



Autorité de protection des données
Gegevensbeschermingsautoriteit

Advies nr. 115/2023 van 18 juli 2023

Betreft: Adviesaanvraag over een ontwerp van Koninklijk besluit tot wijziging van het koninklijk besluit van 13 juni 2014 tot vaststelling van, enerzijds, de specifieke reglementaire, administratieve, technische en organisatorische maatregelen teneinde de naleving van de voorschriften over de bescherming van individuele gegevens of de gegevens over individuele eenheden en over de statistische geheimhouding te verzekeren en van, anderzijds, de voorwaarden waaronder het Nationaal Instituut voor de Statistiek kan handelen als tussenpersoon bij een latere verwerking voor statistische doeleinden (CO-A-2023-213)

Vertaling¹

Het Kenniscentrum van de Gegevensbeschermingsautoriteit (hierna "de Autoriteit");
aanwezig: de dames Cédric Morlière, Nathalie Raghenon en Griet Verhenneman, en de heren Yves-Alexandre de Montjoye en Bart Preneel;

Gelet op de wet van 3 december 2017 *tot oprichting van de Gegevensbeschermingsautoriteit*, met name de artikelen 23 en 26 (hierna "WOG");

Gelet op artikel 25, derde lid, van de WOG, volgens hetwelk de beslissingen van het Kenniscentrum bij meerderheid van stemmen worden aangenomen;

Gelet op Verordening (EU) 2016/679 *van het Europees Parlement en de Raad van 27 april 2016 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 95/46/EG* (hierna "AVG");

Gelet op de wet van 30 juli 2018 *betreffende de bescherming van natuurlijke personen met betrekking*

¹ Voor de oorspronkelijke versie van de tekst, die collegiaal werd gevalideerd, cf. de Franse versie van de tekst, die beschikbaar is in de FR-versie van de rubriek "adviezen" van de website van de Autoriteit.

tot de verwerking van persoonsgegevens (hierna "WVG");

Gelet op de adviesaanvraag van de heer Pierre-Yves Dermagne, vice-eersteminister en minister van Economie en Werk, ontvangen , op 24 mei 2023;

Gelet op de aanvullende informatie ontvangen op 13 juni 2023;

Brengt op 18 juli 2023 het volgende advies uit:

I. Onderwerp en context van de aanvraag

1. De heer Yves Dermagne, vice-eersteminister en minister van Economie en Werk, vraagt het advies van de Autoriteit over een ontwerp van Koninklijk besluit tot wijziging van het koninklijk besluit van 13 juni 2014 tot vaststelling van, enerzijds, de specifieke reglementaire, administratieve, technische en organisatorische maatregelen teneinde de naleving van de voorschriften over de bescherming van individuele gegevens of de gegevens over individuele eenheden en over de statistische geheimhouding te verzekeren en van, anderzijds, de voorwaarden waaronder het Nationaal Instituut voor de Statistiek kan handelen als tussenpersoon bij een latere verwerking voor statistische doeleinden (hierna "het ontwerp KB").
2. De belangrijkste wijzigingen die het ontwerp van Koninklijk Besluit aanbrengt in artikel 2 van het voornoemde Koninklijk Besluit van 2014 geven gevolg aan het voornoemde advies nr. 127/2021² van de Autoriteit in die zin dat de gebruikte terminologie wordt geactualiseerd (begrip pseudonimisering in plaats van "codering", "concordantiesleutels in plaats van "logische sleutels",) en in die zin dat de functionaris voor gegevensbescherming van het NIS (bijna³) geen besluitvormende functies meer krijgt toegewezen bij de uitvoering van gegevensverwerking die noodzakelijk is voor de uitvoering van de openbaredienststopdrachten van het NIS. Voor zover nodig geeft de Autoriteit in dit advies ook haar mening over de bepalingen van het voornoemde Koninklijk Besluit van 2014 die momenteel niet worden gewijzigd.
3. De Autoriteit heeft twee recente adviezen uitgebracht over de voorgestelde wijzigingen van de bovengenoemde wet van 4 juli 1962, die hebben geleid tot de bovengenoemde wet van 25 september 2022⁴. Aangezien deze adviezen aanbevelingen bevatten over de organisatorische en technische

² Advies nr. 127/2021 van 28 juli 2021 betreffende een voorontwerp van wet tot wijziging van de wet van 4 juli 1962 betreffende de openbare statistiek.

³ Cf. infra.

⁴ Namelijk advies 127/2021 van 28 juli 2021 over het voorontwerp tot wijziging van de wet van 4 juli 1962 betreffende de Openbare statistiek en advies 32/2022 over de artikelen 7, 25, 1° en 47 van het wetsontwerp houdende diverse bepalingen

maatregelen die moeten worden genomen bij de opmaak van overheidsstatistieken, wordt de auteur van het ontwerp van koninklijk besluit daarnaar verwezen voor aspecten die niet in dit advies aan bod komen.

II. Onderzoek

a. Hoofdstuk 1 van het ontwerp KB met als titel «Reglementaire, administratieve, technische en organisatorische maatregelen die bij iedere verwerking van gegevens moeten toegepast worden

i. Minimum aard van de opgelegde maatregelen

4. Hoofdstuk 1 van het ontwerp van koninklijk besluit bevat een lijst van maatregelen die het NIS moet nemen om de beveiliging te verzekeren van de gegevensverwerking die zij uitvoert in de uitoefening van haar opdracht, in overeenstemming met artikel 17quater van voornoemde wet van 1962, dat aan de Koning de opdracht delegeert om «*de specifieke reglementaire, administratieve, technische en organisatorische voorschriften (te bepalen) teneinde de naleving van de voorschriften over de bescherming van individuele persoonsgegevens en gegevens over individuele eenheden en over de statistische geheimhouding te verzekeren*».
5. Zelfs als het opleggen van dergelijke maatregelen passend is in het kader van de bescherming van persoonsgegevens gelet op de aanzienlijke risico's voor de rechten en vrijheden van betrokkenen die voortvloeien uit de activiteiten van instellingen die verantwoordelijk zijn voor officiële statistieken (vanwege de risico's die de gegevensverwerking bij deze activiteiten met zich meebrengt, zowel vanuit het oogpunt van het aantal betrokkenen als vanuit het oogpunt van de omvang en gedetailleerdheid van de gegevens die over hen worden verwerkt en de gegevensbankkoppelingen die deze activiteiten vereisen), merkt de Autoriteit op dat er geen sprake kan zijn van het opstellen van een uitputtende lijst van dergelijke maatregelen, aangezien het de verwerkingsverantwoordelijke, d.w.z. het NIS, is om te kiezen voor passende en geschikte technische en organisatorische maatregelen, afhankelijk van de specifieke risico's die voortvloeien uit de specifieke gegevensverwerking die het uitvoert in het kader van zijn statistische programma's en de vragen waarop het moet reageren krachtens artikel 15 van de bovengenoemde wet van 1962. Deze maatregelen moeten altijd worden aangepast aan de huidige stand van de techniek en aan technische ontwikkelingen (art. 25 AVG). Daarom wordt

inzake de Economie. Dit laatste advies heeft betrekking op de federale wet op de overheidsstatistieken voor zover deze betrekking heeft op de wettelijke machtiging die aan de NIS is verleend om gegevens over het verkeer en de locatie van abonnees te ontvangen die operatoren moeten bewaren krachtens de artikelen 122 en 123 van de wet van 13 juni 2005 betreffende de elektronische communicatie.

aanbevelen de titel van het koninklijk besluit en van hoofdstuk 1 te wijzigen en in plaats daarvan een lijst van minimale maatregelen op te nemen die door het NIS moeten worden genomen.

ii. Schriftelijk beveiligingsbeleid

6. In ontwerpartikel 1 moet, om dezelfde redenen als hierboven uiteengezet, worden bepaald dat het NIS verplicht is zijn schriftelijk veiligheidsbeleid voortdurend bij te werken. Met dit beleid voldoet het NIS aan haar verantwoordingsplicht zoals vastgelegd in artikel 24 van de AVG, waarin staat dat iedere verwerkingsverantwoordelijken «passende technische en organisatorische maatregelen treft om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met de AVG wordt uitgevoerd ».

iii. Minimale technische maatregelen

7. Het ontwerpartikel 2 van het koninklijk besluit bevat een lijst van specifieke maatregelen die door het NIS moeten worden vastgesteld. De auteur van het ontwerp van KB beschrijft ze als technisch, organisatorisch en juridisch.
8. Volgens de bewoordingen van artikel 2, 1ste lid, 1^o bestaan de technische maatregelen⁵ uit «*de classificatie van gegevens, het beheer van de toegang tot geclassificeerde gegevens, de specifieke maatregelen betreffende de persoonsgegevens met directe identificatienummers, de voorlichting en opleiding van het personeel, de pseudonimisering van gegevens en de bescherming van de concordantiesleutels waarmee studiegegevens terug kunnen worden gekoppeld aan de directe identificatiegegevens*». In de rest van deze ontwerpbeoordeling wordt uiteengezet waaruit elk van deze maatregelen bestaat.
9. Ten eerste merkt de Autoriteit op dat de gebruikte begrippen die nog niet zijn gedefinieerd, een definitie moeten krijgen in de bovengenoemde wet uit 1962, namelijk het begrip "direct identificeerbaar".
10. Het vaststellen van het gegevensclassificatieniveau gekoppeld aan (i) de mate van identificeerbaarheid van de betrokkenen en (ii) de mate van gevoeligheid van de informatie die op hen betrekking heeft, is een passende maatregel. Dit zijn de relevante criteria voor het beoordelen van de omvang van het risico van een verwerking voor betrokkenen. Het veiligheidsniveau dat voor elke verwerking moet worden bereikt, moet in verhouding staan tot dit risiconiveau.

⁵ Die als minimaal gekwalificeerd moeten worden (zie hierboven).

11. De Autoriteit is van mening dat dit gevolg duidelijker moet worden gemaakt in punt 1.1 van ontwerpartikel 2, dat momenteel alleen de verschillende classificatieniveaus vermeldt zonder deze te kwalificeren en alleen het volgende bepaalt « *de classificatie van gegevens bepaalt het niveau van gegevensbescherming* ».
12. Bovendien moet worden bepaald dat zelfs gepseudonimiseerde persoonsgegevens die gevoelig zijn als bedoeld in de artikelen 9 en 10 van de AVG, strengere beschermingsmaatregelen vereisen dan gepseudonimiseerde persoonsgegevens die deze kenmerken niet hebben.
13. Ten slotte moet het ontwerp van KB ook de begrippen "globale gegevens" en "anonieme gegevens" definiëren, die in deze classificatie zijn opgenomen.
14. Met betrekking tot het begrip "anonieme gegevens" wil de Autoriteit erop wijzen dat het anonimiseren van persoonsgegevens niet alleen bestaat uit het verwijderen van informatie die de personen waarop de gegevens betrekking hebben direct identificeert (achternaam, voornaam, uniek identificatienummer, adres, enz.) maar ook de informatie waarmee ze kunnen worden geïdentificeerd door een proces van individualisering, correlatie of gevolgtrekking.. Het ontwerp van KB moet daarom een definitie van dit begrip bevatten die deze vereiste hoge norm weerspiegelt.
15. Wat betreft het begrip " globale gegevens ", begrijpt de Autoriteit dat de auteur van het ontwerp van KB doelt op het begrip geaggregeerde gegevens, aangezien - zoals de Autoriteit al de gelegenheid heeft gehad aan te geven⁶ -, de term veralgemening wordt gebruikt om te verwijzen naar het technische proces van het minder nauwkeurig maken van de gegevens van een betrokkene (bijvoorbeeld zijn geboortedatum vervangen door zijn leeftijd, zijn adres door een postcode) ; wat niet belet dat veralgemeende gegevens nog steeds verwijzen naar een enkele persoon en nog steeds persoonsgegevens vormen als de persoon of personen op wie ze betrekking hebben, geïdentificeerd of identificeerbaar zijn in de zin van artikel 4. 1 van de AVG. Daarentegen verwijst aggregatie naar het technische proces van het samenbrengen van informatie over meerdere mensen op zo'n manier dat elk stukje data verwijst naar minstens één groep mensen. Informatie over het aantal mensen dat op een bepaalde datum van Luik naar Brussel reisde of het aantal vrouwen dat in een bepaalde gemeente woont, zijn bijvoorbeeld geaggregeerde gegevens⁷. De Autoriteit beveelt daarom aan het

⁶⁶ Zie hiervoor de overwegingen 53 en volgende van het advies 35/2023 van 9 februari 2023 *sur le projet de décret introduisant dans le Code wallon de l'Action sociale et de la santé des dispositions relatives aux programmes de médecine préventive* (geen vertaling in het Nederlands).

⁷ Geaggregeerde gegevens kunnen als anoniem worden beschouwd, afhankelijk van de aggregatieparameters en, waar van toepassing, de toevoeging van ruis.

begrip "globale gegevens" te vervangen door "geaggregeerde gegevens" en het te definiëren in overeenstemming met de bovenstaande redeneringen.

16. Wat betreft de maatregelen die het NIS moet nemen om de toegang tot andere dan "*globale en anonieme*" gegevens te beheren, wordt aanbevolen dat het ontwerp van KB meer regelgevend is. Bepalen dat de toegang «*zo dichtbij mogelijk wordt beheerd*», d.w.z. dat deze toegang alleen wordt verleend aan personen «*die ervan op de hoogte moeten zijn*», lijkt onvoldoende. Echter, ingevolge het bovengenoemde advies nr. 127/2021 van de Autoriteit, bepaalt artikel 17 van de bovengenoemde wet van 1962 nu al dat uitsluitend NIS-medewerkers die belast zijn met het verzamelen van gegevens en degenen die belast zijn met kwaliteitscontrole en, indien van toepassing, de koppeling, toegang hebben tot persoonsgegevens met directe identificatoren. Om een geschiktere regeling te bieden voor de minimumeisen voor het toegangsbeheer voor de door de NIS verzamelde gegevens, moet enerzijds de noodzaak om kennis te nemen expliciet worden gekoppeld aan het concrete doel dat de met een specifiek statistisch onderzoek belaste ambtenaar nastreeft en aan zijn of haar specifieke werkteerrein⁸, waarbij dit doel zowel de reikwijdte van de te raadplegen gegevens als de noodzakelijke periode gedurende welke deze toegang moet worden verleend, afbakt. Er moet ook expliciet worden vermeld dat het beheer van deze toegang in overeenstemming zal zijn met artikel 17 van de bovengenoemde wet uit 1962.
17. Ten tweede merkt de Autoriteit op dat verzoeken om toegang niet moeten worden goedgekeurd door de functionaris voor gegevensbescherming (aangezien dit een besluitvormende functie is bij het uitvoeren van een gegevensverwerking die krachtens de artikelen 38 en 39 van de AVG niet onder zijn bevoegdheid valt), maar kunnen worden ingediend nadat hij zijn advies heeft gegeven.
18. Gezien de gevoeligheid van de toegang tot concordantiesleutels, waarmee de identiteit kan worden achterhaald van personen van wie het NIS gegevens heeft gepseudonimiseerd, beveelt de Autoriteit bovendien aan dat het NIS specifieke maatregelen neemt om de toegang tot deze sleutels te loggen. Zij verwijst in dit verband naar haar eerder genoemde advies van 2021, waarin zij aanbeveelt in de regelgeving expliciet te vermelden welke soorten functies binnen het NIS toegang mogen hebben tot deze sleutels, en het NIS te verplichten een logboek bij te houden van de toegang tot deze sleutels, waarin wordt beschreven wie wanneer toegang had en waarom. Aangezien dit niet was voorzien in de voornoemde wet van 1962, moet het worden opgenomen in het ontwerp van Koninklijk Besluit.
19. Punt 1.3. van artikel 2 van het voormelde KB van 2014 gaat over de «*specifieke maatregelen betreffende de persoonsgegevens met directe identificatienummers*». Deze bepaling, die betrekking

⁸ Zoals bepaald in de Europese Verordening 553/2013 betreffende de Europese statistiek.

heeft op maatregelen voor het loggen van toegang tot dit soort gegevens, wordt niet aangepast door het ontwerp van KB. De Autoriteit merkt in dit verband op dat, aangezien gepseudonimiseerde gegevens altijd persoonsgegevens zijn, het passend is dat zij ook vallen onder deze verplichting tot logging van de toegang die aan het NIS wordt opgelegd; te meer daar het onder de bevoegdheid van het NIS valt om gepseudonimiseerde gegevens mee te delen aan een reeks ontvangers die zijn opgesomd in artikel 15 van de bovengenoemde wet van 1962; zelfs indien dit betekent dat het NIS daartoe strekkende verbintenissen van voornoemde ontvangers moet opnemen in de vertrouwelijkheidsovereenkomst die moet worden gesloten krachtens artikel 15bis van voornoemde wet van 1962 ; dit zou het NIS ook in staat stellen na te gaan of de ontvangers voldoen aan de statistische beginselen van onpartijdigheid, objectiviteit en professionele onafhankelijkheid als bedoeld in artikel 1bis, lid 1, 4° van voornoemde wet van 1962. Meer fundamenteel merkt de Autoriteit op dat het ontwerp van Koninklijk Besluit niet voorziet in de beveiliging van de mededeling van gepseudonimiseerde gegevens door het NIS overeenkomstig artikel 15 van de voornoemde wet van 1962. In dit verband vestigt de Autoriteit de aandacht van de wetgever op het feit dat het meer in overeenstemming is met de beginselen inzake gegevensbescherming om te bepalen dat deze gegevensverstrekking plaatsvindt binnen het NIS-informatiesysteem (via een specifiek voor dit doel ingerichte dataroom), zodat de gepseudonimiseerde gegevens de NIS " data room " niet verlaten. Het is belangrijk dat het NIS controle kan houden over het gebruik van deze gegevens, waardoor het risico op misbruik van de gegevens afneemt. De Autoriteit beveelt ten zeerste aan om een bepaling in die zin op te nemen in het ontwerp van Koninklijk Besluit.

20. Wat betreft het kwaliteitsniveau van de logging die van het NIS wordt verlangd, wordt aanbevolen dat deze verplichte logging een verwijzing bevat naar de statistische studie of het specifieke dossier (dossiernummer) waarvoor de verzoeken om persoonsgegevens zijn gedaan. Zonder deze informatie is het onmogelijk om het bestaan van buitensporige verzoeken voor een specifieke taak of een mogelijk misbruik van het doel te detecteren.
21. Tot slot wordt, nog steeds in punt 1.3 van artikel 2 van het ontwerp van KB, aanbevolen om het NIS te verplichten een geautomatiseerd systeem op te zetten voor de detectie van abnormale toegang tot persoonsgegevens (bv. op basis van abnormale frequentie en omvang).
22. Punt 1.4 van artikel 2 van het voornoemde KB van 2014 heeft betrekking op de voorlichting en opleiding van NIS-personeel. Het is raadzaam om ervoor te zorgen dat het bewustwordingsproces van het personeel niet gericht is op informatiebeveiliging, maar op de bescherming van persoonsgegevens (waaronder informatiebeveiliging valt), met inbegrip van de waarborgen voor de rechten en vrijheden van betrokkenen die zijn vastgelegd in de bovengenoemde wet uit 1962.

23. Punt 1.5 betreft de pseudonimisering van de gegevens. Het ontwerp van KB vervangt de huidige bepaling door te bepalen dat :

«De gegevens worden op zodanige wijze verwerkt dat deze gegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld».

24. Ten eerste vraagt de Autoriteit zich af of het doel om te waarborgen dat de gegevens niet worden toegeschreven aan een identificeerbare persoon geen vergissing is, aangezien gepseudonimiseerde gegevens uit de aard der zaak gegevens zijn die betrekking hebben op een identificeerbare persoon, aangezien aanvullende informatie (d.w.z. de concordantiesleutel of, meer in het algemeen, het de-identificatiegeheim) het mogelijk maakt de persoon opnieuw te identificeren.

25. Bovendien merkt de Autoriteit op dat deze ontwerpbeepaling niet voldoende specificeert welke gegevens eronder vallen. Verwijzen naar "de gegevens" zonder enige andere precisering biedt niet de vereiste voorspelbaarheid en rechtszekerheid. Zoals de Autoriteit het begrijpt, is dit het geval wanneer het NIS projecten uitvoert op het gebied van openbare statistiek die alleen kunnen worden uitgevoerd met behulp van gepseudonimiseerde gegevens, of wanneer het NIS reageert op verzoeken om toegang die tot hen worden gericht op grond van artikel 15 van de bovengenoemde wet van 1962, waaraan ook alleen kan worden voldaan met behulp van dergelijke gegevens. Dit moet worden verduidelijkt.

26. Ook wordt aanbevolen om in punt 1.5 toe te voegen dat het NIS de techniek of combinatie van technieken kiest die het meest geschikt is en in overeenstemming is met de huidige beste praktijken om de risico's voor de betrokkenen tot een minimum te beperken, en zijn keuzes schriftelijk documenteert, voor elk project voor openbare statistieken of voor elk relevant verzoek om toegang⁹. In dit verband wordt verwezen naar de opmerkingen van de Autoriteit in haar voornoemde advies van 2021¹⁰. Het NIS zal met name zorgen voor een strikte minimalisering van de verwerkte gegevens overeenkomstig artikel 5.1.c), van de AVG.

27. Vervolgens merkt de Autoriteit op dat het bovengenoemde Koninklijk Besluit van 2014 alleen betrekking heeft op maatregelen voor het pseudonimiseren van gegevens, terwijl bepaalde statistische studies kunnen worden uitgevoerd met behulp van anonieme gegevens¹¹. In het ontwerp van KB moet daarom een specifiek punt worden opgenomen met betrekking tot de anonimiseringsprocedures van

⁹ D.w.z. waarvoor gepseudonimiseerde gegevens moeten worden verwerkt/doorgegeven en waaraan niet kan worden voldaan met geanonimiseerde gegevens.

¹⁰ Zie met name de overwegingen 7 en 34.

¹¹ Zie over dit onderwerp de opmerkingen van de Autoriteit in haar bovengenoemde advies van 2021 in overweging 45 e.v.

het NIS en het gebruik van systemen die voldoen aan de huidige beste praktijken en naar behoren schriftelijk zijn gedocumenteerd.

28. Bovendien moet expliciet worden vermeld dat het NIS in elk geval alle passende maatregelen zal nemen om te voorkomen dat gegevens waarmee de betrokkenen kunnen worden geïdentificeerd, moeten worden bewaard. In dit verband verwijst de Autoriteit naar haar bovengenoemde advies van 2021¹².

29. Punt 1.6 van artikel 2 van het voornoemde koninklijk besluit 2014, dat betrekking heeft op de bescherming van concordantiesleutels, werd eveneens aangepast om voortaan in het volgende te voorzien:

«om veiligheidsredenen worden de concordantiesleutels gecodeerd wanneer hun archivering noodzakelijk is. De decodering van de concordantiesleutels kan alleen worden gedaan na advies van de functionaris voor gegevensbescherming».

30. Naast de hierboven aanbevolen maatregelen betreffende de logging van de toegang tot concordantiesleutels moet worden bepaald, zoals de Autoriteit in haar bovengenoemd advies van 2021 heeft uitgelegd, dat het NIS het gebruikte pseudonimiseringsgeheim¹³ bewaart door middel van passende technische en organisatorische maatregelen, afhankelijk van het gebruikte pseudonimiseringsscenario, die met name de fysieke scheiding van het pseudonimiseringsgeheim van de onderzoeksgegevens en de verwijdering van het pseudonimiseringsgeheim van elk risicovol opslagmedium omvatten. Er moet ook worden opgemerkt dat de versleuteling van pseudonimiseringsgeheimen wordt uitgevoerd in overeenstemming met de huidige beste praktijken in het geval van geautomatiseerde opslag, waarbij de sleutelopslag en het sleutelbeheer worden aangepast aan het gebruikte versleutelingstype.

31. Met betrekking tot punt 1.7 inzake de pseudonimisering van gegevens die worden verstrekt op grond van artikel 15 van de bovengenoemde wet van 1962, verwijst de Autoriteit naar haar eerdere overwegingen over dit onderwerp. Voor het overige plaatst de Autoriteit vraagtekens bij de toevoeging van het woord «vooral» bij het bepalen van de omstandigheden waarin dezelfde statistische eenheid een identiek pseudoniem krijgt voor meerdere mededelingen die overeenkomstig artikel 15 van de bovengenoemde wet van 1962 worden uitgevoerd, namelijk «*wanneer er opvolging van de eenheden nodig is (panelenenquête en longitudinale studies)*». Bij gebrek aan een naar behoren gemotiveerde specifieke rechtvaardiging die moet worden opgenomen in het verslag aan de Koning, moet de term "vooral" worden geschrapt. De Autoriteit vraagt zich ook af waarom panelonderzoeken van niet-

¹² Zie in het bijzonder de aanbevelingen voor maatregelen om te voorkomen dat gegevens over non-respondenten van NIS-enquêtes worden bewaard, terwijl tegelijkertijd wordt voorkomen dat deze mensen bij een volgende enquête worden benaderd.

¹³ aangezien pseudonimisering van gegevens kan worden bereikt met andere technieken dan codering.

longitudinale aard een dergelijke procedure vereisen. Bij gebrek aan enige motivering op dit punt in het verslag aan de Koning, moet ook de verwijzing naar dit voorbeeld worden geschrapt.

iv. Minimale organisatorische maatregelen

32. Punt 2° van artikel 2 van het voornoemde koninklijk besluit 2014 somt de organisatorische maatregelen van het NIS op. Om de hierboven uiteengezette redenen moet worden opgemerkt dat dit minimummaatregelen zijn.
33. Punt 3° van dit punt 2° van artikel 2 in ontwerp bepaalt :«*het Nationaal Instituut voor de Statistiek zorgt voor controle op het gebruik van de concordantiesleutels waarmee de gegevens opnieuw geïdentificeerd kunnen worden, om te vermijden dat ze voor andere dan statistische of wetenschappelijke onderzoeksdoeleinden gebruikt worden*». Om de hierboven uiteengezette redenen moet worden verwezen naar de concordantiesleutels en/of een ander pseudonimiseringsgeheim dat is gebruikt om de gegevens te pseudonimiseren. Bovendien moet, in plaats van in het algemeen te verwijzen naar alle andere doeleinden dan statistisch of wetenschappelijk onderzoek, worden gespecificeerd - met inachtneming van het doelbeginsel en als waarborg voor de rechten en vrijheden van de betrokkenen - dat dit geen andere doeleinden kunnen zijn dan de specifieke doeleinden van statistisch of wetenschappelijk onderzoek waarvoor de gegevens zijn gepseudonimiseerd.
34. De Autoriteit merkt op dat het veiligstellen van de configuratie van concordantiesleutels en de controle op het gebruik ervan noodzakelijkerwijs gepaard moet gaan met toezicht door het NIS op de samenstelling van gepseudonimiseerde gegevenstabellen die beschikbaar worden gesteld aan haar thematische afdelingen die verantwoordelijk zijn voor de productie van statistieken. Er moet voor worden gezorgd dat deze verschillende tabellen niet meer dan 15 identieke gegevenscategorieën bevatten¹⁴ (met betrekking tot dezelfde personen) (in het geval dat er meerdere tabellen aan hen beschikbaar worden gesteld) en dat het AVG-beginsel van minimalisering strikt wordt nageleefd bij het maken van deze tabellen. De Autoriteit beveelt aan om een organisatorische maatregel in die zin toe te voegen aan het ontwerp van KB.

v. Juridische maatregelen:

35. Wat de in punt 3° van ontwerpartikel 2 opgesomde juridische maatregelen betreft, zijn de aangebrachte wijzigingen louter technisch. De Autoriteit is van oordeel dat de geheimhoudingsplicht

¹⁴ Er is met name aangetoond dat 15 demografische kenmerken voldoende zijn om een persoon uniek te heridentificeren. Rocher, L., et al. 2019. Estimating the success of re-identifications in incomplete datasets using generative models. Nature communications, 10(1), blz.1-9. <https://www.nature.com/articles/s41467-019-10933-3>

en de verplichting tot statistische geheimhouding niet alleen moeten gelden voor NIS-werknemers, maar ook voor alle verwerkers die door het NIS worden ingeschakeld¹⁵, alsmede voor personen die van het NIS gepseudonimiseerde gegevens ontvangen overeenkomstig artikel 15 van de bovengenoemde wet van 1962. Bovendien is het raadzaam om, als garantie voor de betrokken personen, expliciet te bepalen dat deze geheimhoudingsplicht ook na het beëindigen van de functie blijft gelden.

b. Hoofdstuk 2 van het ontwerp van koninklijk besluit dat handelt over de voorwaarden waaronder het NIS kan optreden als tussenpersoon met het oog op verdere verwerking voor statistische doeleinden (art. 3 tot 5)

36. Hoofdstuk 2 van het ontwerp van KB behandelt de voorwaarden waaronder het NIS kan optreden als tussenpersoon met het oog op verdere verwerking voor statistische doeleinden, overeenkomstig artikel 17quater, §2 van de voornoemde wet van 1962.
37. De Autoriteit merkt op dat in de bovengenoemde wet van 1962 geen duidelijke definitie is opgenomen van wat deze openbare dienstverleningsopdracht van het NIS inhoudt (wat ook moet worden verholpen). Zoals duidelijk blijkt uit het voornoemde koninklijk besluit van 2014, is het doel van de opdracht die aan het NIS als tussenpersoon is toevertrouwd om zowel externe als interne databanken¹⁶ zonder verdere specificatie te koppelen met het oog op het genereren van gepseudonimiseerde gegevens. Ook hier merkt de Autoriteit op dat de verwijzing naar het genereren van geanonimiseerde gegevens is weggelaten; ook dit moet worden gecorrigeerd.
38. Onder voorbehoud van het standpunt van de Raad van State, moet vooraf beoordeeld worden of het NIS dit soort diensten als tussenpersoon mag uitvoeren in overeenstemming met de Europese regels inzake officiële statistieken, gezien haar statuut van nationale statistisch instituut.
39. Vanuit een strikt oogpunt van gegevensbescherming is een tussenpersoon die gegevens anonimiseert of pseudonimiseert met het oog op de verstrekking ervan voor statistische onderzoeksdoeleinden een vertrouwde derde zoals bedoeld in artikel 202 e.v. van de WVG en moet daarom de genoemde garanties bieden (onderwerping aan het beroepsgeheim en garantie van onafhankelijkheid ten opzichte van de oorspronkelijke verwerkingsverantwoordelijken die de gegevens hebben verzameld en de latere verwerkingsverantwoordelijken die de statistische onderzoeken zullen uitvoeren) en deskundig zijn op het gebied van gegevensbeschermingstechnieken.

¹⁵ Op voorwaarde dat ze voldoen aan de vereiste criteria wat betreft opleiding en kwalificaties van het personeel, in overeenstemming met de Europese code van goede praktijken op het gebied van officiële statistieken. Dit soort eisen kan ook worden toegevoegd aan de organisatorische maatregelen.

¹⁶ De Autoriteit verwijst in dit verband naar haar opmerkingen in overweging 58 van haar voornoemde advies 127/2021.

40. De betrokkenheid van een tussenpersoon bij dit soort risicovolle verwerkingen (voor zover er sprake is van databankkoppelingen) vormt een garantie voor betrokkenen, aangezien het risico van depseudonimisering kleiner is doordat het geheim van de pseudonimisering door deze vertrouwde derde partij wordt bewaard¹⁷.
41. Zoals de Commissie voor bescherming van de persoonlijke levenssfeer, de rechtsvoorganger van de Autoriteit, al aangaf, mag een dergelijke vertrouwde derde, de gegevens die zij verzamelt om haar vertrouwensdiensten te verlenen (pseudonimisering, koppeling, anonimisering) niet gebruiken voor andere doeleinden dan de specifieke koppelings- en pseudonimiserings- of anonimiseringsdoeleinden die hem zijn toevertrouwd¹⁸. Toestaan dat het NIS de gegevens die het heeft verwerkt om een van zijn specifieke taken als tussenpersoon uit te voeren, opnieuw gebruikt voor zijn eigen generieke doeleinden op het gebied van openbare statistieken, roept niet alleen vragen op met betrekking tot het finaliteitsbeginsel van de AVG en de risico's die een dergelijke massale centralisatie en hergebruik van gegevens met zich meebrengt voor de rechten en vrijheden van de betrokkenen (gezien de massa en het zeer hoge detailleringniveau van de betrokken gegevens), maar ook met betrekking tot het beginsel van statistische finaliteit dat is vastgelegd in artikel 1bis van de bovengenoemde wet van 1962, dat het volgende bepaalt *«gegevens die voor een welbepaald statistisch doel werden verzameld mogen enkel voor andere statistische doeleinden worden gebruikt, wanneer die met het eerste doel verenigbaar zijn»*.
42. Daarnaast vraagt de Autoriteit zich, onder voorbehoud van het standpunt van de Raad van State, ook af of een dergelijk hergebruik verenigbaar is met de vereisten van professionele onafhankelijkheid van een statistische instantie ten opzichte van zowel de publieke als de particuliere sector, aangezien het NIS als tussenpersoon een eigen belang heeft bij de gegevens die het verwerkt.¹⁹

¹⁷ Zie art. 202, §2, WVG.

¹⁸ Zie in dit verband de aanbeveling 02/2010 van de Commissie van 31 maart 2010 omtrent de privacybeschermende rol van Trusted Third Parties (TTP of vertrouwde derde) bij gegevensuitwisseling, blz. 6. In diezelfde aanbeveling wordt overigens ook het volgende bevestigd *«een TTP moet de persoonsgegevens vernietigen die hem door de verantwoordelijken van de oorspronkelijke verwerking werden bezorgd, zodra hij zijn anonimiseringsopdracht heeft vervuld, tenzij het een opdracht betreft waaruit voortvloeit dat hij de gegevens moet bewaren»*.

¹⁹ Met betrekking tot de vraag hoe lang het NIS de gegevens bewaart die zij in het kader van haar taken verzamelt, verwijst de Autoriteit naar haar opmerkingen in de overwegingen 56 e.v. van haar voornoemde advies nr. 127/2021, waarin met name wordt benadrukt dat *«Indien het NIS de persoonsgegevens die het verzamelt en pseudonimiseert echter nooit verwijdert zonder de gebruikte pseudonimiseringssleutels ooit te vernietigen, leidt dit tot een permanente centralisatie vanwege het NIS van een enorme hoeveelheid uiteenlopende persoonsgegevens over de Belgische bevolking; hetgeen een belangrijke inmenging vormt in het recht van de betrokkenen op bescherming van persoonsgegevens, wat vragen doet rijzen met betrekking tot artikel 1.bis van de wet openbare statistiek²⁷ en de beginselen van finaliteit en evenredigheid van het recht op gegevensbescherming. Zelfs wanneer de AVG de verdere verwerking voor statistische studies en wetenschappelijk onderzoek toestaat, impliceert de naleving van het finaliteitsbeginsel dat de modaliteiten van de verdere verwerking van gegevens beperkt moeten blijven tot wat strikt noodzakelijk is voor de latere uitvoering van deze statistische studie of dit wetenschappelijk onderzoek»*.

43. Gelet op het voorgaande dienen de artikelen 3 en 5 van het voornoemde koninklijk besluit van 2014 derhalve te worden aangepast om te specificeren (i) dat deze opdracht van tussenpersoon alleen door het NIS mag worden uitgevoerd wanneer dit noodzakelijk is in geval van een verzoek als bedoeld in artikel 15 van de wet en (ii) om de mogelijkheid voor het NIS weg te nemen om de gegevens die in het kader van deze dienstverlening voor deze derden zijn verzameld, voor eigen doeleinden te hergebruiken. Het begrip derden dat in artikel 3 van het ontwerp van KB wordt gebruikt, moet ook worden verduidelijkt door te verwijzen naar de derden waarnaar wordt verwezen in artikel 15 van de voornoemde wet van 1962. Zodra de koppelingen voor de derden zijn gerealiseerd, moeten de gegevens worden vernietigd in overeenstemming met de statuut van vertrouwde derde van de tussenpersonen. Dit zou ook uitdrukkelijk omschreven moeten worden.
44. Het spreekt ook voor zich dat als het NIS dergelijke koppelings-, pseudonimiserings- en anonimiseringsverwerkingen uitvoert, het zal moeten worden gekwalificeerd als de verwerkingsverantwoordelijke voor de genoemde koppelings-, pseudonimiserings- en anonimiseringsverwerkingen. Dit moet worden verduidelijkt in het ontwerp van KB.
45. Daarnaast beveelt de Autoriteit aan dat de wetgever ingrijpt om dit statuut van vertrouwde derde te consolideren door een passend kader voor dit soort dienstverleners te scheppen. Er moet hen een minimum aantal specifieke verplichtingen worden opgelegd als garantie voor de rechten en vrijheden van de betrokkenen, gelet op de specifieke risico's voor de gegevensbescherming die deze activiteiten van het koppelen van verschillende gegevensbanken en de grootschalige verwerking die deze activiteiten met zich meebrengen, alsmede om de kwaliteit te garanderen van de diensten die zij in dit kader verlenen. Het is aan te raden dat de auteur van het ontwerp hierover nadenkt. Een gedeeltelijke inspiratiebron kan worden gevonden in de bepalingen van de Europese Eidas Verordening²⁰, die andere soorten vertrouwde derden regelt.
46. Met betrekking tot artikel 4 van voormeld koninklijk besluit van 2014 wordt verwezen naar de opmerkingen hierboven gemaakt over artikel 2, eerste lid, 2°, litera 3°, die mutatis mutandis van toepassing zijn.

²⁰ Verordening (EU) nr. 910/2014 van 23 juli 2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG.

Om deze redenen,

is de Autoriteit van mening

dat het voorontwerp als volgt moet worden aangepast:

1. Verduidelijking dat de aan het NIS opgelegde maatregelen, minimummaatregelen zijn (overw. 4 en 5 en 32) ;
2. Het NIS verplichten om zijn schriftelijk veiligheidsbeleid bij te werken (overw. 6) ;
3. Toevoeging van definities van bepaalde gebruikte begrippen om een correct niveau van rechtszekerheid te waarborgen (overw. 9 en 13 tot 15) ;
4. Specificering van de maatregelen die vereist zijn voor het beheer van de toegang tot de door het NIS verwerkte gegevens, met inbegrip van de vaststelling van het vereiste kwaliteitsniveau van de maatregelen voor het loggen van de toegang tot zowel de gegevens als de concordantiesleutels, in overeenstemming met de overwegingen 6 tot 20 ;
5. Afschaffing van de besluitvormende rol bij de verwezenlijking van de gegevenverwerking van de functionaris voor gegevensbescherming (overw. 17 en 46) ;
6. Opleggen aan het NIS om een geautomatiseerd systeem op te zetten om abnormale verzoeken om toegang tot gegevens te detecteren (overw. 21) ;
7. Gegevensbescherming opnemen in de lijst van onderwerpen waarvoor het NIS-personeel, dat verantwoordelijk is voor de verwerking van persoonsgegevens, moet worden opgeleid (overw. 22) ;
8. Aanpassing van ontwerpartikel 15 betreffende de pseudonimisering van gegevens door het NIS overeenkomstig de overwegingen 24 tot 26 ;
9. Opname van het anonimiseringsproces in de door het NIS te nemen maatregelen (overw. 27 en 28 en 37) ;
10. Opname van specifieke maatregelen om concordantiesleutels te beschermen (overw. 30 en 33) ;
11. Toevoeging van een organisatorische maatregel die het NIS verplicht toezicht te houden op de configuratie van de gegevenstabellen die aan zijn thematische diensten ter beschikking worden gesteld, om ervoor te zorgen dat deze de vereiste garanties bieden als omschreven in overweging 34 ;
12. Aanpassing van ontwerpartikel 17, dat betrekking heeft op de pseudonimisering van gegevens die door het NIS zijn verstrekt overeenkomstig artikel 15 van de bovengenoemde wet van 1962, overeenkomstig de overweging 31 ;
13. Uitbreiding van de categorieën personen die onder de geheimhoudingsplicht en het statistisch geheim vallen en van de periode waarin zij aan deze verplichtingen onderworpen blijven (overweging 35) ;
14. Verduidelijking van de inhoud van de opdracht van de tussenpersoon die zowel in de voornoemde wet van 1962 als in het ontwerp van K aan het NIS wordt toevertrouwd (overw. 37 en 38 en 43)

en oplegging van specifieke wettelijke verplichtingen aan dit type tussenpersoon - om in te staan voor zowel het bestaan van specifieke waarborgen voor de betrokkenen bij de uitoefening van dit type taak, dat de koppeling van verschillende gegevensbanken en een grootschalige gegevensverwerking inhoudt - als voor een kwaliteitsgarantie van de diensten die de derde vertrouwde partij levert (overw. 45) ;

15. Verwijdering van bepalingen die het NIS toestaan gegevens te verwerken die onverenigbaar zijn met haar statuut van vertrouwde derde (hergebruik van voor derden verzamelde gegevens voor haar eigen behoeften (overw. 41 tot 43) ;
16. Verduidelijking dat het NIS optreedt als verwerkingsverantwoordelijke bij de verwerking van gegevens met het oog op koppeling, pseudonimisering en feitelijke anonimisering als tussenpersoon bij de beantwoording van verzoeken van derden als bedoeld in artikel 15 van voornoemde wet van 1962 (overw. 44).

Voor het Kenniscentrum,
(get.) Cédrine Molière, Directeur