Sectoraal comité van het Rijksregister

Beraadslaging RR nr 29/2013 van 17 april 2013

Betreft: aanvraag van de Vlaamse Overheid - Departement Leefmilieu, Natuur en Energie om het identificatienummer van het Rijksregister te gebruiken met het oog op gebruikers- en toegangsbeheer voor e-government toepassingen en tot aanpassing van beraadslaging RR nr. 34/2011 (RN-MA-2012-291)

Het Sectoraal comité van het Rijksregister, (hierna "het Comité");

Gelet op de wet van 8 augustus 1983 *tot regeling van een Rijksregister van de natuurlijke personen* (hierna "WRR");

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 31*bis*;

Gelet op het koninklijk besluit van 17 december 2003 *tot vaststelling van de nadere regels met betrekking tot de samenstelling en de werking van bepaalde Sectorale comités opgericht binnen de Commissie voor de bescherming van de persoonlijke levenssfeer*;

Gelet op de aanvraag van de Vlaamse Overheid - Departement Leefmilieu, Natuur en Energie ontvangen op 20/09/2012;

Gelet op de bijkomende inlichtingen ontvangen op 03/10/2012 en 16/10/2012;

Gelet op de aanvraag van het technisch en juridisch advies gericht aan de Federale Overheidsdienst Binnenlandse Zaken op 11/10/2012;

Gelet op het verslag van de Voorzitter;

Beslist op 17 april 2013, na beraadslaging, als volgt:

I. VOORWERP VAN DE AANVRAAG

1. De aanvraag heeft tot doel om het Departement Leefmilieu, Natuur en Energie van de Vlaamse Overheid, hierna de aanvrager genoemd, te machtigen om:

   - een toegang te bekomen tot het gegeven vermeld in artikel 3, eerste lid, 1° WRR;
   - het identificatienummer van het Rijksregister te gebruiken;
     met het oog op gebruikers- en toegangsbeheer voor e-government toepassingen.

II. ONDERZOEK VAN DE AANVRAAG

2. De afdeling Milieuhandhaving, Milieuschade en Crisisbeheer van de aanvrager werd reeds gemachtigd om toegang te hebben tot een aantal gegevens van het Rijksregister en het identificatienummer te gebruiken.[1]

3. Bijgevolg kan het onderzoek van het Comité zich hier beperken tot het nagaan of:

   - het nieuwe doeleinde waarvoor gebruik van het nummer gevraagd wordt, welbepaald, uitdrukkelijk omschreven en gerechtvaardigd is in de zin van artikel 4, § 1, 2°, WVP;
   - het gebruik van het nummer proportioneel is in het licht van het doeleinde (artikel 4, § 1, 3°, WVP).

4. De vraag tot toegang tot het gegeven 'naam' en 'voornaam' is zonder voorwerp. Uit de aanvraag leidt het Comité af dat de aanvrager eigenlijk geen fysieke toegang tot het Rijksregister beoogt, maar alleen de naam en de voornamen, die door Fedict worden meegedeeld n.a.v. een positieve identificatie en authenticatie, wil opslaan en gebruiken met het oog op de organisatie van het gebruikers- en toegangsbeheer.

[1] Beraadslaging RR nr. 62/2011 van 16 november 2011.

A. DOELEINDE

5. De aanvrager wenst het identificatienummer van het Rijksregister te benutten voor het gebruikers- en toegangsbeheer van het milieuloket dat hij beheert en van webtoepassingen en webservices in het algemeen. Het milieuloket is een portaalsite via dewelke burgers, bedrijven en ambtenaren op geïntegreerde wijze voor hen relevante milieuinformatie kunnen opvragen.

6. Onderdeel van het milieuloket zijn onder meer volgende toepassingen:

   - toegang tot het integraal milieujaarverslag (IMJV) loket voor bedrijven met het oog op de vervulling van informatieverplichtingen en/of de indieningen van een milieu- of natuurvergunningsaanvraag[2];
   - toegang tot diverse loketten voor het online digitaal indien van dossiers en aanvragen zoals milieuvergunningen en erkenningen, rapporten in het kader van milieueffect- en veiligheidsrapportage, erkende boorbedrijven, e.d.;
   - toegang tot backoffice systemen voor de gemeenten, provincies en ambtenaren van de Vlaamse Overheid voor het afhalen van ingediende vergunningsaanvragen, integrale milieujaarverslagen, bedrijfsgegevens, conformiteitsattesten van zendantennes, e.d.;
   - toegang tot backoffice systemen voor de Vlaamse ambtenaren in het kader van dossierafhandeling inzake veiligheidsrapportage, milieueffectrapportage, milieuinspectie, e.d.

7. De aanvrager werd met bovenstaande taken belast onder meer krachtens:

   - het besluit van de Vlaamse Regering van 3 juni 2005 *met betrekking tot de organisatie van de Vlaamse administratie* (art. 13);
   - het Vlaams decreet van 5 april 1995 *houdende algemene bepalingen inzake milieubeleid* (Titel XV, Hoofdstuk VIII)*;*
   - het Vlaams decreet van 21 oktober 1997 *betreffende het natuurbehoud en het natuurlijk milieu* (art. 13);
   - het Vlaams decreet van 28 juni 1985 *betreffende de milieuvergunning;*
   - het besluit van de Vlaamse Regering van 2 april 2004 *tot invoering van het integrale milieujaarverslag.*

8. Het betreft dus een welbepaald en uitdrukkelijk omschreven doeleinde in de zin van artikel 4, § 1, 2°, WVP. De verwerking van persoonsgegevens met het oog op de realisatie van het doeleinde, is gestoeld op artikel 5, eerste lid, e), WVP. Het betreft bijgevolg ook een gerechtvaardigd doeleinde.

---

[2] Zie beraadslaging RR nr. 35/2004 van 25 november 2004.

B. PROPORTIONALITEIT

B.1. Ten overstaan van het identificatienummer van het Rijksregister

9. Momenteel beheert de aanvrager zelf een gebruikersdatabank. De registratie van een nieuwe gebruiker gebeurt aan de hand van het e-mail adres en eventueel telefonisch contact. De authenticatie van de gebruiker gebeurt aan de hand van een gebruikersnaam en bijhorend paswoord die onderdeel zijn van het gebruikersaccount van de gebruiker. Deze werkwijze geeft veel kans op fouten omdat er geen exacte identificatie en sterke authenticatie mogelijk is.

10. De aanvrager wenst over te stappen op een systeem waarbij gebruikers zich aanmelden hetzij via hun eID, hetzij via het federaal token. Toegangsrechten zouden dan worden gekoppeld aan het identificatienummer van het Rijksregister van de betrokkene.

11. Het is essentieel voor de goede werking van het systeem dat gebruikers correct geïdentificeerd worden. Dit betekent dat misverstanden die kunnen ontstaan n.a.v. homonymie en foutieve schrijfwijzen uitgesloten moeten worden teneinde de verdere stappen van authenticatie en autorisatie niet te hypothekeren. De elektronische identificatie, authenticatie en autorisatie moeten gebeuren op een beveiligde en zekere manier. De aanvrager moet zeker zijn van de identiteit van de persoon die een webtoepassing of webservice wenst te gebruiken omdat langs deze kanalen enerzijds toegang wordt verleend tot een aantal persoonsgegevens en anderzijds handelingen kunnen worden gesteld. Om autorisatie te kunnen verlenen moet de aanvrager – ongeacht of daartoe een token of de eiD gebruikt wordt - bepaalde gebruikersgegevens bewaren zodat op elk ogenblik tot authenticatie kan worden overgegaan en het recht op toegang kan worden bepaald. Hij opteert ervoor om daartoe naast de naam en de voornamen ook het identificatienummer van het Rijksregister te bewaren. Aan de hand van het unieke identificatienummer van het Rijksregister kan een persoon precies geïdentificeerd worden en kunnen tevens alle raadplegingen en handelingen worden getraceerd.

12. Het door de aanvrager gewenste gebruik van het identificatienummer is, in het licht van het opgegeven doeleinde, in overeenstemming met artikel 4, § 1, 3°, WVP.

B.2. Ten opzichte van de duur van de machtiging

13. De aanvrager wenst een machtiging voor onbepaalde duur. Het Comité stelt vast dat de diverse reglementaire bepalingen die de aanvrager met de realisatie van een aantal doeleinden belasten, niet in de tijd beperkt zijn. In het licht van de doeleinden is een machtiging van onbepaalde duur gepast (artikel 4, § 1, 3°, WVP).

B.3. Ten opzichte van de bewaringstermijn

14. De aanvrager stelt geen concrete termijn vast gedurende dewelke het identificatienummer bijgehouden wordt, maar geeft aan het nummer te zullen bewaren zo lang als nodig. De duur van de bewaringstermijn is gekoppeld enerzijds aan de periode van activiteit van een bepaalde gebruiker en anderzijds aan de geldende bewaringstermijnen.

15. Rekening houdend met het voorgaande stelt het Comité vast dat het inderdaad moeilijk is om een concrete bewaringstermijn voorop te stellen. Op voorwaarde dat de aanvrager de accounts en dossiers die niet langer actief zijn, archiveert of vernietigt overeenkomstig het archiefdecreet van 9 juli 2010, handelt hij in overeenstemming met artikel 4, § 1, 5°, WVP.

16. In de mate dat het rijksregisternummer bewaard wordt in de loggings, met het oog op de traceerbaarheid van de verrichte raadplegingen of handelingen, ligt het voor de hand dat het identificatienummer in die context bewaard wordt zolang de loggings moeten worden bijgehouden.

B.4. Intern gebruik en/of mededeling aan derden

17. Uit de aanvraag blijkt dat de aanvrager het identificatienummer van het Rijksregister enkel gebruikt met het oog op zijn interne werkzaamheden.

18. Het Comité neemt hiervan akte en vestigt de aandacht op wat hierna onder punt B.5 wordt vermeld m.b.t. netwerkverbindingen.

B.5. Netwerkverbindingen

19. De aanvrager wenst voor haar gebruikers- en toegangsbeheersysteem gebruik te maken van de basisdiensten geleverd door de Vlaamse Dienstenintegrator[3], in het bijzonder de dienst VO-ACM/IDM (Vlaamse Overheid- Access Control Management / Identity Management). In de toekomst zal een gebruiker zich kunnen aanmelden hetzij via zijn/haar eID, hetzij via het federaal token. Authenticatie verloopt steeds via de dienst VO-ACM/IDM, die op zijn beurt gebruik maakt van de Federal Authentication Service (FAS). Bij een succesvolle authenticatie geeft de FAS de naam, de voornaam en het rijksregisternummer automatisch door aan de dienst VO-ACM/IDM. De dienst VO-ACM/IDM beheert een gebruikersdatabank waarin attributen en rollen van gebruikers gekoppeld worden aan hun identificatienummer.[4] In een aantal gevallen is de toegang tot een specifieke dienst of functionaliteit beperkt tot personen met een toegekende

---

[3] Artikel 3, §1 van het decreet van 13 juli 2012 *houdende de oprichting en organisatie van een Vlaamse dienstenintegrator* wijst DAB Informatie Vlaanderen aan als Vlaamse Dienstenintegrator.

[4] De Vlaamse Dienstenintegrator werd hiertoe gemachtigd bij beraadslaging RR nr. 34/2011 van 18 mei 2011, met uitbreidingen bij beraadslagingen RR nr. 43/2011, RR nr. 66/2011, RR nr. 44/2012, RR nr. 60/2012.

hoedanigheid (bv. Vlaams ambtenaar, gemeente ambtenaar). Waar van toepassing wordt deze hoedanigheid samen met de naam en het identificatienummer van de betrokkene doorgegeven naar het milieuloket.

20. Autorisatie van de gebruikers om toegang te krijgen tot de verschillende onderdelen van het milieuloket gebeurt door de aanvrager. Hij beheert hiertoe een gebruikersdatabank waarin de toegangsrechten toegekend aan elke gebruiker bewaard worden.

21. Is een gebruiker niet gekend in VO-ACM/IDM, dan zal enkel het identificatienummer doorgegeven worden aan het milieuloket. Hetzelfde geldt wanneer een gebruiker met een bepaalde rol of hoedanigheid ervoor kiest zich als gewone burger aan te melden. Aan de hand van het identificatienummer kunnen relevante gegevens opgezocht worden in de verschillende databanken van het milieuloket, voor zover die hierover beschikken en het gebruik gemachtigd is. In dit geval wordt het identificatienummer van de gebruiker niet opgeslagen na afloop van de sessie in het milieuloket.

22. Het Comité acht het aangewezen de machtiging van de Vlaamse Dienstenintegrator uit te breiden tot professionele gebruikers in het algemeen.

23. Vanuit een bekommernis van volledigheid benadrukt het Comité dat:

    - indien er later andere netwerkverbindingen mochten tot stand komen, de aanvrager het Comité daarvan voorafgaandelijk op de hoogte moet brengen;
    - het identificatienummer van het Rijksregister in ieder geval slechts gebruikt kan worden in relaties met derden voor zover het kadert in de doeleinden met het oog op dewelke deze laatsten eveneens gemachtigd werden om dit nummer te gebruiken.

C. UITBOUW GEBRUIKERS- EN TOEGANGSBEHEERSYSTEEM

24. Het gebruikers- en toegangsbeheerssysteem voorgesteld door de aanvrager vertrouwt er op dat derden stipt bijhouden wie welke hoedanigheid heeft binnen een organisatie (bv. Vlaams ambtenaar, werknemer van een milieuadviesbureau). De aanvrager geeft aan hiervoor gebruik te willen maken van authentieke bronnen waar mogelijk, hetgeen in lijn ligt met aanbeveling nr. 01/2008 van 24 september 2008 van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer *met betrekking tot het gebruikers- en toegangsbeheer in de overheidssector*.

25. Het Comité stelt vast dat er in e-government toepassingen in grote lijnen op twee manieren omgegaan wordt met gebruikers uit de privé-sector.
    Enerzijds zijn er systemen die rechtstreeks een account aanmaken voor een bepaalde persoon binnen een onderneming om toegang te krijgen tot de toepassing, al dan niet met initiële controle of de betrokkene wel degelijk hiertoe bevoegd is. Voor de hand liggend nadeel van dit

systeem is dat het voor een onderneming moeilijk is het overzicht te behouden en dat wijzigingen in personeelsbestand of in takenverdeling de nodige opvolging moet krijgen, mogelijks in een veelheid van externe toepassingen.

Anderzijds zijn er systemen waarbij de verantwoordelijkheid voor toegang tot meerdere e-government toepassingen finaal bij één enkele persoon binnen de onderneming rust. Deze persoon kan dan door delegatie van bevoegdheid ervoor zorgen dat de juiste persoon binnen de onderneming toegang krijgt tot welbepaalde e-government toepassingen. Een wijziging in personeel of een verschuiving van taken kan en moet dan ook door deze persoon opgevolgd worden. Externe toepassingen kunnen automatisch gevolgen koppelen aan de doorgevoerde wijzigingen.

26. Dit laatste systeem is nota bene in gebruik in het domein van de sociale zekerheid, de vennootschapsbelastingen en in het e-health platform. Voormelde domeinen doen beroep op een databank waarin voor elke deelnemende onderneming een 'verantwoordelijke toegang entiteit' (VTE) geregistreerd wordt. Hiertoe wordt in de KBO eerst nagegaan wie als wettelijke vertegenwoordiger van een onderneming mag optreden, het is deze persoon die een VTE aanduidt. Deze VTE kan volgens bepaalde regels taken en bevoegdheden toewijzen aan personen naargelang de behoefte binnen de organisatie.

27. Het Comité is van oordeel dat deze VTE databank beantwoordt aan de functionele definitie van een authentiek bron.[5] De beheerder van de VTE databank valideert dit gegeven en biedt specifieke garanties ten aanzien van de juistheid, de volledigheid en de beschikbaarheid van dit gegeven. Het gegeven VTE wordt éénmalig geregistreerd en is vervolgens bruikbaar voor verschillende overheden.

28. Het Comité meent dat het inschakelen van de VTE van ondernemingen, en desgevallend van andere entiteiten, de norm moet worden in gebruikers- en toegangsbeheer voor e-government toepassingen om het risico op onrechtmatige toegang tot gegevens te beperken. Het Vlaams e-gov decreet spoort overigens alle entiteiten van de Vlaamse administratie aan om gegevens uit authentieke bronnen op te halen voor de uitbouw van het elektronische bestuurlijke gegevensverkeer.[6] De memorie van toelichting bij dit e-gov decreet wijst er op dat naast Vlaamse authentieke bronnen ook rekening moet gehouden worden met authentieke bronnen op andere bestuurlijke niveaus.[7]

29. Het Comité beslist daarom de huidige machtiging toe te kennen op voorwaarde dat de VTE databank in het gebruikers- en toegangssysteem ingepast wordt. Evenwel erkent het Comité dat

---

[5] Aanbeveling van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer nr. 9/2012 van 23 mei 2012, nr. 5.

[6] Artikel 3 Vlaams decreet van 18 juli 2008 *betreffende het elektronische bestuurlijke gegevensverkeer.* Een verplichting geldt voor authentieke bronnen aangeduid door de Vlaamse Regering, cf. artikel 4 van hetzelfde decreet.

[7] Vl. Parl., 2007-2008, 1712/1, p. 31.

deze inpassing de nodige tijd vraagt voor voorbereiding, ontwikkeling en uitrol. In het licht hiervan staat het Comité een overgangstermijn van één jaar toe. Gedurende deze termijn mag de aanvrager het identificatienummer gebruiken voor de professionele gebruikers die zij toegang wenst te verlenen tot het milieuloket. De machtiging neemt van rechtswege een einde indien na afloop van deze termijn de toegang voor professionele gebruikers niet onderworpen is aan het toezicht van de VTE.

D. BEVEILIGING

D.1. Consulent inzake informatiebeveiliging

30. De identiteit van de consulent inzake informatiebeveiliging werd niet meegedeeld.

31. Artikel 10 WRR verplicht iedere instantie die toegang tot of mededeling van de gegevens van het Rijksregister verkrijgt om een consulent inzake informatiebeveiliging aan te stellen. Een consulent inzake informatiebeveiliging moet in alle onafhankelijkheid de informatiebeveiliging kunnen appreciëren. De identiteit van de consulent inzake informatiebeveiliging moet aan het Comité meegedeeld worden. Hierbij moet gespecificeerd worden:

- het functieprofiel, met aanduiding van de plaats in de organisatie, de resultaatgebieden en de vereiste competenties;
- de vorming die de betrokkene heeft genoten of zal genieten;
- de tijd die de betrokkene aan de functie kan besteden;
- de eventuele andere functies die de betrokkene uitoefent en die niet onverenigbaar mogen zijn met de functie van consulent inzake informatiebeveiliging.

D.2. Informatiebeveiligingsbeleid

32. Er werd door de aanvrager geen enkele informatie m.b.t. het informatiebeveiligingsbeleid verschaft.

33. Het Comité wenst dat de aanvrager een conformiteitsverklaring inzake het informatiebeveiligingssysteem dat het voorwerp is van de machtigingsaanvraag voor toegang tot of verbinding met het Rijksregister bezorgt.

34. Het Comité benadrukt dat loggings dienen te worden bijgehouden teneinde te registreren wie, omwille van welke reden, op een bepaald tijdstip, een bepaald dossier heeft geraadpleegd op basis van het rijksregisternummer.

D.3. Personen die toegang hebben tot de gegevens en die het identificatienummer van het Rijksregister mogen gebruiken en lijst van deze personen

35. Uit de aanvraag blijkt dat de veiligheidsconsulent, de beheerder van het gebruikers- en toegangsbeheersysteem en de medewerkers van de help desk toegang zullen hebben tot het identificatienummer met het oog op de uitvoering van hun taken.

36. Zoals artikel 12 van de WRR het vereist, moet de aanvrager een lijst opstellen van de personen die het identificatienummer van het Rijksregister gebruiken. Die lijst moet voortdurend worden bijgewerkt en ter beschikking worden gehouden van het Comité.

37. Bovendien moeten die personen een document ondertekenen waarin zij verklaren de beveiliging en de vertrouwelijkheid van de gegevens te bewaren.

38. Het Comité verzoekt de aanvrager om de noodzakelijk maatregelen te nemen om de loggings te registreren zodat de toegangen kunnen worden gecontroleerd.

DEZE REDENEN

het Comité

1° **machtigt** de aanvrager om voor het doeleinde vermeld in punt 0 en onder de voorwaarden bepaald in deze beraadslaging voor onbepaalde duur het identificatienummer van het Rijksregister te gebruiken.

2° **bepaalt** dat deze machtiging slechts uitwerking zal krijgen wanneer het Comité aan de hand van door de begunstigde van de machtiging verstrekte inlichtingen zal hebben vastgesteld dat hij beschikt over een consulent inzake informatieveiligheid die de nodige waarborgen biedt (zie punt D.1) en dat hij aan de onder punt D.2 vermelde veiligheidsvereisten voldoet. Het Comité wenst hiertoe een naar waarheid ingevulde vragenlijst betreffende de consulent inzake informatiebeveiliging en beveiligingsvragenlijst te ontvangen;

3° **bepaalt** dat de machtiging verleend bij beraadslaging RR nr. 35/2004 komt te vervallen zodra de huidige machtiging in werking treedt;

4° **breidt** de machtiging verleend bij beraadslaging RR nr. 34/2011 uit met de doelgroep professionele gebruikers;

5° **bepaalt** dat bij wijze van overgangsmaatregel de aanvrager het identificatienummer mag gebruiken voor de professionele gebruikers die zij toegang wenst te verlenen tot het milieuloket zonder tussenkomst van de Verantwoordelijke Toegang Entiteit;

6° bepaalt dat deze machtiging van rechtswege een einde neemt indien na afloop van een termijn van één jaar na datum van deze beraadslaging de toegang voor professionele gebruikers niet onderworpen is aan het toezicht van de VTE van de onderneming;

7° bepaalt dat de aanvrager voor afloop van deze termijn een verslag dient te bezorgen aan het Comité over de inpassing van de VTE databank in zijn gebruikers- en toegangsbeheersysteem;

8° bepaalt dat indien op een later tijdstip een wijziging wordt aangebracht aan de organisatie van de informatieveiligheid die een impact kan hebben op de antwoorden die met het veiligheidsformulier aan het Comité werden verstrekt (aanstelling van een consulent inzake informatieveiligheid en antwoorden op de vragen m.b.t. de organisatie van de veiligheid), de aanvrager een nieuwe vragenlijst i.v.m. de stand van de informatieveiligheid naar waarheid moet invullen en aan het Comité moet bezorgen. Het Comité meldt de ontvangst ervan en behoudt het recht om daarop later eventueel te reageren;

9° bepaalt dat wanneer het Comité de begunstigde een vragenlijst betreffende de informatieveiligheid stuurt, deze laatste die vragenlijst waarheidsgetrouw moet invullen en terugsturen aan het Comité. Dit laatste zal de ontvangst bevestigen en hierop reageren indien hiertoe aanleiding bestaat.

De Wnd. Administrateur, De Voorzitter,

(get.) Patrick Van Wouwe (get.) Mireille Salmon