Informatieveiligheidscomité

Kamer sociale zekerheid en gezondheid

IVC/KSZG/21/288

BERAADSLAGING NR. 19/166 VAN 1 OKTOBER 2019, GEWIJZIGD OP 6 JULI 2021, MET BETREKKING TOT HET REGLEMENT TOT VASTSTELLING VAN DE CRITERIA VOOR DE TOEPASSING VAN EEN CIRKEL VAN VERTROUWEN DOOR EEN ORGANISATIE IN HET KADER VAN DE UITWISSELING VAN GEZONDHEIDSGEGEVENS

Het Informatieveiligheidscomité,

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

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 13 december 2006 *houdende diverse bepalingen betreffende gezondheid*, in het bijzonder artikel 42, § 2, 3°, gewijzigd bij de wet van 5 september 2018;

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 het auditoraatsrapport van het eHealth-platform van 25 juni 2021;

Gelet op het verslag van de heer Bart Viaene;

Beslist op 6 juli 2021, na beraadslaging, als volgt:

I. ONDERWERP

1. In het kader van het reglement met betrekking tot de therapeutische relaties ("nota betreffende de elektronische bewijsmiddelen van een therapeutische relatie en van een zorgrelatie", die goedgekeurd werd door het Beheerscomité van het eHealth-platform op 13 november 2018 en door het Informatieveiligheidscomité op 4 december 2018) wordt er verwezen naar het begrip "circle of trust". Ter herinnering, een "circle of trust" kan worden gedefinieerd als "een groep gebruikers van een organisatie waarvoor de organisatie zelf, op verschillende niveaus, maatregelen inzake informatieveiligheid neemt en toeziet op de naleving ervan, zodat andere organisaties redelijkerwijze erop kunnen vertrouwen dat deze veiligheidsmaatregelen nageleefd worden en ze die niet zelf dienen te organiseren of te controleren".

2. Het is gebleken dat naargelang de regio maar ook naargelang het type organisatie, de toepassingsregels voor dit principe van circle of trust kunnen verschillen. Het eHealth-platform heeft daarom het initiatief genomen om dit principe te concretiseren teneinde de coherentie ervan voor de hele sector te garanderen. Het is immers essentieel dat er minimale regels worden vastgesteld voor de organisaties die de circle of trust toepassen. Deze concretisering van het principe is essentieel voor het behoud van het vertrouwen in het systeem vanwege de verschillende actoren.

3. Tijdens zijn vergadering van 4 september 2019 heeft het Beheerscomité van het eHealth-platform de "nota met betrekking tot het reglement tot vaststelling van de criteria voor de toepassing van een cirkel van vertrouwen door een organisatie in het kader van de uitwisseling van gezondheidsgegevens" in tweede lezing goedgekeurd. Dit reglement is bijgevoegd als bijlage en is ook beschikbaar op de website van het eHealth-platform[1].

4. Cirkels van vertrouwen kunnen worden georganiseerd door tal van organisaties, zoals ziekenhuizen, organisaties belast met indicatiestellingen in het kader van BelRAI, ziekenfondsen, enz. Opdat andere organisaties dan de organisatie die een cirkel van vertrouwen instelt, daarin rechtmatig vertrouwen zouden kunnen hebben, worden criteria vastgelegd waaraan elke organisatie die dergelijke cirkel van vertrouwen wenst te organiseren moet voldoen. Deze criteria verwijzen maximaal naar reeds bestaande Europese en Belgische regelgeving, zoals de Algemene Verordening Gegevensbescherming (AVG). Zij doen geen afbreuk aan deze regelgeving, die ten volle blijft gelden, maar preciseren in een aantal gevallen de wijze waarop aan deze regelgeving dient te worden voldaan.

5. Na advies van het Beheerscomité van het eHealth-platform van 11 juni 2019 en van de werkgroep Toegang van het Overlegcomité met de gebruikers van het eHealth-platform op 27 augustus 2019, werd een lijst van 13 criteria vastgesteld:

1° register van de verwerkingsactiviteiten;
2° precisering van de rechtsgronden voor de verwerking van bijzondere categorieën van persoonsgegevens;
3° verwerkingsbeperking;
4° authenticatie van de identiteit van de gebruiker;

[1] https://www.ehealth.fgov.be/ehealthplatform/nl/reglementen.

5° verificatie van de relevante kenmerken en relaties van de gebruiker;
6° interne logging;
7° audittrail;
8° informatie, vorming en sensibilisering;
9° interne controle;
10° naleving beraadslagingen Informatieveiligheidscomité;
11° opname in de authentieke bron Cobrha als organisatie die een cirkel van vertrouwen organiseert;
12° openbare documentatie;
13° externe controle.

6. Na advies van het Beheerscomité van het eHealth-platform van 8 juni 2021 is beslist dat de kleinere instanties die minder geïnformatiseerd zijn, een CoT-light zullen mogen implementeren, dat wil zeggen dat de criteria 6 (interne logging) en 7 (audittrail) niet moeten worden toegepast. Het Beheerscomité is er zich immers van bewust dat het voor kleine, minder geïnformatiseerde instellingen moeilijk is om te voldoen aan alle criteria van een "circle of trust" en heeft daarom beslist om uitzonderlijk de mogelijkheid te bieden om een "circle of trust light" te implementeren. Deze "circle of trust light" vormt een uitzondering op het vlak van implementatie van een user and access management (UAM) zoals ontwikkeld door de basisdiensten van het eHealth-platform. De bedoeling van deze uitzondering is om de invoering van minimale maatregelen op het vlak van naleving van de informatieveiligheidsprincipes aan te moedigen, rekening houdend met de graad van informatisering van de kleine instellingen.

II. BEVOEGDHEID

7. Krachtens artikel 11 van de wet van 21 augustus 2008 *houdende oprichting en organisatie van het eHealth-platform* vereist elke mededeling van persoonsgegevens door of aan het eHealth-platform een beraadslaging van de kamer sociale zekerheid en gezondheid van het Informatieveiligheidscomité.

8. Bij beraadslaging nr. 09/008 van 20 januari 2009, laatst gewijzigd op 15 juni 2010, heeft het Comité zich in het bijzonder uitgesproken over de toepassing van het geïntegreerde gebruikers- en toegangsbeheer door het eHealth-platform bij de uitwisseling van persoonsgegevens. Een betrouwbaar systeem van gebruikers- en toegangsbeheer bepaalt welke gebruiker, in welke hoedanigheid en in welke omstandigheden, toegang mag hebben tot welke types van persoonsgegevens met betrekking tot welke personen en welke periode.

9. Het Informatieveiligheidscomité oordeelt bijgevolg dat het bevoegd is.

III. BEHANDELING

10. De verwerking van persoonsgegevens is enkel toegelaten voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. De verwerking van persoonsgegevens die de gezondheid betreffen is in principe verboden[2].

[2] Art. 9, § 1, van de AVG

11. Het verbod geldt echter niet wanneer de verwerking noodzakelijk is voor doeleinden van preventieve of arbeidsgeneeskunde, voor de beoordeling van de arbeidsgeschiktheid van de werknemer, medische diagnosen, het verstrekken van gezondheidszorg of sociale diensten of behandelingen dan wel het beheren van gezondheidszorgstelsels en -diensten of sociale stelsels en diensten, op grond van Unierecht of lidstatelijk recht, of uit hoofde van een overeenkomst met een gezondheidswerker[3].

12. De verwerking van persoonsgegevens, inzonderheid van persoonsgegevens m.b.t. de gezondheid, dient te geschieden met de nodige maatregelen inzake informatieveiligheid en bescherming van de persoonlijke levenssfeer. Een belangrijk aspect daarvan is de waarborg dat de persoonsgegevens enkel worden verwerkt voor rechtmatige doeleinden en door personen die, voor het bereiken van die doeleinden, nood hebben aan de verwerking van persoonsgegevens m.b.t. de betrokkene. In een systeem van gedeelde verwerking van persoonsgegevens door tal van actoren, vereist het bieden van dergelijke waarborg een duidelijke vastlegging van de verantwoordelijkheden van elkeen. Het reglement wil hiertoe bijdragen door het preciseren van het concept van 'cirkels van vertrouwen'.

13. Het Comité benadrukt dat, naast de regels die vastgesteld zijn in de voormelde beraadslaging nr. 09/008, het zeer belangrijk is dat er vaste regels zijn voor de toepassing van een "cirkel van vertrouwen".

14. Het Comité herinnert eraan dat het lidmaatschap van een "cirkel van vertrouwen" de groep gebruikers van een organisatie of de organisatie zelf niet vrijstelt van de naleving van 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) en van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens. Dit geldt ook voor het lidmaatschap van een "circle of trust light".

[3] Art 9, § 2, h) van de AVG

De kamer sociale zekerheid en gezondheid van het informatieveiligheidscomité

keurt het bijgevoegde reglement tot vaststelling van de criteria voor de toepassing van een cirkel van vertrouwen door een organisatie in het kader van de uitwisseling van gezondheidsgegevens goed.

Bart VIAENE
Voorzitter