Advies nr 12/2009 van 29 april 2009

Betreft: adviesaanvraag vanwege de FOD Binnenlandse Zaken m.b.t. een aantal vragen die rezen naar aanleiding van beraadslaging RR 19/2008 (A/2009/007)

De Commissie voor de bescherming van de persoonlijke levenssfeer;

Gelet op de wet van 8 december 1992 *tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens* (hierna WVP), inzonderheid artikel 29;

Gelet op het verzoek om advies van de heer Guido DE PADT, minister van Binnenlandse Zaken ontvangen op 06/03/2009;

Gelet op het verslag van de heer Frank SCHUERMANS;

Brengt op 29 april 2009 het volgend advies uit:

I. WAT VOORAFGING

1. Op 28 april 2008 diende de Federale Overheidsdienst Informatie- en Communicatietechnologie (Fedict), bij het Sectoraal comité van het Rijksregister een aanvraag in om gemachtigd te worden om een toegang te bekomen tot de informatiegegevens van het Rijksregister en om het identificatienummer ervan te gebruiken met het oog op het testen, de correctie en het onderhoud van computertoepassingen die via UME, FSB en Web Services[1] een verbinding hebben met het Rijksregister.

2. Bij beraadslaging RR nr. 19/2008 van 7 mei 2008 verleende het Sectoraal comité van het Rijksregister de gevraagde machtiging onder de volgende voorwaarden:

a. de veiligheidsconsulent van Fedict stelt voorafgaand aan de interne test-, correctie- en onderhoudswerkzaamheden de populatie vast waarop mag getest worden;
b. deze populatie bevat maximaal 10.000 personen;
c. de veiligheidsconsulent houdt nauwgezet toezicht op het respecteren van deze parameters door de personen die concreet de werkzaamheden verrichten;
d. de testresultaten worden maximum 1 jaar bewaard in een beveiligde omgeving;
e. de logs van de testactiviteiten worden minstens 10 jaar bewaard;
f. de toepassingen van Fedict moeten ten overstaan van het Rijksregister enkel geauthenticeerd worden aan de hand van een certificaat van toepassing, dus zonder dat aan het Rijksregister de identiteit van de eindgebruiker moet worden meegedeeld.

3. Deze beraadslaging is kennelijk problematisch voor de Federale Overheidsdienst Binnenlandse Zaken omdat ze de rol en de taken van het Rijksregister als beheerder van de elektronische identiteit in België en tussenpersoon in de uitwisseling van identiteitsgebonden informatie in twijfel zou trekken. Ze zou ook de transparantieverplichting, voorzien door artikel 6, § 3, 3°, van de wet van 19 juli 1991 *betreffende de bevolkingsregisters, de identiteitskaarten, de vreemdelingenkaarten en de verblijfsdocumenten en tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen,* hypotheceren.

---

[1] De UME (Universal Messaging Engine) is het instrument dat ontwikkeld werd door Fedict om via gestandaardiseerde berichten communicatie mogelijk te maken met en tussen de verschillende systemen van de Federale Overheid. De UME is geëvolueerd naar de FSB (Federal Service Bus). Deze FSB gaat nog "intelligenter" tewerk dan de UME bij het verwerken van berichten, waardoor het voor bevoegde ambtenaren en ondernemingen nog eenvoudiger wordt om de verschillende computertoepassingen en gegevensbestanden van de Federale Overheid te benaderen. Web Services maakt het mogelijk om op afstand (meestal over het internet) vanaf een cliënt-computer een dienst op te vragen aan een server, bijvoorbeeld de levering van gegevens.

4. Hierop aansluitend wenst de Federale Overheidsdienst Binnenlandse Zaken de zienswijze (het advies) van de Commissie te vernemen m.b.t. 3 pijnpunten, namelijk:

- De rol en verantwoordelijkheden bij het beheer van de elektronische identiteit in België;
- de transparantieverplichting;
- het doeleinde waarvoor een machtiging werd verleend.

II. TEN GRONDE

2.1. Voorgaande opmerking

5. De Commissie wenst vooraf op te merken dat zij zich niet van de indruk kan ontdoen dat de adviesaanvraag haar in de rol van beroepsinstantie plaatst voor beslissingen genomen door één van de sectorale comités. Dit is geenszins reglementair voorzien en de Commissie heeft geenszins de intentie om dergelijke rol te vervullen.

6. Als er vragen zijn omtrent een beraadslaging, dan is het aangewezen dat in de eerste plaats met het betrokken sectoraal comité in discussie wordt getreden.

7. De Commissie kan een verzoek om advies echter niet naast zich neerleggen en heeft zich dan ook gebogen over de voorgelegde vragen.

2.2. Rol en verantwoordelijkheden bij het beheer van de elektronische identiteit in België

8. De Federale Overheidsdienst Binnenlandse Zaken merkt op dat Fedict evolueert naar een intermediair platform en dienstenintegrator. Het toekennen van dergelijke bevoegdheden op basis van een eenvoudige machtiging van het Sectoraal comité van het Rijksregister is strijdig met de grondwettelijke en wettelijke bepalingen die de persoonlijke levenssfeer beschermen.

9. Er kan niet ontkend worden dat de kans groot is dat Fedict mettertijd inderdaad de rol van dienstenintegrator op zich neemt. Dat dit een gepaste wettelijke omkadering vereist, staat buiten kijf. Er is daartoe trouwens een wetsontwerp in voorbereiding. Op 24 oktober 2008 werd het advies van de Commissie ingewonnen m.b.t. een voorontwerp van wet *houdende oprichting en organisatie van een Federale Dienstenintegrator*[2]**.**

[2] De Commissie verleende een positief advies nr.41/2008 van 17 december 2008.

10. De voornoemde machtiging van het Sectoraal comité van het Rijksregister werd verleend rekening houdend met:

- artikel 5, eerste lid, 1°, van de wet van 8 augustus 1983 *tot regeling van een Rijksregister van de natuurlijke personen* (hierna WRR), krachtens hetwelk aan Belgische openbare overheden een machtiging kan verleend worden voor de informatiegegevens die zij gemachtigd zijn te kennen uit hoofde van een wet, een decreet of een ordonnantie;

- artikel 5, tweede lid, WRR dat een toegang afhankelijk stelt van een welbepaald, duidelijk omschreven en wettig doeleinde en verder bepaalt dat deze moet worden beperkt tot gegevens die ter zake dienend en niet overmatig zijn rekening houdend met die doeleinden;
- artikel 5, derde lid, WRR dat bepaalt dat moet worden nagegaan of de mededeling in overeenstemming is met de WVP;
- het koninklijk besluit van 11 mei 2001 *houdende oprichting van de Federale Overheidsdienst Informatie- en communicatietechnologie*, waarin het actuele takenpakket van Fedict wordt vastgelegd.

11. Een van de opdrachten van Fedict bestaat in het uitwerken van de basisarchitectuur voor een efficiënte inzet van de informatie- en communicatietechnologie ter ondersteuning van de gemeenschappelijke strategie inzake e-government, het opvolgen van de naleving ervan (artikel 2, § 1, 4°, van het koninklijk besluit van 11 mei 2001). In uitvoering van deze bepaling ontwikkelde Fedict een UME, een FSB en Webservices die ter beschikking gesteld worden van de federale overheden zodat zij elektronisch berichten kunnen uitwisselen. Het is dan ook de bedoeling dat behoorlijk gemachtigden langs die weg over een toegang tot het Rijksregister kunnen beschikken.

12. De bekritiseerde beraadslaging stipt terecht aan: *"De ontwikkeling van dergelijke toepassingen is echter op zich geen garantie voor een kwaliteitsvolle dienstverlening. Pas nadat een toepassing met goed gevolg werd getest – wat eventueel het aanbrengen van correcties impliceert - kan zij in productie gesteld worden. Daarna moet het onderhoud van de toepassing verzekerd worden. Dit hele proces, dat wezenlijk is voor het uitwerken van e-government projecten, situeert zich binnen de reglementaire opdrachten van de aanvrager."*

13. De machtiging werd dus verleend met het oog op een welbepaald doeleinde dat zijn basis vindt in een van kracht zijnd koninklijk besluit. De stelling dat het Sectoraal comité van het Rijksregister dat het met de beraadslaging RR nr. 19/2008 aan Fedict de hoedanigheid van dienstenintegrator

toebedeelt, is dan ook onjuist. De verdere commentaren die de Federale Overheidsdienst Binnenlandse Zaken in verband met de problematiek "dienstenintegrator" formuleert, zijn dan ook niet ter zake dienend.

14. Uit het schrijven van de Federale Overheidsdienst Binnenlandse Zaken meent de Commissie te mogen afleiden dat de oprichting van een federale dienstenintegrator door eerstgenoemde ervaren wordt als een bedreiging voor de veiligheid en transparantie van de gegevens en gegevensstromen.

15. De Commissie is van oordeel dat deze vrees ongegrond is. De tussenkomst van een dienstenintegrator heeft normaal een positieve invloed op de veiligheid van gegevens en gegevenstromen. De transparantie komt evenmin in het gedrang, mits de nodige afspraken worden gemaakt en de nodige organisatorische maatregelen worden genomen.

16. De Commissie verwijst in dit verband naar de principes uiteengezet in haar aanbeveling nr. 01/2008 van 24 september 2008 *met betrekking tot het toegangs- en gebruikersbeheer in de overheidssector*. Zij zal trouwens op een van haar volgende zittingen een advies uitbrengen m.b.t. dienstenintegratie.

17. Deze principes gekoppeld aan een wetgevende omkadering bieden voldoende waarborgen voor transparantie en veiligheid.

2.3. Transparantieverplichting

18. Artikel 6, § 3, 3°, van de wet van 19 juli 1991 bepaalt dat de houder van een EID via deze kaart "*kennis kan nemen van alle overheden, instellingen en personen die, gedurende de laatste zes maanden, zijn gegevens bij het bevolkingsregister of het Rijksregister van de natuurlijke personen hebben geraadpleegd of bijgewerkt*."

19. Het feit dat toepassingen ten overstaan van het Rijksregister worden geauthenticeerd aan de hand van een certificaat van toepassing betekent volgens de Federale Overheidsdienst Binnenlandse Zaken dat:

- de door artikel 6, § 3, 3°, van de wet van 19 juli 1991 ingebouwde transparantie op de helling wordt gezet omdat het niet nodig wordt geacht dat het Rijksregister de gegevens bewaart die toelaten de eindgebruiker te identificeren,;
- het gebruik van de EID als authenticatie-instrument in vraag wordt gesteld.

20. De discussie m.b.t. de draagwijdte van artikel 6, § 3, 3°, van de wet van 19 juli 1991 is niet nieuw. De Commissie boog zich hier reeds over op de zitting van 8 februari 2006 en maakte haar standpunt dienaangaande bij schrijven van 24 februari 2006 kenbaar aan de Federale Overheidsdienst Binnenlandse Zaken. Dit standpunt is nog steeds actueel. Het werd echter enkel bilateraal gecommuniceerd. Vandaar dat het hier voor een goed begrip wordt herhaald:

"***Draagwijdte van de uitdrukking "persoon"***

Artikel 6, § 3, tweede lid, 3°, van de wet van 19 juli 1991 zegt inderdaad dat de houder van een identiteitskaart recht heeft op "kennisname van alle overheden, instellingen en personen die, gedurende de laatste zes maanden, zijn gegevens bij het bevolkingsregister of het Rijksregister van natuurlijke personen hebben geraadpleegd of bijgewerkt….". Het koninklijk besluit van 13 februari 2005 tot vaststelling van de datum van inwerkingtreding en van het stelsel van het recht tot kennisname van de overheden, instellingen en personen die de informatiegegevens die zijn opgenomen in de bevolkingsregisters of in het Rijksregister van de natuurlijke personen hebben geraadpleegd of bijgewerkt, genomen ter uitvoering van dit artikel nam deze terminologie over.

De Commissie is van oordeel dat de woorden "overheden, instellingen en personen" in voormeld artikel, ingegeven zijn door de instanties die in toepassing van artikel 5 van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, kunnen gemachtigd worden om toegang te hebben tot of mededeling te bekomen van de informatiegegevens van het Rijksregister en dat zijn - in algemene termen - overheden, instellingen, (natuurlijke- of rechts)personen.

Op basis van artikel 5, eerste lid, 3°, van de wet van 8 augustus 1983 kunnen zowel natuurlijke personen als rechtspersonen gemachtigd worden, voor zover ze als onderaannemer handelen. Het is deze categorie gemachtigden waarnaar de uitdrukking "personen" in artikel 6, § 3, tweede lid, 3°, van de wet van 19 juli 1991 verwijst. Wanneer er namens een dergelijke gemachtigde een raadpleging gebeurt, zal dus hetzij de naam van de natuurlijke persoon, hetzij de naam van de rechtspersoon vermeld worden.

De Commissie steunt zich daarbij op de onderliggende finaliteit van deze bepaling, namelijk enerzijds de bekommernis om de persoonlijke levenssfeer optimaal te beschermen, wat onder meer inhoudt dat een burger de mogelijkheid geboden wordt te vernemen wie zijn gegevens geraadpleegd heeft (transparantie, informatieplicht) en anderzijds de burger de mogelijkheid te bieden om een signaalfunctie te vervullen, daar hij het best geplaatst is om "abnormale" raadplegingen te detecteren, die tot sancties kunnen leiden.

De Commissie stelt vast dat de loutere mededeling van de naam van de ambtenaar die de raadpleging deed, de burger niets leert over het waarom van de raadpleging en de al dan niet regelmatigheid van de raadpleging. Bijgevolg moet de mededeling van de naam van de ambtenaar, rekening houdend met deze doeleinden, als overmatig beschouwd worden in het licht van artikel 4, § 1, 3°, WVP.

Het recht van de burger om te weten wie zijn gegevens raadpleegde wordt ten volle uitgevoerd wanneer hem gemeld wordt namens welke gemachtigde dit geschiedde. Om te weten waarom een raadpleging gebeurde of om zich een oordeel te kunnen vormen over de al dan niet regelmatigheid van een raadpleging moet er hoe dan ook steeds met de verantwoordelijke/ aansprakelijke, zijnde houder van de machtiging, contact opgenomen worden. Deze moet immers kunnen aantonen waarom diens aangestelde op een bepaalde datum de gegevens van een bepaalde persoon raadpleegde. Dit impliceert dat de gemachtigde aantoont dat:

- *de betrokkene een dossier bij hem heeft;*
- *een raadpleging van de gegevens van de betrokkene gebeurde in het kader van een operatie in het dossier overeenkomstig de modaliteiten van de machtiging.*

Het is dus belangrijk dat de burger indien hij vragen heeft weet, op basis van de lijst van de instanties die zijn gegevens raadpleegden, tot wie hij zich moet richten om tekst en uitleg te krijgen. De gemachtigde is het best geplaatst om dat te doen, gelet op zijn concrete know-how. De aandacht wordt er op gevestigd dat het feit dat een raadpleging gebeurde door een gemachtigde bij wie de burger geen dossier heeft, niet ipso facto betekent dat die raadpleging onregelmatig was. Ter illustratie hiervan kan verwezen worden naar een fonetische bevraging van het rijksregister. Hierbij zullen de gegevens van al diegene die er als "hit" uitkomen gecontroleerd worden om de juiste persoon – die bij de gemachtigde een dossier heeft - te vinden. Het is de gemachtigde die in begrijpbare termen aan de burger moet uitleggen dat zijn gegevens gecontroleerd werden in het kader van het eliminatieproces n.a.v. een fonetisch bevraging in een welbepaald dossier.

In die optiek is de Commissie van oordeel dat een loutere vermelding van de gemachtigde, bijvoorbeeld FOD Justitie, onvoldoende nauwkeurig is. De burger moet gericht contact kunnen leggen. Dit vereist de nauwkeurige vermelding van de dienst van de gemachtigde van waaruit de raadpleging is gebeurd en de contactpersoon tot wie men zich kan richten voor nadere informatie. Deze is ertoe gehouden aan de betrokken persoon de adresgegevens te verstrekken van de verantwoordelijke voor de verwerking in kwestie of van zijn aangestelde voor de gegevensbescherming alsook bijkomende toelichting over dit onderwerp (doeleinden,…) zodat het

opzet van de wetgever om aan de betrokken personen een bijkomende bescherming te waarborgen ook daadwerkelijk in de praktijk wordt gerealiseerd.

Deze zienswijze betekent geenszins dat een werknemer straffeloos kan misbruik maken van de toegang tot het Rijksregister.

De gemachtigde is verantwoordelijk voor het correct gebruik van de machtiging die hem werd verleend. Hij is het dus die er in de eerste plaats over moet waken dat zijn werknemers geen misbruik maken van de machtiging. Dit betekent dat hij over een gedetailleerd systeem van logins moet beschikken dat reikt tot de individuele persoon (zie ook punt 6 van de "Referentiemaatregelen voor de beveiliging van elke verwerking van persoongegevens" opgesteld door de Commissie).

Dergelijk systeem is onontbeerlijk. Het stelt de gemachtigde in staat om zelf pro-actief op te treden wanneer bijvoorbeeld het aantal raadplegingen van één van zijn werknemers een abnormale stijging zou vertonen. Het laat hem eveneens toe om op eigen initiatief op regelmatige tijdstippen de toegang van zijn werknemers te controleren.

Kortom het is het instrument bij uitstek om ingeval van een interpellatie door of namens een burger over een bepaalde raadpleging, deze dienaangaande tekst en uitleg te verschaffen (verantwoorden).

Blijkt een raadpleging onregelmatig, dan weet hij wie van zijn werknemers in de fout is gegaan en zal deze laatste ter verantwoording kunnen geroepen worden, hetzij naar aanleiding van een klachtprocedure voor de Commissie, hetzij naar aanleiding van een gerechtelijke procedure.

Het feit dat de werknemers weten dat hun toegang tot de gegevens geregistreerd wordt, zal hen ertoe aansporen om hun toegang tot de gegevens correct te gebruiken daar ze desgevallend ter verantwoording kunnen geroepen worden (zal paal en perk stellen aan de courante praktijk om bijvoorbeeld zijn paswoord ook aan collega's toe te vertrouwen).

PRAKTISCHE MODALITEITEN BETREFFENDE DE REALISATIE VAN DIT RECHT

Met betrekking tot de uitvoeringsmodaliteiten die in de praktijk moeten voorzien worden voor de elektronische toegang, voorzien bij artikel 6, § 3, tweede lid, 3°, van de voormelde wet van 19 juli 1991, voorziet artikel 2 van het KB van 13/02/2005[3] *dat dit recht wordt uitgeoefend «door middel*

[3] KB van 13 februari 2005 tot vaststelling van de datum van inwerkingtreding en van het stelsel van het recht tot kennisname van de overheden, instellingen en personen die de informatiegegevens die zijn opgenomen in de bevolkingsregisters of in het Rijksregister van de natuurlijke personen hebben geraadpleegd of bijgewerkt, B.S. 28-02-2005

van een met een computer, aangesloten op Internet, verbonden leestoestel en met behulp van de Internetsite van het Rijksregister».

De Commissie meent dat, wanneer een burger zich vragen stelt aangaande de bestemmelingen van zijn persoonsgegevens, deze burger zich moet kunnen wenden tot de beheerder van de bedoelde persoonsgegevens. Met andere woorden, indien het gaat om persoonsgegevens die bijgehouden worden door het Rijksregister, moet iedere burger zijn aanvraag richten tot het bedoeld Rijksregister (ook indien de bestemmeling er niet rechtstreeks toegang toe kreeg via de diensten van het Rijksregister maar op indirecte wijze door toedoen van een tussenkomende organisatie). Dit beginsel vloeit voort uit artikel 10 van de WVP en haar uitvoeringsmodaliteiten voorzien in het KB van 2001.

Behoudens de bepalingen van het voormelde artikel 2 verwijst de Commissie naar het administratief beginsel van de scheiding van besturen, naar het feit dat de diensten van het Rijksregister onder de bevoegdheid vallen van de Minister van Binnenlandse Zaken en naar het feit dat de tussenkomende organisaties die toegang hebben tot het Rijksregister om informaties van dit register aan andere organismen mee te delen, in voorkomend geval kunnen afhangen van een andere minister dan deze van Binnenlandse Zaken.

De informatie met betrekking tot de bestemmeling van een rechtstreekse raadpleging wordt bij de diensten van het Rijksregister zelf bewaard.

Wanneer men geconfronteerd wordt met een onrechtstreekse raadpleging (bijvoorbeeld via de Kruispuntbank van de Sociale Zekerheid) stelt zich de vraag of de informatie met betrekking tot de eindbestemmeling eveneens door de diensten van het Rijksregister moet bijgehouden worden.

De Commissie stelt vast dat artikel 6, § 3, van de voormelde wet van 1991 en het koninklijk besluit ter uitvoering ervan, dit niet opleggen.

Het belangrijkste voor de burger is dat hij de gevraagde informaties krijgt en dat deze correct zijn.

De Commissie is van mening dat het in deze hypothesen niet noodzakelijk is dat de diensten van het Rijksregister de "bestanden" krijgen van de verbindingen met de servers van een tussenkomende organisatie en de identiteit van de eindbestemmelingen van de bedoelde gegevens van het Rijksregister bijhouden; er kan worden opgemerkt dat deze diensten op die wijze, in bepaalde gevallen toegang zouden kunnen krijgen tot gevoelige informatie van de betrokken personen zoals, bijvoorbeeld, de naam van het ziekenfonds waarbij een persoon is aangesloten.

Bij gelegenheid van een vraag van een betrokken persoon tot inzage van de raadplegingen van zijn persoonsgegevens die plaatsvonden bij het Rijksregister, kan het zijn dat een van deze raadplegingen gebeurde door toedoen van een tussenkomend organisme. In deze gevallen kan overwogen worden de burger te verwijzen naar dit tussenkomend organisme, bijvoorbeeld door middel van een hyperlink opdat deze laatste hem de gevraagde informatie, in het kader van het artikel 6, § 3, tweede lid, 3° van de wet van 19 juli 2001, zou kunnen mededelen.
In die mate is de Commissie van mening dat de burgers hun aanvragen tot inzage moeten richten tot de diensten van het Rijksregister en dat de antwoorden op de bedoelde vragen in voorkomend geval, kunnen verstrekt worden door een derde organisme…

21. Deze lezing en toepassing van artikel 6, § 3, tweede lid, 3°, van de wet van 19 juli 1991 sluit naadloos aan bij de principes volgens dewelke toegangs- en gebruikersbeheer georganiseerd wordt (aanbeveling nr. 01/2008) en de principes volgens dewelke dienstenintegratie georganiseerd moet worden.

22. Dat het standpunt van het Sectoraal comité van het Rijksregister en de Commissie het gebruik van minderwaardige authenticatiesystemen zou bevoordelen ten koste van de EID als authenticatie-instrument is onjuist. Aan het gebruik van een toepassing die zich t.o.v. het Rijksregister authenticeert door middel van een certificaat van toepassing, is noodzakelijkerwijze een toegangs-en gebruikersbeheer gekoppeld. In dat verband wordt in punt 14 van de aanbeveling nr. 01/2008 uitdrukkelijk gesteld: *"De Commissie is van oordeel dat de elektronische authenticatie van de identiteit bij voorkeur gebeurt aan de hand van de elektronische identiteitskaart (EID) daar zij de meeste garanties biedt. Ze combineert het bezit van een specifiek document met het beschikken over een bepaalde kennis (pincode)."*

23. Samenvattend is de Commissie dus van oordeel dat:

- het optreden van een of meerdere dienstenintegratoren de transparantie waarin voorzien wordt door artikel 6, § 3, tweede lid, 3°, van de wet van 19 juli 1991 niet in het gedrang brengt;
- voormeld artikel in hoofde van het Rijksregister geen verplichting inhoudt om zelf de informatie m.b.t. de eindgebruiker op te slaan;
- het werken met toepassingen die zich ten overstaan van het Rijksregister authenticeren met een certificaat van toepassing, ontmoedigt geenszins het gebruik van de EID als authenticatie-instrument, integendeel.

2.4. Doeleinde waarvoor de machtiging werd verleend en toegang tot de productieomgeving

24. Onder deze hoofding worden door de Federale Overheidsdienst Binnenlandse Zaken bedenkingen geformuleerd m.b.t. het doeleinde waarvoor de machtiging werd verleend, de proportionaliteit van de toegang en de bewaartermijn van de gegevens.

25. De Commissie vestigt er de aandacht op dat het Sectoraal Comité van het Rijksregister m.b.t. tot deze punten over een soevereine appreciatiebevoegdheid beschikt en dat het niet aan de Commissie is om zich op dat gebied in de plaats van een van haar sectorale comités te stellen.

26. Volledigheidshalve vestigt de Commissie in dit verband de aandacht op de volgende punten.

27. Uit de beraadslaging blijkt dat het testen met gegevens van het Rijksregister zal gebeuren ten behoeve van gemachtigde instanties die over een toegang tot het Rijksregister beschikken. De doeleinden waarvoor instanties toegang vragen tot het Rijksregister zijn altijd gelieerd aan hun eigen opdrachten en/of werkzaamheden. Gegevens van het Rijksregister voor loutere testdoeleinden gebruiken, is dus op basis van de gebruikelijke machtigingen niet mogelijk. De verleende machtiging maakt dit mogelijk voor Fedict, de ontwerper en aanbieder van de toepassingen ten behoeve van gemachtigde instanties.

28. Het gaat hier dus wel degelijk om een specifiek doeleinde. Wanneer een burger nagaat wie zijn gegevens raadpleegde, zal dus duidelijk blijken dat zijn gegevens voor testdoeleinden werden gebruikt. Fedict zal als begunstigde gemachtigde, in geval van interpellatie, moeten aangeven met het oog op de toepassing van welke gemachtigde instantie de test gebeurde.

29. De Federale Overheidsdienst Binnenlandse Zaken stelt ook de proportionaliteit van de verleende permanente toegang ter discussie. Dit dossier werd destijds ook bezorgd aan de Federale Overheidsdienst Binnenlandse Zaken met het oog op het inwinnen van het door artikel 31, § 3, eerste lid, WVP voorgeschreven technisch en juridisch advies. In dit technisch en juridisch advies, dat het Comité op 5 mei 2008 ontving, werd echter geen enkele opmerking geformuleerd met betrekking tot de voorgestelde permanente toegang.

30. De *ratio legis* van de verleende permanente toegang:

- het testen en onderhouden van toepassingen gebeurt niet volgens een bepaalde periodiciteit maar afhankelijk van behoeften en eventuele incidenten;
- er kan op voorhand niet worden bepaald wanneer Fedict behoefte heeft aan testgegevens.

31. Een permanente toegang biedt Fedict dus de mogelijkheid om, wanneer dit met het oog op de finaliteit bepaald in de beraadslaging RR nr. 19/2008 nodig is, testgegevens uit het Rijksregister te halen. Het zou weinig praktisch zijn om te verlangen dat Fedict geval per geval om een toegang zou verzoeken. Het is dus een permanente toegang die niet tot gevolg heeft dat het Rijksregister permanent door Fedict wordt bevraagd.

32. Het Sectoraal comité van het Rijksregister beoordeelde de bewaringstermijn op basis van het dossier dat werd ingediend door Fedict. In haar technisch en juridisch advies uitte de Federale Overheidsdienst Binnenlandse Zaken geen kritiek op de voorgestelde bewaringstermijn van maximaal 1 jaar.

33. In de beraadslagingen van het Sectoraal comité van het Rijksregister wordt geregeld een maximale bewaringstermijn vooropgesteld. Dit gebeurt in gevallen waarin, afhankelijk van de situatie, de gegevens in sommige gevallen vroeger kunnen vernietigd worden dan andere. In dergelijk geval is het altijd de verantwoordelijkheid van de gemachtigde om ervoor te zorgen dat hij de gegevens vernietigt zodra ze geen nut meer hebben, zelfs voor het verstrijken van die termijn. Als naar aanleiding van een controle blijkt dat dit niet gebeurde, stelt hij zich bloot aan sancties.

34. De Commissie stelt vast dat een maximale bewaringstermijn in tal van andere dossiers nooit leidde tot enige opmerking dienaangaande in de technische en juridische adviezen vanwege de Federale Overheidsdienst Binnenlandse Zaken.

35. Tot slot vestigt de Federale Overheidsdienst Binnenlandse Zaken er de aandacht op dat er thans bij het Rijksregister een testset beschikbaar is. Het Sectoraal comité van het Rijksregister interpelleerde inmiddels Fedict en Corve om te verifiëren of die testset tegemoet komt aan hun behoeften. Indien dat het geval is, zal dit Comité gepaste actie ondernemen. Hoe dan ook, de discussie over het testen op de productiedata kan opgelost worden indien de diensten van het Rijksregister een representatieve performante acceptatieomgeving - een kopie met dezelfde functionaliteiten als het eigenlijke Rijksregister – ter beschikking stellen, wat tot nu toe niet het geval is.

DE COMMISSIE

is van oordeel dat de opmerkingen geformuleerd door de Federale Overheidsdienst Binnenlandse Zaken op beraadslaging RR nr. 19/2008 van 7 mei 2008 niet van aard zijn om deze ter discussie te stellen.

Voor de Administrateur m.v. De Voorzitter

(get.) Patrick Van Wouwe (get.) Willem Debeuckelaere