



## Advies nr. 66/2018 van 25 juli 2018

**Betreft:** Ontwerp van koninklijk besluit tot wijziging van het koninklijk besluit van 12 augustus 1993 houdende de organisatie van de informatieveiligheid bij de instellingen van sociale zekerheid en het koninklijk besluit van 20 september 2012 houdende de organisatie van de informatieveiligheid bij het eHealth-platform en houdende vaststelling van de opdrachten en de bevoegdheden van de geneesheer onder wiens toezicht en verantwoordelijkheid de verwerking van persoonsgegevens betreffende de gezondheid door het eHealth-platform gebeurt (CO-A-2018-051).

De Gegevensbeschermingsautoriteit (hierna "de Autoriteit");

Gelet op de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit, inzonderheid de artikelen 23 en 26;

Gelet op het verzoek om advies van Mevr. M. De Block, Minister van Sociale Zaken en Volksgezondheid, ontvangen op 20 juni 2018;

Gelet op het verslag van Dhr. J. Baret;

Brengt op 25 juli 2018 het volgend advies uit:

## **I. VOORWERP EN CONTEXT VAN DE ADVIESAANVRAAG**

1. De Minister van Sociale Zaken en Volksgezondheid (hierna "de aanvrager") verzocht op 20 juni 2018 het advies van de Autoriteit over een Ontwerp van koninklijk besluit *tot wijziging van het koninklijk besluit van 12 augustus 1993 houdende de organisatie van de informatieveiligheid bij de instellingen van sociale zekerheid en het koninklijk besluit van 20 september 2012 houdende de organisatie van de informatieveiligheid bij het eHealth-platform en houdende vaststelling van de opdrachten en de bevoegdheden van de geneesheer onder wiens toezicht en verantwoordelijkheid de verwerking van persoonsgegevens betreffende de gezondheid door het eHealth-platform gebeurt* (hierna "het Ontwerp").
2. In het begeleidend schrijven bij de adviesaanvraag wordt aangegeven dat het Ontwerp tot doel heeft om bestaande reglementaire bepalingen aan te passen conform de nieuwe terminologie die wordt ingevoerd ingevolge de AVG.
3. Het Ontwerp dient ook samengelezen te worden met het wetsontwerp tot oprichting van de informatieveiligheidscomités<sup>1</sup> dat op 19 juli 2018 werd goedgekeurd door de Kamer van Volksvertegenwoordigers. De artikelen 24 & 48 van dit wetsontwerp hebben tot doel om aanpassingen door te voeren aan respectievelijk artikel 25 van de wet van 15 januari 1990 *houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid* & aan artikel 10 van de wet van 21 augustus 2008 *houdende oprichting en organisatie van het eHealth-platform*. Deze geplande aanpassingen zouden samengevat inhouden dat door de geviseerde instanties functionarissen voor gegevensbescherming zullen aangesteld worden en deze nieuwe bepalingen zullen meteen ook een rechtsbasis vormen voor de in het Ontwerp voorgestelde wijzigingen.

## **II. ONDERZOEK VAN DE ADVIESAANVRAAG**

4. De Autoriteit stelt vast dat de wijzigingen die door het Ontwerp worden beoogd geen aanleiding geven tot opmerkingen in het licht van de AVG. Deze bepalingen strekken er inderdaad toe om de terminologie in de hoger geciteerde KB's van 12 augustus 1993 en 20 september 2012 in overeenstemming te brengen met de AVG.

---

<sup>1</sup> Het betreft het wetsontwerp *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 95/46/EG* (DOC 54 3185/001 [http://www.dekamer.be/doc/flwb/pdf/54/3185/54k3185001.pdf#search="informatieveiligheidscomité](http://www.dekamer.be/doc/flwb/pdf/54/3185/54k3185001.pdf#search=) ). Zie in dit verband het advies van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer nr. 34/2018 van 11 april 2018, in het bijzonder de randnummers 14 t.e.m. 20.

5. De Autoriteit merkt tegelijk op dat de 2 geciteerde KB's dienen gelezen en toegepast te worden conform de AVG en dat elke functionaris voor gegevensbescherming die in deze context wordt aangesteld in de praktijk ook aan alle AVG-voorwaarden dient te voldoen<sup>2</sup>. Door de aanvrager wordt er bijvoorbeeld voor gekozen om de rol van functionaris voor gegevensbescherming toe te bedelen aan dezelfde persoon die ook adviezen verleent op het vlak van informatieveiligheid. In dit verband brengt de Autoriteit het standpunt in herinnering dat door de Commissie voor de Bescherming van de Persoonlijke Levenssfeer (hierna CBPL) werd ingenomen in randnummer 31 van haar aanbeveling nr. 04/2017:

*“In het verleden ontwikkelde de CBPL een jurisprudentie in toepassing waarvan zij een duidelijk onderscheid maakte tussen de functies van veiligheidsconsulent en functionaris voor gegevensbescherming, doch zonder er zich tegen te verzetten dat eenzelfde persoon deze functies zou cumuleren voor zover de wet hem de onontbeerlijke onafhankelijkheid waarborgde voor de vervulling van deze dubbele taak (...) Deze jurisprudentie kan vandaag niet worden aangewend om in alle gevallen te besluiten dat de vandaag in dienst zijnde veiligheidsconsulent automatisch de functionaris voor gegevensbescherming van morgen wordt. Zoals reeds vermeld is het voortaan afgemeten aan de functie van functionaris voor gegevensbescherming zoals beschreven in de AVG dat dit aspect moet worden onderzocht.”*

6. De Autoriteit kan zich in onderhavig advies aldus niet uitspreken over de AVG-conformiteit van alle aanstellingen van functionarissen voor gegevensbescherming die zullen plaatsvinden op basis van de twee hoger geciteerde KB's die ingevolge het Ontwerp gewijzigd zullen worden. Zoals ook reeds aangehaald door de CBPL, kan zij zich om verschillende redenen niet op dit pad begeven:

*“a. Volgens de AVG heeft de toezichthoudende autoriteit niet de bevoegdheid gekregen om de keuze van de verwerkingsverantwoordelijke of de verwerker voor een functionaris voor gegevensbescherming te valideren. In dit opzicht dient de mededeling van de contactgegevens van de functionaris voor gegevensbescherming aan de toezichthoudende autoriteit zoals voorzien in artikel 37.7 op generlei wijze beschouwd te worden als een vraag om akkoord of validatie van de DPA met betrekking tot deze aanduiding. Een dergelijke benadering zou strijdig zijn met de accountability.*

---

<sup>2</sup> Voor richtlijnen dienaangaande, zie:

- Info op website AUTORITEIT: <https://www.gegevensbeschermingsautoriteit.be/themadossier-functionaris-voor-gegevensbescherming>

- Aanbeveling CBPL nr. 04/2017

([https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/aanbeveling\\_04\\_2017\\_0.pdf](https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/aanbeveling_04_2017_0.pdf))

- Richtlijnen Groep 29 (WP 243)

([https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/wp243rev01\\_nl.pdf](https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/wp243rev01_nl.pdf))

*b. De nodige flexibiliteit moet overgelaten worden aan de verwerkingsverantwoordelijken en verwerkers met betrekking tot de manier waarop zij de taken en rol van elkeen in hun schoot wensen te organiseren. Een uniek organisatorisch model moet niet worden opgelegd.*

*c. De CBPL moet haar volledige onafhankelijkheid bewaren met het oog op de controles die zij genoopt zou worden uit te voeren, bijvoorbeeld ingevolge klachten tegen de verwerkingsverantwoordelijke of de verwerker, of op eigen initiatief. Hebben deze verwerkingsverantwoordelijken of verwerkers een functionaris voor gegevensbescherming aangewezen zodra zij hiertoe genoopt werden? Is deze functionaris effectief onafhankelijk? Bezit hij de vereiste kwalificaties? Beschikt hij over de nodige tijd om zijn taken effectief te vervullen?”<sup>3</sup>*

7. Bovendien wijst de Autoriteit er op dat het de verantwoordelijkheid van de aanvrager betreft om er voor te zorgen dat de volledige tekst van de twee hoger geciteerde KB's in overeenstemming zal worden gebracht met de AVG. Ten einde de aanvrager bij te staan in deze lopende oefening en zonder hierbij alle AVG-verplichtingen expliciet in de tekst van de twee geciteerde KB's geïntegreerd te willen zien<sup>4</sup>, vestigt de Autoriteit uit eigen beweging<sup>5</sup> de aandacht op de volgende punten:

- In het KB van 12 augustus 1993
  - dient in artikel 4, derde lid – dat handelt over de criteria op basis waarvan het Informatieveiligheidscomité functionarissen voor gegevensbescherming zal aanwijzen – voor alle duidelijkheid ook verwezen te worden naar de criteria vervat in de artikelen 37-38 AVG;
  - dient telkens wanneer naar “(informatie)veiligheid” verwezen wordt (zoals bv in artikel 3, 6, 7 & 8), eveneens expliciet naar het aspect “bescherming van persoonsgegevens” verwezen te worden;
  - zouden de artikelen 3 & 4<sup>6</sup> kunnen samengevoegd worden, bv. onder de noemer “informatieveiligheids –en dataproctiedienst”. De opdeling tussen

<sup>3</sup> Randnummer 25 van aanbeveling CBPL nr. 04/2017.

<sup>4</sup> De AVG is immers rechtstreeks van toepassing en prevaleert op de twee geciteerde KB's. Vanuit legistiek oogpunt dienen herhalingen van de AVG in nationaal recht ook vermeden te worden. De twee geciteerde KB's moeten hoe dan ook dus steeds samengelezen worden met de AVG en in geval van tegenstrijdigheid tussen nationale bepalingen en de AVG, heeft de AVG voorrang. Dit neemt niet weg dat de twee KB's zo goed mogelijk dienen afgestemd te worden op de AVG-voorschriften, vandaar de bijkomende aanbevelingen van de Autoriteit in randnummer 7 van onderhavig advies.

<sup>5</sup> Strikt genomen verzocht de aanvrager de Autoriteit immers enkel om advies te verlenen op het Ontwerp en niet op bepalingen die geen deel uitmaken van het Ontwerp, zoals sommige bepalingen van de twee geciteerde KB's.

<sup>6</sup> “Art. 3. De informatieveiligheidsdienst heeft een adviserende, stimulerende, documenterende en controlerende opdracht.

*De informatieveiligheidsdienst adviseert de verantwoordelijke voor het dagelijks bestuur van zijn instelling, op diens verzoek of op eigen initiatief, omtrent alle aspecten van de informatieveiligheid. Het advies wordt schriftelijk en gemotiveerd uitgebracht, tenzij de risico's niet voldoende ernstig zijn. Binnen de tijdsspanne vereist door de omstandigheden, maar met een maximum*

beide artikelen – artikel 4 handelt met name over de functionaris voor gegevensbescherming, terwijl artikel 3 over de dienst handelt die onder zijn leiding staat – zal immers, in het bijzonder na de integratie van de door het Ontwerp beoogde wijzigingen, artificieel/nodeloos complex ogen;

- o dient artikel 5 te worden aangepast. Momenteel luidt dit artikel immers als volgt: *“De informatieveiligheidsdienst werkt onder het rechtstreeks functioneel gezag van de verantwoordelijke voor het dagelijks bestuur van de instelling.”* De Autoriteit stelt voor om de woorden *“rechtstreeks functioneel gezag”* te vervangen door eenvoudigweg *“gezag”*, om te vermijden dat de indruk zou ontstaan dat de functionaris instructies ontvangt met betrekking tot de uitvoering van zijn of haar taken, wat in strijd is met artikel 38.3 AVG. In overweging 97 AVG wordt hieraan toegevoegd dat functionarissen voor gegevensbescherming *“dienen in staat te zijn hun taken en verplichtingen onafhankelijk te vervullen, ongeacht of zij in dienst zijn van de verwerkingsverantwoordelijke”*<sup>7</sup>.

- In het KB van 20 september 2012
  - o dient telkens wanneer naar de notie *“(informatie)veiligheid(sdienst)”* verwezen wordt (zoals bv in artikel 2, 3 & 4 van het KB van 20 september

---

*van drie maanden, beslist de verantwoordelijke voor het dagelijks bestuur het advies al dan niet op te volgen en deelt hij de veiligheidsdienst de genomen beslissing mee. In geval de beslissing van een schriftelijk advies afwijkt, dient de mededeling ervan op een schriftelijke en gemotiveerde wijze te geschieden.*

*De informatieveiligheidsdienst bevordert de naleving van de veiligheidsvoorschriften opgelegd door of krachtens een wets- of reglementsbeplating en het aannemen van een veiligheidsgedrag bij de personen tewerkgesteld in de instelling.*

*De informatieveiligheidsdienst legt de nodige documentatie aan met betrekking tot de informatieveiligheid.*

*De informatieveiligheidsdienst ziet toe op de naleving binnen de instelling van de veiligheidsvoorschriften opgelegd door of krachtens een wets- of reglementsbeplating. Alle vastgestelde inbreuken worden schriftelijk en uitsluitend aan de verantwoordelijke voor het dagelijks bestuur van de instelling meegedeeld, vergezeld van de nodige adviezen om dergelijke inbreuken in de toekomst te vermijden.*

*Art. 4. De informatieveiligheidsdienst wordt geleid door de veiligheidsconsulent. De veiligheidsconsulent kan zich laten bijstaan door één of meer adjuncten.*

*De veiligheidsconsulent en zijn eventuele adjuncten in de beheersinstellingen van een secundair netwerk en de instellingen die niet behoren tot een secundair netwerk worden aangesteld na advies van het Toezichtscomité.*

*Vooraleer zijn advies uit te brengen, gaat het Toezichtscomité inzonderheid na of de betrokkenen voldoende kennis en beschikbare tijd hebben voor de goede uitvoering van hun opdracht en geen activiteiten uitoefenen die onverenigbaar zijn met de opdracht. De identiteit van de veiligheidsconsulent en zijn eventuele adjuncten wordt na hun aanstelling onverwijld meegedeeld aan het Toezichtscomité.*

*Na hun aanstelling wordt de identiteit van de veiligheidsconsulent en zijn eventuele adjuncten in de andere instellingen dan deze bedoeld in het tweede lid, meegedeeld aan de beheersinstelling van het betrokken secundair netwerk en door deze instelling onverwijld aan het Toezichtscomité.*

*De veiligheidsconsulenten en hun eventuele adjuncten kunnen niet van deze functie worden ontheven wegens meningen die zij uiten of daden die zij stellen in het kader van de goede uitoefening van hun functie.”*

<sup>7</sup> De Groep 29 gaf hierover in haar WP243 de volgende duiding: *“(…) Dit betekent dat functionarissen voor gegevensbescherming bij het vervullen van hun taken krachtens artikel 39 geen instructies mogen ontvangen over hoe ze een bepaalde aangelegenheid moeten behandelen, bijvoorbeeld tot welk resultaat ze moeten komen, hoe ze een klacht moeten onderzoeken, of nog of ze al dan niet de toezichthoudende autoriteit moeten raadplegen. Daarenboven mogen ze ook geen instructies ontvangen om een bepaald standpunt in te nemen in een aangelegenheid die verband houdt met de wet op de gegevensbescherming, bijvoorbeeld een specifieke interpretatie van de wet. (...)”*

- 2012), eveneens expliciet naar het aspect “bescherming van persoonsgegevens” verwezen te worden;
- dient telkens de term “informatieveiligheidsconsulent” te worden vervangen door de term “functionaris voor gegevensbescherming” (cf. bv. artikelen 7 & 8 van het KB van 20 september 2012, die – in tegenstelling tot artikel 3 van hetzelfde KB – niet worden gewijzigd ingevolge artikel 11 van het Ontwerp);
  - dient de term “persoonsgegevens die de gezondheid betreffen” telkens vervangen te worden door de AVG-notie “gegevens over gezondheid”<sup>8</sup>;
  - zou in artikel 9, eerste lid, voor alle duidelijkheid kunnen bepaald worden dat de voorstellen van de beroepsbeoefenaar in de gezondheidszorg niet alleen aan de verantwoordelijke voor het dagelijks bestuur, maar ook aan de functionaris voor gegevensbescherming worden overgemaakt (maar dit vloeit eigenlijk ook voort uit artikel 38.1. AVG);
  - dient de in artikel 9, laatste lid, voorziene interne melding van inbreuken in verband met persoonsgegevens afgestemd te worden op de artikelen 33 & 34 AVG, opdat dergelijke inbreuken door de verwerkingsverantwoordelijke desgevallend ook binnen de door de AVG gestelde termijnen zouden gemeld worden aan de Autoriteit en aan de betrokkene. Momenteel voorziet artikel 9, laatste lid, van het KB van 20 september 2012 immers niet in termijnen;
  - zou in artikel 10 voor alle duidelijkheid kunnen bepaald worden dat de beroepsbeoefenaar in de gezondheidszorg pas na advies van de functionaris voor gegevensbescherming de personen zal aanwijzen die binnen het eHealth-platform betrokken worden bij de verwerking van gegevens over gezondheid (maar dit vloeit eigenlijk ook voort uit artikel 38.1. AVG).

## OM DEZE REDENEN

Brengt de Autoriteit een **gunstig advies** uit aangaande het Ontwerp en dit onder de uitdrukkelijke voorwaarde dat

- elke functionaris voor gegevensbescherming die in deze context in de praktijk wordt aangesteld ook aan alle AVG-voorwaarden voldoet (randnummers 5&6);

---

<sup>8</sup> Artikel 4, 15), AVG.

- de aanvrager bijkomende aanpassingen aan voornoemde KB's van 12 augustus 1993 en 20 september 2012 aanbrengt ten einde deze in conformiteit te brengen met de AVG (randnummer 7);

De Wnd. Administrateur,

De Voorzitter,

(get.) An Machtens

(get.) Willem Debeuckelaere