Sectoraal comité van het Rijksregister

Aanbeveling RR nr 01/2015 van 18 februari 2015

Betreft: Aanbeveling aan de gemeenten en lokale besturen betreffende de informatiebeveiliging waarmee de toegangen tot het Rijksregister en de daaruit volgende verwerkingen van Rijksregistergegevens moeten worden omkaderd (RN-AR-2014-001)

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"); in het bijzonder artikel 16, eerste lid, 3°;

Gelet op het verslag van de Voorzitter;

Brengt op 18 februari 2015, volgende aanbeveling uit

I. ONDERWERP VAN DE AANBEVELING

1. Naar aanleiding van het onderzoek van klachten van burgers betreffende onrechtmatig gebruik van gegevens van het Rijksregister in de schoot van gemeenten en lokale besturen alsook de vaststelling, bij contacten met deze laatsten aangaande specifieke machtigingen, van een zwakke informatiebeveiliging in hun schoot en zelfs een onaangepaste beschikbaarheid van deze gegevens bij een controle in situ, heeft het Comité het opportuun geacht in deze aanbevelingen de belangrijkste aspecten van de informatiebeveiliging te verzamelen en te herhalen waarmee door de gemeenten en lokale besturen rekening moet worden gehouden bij toegang tot de gegevens van het Rijksregister en bij de verwerking ervan.

2. Het Rijksregister is het informatieverwerkingssysteem dat instaat voor de centrale registratie, opslag en mededeling van informatiegegevens met betrekking tot de identificatie van natuurlijke personen of met andere woorden de burgers. Bij de eerste inschrijving van een persoon in het Rijksregister wordt een identificatienummer toegekend: het Rijksregisternummer.

3. Het Rijksregister wordt onder andere aangevuld door elke Belgische gemeente vanuit haar bevolkingsregister.

4. Voor de dagelijkse uitoefening van hun opdrachten dienen de gemeenten en lokale besturen te beschikken over een toegang tot de gegevens die centraal opgenomen zijn in het Rijksregister en lokaal in hun bevolkingsregister en dienen zij deze gegevens te verwerken.

5. In het algemeen bestempelt men deze gegevens, waaronder het Rijksregisternummer, nadien als "gegevens van het Rijksregister". Zo zal de benaming *'verwerking van Rijksregistergegevens'* zowel slaan op de eigenlijke toegang tot de Rijksregistergegevens door de gemeenten en lokale besturen als op de opeenvolgende verwerkingen van de verkregen gegevens en de benaming *'toegang tot Rijksregistergegevens'* op elke toegang, hetzij centraal bij het Rijksregister of lokaal bij het bevolkingsregister of via een lokale kopie van de gegevens van het Rijksregister.

6. Vermits de gegevens van het Rijksregister per definitie persoonsgegevens zijn, wil het accent dat in deze aanbevelingen vooral gelegd wordt op de specifieke informatiebeveiligingsaspecten voor de verwerkingen van Rijksregistergegevens door de gemeenten en lokale besturen niet vooruitlopen op het belang van de informatiebeveiliging voor persoonsgegevens in het algemeen in de schoot van deze laatsten waarvoor wij verwijzen naar de "*Referentiemaatregelen voor de beveiliging van elke verwerking van*

persoonsgegevens"[1] alsook naar de "*Richtsnoeren met betrekking tot de informatiebeveiliging van persoonsgegevens in steden en gemeenten*[2]" die door de Commissie voor de bescherming van de persoonlijke levenssfeer werden uitgevaardigd en waarnaar de gemeenten en lokale besturen zich vanzelfsprekend moeten schikken.

7. Aangezien de informatiebeveiliging voortdurend evolueert zullen deze aanbevelingen progressief worden aangepast aan de verschillende wettelijke, technische of andere evoluties.

II. DE GROTE PRINCIPES

8. Uit de specificiteit van de verwerkingen van Rijksregistergegevens door de gemeenten en lokale besturen en het eigen wettelijk kader waardoor deze worden geregeld, kan met de grote principes afleiden die voortdurend moeten dienen als 'leidraad' gedurende de gehele levensduur van het informatiesysteem dat de verwerking van deze gegevens toelaat, en dit vanaf de voorbereidende en ontwikkelingsfasen tot de fase van operationeel gebruik, via de realisatie- en productiefase, om de informatiebeveiligingsdoeleinden te bepalen die door de gemeenten en lokale besturen moeten verwezenlijkt worden om de wet te eerbiedigen.

9. Deze grote principes zijn:

Consulent inzake informatiebeveiliging

10. De gemeenten en lokale besturen moeten beschikken over een consulent inzake informatiebeveiliging als verantwoordelijke voor het toezicht en de controle op de uitvoering van het informatiebeveiligingsbeleid. Hij zal er in het bijzonder op toezien dat de gegevens van het Rijksregister correct worden verwerkt.

Beveiligingsbeleid

11. De gemeenten en lokale besturen moeten beschikken over een kwaliteitsvol beveiligingsbeleid waarin duidelijk de strategieën en maatregelen worden verduidelijkt om de toegangen tot de gegevens van het Rijksregister alsook de verwerkingen ervan te beveiligingen.

---

1 http://www.privacycommission.be/sites/privacycommission/files/documents/referentiemaatregelen_voor_de_beveiliging_van_elke_verwerking_van_persoonsgegevens_0.pdf

2 http://www.privacycommission.be/sites/privacycommission/files/documents/steden_en_gemeenten_informatiebeveiliging_0.pdf

Voorafgaande machtiging

12. Elke verwerking van gegevens van het Rijksregister uitgevoerd door de gemeenten en lokale besturen moet toegestaan zijn door de wet of vooraf gemachtigd door het Comité.

Toegangsbeleid

13. De gegevens van het Rijksregister mogen te allen tijde slechts toegankelijk zijn voor de gebruikers of toepassingen die hiertoe uitdrukkelijk werden gemachtigd.

Minimalisering van de gegevens

14. Iedere verwerking van gegevens van het Rijksregister moet zo worden georganiseerd dat uitsluitend de gegevens worden verwerkt (getoond, opgeslagen, enz.) die strikt noodzakelijk en relevant zijn in het licht van het doeleinde dat beoogd wordt met deze toegang.

Onverenigbaar doeleinde

15. De gegevens die van het Rijksregister werden verkregen voor een bepaald doeleinde mogen niet gebruikt worden voor een doeleinde dat hiermee onverenigbaar is.

Recht op informatie

16. Iedere persoon van wie gegevens van het Rijksregister werden verwerkt door een gemeente of lokaal bestuur moet kunnen geïnformeerd worden over de redenen van deze verwerken.

III. AANBEVELINGEN

17. Voor de toepassing van deze grote principes op de verwerkingen van gegevens van het Rijksregister door de gemeenten en lokale besturen kunnen volgende aanbevelingen worden geformuleerd:

Consulent inzake informatiebeveiliging

18. De gemeenten en lokale besturen moeten een consulent inzake informatiebeveiliging aanduiden en diens identiteit aan het Comité meedelen.

19. Zij moeten aan de consulent inzake informatiebeveiliging de noodzakelijke opleidingen aanbieden opdat hij zijn functie correct kan uitoefenen en zijn competentieniveau in de tijd kan bewaren.

20. Zij moeten voorzien in de praktische modaliteiten zodat de consulent inzake informatiebeveiliging over alle nuttige en noodzakelijke informatie beschikt om zijn functie normaal te kunnen uitoefenen.

21. De consulent inzake informatiebeveiliging is in de schoot van zijn gemeente verantwoordelijk voor het toezicht en de controle op de uitvoering van het beveiligingsbeleid. Hij zal er onder meer op toezien dat de gegevens van het Rijksregister correct en conform deze aanbevelingen worden verwerkt en alle noodzakelijke controles uitvoeren om zich hiervan te vergewissen.

Informatiebeveiligingsbeleid

22. De gemeenten en lokale besturen moeten beschikken over een kwaliteitsvol informatiebeveiligingsbeleid waarin onder meer duidelijk de strategieën en maatregelen worden verduidelijkt om de toegangen tot de gegevens van het Rijksregister alsook de verwerkingen ervan te beveiligingen.

23. Dit beveiligingsbeleid moet onder meer de basisbeginselen bevatten van de informatiebeveiliging die eigen is aan verwerkingen van Rijksregistergegevens, de verschillende aspecten van sensibilisering van de gebruikers hiervan alsook de sancties ingeval van inbreuken op de regels inzake bescherming van deze gegevens.

24. De gemeenten en lokale besturen moeten voorzien in de noodzakelijke middelen voor de invoering en het behoud van het beveiligingsbeleid en dit zowel op het gebied van human ressources als qua materiële, logistieke en financiële middelen.

25. Teneinde hen te steunen bij dit beleid heeft de Commissie voor de bescherming van de persoonlijke levenssfeer de "*Richtsnoeren met betrekking tot de informatiebeveiliging van persoonsgegevens in steden en gemeenten*[3]" gepubliceerd waarnaar het Comité verwijst.

Voorafgaande machtiging en beoordeling van de doeleinden

26. De gemeenten en lokale besturen moeten zich ervan vergewissen dat de door hen uitgevoerde verwerkingen van Rijksregistergegevens wel degelijk toegelaten zijn hetzij door de wet, voor de doeleinden die zich situeren binnen de bevoegdheden die hen reglementair werden verleend, hetzij door een machtiging van het Comité wanneer het gaat om een

[3] http://www.privacycommission.be/sites/privacycommission/files/documents/steden_en_gemeenten_informatiebeveiliging_0.pdf

specifiek doeleinde, en dat de verwerkingen uitsluitend worden uitgevoerd voor de doeleinden waarvoor oorspronkelijk een machtiging werd verleend.

27. Voor alle verwerkingen van Rijksregistergegevens waarvoor dit niet het geval zou zijn dient een specifieke machtigingsaanvraag te worden ingediend bij het Comité.

28. Duidelijke en nauwkeurig gedefinieerde procedures moeten worden ingevoerd om te verzekeren dat iedere verwerking van Rijksregistergegevens, en in het bijzonder iedere raadpleging van deze gegevens, uitsluitend mogelijk is op grond van een voorafgaande beslissing van het college van burgemeester en schepenen en dit na controle en beoordeling van het doeleinde dat inherent is aan deze verwerking en nadat hierover voldoende informatie werd verspreid in de gemeente zodat eenieder duidelijk weet wat toegelaten en niet toegelaten is.

Identificatie van de informatie en de dragers

29. De gemeenten en lokale besturen moeten voorzien in beheerprocedures zodat een inventaris kan gemaakt worden met de lokalisatie van al de gegevens van het Rijksregister op om het even welke drager (papier, elektronische drager, enz.) alsook van de verschillende processen en toepassingen om deze te verwerken zodat het risico voor de gegevens kan geëvalueerd worden en de toegang tot deze dragers, het beheer ervan en de verwerking van de bedoelde gegevens, georganiseerd kan worden overeenkomstig onderhavige aanbevelingen.

Toegangsbeleid

30. De gegevens van het Rijksregister mogen te allen tijde slechts toegankelijk zijn voor de gebruikers of toepassingen die hiertoe uitdrukkelijk werden gemachtigd en dit alleen in geval van gerechtvaardigde noodzaak (need to know basis).

31. Hiertoe dienen de gemeenten en lokale besturen te beschikken over een gebruikers- en toegangsbeheersysteem dat toelaat elke toegang tot de gegevens van het Rijksregister te beveiligen, ongeacht of het gaat om een rechtstreekse toegang tot het Rijksregister of tot een lokale kopie met Rijksregistergegevens en dit via een identificatie-, authenticatie en machtigingsysteem ongeacht of de toegang uitgaat van een gebruiker of via een proces of een systeem.

32. Het identificatiesysteem moet uitdrukkelijk toelaten iedere individuele gebruiker te identificeren alsook ieder proces of systeem.

33. Het authenticatiesysteem (paswoord, eID, enz.) moet iedere aanvrager van een toegang (gebruiker of systeem) toelaten te bewijzen wie hij beweert te zijn.

34. Indien mogelijk dient de elektronische authenticatie van een gebruiker bij voorkeur te gebeuren aan de hand van de elektronische identiteitskaart (eID) aangezien deze maximale waarborgen biedt.

35. Indien de authenticatie van de gebruikers gebeurt aan de hand van paswoorden dienen deze beheerd te worden op basis van een formele procedure (aantal digits, complexiteit, vernieuwing, enz.).

36. Het machtigingsysteem dient zich ervan te vergewissen dat elke aanvrager van een toegang (gebruiker of systeem) zich wel degelijk enkel toegang verschaft tot de gegevens van het Rijksregister waarvoor hij gemachtigd is, met andere woorden uitsluitend tot die gegevens die strikt noodzakelijk zijn voor de verwezenlijking van de doeleinden die inherent zijn aan zijn functie.

37. Dit toegang- en gebruikersbeheer dient de toegang van de verschillende informatiebeheerders (system administrator, system operator, ontwikkelaar, enz.) te beperken tot het strikte minimum.

38. Teneinde elke onrechtmatige toegang te vermijden dienen alle toepassingen die een toegang mogelijk maken tot de gegevens van het Rijksregister te voorzien in een vrij korte inactiviteitsduur (timeout) waarna de sessie automatisch wordt afgebroken.

39. De gemeenten en lokale besturen moeten de nominatieve lijst bijhouden van de personen die gemachtigd zijn om toegang te hebben tot persoonsgegevens en om deze te verwerken met de identificatiemiddelen die zij gebruiken om toegang te verkrijgen tot de verschillende systemen alsook hun respectievelijke toegangsrechten.

40. De aandacht van de gebruikers dient in het bijzonder gevestigd te worden op hun eigen verantwoordelijkheid wat betreft een efficiënte beveiliging van de toegang, meer bepaald op het gebied van het gebruik van paswoorden of andere identificatiemiddelen en de veiligheid van het gebruikte materiaal.

Minimalisering van de gegevens

41. De gemeenten en lokale besturen moeten ervoor zorgen dat iedere verwerking van gegevens van het Rijksregister zo wordt georganiseerd dat uitsluitend de gegevens worden verwerkt (getoond, opgeslagen, enz.) die strikt noodzakelijk en relevant zijn in het licht van het doeleinde dat beoogd wordt met deze toegang.

42. Zij moeten erover waken dat na een verwerking van Rijksregistergegevens geen enkel onnodig spoor van deze gegevens achter blijft in een lokale kopie op om het even welke drager noch op een van de betrokken technische systemen (logs, back-ups, koppelingsgegevens, enz.) die noodzakelijk zijn voor de uitvoering van de verwerking.

43. Zij moeten er in het bijzonder op toezien dat de uitwissing van Rijksregistergegevens op magnetische drager alsook de vernietiging van elke mogelijke andere drager met deze gegevens op een gecontroleerde en onomkeerbare wijze plaatsvindt.

Traceren van de toegangen

44. De gemeenten en lokale besturen moeten ervoor zorgen dat voor iedere toepassing die toegang verleent tot Rijksregistergegevens, ongeacht of het gaat om een rechtstreekse toegang tot het Rijksregister of tot een lokale kopie met Rijksregistergegevens, een logging plaatsvindt van alle toegangen, ongeacht of de toegang uitgaat van een gebruiker of van een systeem.

45. Deze logging moet de activiteiten omvatten van de verschillende informatiebeheerders (system administrator, system operator, ontwikkelaar, enz.).

46. Deze logging moet tevens de identificatie bevatten van de individuele gebruiker of van het proces of het systeem dat toegang had tot de gegevens, welke gegevens werden geraadpleegd, de wijze waarop de toegang plaatvond (raadpleging, wijziging, enz.), wanneer de toegang plaatsvond, alsook de reden hiervoor.

47. Indien nodig dienen de toepassingen die een gebruikerstoegang tot de Rijksregistergegevens toelaten te voorzien in de verplichte registratie door de gebruiker van de reden van de toegang.

48. Deze logging moet periodiek en regelmatig worden gecontroleerd teneinde iedere inbreuk op het toegangsbeleid of anomalie te detecteren en de nodige maatregelen te nemen.

49. In het algemeen dienen loggings gedurende ten minste 10 jaar[4] bewaard te worden.

Opleiding en informatieverstrekking aan de gebruikers en medewerkers

50. De gemeenten en lokale besturen moeten alle noodzakelijke maatregelen nemen opdat iedere persoon (intern of extern) die tussenkomt bij de verwerking van Rijksregistergegevens correct wordt opgeleid voor de uitoefening van zijn functie en

[4] RR 40/2010 (http://www.privacycommission.be/sites/privacycommission/files/documents/beraadslaging_RR_40_2010_0.pdf) of
RR 45/2010 (http://www.privacycommission.be/sites/privacycommission/files/documents/beraadslaging_RR_45_2010.pdf)

geïnformeerd over zijn verantwoordelijkheid inzake beveiliging alsook voortdurend voldoende geïnformeerd over zijn plichten en verantwoordelijkheden bij deze verwerkingen zoals onder meer over het beroepsgeheim, de verplichting om alles in het werk te stellen om de vertrouwelijkheid, de integriteit en de beschikbaarheid van de verwerkte Rijksregistergegevens te bewaren, alsook over de verplichting om elk veiligheidsrisico of –incident met betrekking tot deze gegevens te melden.

Zij zullen er onder meer over waken:

51. een vertrouwelijkheidsverbintenis te laten ondertekenen zodat enkel toegang wordt verleend tot Rijksregistergegevens of deze worden meegedeeld aan gemachtigde personen;

52. dat alle noodzakelijk e maatregelen worden genomen om het risico te beperken dat bij vergissing of voorzienbare kwaadwilligheid aan een niet-gemachtigde persoon toegang wordt verleend;

53. een sanctieprocedure in te voeren ingeval van inbreuken op de veiligheidsregels inzake gegevensbescherming.

Onderaanneming

54. Als de verwerking van Rijksregistergegevens geheel of gedeeltelijk wordt toevertrouwd aan een onderaannemer dienen de gemeenten en lokale besturen erover te waken dat in het onderaannemingscontract dezelfde informatiebeveiligingsverplichtingen worden opgenomen dan deze die van kracht zijn in de schoot van het organisme zelf.

Ontwikkeling van toepassingssystemen

55. De gemeenten en lokale besturen moeten erover waken dat de toepassingen bedoeld voor het verwerken van Rijksregistergegevens ontwikkeld worden volgens het 'Privacy by Design' principe dat erin bestaat bij de ontwikkeling van producten en diensten van bij het concept en gedurende de volledige levensduur van de bedoelde technologie, rekening te houden met de aspecten van bescherming van persoonsgegevens en in onderhavig geval, de bescherming van Rijksregistergegevens alsook de eerbiediging van de waarden die hieruit voortvloeien.

56. De ontwikkeling van nieuwe toepassingen bestemd voor het verwerken van Rijksregistergegevens moet dus gebaseerd zijn op een gestructureerde benadering die de onderhavige aanbevelingen verplicht toepast vanaf het stadium van het concept, deze van bij het begin optimaal integreert in de initiële specificaties en erover waakt dat er rekening mee wordt gehouden gedurende de volledige levensduur van de bedoelde toepassing.

57. Bij het concept en ontwikkeling van dergelijke toepassingen zal er in het bijzonder voor gezorgd worden dat eens de bedoelde verwerking is uitgevoerd, geen enkel onnodig spoor van de Rijksregistergegevens achter blijft in geen van de betrokken technische systemen (logs, back-ups, koppelingsgegevens, enz.) die noodzakelijk zijn voor de uitvoering van de verwerking.

Toezicht, herziening en onderhoud

58. Gelet op de huidige situatie wordt aan de gemeenten en lokale besturen ten stelligste aanbevolen om zo spoedig mogelijk een audit uit te voeren naar de efficiëntie van hun huidig beveiligingsbeleid teneinde zich ervan te verzekeren dat de verwerkingen van Rijksregistergegevens die door hen worden uitgevoerd conform de huidige aanbevelingen gebeuren. Hiertoe dienen de gebruikte toepassingen en de praktische organisatie voor de verwezenlijking van deze verwerkingen grondig te worden geanalyseerd om eventuele tekortkomingen in het licht van deze aanbevelingen te detecteren en de nodige corrigerende maatregelen te plannen en uit te voeren.

59. Eens een coherent informatiebeveiligingsbeleid werd ingevoerd moeten zij er op toezien dat de technische en organisatorische maatregelen voor de beveiliging van de Rijksregistergegevens geldig blijven in de tijd en regelmatig worden herzien.

60. Hiertoe dienen zij zich onder meer te verzekeren van een permanent toezicht op de verwerkingen, op de evolutie van de middelen en op de analyse van de loggings om noodzakelijk onderhoud tijdig te detecteren en de maatregelen te nemen die zich opdringen.

61. De consulent inzake informatiebeveiliging zal een essentiële rol vervullen bij dit toezicht en controle.

Voor de Wnd. Administrateur, afw.

(get.) An Machtens
Wnd. Afdelingshoofd ORM

De Voorzitter,

(get.) Mireille Salmon