Informatieveiligheidscomité
Kamer federale overheid

BERAADSLAGING NR. 20/057 VAN 3 NOVEMBER 2020 BETREFFENDE DE MEDEDELING VAN PERSOONSGEGEVENS DOOR DE FOD FINANCIEN AAN DE FOD BOSA IN HET KADER VAN HET TESTEN VAN HET AANLEGGEN VAN EEN AUDIT TRAIL BIJ HET GEBRUIK VAN DE EBOX VOOR NATUURLIJKE PERSONEN

Gelet op de wet van 15 augustus 2012 *houdende oprichting en organisatie van een federale dienstenintegrator*, in het bijzonder artikel 35/1, §1, eerste lid en §2;

Gelet op de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit, in het bijzonder de artikelen 111 en 114;

Gelet op de wet van 5 september 2018 *tot oprichting van het informatieveiligheidscomité en tot wijziging van diverse wetten betreffende de uitvoering van verordening (EU) 2016/679 van 27 april 2016 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van richtlijn*, in het bijzonder artikel 98;

Gelet op de aanvraag van de FOD Beleid en Ondersteuning;

Gelet op het verslag van de voorzitster.

I. ONDERWERP

1. Het voormalig Sectoraal comité van het Rijksregister heeft bij beraadslaging nr. 19/2008 van 7 mei 2008 de toelating verleend aan de Federale Overheidsdienst Informatie en Communicatietechnologie (hierna 'Fedict') om toegang te hebben tot de informatiegegevens van het Rijksregister en om het identificatienummer ervan te gebruiken met het oog op het testen, het corrigeren en het onderhoud van computertoepassingen die via UME, FSB en Web Services een verbinding hebben met het Rijksregister.

2. Het voormalig Sectoraal comité van het Rijksregister heeft in voormelde beraadslaging vastgesteld dat Fedict - met het oog op een kwaliteitsvolle dienstverlening - regelmatig computertoepassingen moet testen, eventueel corrigeren en onderhouden die een verbinding hebben met het Rijksregister, en andere authentieke bronnen zoals de KSZ, via de UME, FSB en de Web Services. Slechts op die manier kunnen de efficiënte werking, de veiligheid en de continue beschikbaarheid van een toepassing worden verzekerd. Bij deze testen worden de computertoepassingen gebruikt en komt er dus een toegang tot de authentieke bron, destijds het Rijksregister, tot stand alsof het om een echte transactie gaat. Ook het

identificatienummer wordt gebruikt alsof het om een echte transactie met de authentieke bron gaat. Zonder het uitvoeren van reële transacties is het testen niet efficiënt en kunnen de toepassingen niet gecorrigeerd en onderhouden worden. De toegang tot de gegevens van het Rijksregister en het gebruik van het Rijksregisternummer werden bijgevolg toegestaan, mits een aantal strikte veiligheidsvoorwaarden werden nageleefd:
- de functionaris voor gegevensbescherming (destijds veiligheidsconsulent) van de aanvrager stelt voorafgaand aan de interne test-, correctie- en onderhoudswerkzaamheden de populatie vast op dewelke mag getest worden;
- deze populatie bevat maximaal 10.000 personen;
- de functionaris voor gegevensbescherming houdt nauwgezet toezicht op het respecteren van deze parameters door de personen die concreet de werkzaamheden verrichten.

3. In uitvoering van het koninklijk besluit van 22 februari 2017 *houdende oprichting van de Federale Overheidsdienst Beleid en Ondersteuning* heeft de Federale Overheidsdienst Beleid en Ondersteuning (hierna 'FOD BOSA') de opdrachten en bevoegdheden van de Fedict overgenomen en gecontinueerd[1].

4. Overeenkomstig de wet van 27 februari 2019 *inzake de elektronische uitwisseling van berichten via de eBox* werd de FOD BOSA belast met het aanbieden van een eBox voor natuurlijke personen. De eBox is een beveiligde elektronische brievenbus waarmee overheidsinstanties enerzijds en burgers en ondernemingen anderzijds berichten kunnen uitwisselen.

5. Overeenkomstig artikel 8 van voormelde wet van 27 februari 2019 is de FOD BOSA bij het aanbieden en beheren van de eBox als verwerkingsverantwoordelijke evenals de gebruikers van de eBox voor het uitwisselen van berichten gemachtigd om het Rijksregisternummer te gebruiken voor identificatie en authenticatie van de natuurlijke persoon en voor communicatie tussen de gebruikers en de bestemmelingen.

6. Bij het aanbieden en beheren van de eBox moet de FOD BOSA de nodige technische en organisatorische maatregelen nemen om een op het risico afgestemd beveiligingsniveau te waarborgen en die onder meer de oorsprong en de integriteit van de inhoud van het bericht verzekeren en de vertrouwelijkheid van de inhoud van het bericht waarborgen. FOD BOSA gebruikt ook veilige informaticatechnieken die:
- de gebruiker en de bestemmeling ondubbelzinnig identificeren en authenticeren en het tijdstip van de verzending en ontvangst ondubbelzinnig vaststellen;
- een bewijs van verzending en ontvangst van de zending registreren in het systeem en ter beschikking stellen;
- de identiteit van de gebruiker en de bestemmeling, het tijdstip van de verzending en de ontvangst, de kennisgeving en het uniek nummer toegekend aan het bericht registreren;
- systeemfouten vaststellen en de tijdstippen registreren waarop systeemfouten verhinderen dat er wordt verzonden of ontvangen en deze informatie beschikbaar maken voor de belanghebbenden.[2]

[1] Cfr. art. 7 en het Verslag aan de Koning bij voormeld koninklijk besluit van 22 februari 2017.
[2] Art. 4 van voormelde wet van 27 februari 2019.

7. Een essentieel onderdeel van afdoende technische en organisatorische maatregelen waarin de FOD BOSA moet voorzien, is de vereiste om een *audit trail* aan te leggen: wie heeft op welk ogenblik toegang gehad tot het informatiesysteem en welke verwerkingen werden via dit systeem uitgevoerd. Zodoende kan vastgesteld worden of iemand oneigenlijk gebruik van een informatiesysteem gemaakt heeft of een poging hiertoe ondernomen heeft, kunnen de bevoegde gebruikers van een informatiesysteem verantwoordelijk worden gesteld voor hun handelingen, kunnen incidenten gereconstrueerd worden en kan worden aangetoond of bepaalde wettelijke of reglementaire voorwaarden met betrekking tot de duur of modaliteiten van bewaring en consultatie van gegevens worden nageleefd.

8. De FOD BOSA wenst thans als aanbieder en beheerder van de eBox in samenwerking met de FOD Financiën een test uit te voeren om een *audit trail* bij het gebruik van de eBox (i.e. de verzending van een bericht door een overheidsinstelling aan een burger) aan te leggen. In principe worden tests in een testomgeving uitgevoerd doch in dit geval is de integratieomgeving van de FOD Financiën ontoereikend om een efficiënte test uit te voeren.

9. De test betreft uitsluitend het aanleggen van een *audit trail* in het kader van het gebruik van de eBox: welke instelling (in casu FOD Financiën) heeft op welk ogenblik een bericht verzonden aan welke natuurlijke persoon. Het bericht in kwestie is slechts de mededeling aan de betrokkene dat zijn belastingaangifte of een voorstel van vereenvoudigde aangifte beschikbaar is op de website van de FOD Financiën. De gegevens die noodzakelijk zijn om de test met reële berichten uit te voeren, zijn de volgende:

- Timestamp (tijdsaanduiding van de verzending van het bericht)
- Object_ID_Hashed (RRN of the attendee) - one-way hash van het RRN, SHA-256
- Document provider ID (identificatie van de FOD Financiën)
- API call response code (informatie of een burger consent voor het gebruik van de eBox gegeven heeft of niet)

II. ONDERZOEK VAN DE AANVRAAG

A. BEVOEGDHEID VAN HET COMITE

10. Overeenkomstig art. 35/1, § 1 van de wet van 15 augustus 2012 *houdende oprichting en organisatie van een federale dienstenintegrator* vereist de mededeling van persoonsgegevens door overheidsdiensten en openbare instellingen van de federale overheid aan andere derden dan de instellingen van sociale zekerheid bedoeld in artikel 2, eerste lid, 2°, van de wet van 15 januari 1990 *houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid*, vergt een voorafgaande beraadslaging van de kamer federale overheid van het informatieveiligheidscomité, voor zover de verwerkingsverantwoordelijken van de meedelende instantie en de ontvangende instanties, in uitvoering van artikel 20 van de wet van 30 juli 2018 *betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens*, niet tot een akkoord komen over de mededeling of minstens één van die verwerkingsverantwoordelijken om een beraadslaging verzoekt en de andere verwerkingsverantwoordelijken daarvan in kennis heeft gesteld.

11. Art. 35/1, §2 van voormelde wet van 15 augustus 2012 voorziet er bovendien in dat de kamer federale overheid van het Informatieveiligheidscomité in voorkomend geval een beraadslaging verleent voor het gebruik van het identificatienummer van het Rijksregister

van de natuurlijke personen door de betrokken instanties indien dat noodzakelijk is in het kader van de beoogde mededeling.

12. Het Informatieveiligheidscomité is bijgevolg bevoegd om zich over de beoogde mededeling en het gebruik van het Rijksregisternummer uit te spreken .

B. TEN GRONDE

B.1. VERANTWOORDINGSPLICHT

13. Overeenkomstig artikel 5.2 van de Algemene Verordening Gegevensbescherming (hierna 'AVG' genoemd) zijn de FOD BOSA en de FOD Financiën als verwerkingsverantwoordelijken verantwoordelijk voor het naleven van de beginselen van de AVG en moeten ze in staat zijn dit aan te tonen.

14. Het Informatieveiligheidscomité wijst erop dat de verantwoordelijke voor de verwerking een register van de verwerkingsactiviteiten die onder zijn verantwoordelijkheid plaatsvinden, moet bijhouden overeenkomstig de voorwaarden opgenomen in artikel 30 AVG.

B.2. RECHTMATIGHEID

15. Overeenkomstig art. 5.1 a) AVG moeten persoonsgegevens worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig is. Dit houdt in dat de beoogde verwerking een basis moet vinden in één van de rechtmatigheidsgronden vermeld in artikel 6 AVG.

16. Het Comité stelt vast dat de verwerking noodzakelijk is voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen (art. 6.1 e) AVG). De FOD BOSA heeft, krachtens de wet van 27 februari 2019 *inzake de elektronische uitwisseling van berichten via de eBox* de opdracht om een eBox voor natuurlijke personen aan te bieden. Het dient hierbij de nodige technische en organisatorische maatregelen te treffen om de veiligheid en de confidentialiteit van de gegevens te verzekeren, wat inhoudt dat een *audit trail* moet worden vastgelegd, in samenwerking met de verzenders van de berichten, in casu de FOD Financiën.

17. Gelet op het voorgaande, acht het Informatieveiligheidscomité de beoogde verwerking van persoonsgegevens rechtmatig.

B.3. DOELBINDING

18. Artikel 5.1 b) AVG laat de verwerking van persoonsgegevens slechts toe voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden (principe van doelbinding).

19. Voor de uitvoering van zijn wettelijke opdracht en voor een kwaliteitsvolle dienstverlening, is het noodzakelijk dat de FOD BOSA toepassingen kan testen, eventueel corrigeren en onderhouden. Slechts op die manier kunnen de efficiënte werking, de veiligheid en de continue beschikbaarheid van een toepassing worden verzekerd. Zonder het uitvoeren van reële transacties is het testen in casu echter niet efficiënt en kunnen de toepassingen niet gecorrigeerd en onderhouden worden.

20. Gelet op het voorgaande acht het Informatieveiligheidscomité de doeleinden van de beoogde mededeling van persoonsgegevens als welbepaald, uitdrukkelijk omschreven en gerechtvaardigd.

21. Artikel 5.1 b) AVG stelt tevens dat persoonsgegevens niet verder mogen worden verwerkt op een met de oorspronkelijke doeleinden onverenigbare wijze. Om na te gaan of een doel

van verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens aanvankelijk zijn verzameld, moet de verwerkingsverantwoordelijke, nadat hij aan alle voorschriften inzake rechtmatigheid van de oorspronkelijke verwerking heeft voldaan, onder meer rekening houden met: een eventuele koppeling tussen die doeleinden en de doeleinden van de voorgenomen verdere verwerking; het kader waarin de gegevens zijn verzameld; met name de redelijke verwachtingen van de betrokkenen op basis van hun verhouding met de verwerkingsverantwoordelijke betreffende het verdere gebruik ervan; de aard van de persoonsgegevens; de gevolgen van de voorgenomen verdere verwerking voor de betrokkenen; en passende waarborgen bij zowel de oorspronkelijke als de voorgenomen verdere verwerkingen.

22. Gelet op de wet van 27 februari 2019 *inzake de elektronische uitwisseling van berichten via de eBox*, waarbij het gebruik van het Rijksregisternummer werd opgelegd, en het feit dat de FOD BOSA als verwerkingsverantwoordelijke moet voorzien in afdoende technische en organisatorische maatregelen, inclusief het aanleggen van een *audit trail*, en het gebruik van reële transacties noodzakelijk is voor efficiënt testen, stelt het Informatieveiligheidscomité vast dat er een voldoende koppeling is tussen de doeleinden van de oorspronkelijke inzameling en de doeleinden van de voorgenomen verdere verwerking. Het Informatieveiligheidscomité is dan ook van oordeel dat het doel van de verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens aanvankelijk zijn verzameld

B.4. PROPORTIONALITEIT

B.4.1. Minimale gegevensverwerking

23. Artikel 5.1 b) AVG stelt dat persoonsgegevens ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt, moeten zijn ("minimale gegevensverwerking").

24. Het Informatieveiligheidscomité stelt vast dat de beoogde verwerking van persoonsgegevens, gelet op het doeleinde, beperkt blijft tot de technische gegevens van het bericht en de identificatie van de verzender (de FOD Financiën) en de gehashte identificatie van de bestemmeling (een natuurlijke persoon). Naar analogie met de beslissing van het voormalig Sectoraal comité van het Rijksregister, acht het Informatieveiligheidscomité het aanvaardbaar dat de FOD BOSA de tests kan uitvoeren met reële gegevens in productieomgeving teneinde een *audit trail* te kunnen aanleggen. Het Informatieveiligheidscomité acht het evenwel noodzakelijk dat deze verwerking onderworpen wordt aan volgende voorwaarden:

- de functionaris voor gegevensbescherming van de FOD BOSA stelt voorafgaand aan de interne test-, correctie- en onderhoudswerkzaamheden de populatie vast op dewelke mag getest worden;
- deze populatie bevat maximaal 10.000 personen;
- de functionaris voor gegevensbescherming houdt nauwgezet toezicht op het respecteren van deze parameters door de personen die concreet de werkzaamheden verrichten.

25. Rekening houdend met voormelde voorwaarden, acht het Informatieveiligheidscomité de persoonsgegevens ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt.

B.4.2. Opslagbeperking

26. Aangaande de bewaringstermijn herinnert het Comité er aan dat persoonsgegevens niet langer mogen worden bewaard in een vorm die het mogelijk maakt de betrokkenen te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is.

27. Het Informatieveiligheidscomité neemt akte van het feit dat indien de test niet succesvol is, de gegevens onmiddellijk worden vernietigd. Indien de test succesvol is, worden de gegevens tijdelijk bewaard om te kunnen bewijzen dat de aanvrager en de document sender een succesvolle audit trail hebben aangelegd. In het licht hiervan is het Comité van oordeel dat een bewaringstermijn van de testresultaten van maximum 6 maanden aanvaardbaar is.

B.5. BEVEILIGING

28. Persoonsgegevens moeten door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging („integriteit en vertrouwelijkheid").

29. Het Informatieveiligheidscomité stelt vast dat de FOD BOSA over een functionaris voor gegevensbescherming beschikt en ertoe gehouden is om de richtlijnen inzake beveiliging die gelden voor alle federale overheidsinstellingen opgenomen in het Federaal Beleid voor Informatiebeveiliging (Federal Information Security Policy) te respecteren.

30. Het Informatieveiligheidscomité noteert dat de test in kwestie zal worden uitgevoerd door één, geïdentificeerde persoon van het Directoraat-Generaal Digitale Transformatie van de FOD BOSA, die bovendien een confidentialiteitsverklaring heeft ondertekend. In overleg met de functionaris voor gegevensbescherming van de FOD BOSA wordt het aantal noodzakelijk cases vastgelegd, met een maximum van 10.000. Na de reconstructie van de *audit trail* in samenwerking met de FOD Financiën worden de testgegevens vernietigd na een maximale bewaartermijn van 6 maanden.

31. Het Informatieveiligheidscomité stelt vast dat in het kader van de beoogde test het Rijksregisternummer zou worden gehashed, meer bepaald door middel van een one-way hash SHA 256. Het comité merkt vooreerst op dat een gehashed Rijksregisternummer geen Rijksregisternummer meer is, waardoor mogelijks niet alle beoogde tests zouden kunnen worden uitgevoerd. Bovendien heeft het gebruik van een SHA-256 tot gevolg dat er slechts 36,5 miljoen mogelijkheden zijn en dat een correspondentietabel op een paar seconden kan worden opgemaakt. Het comité is van mening dat indien de FOD BOSA meer dan een symbolische veiligheid wil bekomen, eerder SHA-256 1 miljard keer moet worden toegepast, of nog beter, een hashfunctie zoals Argon2 moet gebruiken met parameters die er voor zorgen dat het hashen van 1 Rijksregisternummer 30-60 seconden duurt en 1 Gbyte RAM vraagt. Op die manier vraagt het terugrekenen of het maken van een tabel een behoorlijke inspanning. Indien de FOD BOSA bovendien wil het hashresultaat wordt afgebeeld als een Rijksregisternummer, kan een *format preserving encryption* gebruiken, al vraagt dit dan wel

het beheer van een geheime sleutel[3]. Het Informatieveiligheidscomité stelt dan ook dat de FOD BOSA in samenwerking met haar functionaris voor gegevensbescherming een hashfunctie dient toe te passen dat een daadwerkelijk én afdoende beveiliging garandeert.

32. Het Comité wijst erop dat artikel 35 AVG in bepaalde gevallen vereist dat de verwerkingsverantwoordelijke vóór de verwerking een beoordeling uitvoert van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens. Het Comité verwijst hieromtrent naar de 'Richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking "waarschijnlijk een hoog risico inhoudt" in de zin van Verordening 2016/679' van de Groep Gegevensbescherming Artikel 29 en de aanbeveling uit eigen beweging nr. 01/2018 van 28 februari 2018 van de Commissie voor de bescherming van de persoonlijke levenssfeer met betrekking tot de gegevensbeschermingseffectbeoordeling en voorafgaande raadpleging .

33. Indien uit deze beoordeling zou blijken dat bijkomende maatregelen moeten worden getroffen, dienen de betrokken partijen op eigen initiatief een aanvraag tot wijziging van onderhavige beraadslaging in. De mededeling van persoonsgegevens mag in voorkomend geval niet plaatsvinden totdat de vereiste toelating van het Comité is bekomen. Indien uit de gegevensbeschermingseffectbeoordeling zou blijken dat er een hoog residuair risico is, dient de aanvrager de beoogde gegevensverwerking voor te leggen aan de Gegevensbeschermingsautoriteit, overeenkomst art. 36.1 AVG.

[3] https://csrc.nist.gov/publications/detail/sp/800-38g/final

Om deze redenen besluit

de kamer federale overheid van het Informatieveiligheidscomité

dat de mededeling van persoonsgegevens door de FOD Financiën aan de FOD BOSA in het kader van het testen van het aanleggen van een *audit trail* bij het gebruik van de eBox voor natuurlijke personen is toegestaan, mits wordt voldaan aan de vastgestelde maatregelen ter waarborging van de gegevensbescherming, in het bijzonder de maatregelen op het vlak van doelbinding, minimale gegevensverwerking, opslagbeperking en informatieveiligheid, op voorwaarde dat:

- de functionaris voor gegevensbescherming van de FOD BOSA stelt voorafgaand aan de interne test-, correctie- en onderhoudswerkzaamheden de populatie vast op dewelke mag getest worden;
- deze populatie bevat maximaal 10.000 personen;
- de functionaris voor gegevensbescherming houdt nauwgezet toezicht op het respecteren van deze parameters door de personen die concreet de werkzaamheden verrichten;
- voor de hashing van het Rijksregisternummer in samenwerking met de functionaris voor gegevensbescherming een hashfunctie wordt toegepast dat een daadwerkelijke en afdoende beveiliging garandeert (zie randnummer 31).

Krachtens artikel 35/1, §2, van de wet van 15 augustus 2012 *houdende oprichting en organisatie van een federale dienstenintegrator* staat het Informatieveiligheidscomité toe dat FOD BOSA het Rijksregisternummer, in gehashte vorm, in productieomgeving gebruikt voor het doeleinde van het testen van het aanleggen van een *audit trail*.

Het Informatieveiligheidscomité wijst erop dat de verwerkingsverantwoordelijken gehouden zijn om, overeenkomstig artikel 35 van de Algemene Verordening Gegevensbescherming, een gegevensbeschermingseffectbeoordeling uit te voeren. Als uit die beoordeling zou blijken dat bijkomende maatregelen moeten worden getroffen om de rechten en vrijheden van de betrokkenen te vrijwaren, dan zijn de partijen ertoe gehouden om de gewijzigde modaliteiten van de gegevensverwerking ter beraadslaging aan het Informatieveiligheidscomité voor te leggen.

M. SALMON

voorzitster

De zetel van de kamer federale overheid van het informatieveiligheidscomité is gevestigd in de kantoren van de federale overheidsinstelling Beleid en Ondersteuning (FOD BOSA), op het volgende adres: Simon Bolivarlaan 30 bus 1, 1000 Brussel.