, zodat er wordt gezorgd voor een solide, toekomstvaste basis voor IMI en gegevensbescherming.

In de tussentijd zal de Commissie de gegevensbescherming in IMI blijven verbeteren, in nauwe samenwerking met de lidstaten en de EDPS, zoals hierna uiteengezet.

7. TOEKOMSTIGE VERBETERINGEN

7.1. Technische verbeteringen

In een toekomstige softwarerelease zullen automatische herinneringen en urgentielijsten worden toegevoegd waarmee een antwoord kan worden geaccepteerd (zodat aanvragen niet langer dan noodzakelijk open blijven). Wat de onlineprocedure voor de rectificatie, afscherming of uitwissing van gegevens betreft, meent de Commissie dat het, aangezien er tot dusver geen aanvragen zijn ingediend en het onwaarschijnlijk is dat er in de toekomst vele zullen zijn, meer gepast is een lichtere procedure te introduceren die naar behoren zal worden gedocumenteerd met de hulp van de gegevensbeschermingsfunctionaris van de Commissie en de EDPS.

7.2. Gegevensbeveiliging

De Commissie zal in 2010 een nieuwe risicobeoordeling uitvoeren met betrekking tot IMI, in overeenstemming met de nieuwe richtsnoeren en normen die zij onlangs heeft vastgesteld, en het beveiligingsplan dienovereenkomstig aanpassen. Daarbij zal er worden bepaald welke systeemonderdelen aandacht vergen, wat de mogelijke bedreigingen zijn en welke maatregelen op infrastructuur- en softwaregebied nodig zijn. Indien bij de risicobeoordeling blijkt dat er aanvullende beveiligingsmaatregelen moeten worden vastgesteld, zullen deze geleidelijk in toekomstige softwarereleases worden verwerkt.

Verder zal er begin 2011 een externe audit plaatsvinden, waarbij de aandacht vooral zal uitgaan naar de prestaties en de stabiliteit van het systeem, maar ook naar bepaalde gegevensbeschermings- en beveiligingskwesties.

7.3. Herziening van de Richtlijn beroepskwalificaties

In de periode 2010-2011 zal een evaluatie van de Richtlijn beroepskwalificaties worden gemaakt; in dit kader zullen ook de administratieve samenwerking en het gebruik van IMI, inclusief gegevensbeschermingskwesties, worden beoordeeld.

8. CONCLUSIES

De Commissie is tevreden over de tenuitvoerlegging van de aanbeveling en de situatie op het gebied van gegevensbescherming in IMI. Niettemin zal zij zich ervoor blijven inspannen om het systeem verder te verbeteren, met name door technische verbeteringen en verbeteringen van de gegevensbeveiliging.

De Commissie is ook voornemens te onderzoeken of het mogelijk is IMI uit te breiden naar andere terreinen van de interne markt en tegelijkertijd lessen te trekken uit nieuwe praktijkervaring met het gebruik van IMI voor het wetgevingsgebied 'diensten'. Bij elk voorstel voor EU-wetgeving zal rekening worden gehouden met deze ontwikkelingen en overwegingen, zodat er wordt gezorgd voor een solide, toekomstvaste basis voor IMI en gegevensbescherming.

In het eerste kwartaal van 2011 zal er een werkdocument over de werking en ontwikkeling van het IMI-systeem in 2010 worden gepubliceerd. In dit verslag zal ook aandacht worden geschonken aan gegevensbescherming.