

<p>Informatieveiligheidscomité Kamer sociale zekerheid en gezondheid</p>
--

IVC/KSZG/22/508

BERAADSLAGING NR. 22/282 VAN 8 NOVEMBER 2022 BETREFFENDE DE MEDEDELING VAN PERSOONSgegevens DOOR FOD VVVL AAN HET EHEALTH-PLATFORM IN HET KADER VAN DE OPRICHTING VAN EEN DPO CONTACTgegevens DATABANK BINNEN HET EHEALTH-PLATFORM

Het Informatieveiligheidscomité, kamer sociale zekerheid en gezondheid (hierna “het Comité” genoemd),

Gelet op de Verordening (EU) nr. 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* (Algemene Verordening Gegevensbescherming of AVG);

Gelet op de wet van 3 december 2017 *tot oprichting van de Gegevensbeschermingsautoriteit*, in het bijzonder artikel 114, gewijzigd bij de wet van 25 mei 2018;

Gelet op de wet van 30 juli 2018 *betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens*;

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 95/46/EG*, in het bijzonder artikel 97;

Gelet op de wet van 21 augustus 2008 *houdende oprichting en organisatie van het eHealth-platform en diverse bepalingen*, in het bijzonder artikel 5, 1°, 2°, 9° ;

Gelet op het auditoraatsrapport van het eHealth-platform van 28 oktober 2022;

Gelet op het verslag van de heer Bart Viaene.

Beslist op 8 november 2022, na beraadslaging, als volgt :

I. ONDERWERP VAN DE AANVRAAG

1. Krachtens artikel 4 van de Wet van 21 augustus 2008 houdende oprichting en organisatie van het eHealth-platform, heeft het eHealth-platform als doel om, door een onderlinge

elektronische dienstverlening en informatie-uitwisseling tussen alle actoren in de gezondheidszorg, georganiseerd met de nodige waarborgen op het vlak van de informatieveiligheid en de bescherming van de persoonlijke levenssfeer, de kwaliteit en de continuïteit van de gezondheidszorgverstrekking en de veiligheid van de patiënt te optimaliseren, de vereenvoudiging van de administratieve formaliteiten voor alle actoren in de gezondheidszorg te bevorderen en het gezondheidsbeleid te ondersteunen.

2. Een belangrijk aspect bij de informatie-uitwisseling is de beschikbaarheid van de diensten van de verschillende actoren. Immers, een onbeschikbaarheid van de informatie over een patiënt kan leiden tot een verstoring in de dienstverlening naar deze patiënt.
3. De beschikbaarheid van de uitgewisselde gegevens kent meerdere bedreigingen. Zo zal een technisch incident op de infrastructuur reeds kunnen leiden tot een onderbreking van de uitwisselingen.
4. Sedert het uitbreken van de COVID-crisis is ook duidelijk geworden dat naast de technische incidenten, de cyberbedreigingen een ernstige impact kunnen hebben op de beschikbaarheid van de systemen. Wanneer zulk een bedreiging zich concretiseert, dan kan deze de getroffen systemen impacteren, maar mogelijks ook snel uitbreiden naar andere partijen.
5. Voor zowel technische incidenten als voor cyberdreigingen is het van groot belang dat de verschillende partijen snel kunnen gecontacteerd worden zodat deze maatregelen kunnen nemen om een mogelijk gevaar adequaat af te wenden of om gepaste maatregelen te nemen om de gevolgen van een incident op de dienstverlening te beperken.
6. In de voorbije 2 jaar heeft de veiligheidsdienst van eHealth Platform samen met het CCB regelmatig waarschuwing gestuurd naar ziekenhuizen betreffende cyberdreigingen die de werking van de systemen van ziekenhuizen konden verstoren. De informatie over de dreigingen werd gestuurd naar de DPO's van de ziekenhuizen die deze verder liet behandelen door de IT afdelingen of de dienst informatieveiligheid van de ziekenhuizen.
7. De informatie over de bedreigingen bleek nuttig voor de ziekenhuizen en de contactlijsten werden op vraag van de DPO's en de IT-afdelingen uitgebreid naar personeel van de IT-afdelingen om de berichten sneller tot bij de betrokkenen te brengen en om ervoor te zorgen dat de onbeschikbaarheid van de DPO niet tot onnodige vertraging zou leiden.
8. Om de ziekenhuizen nog beter te kunnen informeren vraagt eHealth platform toegang te krijgen tot de contactgegevens van de leidinggevenden binnen de ziekenhuizen. Deze contactgegevens zullen enkel gebruikt worden om de ziekenhuizen te informeren over cyberdreigingen of aan de gang zijnde incidenten die een mogelijke bedreiging vormen voor de diensten van het ziekenhuis en die onmiddellijke aandacht vereisen. De gegevens betreffen:
 - Naam ziekenhuis
 - Naam leidinggevende
 - Rol leidinggevende
 - Telefoonnummer
 - GSM nummer

- Email adres

II. BEVOEGHEID

9. Krachtens artikel 4, 1) van de AVG wordt onder persoonsgegevens verstaan alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon; wordt beschouwd als een “ïdentificeerbare natuurlijke persoon” een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor zijn fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit.
10. Krachtens artikel 11 van de wet van 21 augustus 2008 *houdende oprichting en organisatie van het eHealth-platform en diverse bepalingen* vereist elke mededeling van persoonsgegevens door of aan het eHealth-platform een beraadslaging van de kamer sociale zekerheid en gezondheid van het Informatieveiligheidscomité, behalve in de gevallen waarin de wet voorziet.
11. Het Comité acht zich dan ook bevoegd om zich uit te spreken over de mededeling van persoonsgegevens.

III. BEHANDELING VAN DE AANVRAAG

A. TOELAATBAARHEID

12. De verwerking van persoonsgegevens is enkel rechtmatig indien en voor zover minstens één van de voorwaarden vermeld in artikel 6 van de AVG vervuld is. Dit is onder meer het geval wanneer 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 opgedragen¹.
13. Volgens het [Koninklijk Besluit van 12 februari 2008](#) houdende bepaling van de regels volgens welke de beheerder van de ziekenhuizen aan de Minister die de Volksgezondheid onder zijn bevoegdheid heeft, mededeling doet van de identiteit van de personen verantwoordelijk voor het mededelen van gegevens die met de inrichting verband houden., gewijzigd door [Koninklijk Besluit van 9 december 2021](#) waar de beheerder van het ziekenhuis verplicht is om de identiteit (naam, voornaam en rijksregisternummer) en de contactgegevens (vast en/of mobiel (GSM) telefoonnummer en e-mailadres) mee te delen van personen die verantwoordelijk zijn voor het mededelen van gegevens die met het ziekenhuis verband houden.
 - de algemeen directeur,
 - de hoofdarts,

¹ Art. 6, §1, e), van de GDPR.

- het hoofd van het verpleegkundig departement,
 - de persoon of personen die verantwoordelijk zijn voor het mededelen van de financiële toestand en de bedrijfsuitkomsten van het ziekenhuis,
 - de persoon of personen verantwoordelijk voor het mededelen van de statistische gegevens van het ziekenhuis,
 - de functionaris voor gegevensbescherming (Data Protection Officer) bedoeld in artikel 37 van de 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 (algemene verordening gegevensbescherming).
14. Volgens artikel 5, 1°, 2°, 9° van de eHealth-wet² is het eHealth-platform voor de uitvoering van zijn doel belast met het ontwikkelen van een visie en een strategie voor een effectieve, efficiënte en goed beveiligde elektronische dienstverlening en informatie-uitwisseling in de gezondheidszorg, met respect voor de bescherming van de persoonlijke levenssfeer en in nauw overleg met de onderscheiden openbare en private actoren in de gezondheidszorg, het vastleggen van nuttige ICT-gerelateerde functionele en technische normen, standaarden, specificaties en basisarchitectuur voor een inzet van de ICT ter ondersteuning van deze visie en strategie, en het bevorderen van de naleving van de visie, de strategie, de functionele en technische normen, standaarden en specificaties, de basisarchitectuur, evenals het gebruik van het samenwerkingsplatform voor de veilige elektronische gegevensuitwisseling en de basisdiensten en de verwezenlijking van de programma's en de projecten door zoveel mogelijk actoren in de gezondheidszorg. In uitvoering hiervan zijn minimale veiligheidsnormen vastgelegd die o.a. voorzien in warning- en informatieverstrekkingssystemen inzake gegevensbescherming en informatieveiligheid. Daarvoor zijn de contactgegevens nodig.
15. Het Informatieveiligheidscomité is bijgevolg van oordeel dat er een aanvaardbare grond bestaat voor de beoogde verwerking van persoonsgegevens.

B. PRINCIPES MET BETREKKING TOT DE VERWERKING VAN PERSOONSGEGEVENS

16. Volgens artikel 5 van de AVG moeten de persoonsgegevens worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is (rechtmatigheid, behoorlijkheid, transparantie).
17. Krachtens artikel 5, 5°, van de voormelde eHealth-wet, kan het eHealth-platform een databank met persoonsgegevens oprichten ter ondersteuning van een initiatief in het domein van de gezondheid.

² Wet van 21 augustus 2008 houdende oprichting en organisatie van het eHealth-platform, B.S. van 13 oktober 2008, p. 54454.

18. Volgens artikel 5 van de AVG moeten de persoonsgegevens toereikend, ter zake dienend en beperkt zijn tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt (minimale gegevensverwerking).
19. De databank die door het eHealth-platform gehost wordt bevat de identificatie- en contactgegevens die strikt noodzakelijk zijn om de verantwoordelijken van een ziekenhuis te identificeren en contacteren.
20. Het Comité stelt vast dat het eHealth-platform geen enkel persoonsgegeven dat de gezondheid betreft zal bijhouden met betrekking tot de contactpersonen.
21. Krachtens artikel 5 van de AVG moeten de persoonsgegevens worden ingezameld voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden en mogen ze vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt.
22. Deze databank moet het eHealth-platform in de mogelijkheid stellen om de directie van een ziekenhuiste contacteren ingeval een technisch incident of een cyberdreiging een bedreiging kan vormen voor het functioneren van het ziekenhuis.
23. Krachtens artikel 5 van de AVG moeten de persoonsgegevens juist zijn en zo nodig worden geactualiseerd; alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren (juistheid). Hiervoor zal de FOD VVVL op regelmatige basis updates van deze contactlijsten sturen naar het eHealth-platform.
24. Rekening houdend met het doeleinde van de verwerking is het Comité van oordeel dat de beoogde mededeling toereikend, ter zake dienend en niet overmatig is.

C. PRINCIPE VAN TRANSPARANTIE

25. Overeenkomstig artikel 14 van de AVG verstrekt de verwerkingsverantwoordelijke de betrokkene bepaalde informatie wanneer de persoonsgegevens niet bij hem werden verkregen. Deze bepaling geldt echter niet wanneer het verkrijgen of verstrekken van de gegevens uitdrukkelijk is voorgeschreven bij Unie- of lidstatelijk recht dat op de verwerkingsverantwoordelijke van toepassing is en dat recht voorziet in passende maatregelen om de gerechtvaardigde belangen van de betrokkene te beschermen.
26. Krachtens de verplichtingen opgelegd in de GDPR zal het eHealth-platform deze verwerkingen publiceren op zijn website waar ook de andere verwerkingen worden gepubliceerd.
27. Het Comité is van oordeel dat de huidige transparantiemaatregelen toereikend zijn.

D. VEILIGHEIDSMATREGELEN

- 28.** Krachtens artikel 5 van de AVG moeten persoonsgegevens, 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). Deze maatregelen moeten een passend beveiligingsniveau verzekeren, rekening houdend enerzijds met de stand van de techniek ter zake en de kosten voor het toepassen van de maatregelen en anderzijds met de aard van de te beveiligen gegevens en de potentiële risico's.
- 29.** Om de vertrouwelijkheid en de veiligheid van de gegevensverwerking te garanderen, moet iedere instelling die persoonsgegevens bewaart, verwerkt of meedeelt maatregelen nemen in de volgende elf actiedomeinen die betrekking hebben op de informatieveiligheid: veiligheidsbeleid; aanstelling van een functionaris inzake gegevensbescherming; organisatorische en menselijke aspecten van de veiligheid (vertrouwelijkheidsverbintenis van het personeel, regelmatige informatieverstrekking en opleidingen ten behoeve van het personeel inzake bescherming van de privacy en veiligheidsregels); fysieke veiligheid en veiligheid van de omgeving; netwerkbeveiliging; logische toegangs- en netwerkbeveiliging; loggings, opsporing en analyse van de toegangen; toezicht, nazicht en onderhoud; systeem van beheer van de veiligheidsincidenten en de continuïteit (backup-systemen, fault tolerance-systemen, ...) en documentatie.
- 30.** Het Comité stelt vast dat het eHealth-platform beschikt over een functionaris voor gegevensbescherming en voldoet aan deze vereisten inzake informatieveiligheid.

Om deze redenen, verleent

de kamer sociale zekerheid en gezondheid van het informatieveiligheidscomité

krachtens het artikel 5, 1°, 2°, 9° van de wet van 21 augustus 2008 *houdende oprichting en organisatie van het eHealth-platform*, een machtiging voor de oprichting binnen het eHealth-platform van een persoonsgegevensbank met betrekking tot de leidinggevenden van ziekenhuizen,

een machtiging voor de mededeling van de persoonsgegevens zoals beschreven in deze beraadslaging 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

Bart VIAENE
Voorzitter

De zetel van de kamer sociale zekerheid en gezondheid van het informatieveiligheidscomité is gevestigd in de kantoren van de Kruispuntbank van de Sociale Zekerheid, op het volgende adres: Willebroekkaai 38 – 1000 Brussel (tel. 32-2-741 83 11).