Sectoraal comité van het Rijksregister

Beraadslaging RR nr 21/2015 van 25 maart 2015

Betreft: algemene machtiging om het rijksregisternummer te gebruiken bij aanwending van het "Federal Authentication Service" –systeem van FEDICT voor het toegangs- en gebruikersbeheer tot van de informatietoepassingen die ontwikkeld zijn voor opdrachten van algemeen belang (RN-MA-2015-102)

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 technisch en juridisch advies gericht aan de Federale Overheidsdienst Binnenlandse Zaken op 26/11/2014;

Gelet op de vragen die Fedict heeft gesteld ingevolge de beraadslaging nr. 108/2014 goedgekeurd op 10 december 2014, besliste het Comité in zitting op 18 februari 2015 om de beraadslaging nr. 108/2014 te vervangen door onderhavige beraadslaging;

Gelet op de informatie van Fedict, ontvangen op 2 maart 2015;

Gelet op het verslag van de Voorzitter;

Beslist op 25 maart 2015, na beraadslaging, als volgt:

I. ONDERWERP EN CONTEXT VAN DE AANVRAAG

1. Gelet op het groeiend aantal verzoeken om het rijksregisternummer te gebruiken bij de aanwending van het FAS-systeem (Federal Authentication Service) van Fedict, beslist het Comité om onderhavig, eenmalige machtiging goed te keuren. Het Comité nam reeds die beslissing in het kader van de beraadslaging nr. 108/2014 van 10 december 2014 maar gelet op de verschillende vragen en verzoeken om uitleg van Fedict na de publicatie ervan, heeft het Comité op de zitting van 18 februari 2015 beslist het dossier te heropenen en de vorige beraadslaging nr. 108/2014 te vervangen door onderhavige beraadslaging.

2. Dit FAS-systeem kan worden gebruikt door alle overheidsdiensten en –instellingen - ook de ondernemingen of personen belast met een opdracht van openbare dienstverlening - die een beveiligde authenticatieprocedure voor hun informaticatoepassingen willen opzetten middels het afsluiten van een gebruikersovereenkomst met de FOD Informatie- en Communicatietechnologieën. Sommige gebruikers wensen dat Fedict hen in antwoord op ieder authenticatieproces ook het rijksregisternummer van de betrokken personen verstrekt zodat ze kunnen instaan voor het toegangs- en gebruikersbeheer van hun informaticatoepassing.

3. Iedere verantwoordelijke voor de verwerking bedoeld in considerans 10, die aan het Comité een schriftelijke en ondertekende verklaring richt waarin hij zich aansluit bij de voorwaarden van onderhavige, eenmalige machtiging, krijgt toegang tot het Rijksregister en mag het rijksregisternummer gebruiken mits hij de hieronder omschreven voorwaarden eerbiedigt.

4. De naam en het adres van de verantwoordelijken voor de verwerking, die als FAS-gebruiker voor hun gegevensverwerkingen aan het Comité een conformiteitsverklaring hebben gestuurd, onder de voorwaarden vastgesteld in deze beslissing, zullen telkenmale in de bijlage van deze beraadslaging gepubliceerd worden op de website van de Commissie voor de bescherming van de persoonlijke levenssfeer, eens het Comité hen zal hebben ingelicht dat de machtiging voor hen van kracht wordt.

5. Het Comité vestigt de aandacht op het feit dat deze machtiging bedoeld is om de mededelingen in te dekken door Fedict van het rijksregisternummer van de gebruiker[1] van het FAS-systeem. Tot op vandaag kan het FAS-systeem gebruikt worden met deze authenticatiemethodes:

   - identifier met paswoord;
   - identifier met paswoord en token of ander certificaat (zoals een sms of een certificaat uitgereikt door een erkende certificeringsinstantie);
   - elektronische identiteitskaart via een verbonden kaartlezer met pincode;
   - elektronische identiteitskaart via een draadloze kaartlezer zonder pincode.

6. Uit de informatie die Fedict verstrekte, blijkt dat de authenticatiemethode met paswoord en identifier, slechts wordt gebruikt nadat de betrokken persoon zich registreerde met zijn elektronische identiteitskaart[2] (registratieproces om het paswoord en de identifier te verkrijgen die noodzakelijk zijn voor de authenticatie met behulp van de elektronische identiteitskaart).

7. Als de authenticatie van een persoon is geslaagd, verstrekt FAS de positieve authenticatie-informatie waarbij de naam, voornaam en rijksregisternummer van die persoon wordt meegedeeld aan de verantwoordelijke voor de verwerking (in onderhavige machtiging ook omschreven als (”FAS-gebruiker” of “aangeslotene”) zodat hij de toegangen en/of gebruikers (in deze beraadslaging ook omschreven als “betrokken personen”) van zijn informaticatoepassing die op deze authenticatie betrekking hebben zou kunnen beheren.

8. Het Comité kreeg reeds aanvragen om gebruik te maken van het FAS-systeem van Fedict[3] en reageerde daarop steevast gunstig.

---

[1] Onder FAS-gebruiker wordt begrepen de instellingen bedoeld in artikel 5, 1te lid, 1° en 2° die ervoor hebben gekozen gebruik te maken van het FAS-systeem van Fedict voor een beveiligde toegang tot hun informaticatoepassingen.

[2] Men spreekt over de “bootstrap” eID.

[3] Zie daarvoor de volgende RR beraadslagingen: nr. 29/2013 van 17 april 2013 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; nr. 31/2014 van 9 april 2014 betreffende de aanvraag van de Federale Overheidsdienst Personeel en Organisatie voor aanwending van het Rijksregister in het kader van de registratie en authenticatie van de gebruikers van de federale eProcurement toepassingen, nr. 48/2014 van 9 juli 2014 betreffende de aanvraag van het Vlaams Infrastructuurfonds voor Persoonsgebonden Aangelegenheden van het Departement Welzijn, Volksgezondheid en Gezin tot machtiging om het identificatienummer van het Rijksregister te gebruiken voor het gebruikers- en toegangsbeheer van de Inter-VWA-applicatie; nr. 61/2014 van 30 juli 2014 betreffende de aanvraag van Toerisme Vlaanderen om toegang te krijgen tot de informatiegegevens van het Rijksregister en om het identificatienummer ervan te gebruiken met het oog op de opvolging van subsidieaanvragen en de uitbouw van het gebruikers- en toegangsbeheersysteem; nr. 62/2014 van 30 juli 2014 betreffende de aanvraag van de NV Infrabel om het identificatienummer van het Rijksregister te gebruiken met het oog op de organisatie van het toegangs- en gebruikersbeheer van de toepassing Crisscomm en nr. 89/2014 van 29 oktober 2014 betreffende de aanvraag van de FOD Justitie om het Rijksregisternummer te gebruiken met het oog op het e-deposit pilootproject.

II. VOORWAARDEN

A. Verantwoordelijke voor de verwerking, gerechtigde van deze eenmalige machtiging

9. De machtiging om het rijksregisternummer te gebruiken kan worden verleend door het Comité aan "*de Belgische openbare overheden voor de informatiegegevens die zij gemachtigd zijn te kennen uit hoofde van een wet, een decreet of een ordonnantie; en aan de openbare en private instellingen van Belgisch recht voor de informatie die zij nodig hebben voor het vervullen van taken van algemeen belang die hen zijn toevertrouwd door of krachtens een wet, een decreet of een ordonnantie of voor taken die uitdrukkelijk als zodanig erkend worden door het voormelde sectoraal comité*"(artikel 5, 1ste lid, 1° en 2° en artikel 8 van de WRR).

10. Alleen de Belgische, openbare overheden bedoeld in artikel 5, 1ste lid, 1° van de WRR alsook de openbare of private instellingen, bedoeld in artikel 5, 1ste lid, 1° en 2° van de WRR - maar uitsluitend voor de informatie die noodzakelijk is voor de vervulling van de opdrachten van algemeen belang die hen werden toevertrouwd krachtens een wet, decreet of ordonnantie - die aan het Comité een schriftelijke en ondertekende verklaring richten waarin zij zich aansluiten bij de voorwaarden van onderhavige, eenmalige machtiging, zijn gemachtigd om het rijksregisternummer te gebruiken voor de hierna omschreven doeleinden.

11. De betrokken instellingen moeten bij hun verbintenis dat ze de voorwaarden van onderhavige beraadslaging zullen naleven, de ingevulde en ondertekende formulieren voegen met betrekking tot de kandidaat-consulent inzake informatiebeveiliging en de conformiteitsverklaring van zijn beveiligingssysteem zodat het Comité deze kan beoordelen.

B. Doeleinden van de verwerking

12. De conformiteitsverklaring met deze machtiging kan uitsluitend betrekking hebben op het gebruik van het rijksregisternummer door de verantwoordelijke voor de verwerking, FAS-gebruiker, bedoeld in considerans 10, voor het toegangs- en gebruikersbeheer van de informaticatoepassingen, die werden ontwikkeld om hun opdrachten van openbare dienstverlening te kunnen vervullen.

13. Met het FAS-systeem waarbij Fedict het rijksregisternummer van de betrokken persoon meedeelt die zich met succes heeft geauthenticeerd, kan de FAS-gebruiker de toegangen of

de gebruikers van zijn informaticatoepassing beheren. Het toegangsbeheer (met inbegrip van de authenticatie) is een verificatieproces dat de verantwoordelijke voor de verwerking van de informaticatoepassing garandeert dat de betrokken persoon die zich bij zijn informaticatoepassing heeft aangemeld wel degelijk het recht heeft om toegang te krijgen en daadwerkelijk de persoon is die hij beweert te zijn. Zo is een persoonlijke ruimte binnen deze informaticatoepassing alleen toegankelijk voor de persoon die daar toegangsrechten op heeft. Het beheer van de gebruikers bestaat uit het beheer van specifieke rechten (zoals lezen, schrijven,…) binnen die informaticatoepassing waarover de betrokken personen soms beschikken in functie van de hun toegekende rol of mandaten. De bedoelde informaticatoepassingen hebben inderdaad gewoonlijk als doel om de betrokken personen de mogelijkheid te bieden gemakkelijker hun dossier in te kijken, de nodige wijzigingen op te volgen of aan te brengen, om verzoeken in te dienen of documenten te versturen.

C. Rijksregisternummer van de natuurlijke personen

14. Om te vermijden dat onbevoegde personen toegang hebben tot de informatie via de informaticatoepassing van de aangesloten partijen bij deze beraadslaging, moeten zij heel precies geïdentificeerd worden zodat hen een gepast toegangsrecht kan worden toegekend[4].

15. Dit betekent dat iedere vergissing ingevolge homoniemen of spelfouten moet worden uitgesloten om te vermijden dat de identificatie en authenticatie in een verdere fase in gevaar worden gebracht. De elektronische identificatie, authenticatie en machtiging moeten veilig en beveiligd gebeuren. De instelling die haar informaticatoepassing of webservice ter beschikking stelt, moet zeker zijn van de identiteit van de persoon die er gebruik wenst van te maken omdat hij via deze kanalen toegang kan krijgen tot een bepaald aantal persoonsgegevens enerzijds en bepaalde verrichtingen kan uitvoeren anderzijds.

16. Het rijksregisternummer is een passend instrument voor het toegangs- en gebruikersbeheer van een informaticatoepassing. Het gaat om een uniek nummer waarmee een persoon met grote nauwkeurigheid kan worden geïdentificeerd. Hiermee worden namelijk fouten door homoniemen of spelfouten uitgesloten.

17. Het finaliteitsbeginsel houdt in dat elke gerechtigde van een machtiging die een gemachtigde gegevensverwerking verricht voor een doeleinde dat onverenigbaar is met het

[4] Zie hiervoor de beraadslaging nr. 62/2014 van 30 juli 2014 *betreffende de aanvraag van de NV Infrabel om het identificatienummer van het Rijksregister te gebruiken met het oog op de organisatie van het toegangs- en gebruikersbeheer van de toepassing Crisscomm*, blz. 4 punt 11.

doeleinde waarvoor hij werd gemachtigd, een strafbaar feit begaat (artikel 13 WRR en 39 WVP).

D. Duur van deze machtiging

18. De verantwoordelijke voor de verwerking die wil aansluiten kan de algemene machtiging enkel doen gelden voor de levensduur van zijn informaticatoepassing die werd ontwikkeld voor de vervulling van zijn opdrachten van openbare dienstverlening en die gebruik maakt van het FAS-systeem. Zodra de betrokken informaticatoepassing wordt verwijderd, verbindt de aangeslotene er zich toe om dit feit onverwijld aan het Comité mee te delen.

19. Gelet op deze elementen en op voorwaarde dat die voorwaarde wordt nageleefd, is een machtiging van onbepaalde duur gepast (artikel 4, §1, 3° van de WVP).

E. De bewaartermijn

20. Het Comité stelt vast dat het moeilijk is een concrete bewaartermijn te bepalen. Het rijksregisternummer moet bewaard worden zolang het noodzakelijk is de ter beschikking gestelde informaticatoepassing of de webservice te gebruiken.

21. Overigens, als het rijksregisternummer van de betrokken personen wordt bewaard in de loggings ter garantie van de opspoorbaarheid van de raadplegingen of de gedane verrichtingen, is de bewaartermijn van het rijksregisternummer in principe minimum 10 jaar[5]. Het moet voor het toegangs- en gebruikersbeheer inderdaad mogelijk zijn om onregelmatigheden of misbruiken vast te stellen. Gelet op het feit dat een misbruik van verwerkingen op persoonsgegevens strafbaar is, is het aangewezen dat dergelijke loggings gedurende tenminste 10 jaar worden bewaard.

22. Op voorwaarde dat de aangesloten partij, het rijksregisternummer bewaart zolang dat noodzakelijk is voor het toegangs- en gebruikersbeheer van zijn informaticatoepassing, met inbegrip van het bewaren van de loggings die aan een bepaalde periode verbonden zijn zodat hij kan instaan voor het beheer van eventuele voorkomende geschillen, handelt hij in overeenstemming met artikel 4, §1, 5° van de WVP.

---

[5] Zie hiervoor de beraadslaging RR nr. 70/2012 van 5 september 2012 aanvraag tot herziening van de beraadslaging RR nr. 34/2012, punt 18.

F. Intern gebruik en/of mededeling aan derden – eventuele ontvangers

23. Het rijksregisternummer zal uitsluitend intern gebruikt worden door de personeelsleden van de verantwoordelijke voor de verwerking die belast werden met de verwezenlijking van het voormelde doeleinde. Het Comité benadrukt overigens dat het rijksregisternummer uitsluitend mag gebruikt worden in het kader van de toepassingen en/of webservices van de betrokken verantwoordelijken voor de verwerking, ontwikkeld in het kader van hun opdrachten van openbaar belang. Indien de betrokken instelling het rijksregisternummer moet verbinden aan een intern nummer, benadrukt het Comité dat zulks slecht kan voor de verwezenlijking van het voormelde doeleinde. De voornoemde verantwoordelijken voor de verwerking mogen overigens het rijksregisternummer enkel bewaren binnen dit kader.

G. Netwerkverbindingen

24. Uit de informatie die Fedict heeft verstrekt, blijkt dat het gebruik van het rijksregisternummer voor het toegangs- en gebruikersbeheer geen netwerkverbinding vergt.

25. Om volledig te zijn, vestigt het Comité de aandacht erop dat:
    - wanneer er later netwerkverbindingen tot stand komen, de aanvrager het Comité hiervan vooraf moet inlichten;
    - het rijksregisternummer uitsluitend in relatie met derden mag worden gebruikt mits dit valt binnen het kader van de doeleinden waarvoor deze derden eveneens gemachtigd werden dit nummer te gebruiken.

H. Veiligheid

H.1. Consulent inzake Informatiebeveiliging

26. De verantwoordelijke voor de verwerking moet een consulent inzake informatiebeveiliging aanstellen. Deze moet in volledige onafhankelijkheid kunnen oordelen over de veiligheid van de informatie.

27. De identiteit van de consulent inzake informatiebeveiliging moet samen met de aanvraag voor aansluiting bij voorliggende algemene machtiging aan het Sectoraal Comité worden meegedeeld middels de evaluatievragenlijst inzake de kandidaat-consulent inzake informatiebeveiliging.

H.2. informatiebeveiligingsbeleid

28. Er is ook een beveiligingsbeleid ingevoerd waarbij rekening wordt gehouden met de referentiesmaatregelen voor elke verwerking van persoonsgegevens, uitgevaardigd door de Commissie voor de bescherming van de persoonlijke levenssfeer en beschikbaar is op haar website. Dit beleid moet op het terrein in de praktijk worden gebracht zodat de gegevensverwerkingen die werden verricht voor de voormelde doeleinden zowel op organisatorisch als technisch vlak afdoende beveiligd zijn.

29. Alle nuttige informatie hierover wordt bezorgd aan het Sectoraal Comité van het Rijksregister tezelfdertijd met de aanvraag voor aansluiting via de verklaring ad hoc, zodat het Comité in alle onafhankelijkheid de beveiliging van de informatie kan onderzoeken.

H.3. Personen die het identificatienummer gebruiken en lijst van die personen

30. Alleen de personeelsleden van de aangesloten partij, belast met de verwezenlijking van het doeleinde als omschreven onder punt B van deze beraadslaging, mogen het rijksregisternummer gebruiken.

H.4. Onderaanneming

31. Wanneer beroep wordt gedaan op een verwerker voor de hierboven omschreven verwerkingen, moet de gerechtigde van deze eenmalige machtiging een kwaliteitsvolle verwerker kiezen en zijn relatie met die laatste omkaderen met een contract dat beantwoordt aan het vereiste van artikel 16 §1 van de WVP.

I. Toegangs- en gebruikersbeheer met betrekking tot de rol, het mandaat of de hoedanigheid die aan de betrokken personen werden toegekend

32. De aangesloten partijen die beroep doen op het FAS-systeem van Fedict voor hun informaticatoepassingen, waarvan het gebruikers- en toegangsbeheer gebeurt in functie van de/het specifieke rol/hoedanigheid/mandaat waarmee de betrokken personen zijn belast, moeten gebruik maken van het BTB-systeem beheerd door Fedict en dat integraal deel uitmaakt van CSAM. Hiermee kan immers geverifieerd worden of hun gebruikers- en toegangsbeheer voor wat de toegang betreft tot de webtoepassing, gebeurt in functie van d specifieke mandaten, hoedanigheid of rol die aan de betrokken personen werd toegekend.

33. De Commissie oordeelde in de hiernavolgende aanbevelingen overigens dat een sectoraal comité zich niet diende uit te spreken over de technische modaliteiten m.b.t. de organisatie van het toegangs- en gebruikersbeheer, omdat de beginsels inzake de organisatie van dergelijk beheer en het bevragen van authentieke bronnen overeenkomstig de goede praktijk eerst door de Commissie wordt behandeld:

    - de aanbeveling nr.01/2008van 24 september 2008 met betrekking tot het toegangs- en gebruikersbeheer in de overheidssector;
    - aanbeveling uit eigen beweging nr. 09/2012 van 23 mei 2012 in verband met authentieke gegevensbronnen in de overheidssector;
    - aanbeveling uit eigen beweging nr. 03/2009 van 1 juli 2009 in verband met integratoren in de overheidssector.

34. Het Comité gaat akkoord met het feit dat gebruikmaking van het BTB-Systeem de norm moet worden binnen het toegangs- en gebruikersbeheer voor de e-government-applicaties, dit om het risico op onrechtmatige toegang tot de gegevens te beperken. Bijgevolg moet de aangesloten partij die tegemoet komt aan de voorwaarden, bedoeld onder punt 33 van deze beraadslaging, voor zijn toegangsbeheer gebruik maken van het GGA-systeem.

OM DIE REDENEN

Het Comité

1° machtigt iedere openbare overheid en instelling, bedoeld in considerans 10 hierboven, die aan het Comté een schriftelijke en ondertekende verbintenis richten waarin zij verklaren zich aan te sluiten bij de voorwaarden uiteengezet in deze beraadslaging, om voor onbepaalde duur het rijksregisternummer te gebruiken voor de verwezenlijking van het in punt B omschreven doeleinde;

Iedere aanvraag om gerechtigde te worden van deze algemene machtiging moet, op straffe van niet ontvankelijkheid worden gericht aan het Sectoraal Comité van het Rijksregister en ondertekend door de verantwoordelijke voor de verwerking, die zich ertoe verbindt de voorwaarden van deze algemene machtiging te vervullen, aan de hand van het volledig ingevuld aansluitingsformulier dat beschikbaar is op de website van de Commissie samen met de verklaringen betreffende de veiligheid en de evaluatievragenlijst betreffende de consulent inzake informatiebeveiliging. Het Sectoraal comité van het Rijksregister zal na onderzoek, de aangeslotene in kennis stellen van de datum waarop de algemene machtiging voor hem in werking treedt.

2° **bepaalt** dat FEDICT de instellingen pas toegang zal verlenen tot het FAS-systeem als deze verantwoordelijken voor de verwerking hebben voldaan aan de vereisten als omschreven in deze beraadslaging;

3° 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 uit de vragenlijsten betreffende de veiligheid dat aan het Comité werd 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.

4° bepaalt dat wanneer het Comité de gerechtigden van deze machtiging een vragenlijst over het veiligheidsniveau van de informatie toestuurt, de aanvrager deze vragenlijst naar waarheid moet invullen en naar het Comité moet terugsturen. Het Comité meldt de ontvangst ervan en behoudt het recht om daarop later eventueel te reageren.

Voor de Wnd. Administrateur, afw. De Voorzitter,

(get.) An Machtens (get.) Mireille Salmon
Wnd. Afdelingshoofd ORM