Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid
Afdeling "Gezondheid"

SCSZG/17/047

BERAADSLAGING NR. 17/023 VAN 21 MAART 2017 BETREFFENDE DE MEDEDELING VAN PERSOONSGEGEVENS AAN EN DOOR HET EHEALTH-PLATFORM IN HET KADER VAN DE BASISDIENST "VEILIGHEIDSLOGGING"

De afdeling gezondheid van het Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid (hierna "het Sectoraal Comité" genoemd),

Gelet op de wet van 15 januari 1990 *houdende oprichting en organisatie van een Kruispuntbank van de Sociale Zekerheid*, inzonderheid op artikel 37;

Gelet op de wet van 8 december 1992 *tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens;*

Gelet op de wet van 21 augustus 2008 *houdende oprichting en organisatie van het eHealth-platform*;

Gelet op het auditoraatsrapport van het eHealth-platform van 14 maart 2017;

Gelet op het verslag van de heer Yves Roger.

Beslist op 21 maart 2017, na beraadslaging, als volgt:

I. ONDERWERP

1. Het eHealth-platform heeft een webtoepassing ontwikkeld voor de consultatie van de gegevens van veiligheidsloggings. Zodoende zullen informatieveiligheidsconsulenten de veiligheidsloggings gegenereerd door het eHealth-platform via een beveiligde webtoepassing in real time kunnen consulteren.

2. De drie belangrijkste functionaliteiten van deze toepassing zijn:

- het opzoeken van loggegevens op basis van criteria en het op het scherm tonen van de resultaten in een tabel;
- het op het scherm tonen van statistieken (aantal loggegevens gegenereerd per maand en per instelling/toepassing);
- de export van de zoekresultaten in een standaardformaat.

3. De toepassing zal ter beschikking worden gesteld van volgende gebruikers:
- De *Host Security Responsible:* deze rol wordt toegekend aan de veiligheidsverantwoordelijken van de organisatie (een Belgische onderneming) die de toepassingen voor rekening van een platform of een organisatie host. Deze hebben uitsluitend in de acceptatieomgeving[1] toegang tot het geheel van de veiligheidsloggings van de toepassingen die bij hen worden gehost teneinde de correcte logging te kunnen valideren. Zij hebben géén toegang tot de loggegevens in de productieomgeving.
- De *Platform Security Responsible:* deze rol wordt toegekend aan de veiligheidsverantwoordelijken van een platform waarvan de toepassingen afhangen (federale of regionale instelling). Zij hebben toegang tot het geheel van veiligheidsloggings van de toepassingen die op hun platform worden gehost of die ervan afhangen in de productieomgeving.
- De *Organization Treatment Security Responsible*: deze rol wordt toegekend aan de veiligheidsverantwoordelijken van een toepassing voor een organisatie. Zij hebben uitsluitend toegang tot de veiligheidsloggings die worden gegenereerd voor de toepassingen waarvoor zij de verantwoordelijke van de verwerking in een productieomgeving zijn.

4. De gegevensstromen die in het kader van de dienst Veiligheidslogging worden gegenereerd zijn de volgende:
- De handelingen van de gebruikers van de toepassingen worden gelogd op de servers van de toepassingen, meer bepaald: wie heeft wat gedaan, met betrekking tot welke persoon, wanneer en hoe.
- Deze gegevens worden vervolgens meegedeeld aan het databasemanagementsysteem waar ze worden geïndexeerd en worden omgezet in een formaat dat toelaat opzoekingen uit te voeren.
- Wanneer een gebruiker de loggegevens consulteert via de webapplicatie, worden de gegevens gerecupereerd dankzij de zoekmotor van het databasemanagementsysteem en worden ze gefilterd naar gelang het profiel van de gebruiker. Overeenkomstig artikel 46, § 2, tweede lid, van de wet van 15 januari 1990 tot oprichting en organisatie van een Kruispuntbank van de sociale zekerheid is de afdeling gezondheid van het Sectoraal comité onder meer belast met het verzekeren van het toezicht op de naleving van de

[1] Een computertoepassing wordt ontwikkeld in de "*ontwikkelomgeving*", een systeem dat volledig autonoom werkt en geen interactie met andere systemen heeft (de ontwikkelaars zijn de enigen die de ontwikkelomgeving gebruiken). Zodra de ontwikkelaars hun opdracht hebben vervuld, wordt de computertoepassing gekopieerd naar de "*testomgeving*", waarin wordt nagegaan of ze beantwoordt aan de behoeften (ook de interactie met andere systemen wordt daarbij getest). Vervolgens wordt de computertoepassing in de "*acceptatieomgeving*" gebracht, dat is de omgeving waarin de opdrachtgever zelf terecht kan om de computertoepassing te aanvaarden (dat wil zeggen na te gaan of ze functioneert zoals hij dat wenst) en waarin gebruik wordt gemaakt van fictieve persoonsgegevens. Indien de opdrachtgever de computertoepassing goedkeurt, wordt ze ten slotte gekopieerd naar de "*productieomgeving*" waar ze gebruikt kan worden door alle gebruikers met reële persoonsgegevens.

door of krachtens de wet vastgestelde bepalingen tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens die de gezondheid betreffen. Daarbij kan zij alle aanbevelingen formuleren die zij nuttig acht en bijdragen tot het oplossen van principiële problemen of geschillen.

II. BEVOEGDHEID

5. Aangezien de loggegevens persoonsgegevens bevatten betreffende de gebruikers en de personen met betrekking tot dewelke handelingen worden gesteld, vereist de mededeling ervan door of aan het eHealth-platform overeenkomstig artikel 11, eerste lid, van de wet van 21 augustus 2008 *houdende oprichting en organisatie van het eHealth-platform en diverse bepalingen* een principiële machtiging van de afdeling gezondheid van het sectoraal comité van de sociale zekerheid en van de gezondheid.

6. Voor zover de loggegevens persoonsgegevens betreffende de gezondheid bevatten, vereist de mededeling ervan overeenkomstig artikel 42, § 2, 3 °, van de wet van 13 december 2006 *houdende diverse bepalingen betreffende gezondheid* eveneens een machtiging van de afdeling gezondheid van het sectoraal comité van de sociale zekerheid en van de gezondheid vereist.

III. BEHANDELING

7. De mededeling van de persoonsgegevens door het eHealth-platform aan de verschillende categorieën van veiligheidsverantwoordelijken beoogt een gerechtvaardigd doeleinde, namelijk de consultatie mogelijk maken van de loggegevens betreffende het gebruik van de toepassingen waarvoor zij een verantwoordelijkheid dragen.

8. De meegedeelde persoonsgegevens zijn, uitgaande van dat doeleinde, toereikend, relevant en niet overmatig. Ze blijven beperkt tot de informatie omtrent wie welke handeling heeft gesteld, met betrekking tot welke persoon, wanneer en hoe. Hierbij worden de natuurlijke personen geïdentificeerd door het identificatienummer van de sociale zekerheid. Instellingen en rechtspersonen worden geïdentificeerd aan de hand van het in voorkomend geval gebruikte identificatienummer (KBO, RIZIV-nummer, etc.).

9. Het Sectoraal comité stelt vast dat bepaalde veiligheidsloggings ten gevolge van de identiteit van de betrokken zorginstellingen of zorgverleners (bv. psychiatrische ziekenhuizen, bepaalde artsen-specialisten) eveneens gezondheidsgegevens kunnen bevatten. Het Sectoraal comité stelt dat het voorzien in veiligheidsloggings een essentieel onderdeel van de door de privacywet vereiste organisatorische en technische maatregelen ter bescherming van de persoonsgegevens (art. 16, § 4, van privacywet) vormt, zodat de mededeling van persoonsgegevens met een potentieel gezondheidskarakter in het kader van het aanleggen van veiligheidsloggings als toereikend, terzake dienend en relevant moet worden geacht.

10. Er worden drie rollen gecreëerd voor de gebruikers van de dienst ‘Veiligheidsloggings’, meer bepaald *Host Security Responsible, Platform Security Responible* en *Organization Treatment Security Responsible*, die elk specifieke toegangsrechten hebben zoals hoger

verduidelijkt. Aan de hand van volgend voorbeeld kunnen hun specifieke bevoegdheden verduidelijkt worden.

11. Via de toepassing SACEx van het FAGG kunnen Belgische fabrikanten van medische hulpmiddelen zoals implantaten exportcertificaten aanvragen. Deze toepassing genereert veiligheidsloggings ten gevolge van het gebruik van het INSZ. Het is toegankelijk via het eHealth-platform en wordt gehost bij de vzw Smals. Er worden in volgende gevallen veiligheidsloggings gegenereerd:

- Een gebruiker van een Belgische onderneming heeft toegang tot gegevens van de wettelijke vertegenwoordiger (INSZ, naam, voornaam, geboortedatum).
- Een medewerker van het RIZIV consulteert de gegevens van de wettelijke vertegenwoordiger van een onderneming (INSZ, naam, voornaam, geboortedatum) in het kader van de consultatie van het detail van de gegevens van de onderneming.
- Een medewerker van het FAGG consulteert de gegevens van de wettelijke vertegenwoordigers van een onderneming (INSZ, naam, voornaam, geboortedatum) in het kader van de consultatie van het detail van de gegevens van de onderneming.

12. In dit voorbeeld worden de rollen als volgt toebedeeld:

- De *Host Security Responsible* is de veiligheidsverantwoordelijke van Smals. Deze heeft toegang tot de veiligheidsloggings in de acceptatieomgeving teneinde te valideren of de toepassing op correcte wijze veiligheidsloggings neemt. Deze heeft géén toegang tot de veiligheidsloggings in de productieomgeving.
- De *Platform Security Responsible* is de veiligheidsverantwoordelijke van het eHealth-platform. Deze heeft toegang tot het geheel van de veiligheidsloggings van het platform in de productieomgeving waaronder die genomen door de toepassing teneinde bijvoorbeeld te kunnen antwoorden op een vraag van een burger.
- De *Organization Treatment Security Responsible* is de veiligheidsverantwoordelijke van het FAGG. Deze heeft toegang tot de productieomgeving doch enkel tot de veiligheidsloggings die worden gegenereerd door de toepassing waarvan het FAGG de verantwoordelijke voor de verwerking is. In het kader van de toepassing SACEx heeft hij bijgevolg toegang tot de veiligheidsloggings die worden gegenereerd door een gebruiker van een onderneming, door een medewerker van het RIZIV of van zijn eigen organisatie (het FAGG).

13. De toepassing wordt beveiligd via de login-toepassing van het eHealth-platform, hetgeen impliceert dat de toegang van de gebruikers wordt geconfigureerd in het gebruikersbeheer (User Management) door een verantwoordelijke toegang onderneming of een lokaal beheerder van de onderneming. De gebruikers zelf worden geïdentificeerd en geauthentiseerd aan de hand van hun elektronische identiteitskaart.

Om deze redenen, verleent

de afdeling gezondheid van het Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid,

conform de bepalingen van deze beraadslaging, een machtiging voor de mededeling van persoonsgegevens aan en door het eHealth-platform in het kader van de basisdienst "veiligheidslogging".

Yves ROGER
Voorzitter