Sectoraal comité van het Rijksregister

Beraadslaging RR nr 38/2014 van 14 mei 2014

Betreft: aanvraag van het Agentschap voor Binnenlands Bestuur om het identificatienummer van het Rijksregister te gebruiken voor het gebruikers- en toegangsbeheer (RN-MA-2013-351)

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 het Agentschap voor Binnenlands Bestuur ontvangen op 23/09/2013;

Gelet op de bijkomende informatie ontvangen op 11/10/2013 en 26/11/2013;

Gelet op de aanvraag van het technisch en juridisch advies gericht aan de Federale Overheidsdienst Binnenlandse Zaken op 23/12/2013;

Gelet op de beslissing van het Comité van 22/01/2014 waarbij de behandeling van het dossier werd opgeschort teneinde vanwege het Agentschap voor Binnenlands Bestuur nadere toelichting te

krijgen m.b.t. hun engagement om voor wat de OCMW's betreft met de "Beheer toegangsbeheerders" (BTB) , voorheen VTE, te werken;

Gelet op toelichting van het Agentschap voor Binnenlands Bestuur, ontvangen op 06/03/2014;

Gelet op de beraadslaging RR nr. 26/2014 van 9 april 2014, waarbij het luik van de aanvraag dat betrekking had op het gebruik van het identificatienummer van het Rijksregister van personeelsleden en/of medewerkers van OCMW's met het oog op gebruikers- en toegangsbeheer in toepassing van artikel 31*bis*, § 3, vierde lid, WVP werd overgemaakt aan de Commissie voor de bescherming van de persoonlijke levenssfeer;

De Commissie voor de bescherming van de persoonlijke levenssfeer, hierna de Commissie, boog zich op zitting van 30/04/2014 over de problematiek m.b.t. het gebruik van het identificatienummer van het Rijksregister van personeelsleden en/of medewerkers van OCMW's bij het uitbouwen van het gebruikers- en toegangsbeheer;

In het licht hiervan wordt de beraadslaging RR nr. 26/2014 van 9 april 2014 vervangen door de huidige beraadslaging;

Gelet op het verslag van de Voorzitter;

Beslist op 14 mei 2014, na beraadslaging, als volgt:

I. VOORWERP VAN DE AANVRAAG

1. De aanvraag strekt ertoe om het Agentschap voor Binnenlands Bestuur, hierna de aanvrager, te machtigen om het identificatienummer van het Rijksregister te gebruiken voor het gebruikers– en toegangsbeheer onder meer voor de digitale loketten "Mijn Binnenland" en "Mandatendatabank" evenals voor het digitaal tekenplatform.

II. ONDERZOEK VAN DE AANVRAAG

2. Diverse diensten van de aanvrager werden reeds gemachtigd om het identificatienummer te gebruiken.[1]

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

[1] Beraadslagingen RR nrs. 46/2009, 39/2011, nr. 39/2012.

- de doeleinden waarvoor het gebruik gevraagd wordt, welbepaald, uitdrukkelijk omschreven en gerechtvaardigd zijn in de zin van artikel 4, § 1, 2°, WVP;
- het gebruik van het identificatienummer proportioneel is in het licht van de doeleinden (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.

A. DOELEINDEN

5. De aanvrager wenst het identificatienummer van het Rijksregister te benutten voor het gebruikers- en toegangsbeheer van webtoepassingen en webservices in het algemeen. In eerste instantie beoogt de aanvrager gebruik ervan in een nieuw digitaal platform met daarin de volgende toepassingen en componenten:

- Digitaal Loket "Mijn Binnenland": een portaal waar lokale besturen hun transacties en interacties met de aanvrager digitaal kunnen afhandelen en informatie over lopende en verwerkte dossiers kunnen raadplegen;
- Digitaal loket "Mandatendatabank": een webtoepassing waarin lokale besturen zelf informatie over hun mandatarissen en personeelsaantallen kunnen invoeren;
- Beheersplatform Bestandsuitwisseling: een webtoepassing die garandeert dat digitale documentenstromen gestroomlijnd en veilig verlopen;
- Digitaal Tekenplatform: een webtoepassing voor het plaatsen van digitale handtekeningen.

Het platform zal in de toekomst uitgebreid worden met bijkomende componenten, waar nodig afgeschermd door de module gebruikers- en toegangsbeheer.

6. De aanvrager wenst zo veel als mogelijk de processen waarbij er interactie is met lokale besturen te automatiseren. De vele niet gestructureerde gegevensstromen, veelal op papier, worden vervangen door gestructureerde digitale stromen.

7. De processen in kwestie volgen uit de opdrachten toevertrouwd aan de aanvrager[2], in het bijzonder:

- toezicht op de lokale en provinciale overheden met oog op hun bestuurskwaliteit;
- de voorbereiding van de bestuurlijke regelgeving betreffende de lokale en de provinciale besturen;
- de verdeling en het beheer van het Gemeentefonds, Provinciefonds en Stedenfonds;
- de organisatie van de verkiezingen voor de gemeente- en provincieraden en van de betrokkenheid van de Vlaamse overheid bij de verkiezingen van het Vlaams Parlement;
- de voorbereiding van het administratief toezicht op de lokale en provinciale besturen;
- toezicht op de eredienstinstellingen.

8. De taak bestuurlijk toezicht wordt verder geconcretiseerd in organieke bepalingen aangaande gemeenten[3], intergemeentelijke samenwerkingsverbanden[4], provincies[5], OCMW's[6], e.a. Verder verwijst de aanvrager naar heel wat specifieke bepalingen waarin wordt vastgelegd welke documenten en informatie de respectieve besturen en instanties dienen te bezorgen aan de toezichthoudende overheid.

9. Bij de validatie van digitale handtekeningen wenst de aanvrager, in bepaalde gevallen, als extra stap na te gaan of de ondertekenaar identiek is aan de ingelogde persoon. Dit gebeurt door het identificatienummer in het handtekeningscertificaat te vergelijken met het nummer van de persoon ingelogd in de betreffende webtoepassing.

10. Het Comité is van oordeel dat de hierboven vermelde en nagestreefde doeleinden welbepaald, uitdrukkelijk omschreven en gerechtvaardigd zijn in de zin van artikel 4, § 1, 2°, WVP en artikel 5, tweede lid, WRR. De verwerkingen die de aanvrager verricht zijn gestoeld op artikel 5, eerste lid, e), WVP.

---

[2] Art. 4 van het besluit van de Vlaamse Regering van 28 oktober 2005 *tot oprichting van het intern verzelfstandigd agentschap "Agentschap voor Binnenlands Bestuur"*.

[3] Het gemeentedecreet van 15 juli 2005.

[4] Het decreet van 6 juli 2001 *houdende de intergemeentelijke samenwerking*.

[5] Het provinciedecreet van 9 december 2005.

[6] Het decreet 19 december 2008 *betreffende de organisatie van de openbare centra voor maatschappelijk welzijn*.

B. PROPORTIONALITEIT

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

11. De aanvrager wenst het identificatienummer van het rijksregister te gebruiken van medewerkers en mandatarissen (hierna de "gebruikers" genoemd) van de lokale en provinciale besturen waarmee de aanvrager werkt, zijnde: gemeenten, districten, autonome gemeentebedrijven, extern verzelfstandigde agentschappen van gemeenten, intergemeentelijke samenwerkingsverbanden, provincies, autonome provinciebedrijven, extern verzelfstandigde agentschappen van provincies, eredienstbesturen, OCMW's, OCMW-verenigingen, politiezones.

12. 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.

13. 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 web-toepassing of web-service wenst te gebruiken omdat langs deze kanalen enerzijds toegang wordt verleend tot een aantal persoonsgegevens en anderzijds handelingen kunnen worden gesteld.

14. 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.

15. 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.

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

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

17. Er wordt een machtiging voor onbepaalde duur gevraagd, daar de uitvoering en controle van de reglementering waarmee de aanvrager belast is, niet in de tijd beperkt zijn.

18. De Comité stelt vast dat de reglementaire opdracht waarmee de aanvrager is belast, niet in de tijd werd bepaald. In het licht hiervan is een machtiging van onbepaalde duur gepast (artikel 4, § 1, 3°, WVP).

B.3. Ten opzichte van de bewaringstermijn

19. De duur van de bewaringstermijn van het identificatienummer van het Rijksregister is gekoppeld aan de periode van activiteit van een bepaalde gebruiker en de wettelijke vereisten die aan de aanvrager opgelegd worden inzake het bijhouden van specifieke transacties, inclusief de logging. De aanvrager wenst de gegevens te bewaren zolang de doeleinden waarvoor het gebruik van het nummer werd gevraagd dit vereisen en vestigt in dit verband de aandacht op het volgende: zolang gegevens over een dossier bewaard worden in het platform van de aanvrager, is het noodzakelijk de verantwoordelijke voor dit dossier te kennen. De bewaartermijn van dit gegeven is dus rechtstreeks gekoppeld aan de bewaartermijn van de dossiers die de gebruiker behandelt of behandeld heeft. Een concrete bewaringstermijn kan daarom moeilijk vooropgesteld worden. De aanvrager benadrukt wel dat de accounts en de dossiers die niet langer actief zijn, worden gearchiveerd of vernietigd overeenkomstig het archiefdecreet van 9 juli 2010.

20. In de mate dat dit nummer 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. Het platform van de aanvrager zal een aantal webtoepassingen bevatten die gebruikers de mogelijkheid geven verrichtingen te stellen die betrekking hebben op personen. In het kader van het gebruikers- en toegangsbeheer moet geregistreerd worden wanneer een persoon een bepaalde verrichting stelde en op wie deze betrekking had. Dergelijke logging moet toelaten onregelmatigheden of misbruiken vast te stellen. Rekening houdend met het feit dat misbruiken m.b.t. verwerking van persoonsgegevens een strafbaar feit zijn, is het aangewezen dat dergelijke loggings minstens gedurende 10 jaar bewaard worden.

21. In zoverre de aanvrager de hierboven vermelde termijnen in acht neemt, handelt hij conform artikel 4, § 1, 5°, WVP.

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

22. Uit de door de aanvrager meegedeelde informatie blijkt dat het identificatienummer uitsluitend intern zal gebruikt worden, behoudens de uitwisseling met de Vlaamse Dienstenintegrator (cf. hierna luik B.6).

23. Het Comité neemt hiervan akte.

B.5. Netwerkverbindingen

24. De aanvrager wenst voor haar gebruikers- en toegangsbeheersysteem gebruik te maken van de basisdiensten geleverd door de Vlaamse Dienstenintegrator[7], in het bijzonder de dienst VO-ACM/IDM (Vlaamse Overheid- Access Control Management / Identity Management). De dienst VO-ACM/IDM beheert een gebruikersdatabank waarin attributen en rollen van gebruikers (bv. Vlaams ambtenaar, gemeente ambtenaar) gekoppeld worden aan hun identificatienummer.[8]

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

26. Het Comité stelt vast dat het identificatienummer uitsluitend wordt gebruikt voor de uitwisseling van de informatie die noodzakelijk is om het gebruikers- en toegangsbeheer in de praktijk te realiseren zoals beschreven in punt A. De beoogde netwerverbinding is bijgevolg aanvaardbaar.

27. 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.

B.6. Uitbouw gebruikers- en toegangsbeheersysteem

28. De aanvrager geeft aan in de uitbouw van zijn gebruikers- en toegangsbeheersysteem 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*. Enkel in de overblijvende gevallen wenst de aanvrager binnen zijn eigen platform gebruikers en hun attributen te registreren aan de hand van het rijksregisternummer.

---

[7] 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.

[8] De Vlaamse Dienstenintegrator (hierna VDI) 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 en RR nr. 29/2013.

29. De inschakeling van de dienst VO-ACM/IDM van de Vlaamse Dienstenintegrator past in voormelde strategie. De VDI beschikt over verschillende machtigingen tot gebruik van het identificatienummer die in deze context van toepassing zijn:

- Personeelsleden en externe medewerkers, waaronder mandatarissen, van Vlaamse gemeenten en provincies[9];
- Extern verzelfstandigde agentschappen van gemeenten/provincies in privaatrechtelijke vorm[10]
- OCMW-verenigingen in privaatrechtelijke vorm[11].

30. Voormelde machtigingen dekken niet alle lokale besturen waarvoor de aanvrager bevoegd is toezicht uit te oefenen. Uit de aanvraag en de bijkomende toelichting blijkt impliciet de vraag om de machtiging van de VDI uit te breiden tot de ontbrekende doelgroepen, meer bepaald:

- Autonome gemeente- en provinciebedrijven;
- Intergemeentelijke samenwerkingsverbanden;
- OCMW-verenigingen van publiekrecht[12];
- Politiezones;
- Eredienstbesturen;
- OCMW's.

31. De Commissie oordeelde op 30 april 2014 dat het systeem BTB (voorheen VTE-databank, cf. beraadslaging RR nr. 29/2013 en RR nr. 44/2013) dat een wezenlijk bestanddeel vormt van CSAM (Common secure access management) van Fedict door overheidsdiensten moet worden geïntegreerd in het toegangs- en gebruikersbeheer.

32. Zij oordeelde verder dat een sectoraal comité zich niet uitspreekt over de technische modaliteiten in verband met de implementatie van het gebruikers- en toegangsbeheer, voor zover de principes m.b.t. organisatie van dit beheer en de terugkoppeling naar authentieke bronnen gehandeld wordt overeenkomstig de goede praktijken geopperd door de Commissie in:

↳ aanbeveling nr. 01/2008 van 24 september 2008 *met betrekking tot het toegangs- en gebruikersbeheer in de overheidssector*;

---

[9] Beraadslaging RR nr. 34/2011, nr. 9.

[10] 'Professionele gebruikers', cf. beraadslaging RR nr. 29/2013, nr. 22.

[11] Art. 236, 243 en 247/1 van het decreet van 19 december 2008. Het betreft 'Professionele gebruikers' zoals bepaald in beraadslaging RR nr. 29/2013, nr. 22.

[12] Art. 223 van het decreet van 19 december 2008.

↳ aanbeveling nr. 09/2012 van 23 mei 2012 *uit eigen beweging in verband met authentieke gegevensbronnen in de overheidssector;*
↳ aanbeveling nr. 03/2009 uit eigen beweging in verband met integratoren in de overheidssector.

33. Het Comité beaamt dat het inschakelen van het "Beheer Toegangsbeheerders" (BTB) – voorheen 'verantwoordelijke toegang entiteit' (VTE) - de norm moet worden in gebruikers- en toegangsbeheer voor e-government toepassingen om het risico op onrechtmatige toegang tot gegevens te beperken.[13]

34. Het Comité concludeert uit voormelde aanbevelingen dat er een onderlinge integratie moet komen van de gebruikers- en toegangsbeheerssystemen over de overheidsniveaus heen. Dit houdt in dat dienstenintegratoren onderling *credentials* moeten kunnen uitwisselen wanneer medewerkers van de instellingen aangesloten bij één dienstenintegrator toegang moeten hebben tot diensten ontsloten via een andere dienstenintegrator. Deze organisatorische en technische maatregel draagt significant bij tot een coherente beveiliging van de toegang tot vertrouwelijke persoonsgegevens.

35. Het Comité acht het aangewezen de machtiging van de Vlaamse Dienstenintegrator uit te breiden tot de hierboven vermelde rechtspersonen van publiekrecht op voorwaarde dat de BTB databank in het gebruikers- en toegangssysteem ingepast wordt.

C. BEVEILIGING

C.1. Consulent inzake informatiebeveiliging en informatiebeveiligingsbeleid

36. De aanvrager bezorgde een kopie van een evaluatieformulier dat hij anderhalf jaar voordien n.a.v. een andere aanvraag indiende. Het Comité wenst dat een geactualiseerde conformiteitsverklaring en evaluatievragenlijst voor de kandidaat-consulent inzake informatiebeveiliging[14] worden bezorgd zodat het Comité geïnformeerd wordt over de actuele situatie en deze kan beoordelen.

[13] Beraadslaging RR nr. 29/2013, nr. 28.

[14] Indien de betrokkene reeds aanvaard werd als beveiligingsconsulent moeten alleen de eerste 2 bladzijden van het document ingevuld en ondertekend worden bezorgd.

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

37. De medewerkers van de 'service desk' van HP-Belgacom (onderaannemer van de aanvrager) en de lokale beheerders bij de betrokken lokale besturen en entiteiten, zullen het nummer gebruiken.

38. 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.

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

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

OM DEZE REDENEN
het Comité

1°vervangt beraadslaging RR nr. 26/2014 van 9 april 2014 en **machtigt** het Agentschap voor Binnenlands Bestuur en de Vlaamse Dienstenintegrator om voor de doeleinden vermeld in punt A en onder de voorwaarden bepaald in deze beraadslaging voor onbepaalde duur het identificatienummer van het Rijksregister van de doelgroepen vermeld in de beraadslaging te gebruiken.;

Deze machtiging zal slechts uitwerking krijgen nadat:

- het Agentschap voor Binnenlands Bestuur en de Vlaamse Dienstenintegrator aan het Comité een document hebben verstrekt waarin zij zich ertoe verbinden om bij de uitbouw van het gebruikers- en toegangsbeheer het bepaalde in luik B.6. in acht te nemen;
- het Comité aan de hand van door het Agentschap voor Binnenlands Bestuur verstrekte inlichtingen en stukken zal hebben vastgesteld dat zij beschikt over een consulent inzake informatiebeveiliging die de nodige waarborgen biedt en dat zij aan de veiligheidsvereisten voldoet (zie randnummer 34);

2° weigert wat verder werd gevraagd;

3° bepaalt dat indien op een later tijdstip een wijziging wordt aangebracht aan de organisatie van de informatiebeveiliging die een impact kan hebben op de antwoorden die met het veiligheidsformulier aan het Comité werden verstrekt (aanstelling van een consulent inzake informatiebeveiliging en antwoorden op de vragen m.b.t. de organisatie van de beveiliging), het Agentschap voor Binnenlands Bestuur een nieuwe vragenlijst i.v.m. de stand van de informatiebeveiliging naar waarheid moet(en) invullen en aan het Comité moet(en) bezorgen. Het Comité meldt de ontvangst ervan en behoudt het recht om daarop later eventueel te reageren;

4° bepaalt dat wanneer het Comité het Agentschap voor Binnenlands Bestuur een vragenlijst betreffende de informatiebeveiliging 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