Informatieveiligheidscomité
Kamer sociale zekerheid en gezondheid

IVC/KSZG/19/278

BERAADSLAGING NR. 19/152 VAN 3 SEPTEMBER 2019 BETREFFENDE HET GEBRUIK VAN ELEKTRONISCHE IDENTIFICATIEMIDDELEN AANGEBODEN DOOR PRIVEORGANISATIES IN HET KADER VAN DE BASISDIENST 'GEINTEGREERD GEBRUIKERS- EN TOEGANGSBEHEER' VAN HET EHEALTH-PLATFORM IN SAMENWERKING MET DE FEDERALE AUTHENTICATIEDIENST VAN DE FOD BOSA

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);

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*;

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

Gelet op het auditoraatsrapport van het eHealth-platform;

Gelet op het verslag van de heer Bart Viaene;

Beslist op 3 september 2019, na beraadslaging, als volgt:

I. ONDERWERP

1. Overeenkomstig haar wettelijke opdrachten biedt het eHealth-platform een aantal basisdiensten aan, waaronder de dienst 'Geïntegreerd gebruikers- en toegangsbeheer'.

2. De dienst Geïntegreerd gebruikers- en toegangsbeheer van het eHealth-platform heeft als doel om de identificatie, de authenticatie, de verificatie van hoedanigheden en relaties en het beheer van autorisaties van actoren in de gezondheidszorg te vergemakkelijken.

3. Deze dienst is samengesteld uit verschillende componenten die samenwerken om de (unieke) identificatie, authenticatie en verificatie van hoedanigheden en relaties, en het delen van de resultaten van de uitgevoerde controles over toepassingen inzake eGezondheid heen mogelijk te maken. Aldus beschikken gebruikers van de gezondheidszorg die toegang vragen tot de diensten (gehost bij de gezondheidszorginstanties en het eHealth-platform) over single sign on.

4. Deze componenten zijn conform de internationale normen voor de mededelingen tussen organisaties teneinde de veiligheid en de stabiliteit te garanderen en de integratie te vergemakkelijken.

5. Het eHealth-platform wenst, mits voldaan wordt aan voorwaarden beschreven in deze beraadslaging, het gebruik van elektronische identificatiemiddelen aangeboden door privéorganisaties toe te laten wanneer die worden aangeboden in samenwerking met de Federale Authenticatiedienst ("FAS"), voor toegang tot toepassingen binnen de gezondheidssector. De FAS is een dienst aangeboden door de Federale Overheidsdienst Beleid en Ondersteuning, DG Digitale Transformatie (hierna "FOD BOSA"), die verschillende elektronische identificatiemiddelen aanbiedt voor de authenticatie van burgers met het oog op toegang tot overheidstoepassingen.

6. Binnen de samenwerking wordt beroep gedaan op de FAS voor het authenticatiemechanisme, door middel waarvan een persoon het elektronische identificatiemiddel gebruikt om zijn identiteit te bevestigen tegenover een vertrouwende partij.

II. BEHANDELING

7. De aanbieder van een elektronisch identificatiemiddel kan zijn middel aanbieden binnen de gezondheidssector voor toegang van patiënten tot hun medisch dossier mits hij voldoet aan de volgende voorwaarden:

8. De authenticatie geschiedt door een systeem eigen aan de organisatie:

- mits het authenticatiesysteem eigen aan de aanbieder voldoet aan de voorwaarden voor een betrouwbaarheidsniveau 'substantieel' zoals gepreciseerd in de punten 2.1., 2.2.1. element 2, 2.2.3., 2.2.4., 2.3.1. (met uitzondering van element 1) van de bijlage bij de Uitvoeringsverordening (EU) 2015/1502 van de EIDAS-verordening en
- mits het authenticatiemiddel gebruikt in het authenticatiesysteem eigen aan de aanbieder en het activeringsproces ervan voldoet aan de voorwaarden voor een betrouwbaarheidsniveau 'laag' in punt 2.2.1. element 1 en punt 2.2.2. van de bijlage bij de Uitvoeringsverordening (EU) 2015/1502 van de EIDAS-verordening, en het zodanig is ontworpen dat het kan worden verondersteld slechts te worden gebruikt door de persoon aan wie het toebehoort.

9. De aanbieder beschikt over gedocumenteerde methoden en beleid voor het beheer van informatiebeveiliging, benaderingen voor risicobeheersing en andere erkende controlemethoden zodat zij voor het middel voor elektronische identificatie de nodige garanties kunnen geven.

10. De aanbieder beschikt over een doeltreffend beëindigingsplan. Dat plan omvat voorzieningen voor de overdracht van de dienstverlening naar het eHealth-platform of naar een andere overheid aangeduid door het eHealth-platform.

11. De aanbieder van het elektronische identificatiemiddel zal op geen enkele wijze en betreffende geen enkel aspect van het gebruik van het elektronisch identificatiemiddel kosten kunnen aanrekenen aan het eHealth-platform of aan de FOD BOSA.

12. De aanbieder voldoet aan de volgende vereisten inzake bescherming van persoonsgegevens.

De aanbieder van het middel voor elektronische identificatie verwerkt persoonsgegevens, daarbij handelend als verwerkingsverantwoordelijke zoals gedefinieerd in de Algemene Verordening Gegevensbescherming 2016/679 voor alle verwerkingen van persoonsgegevens verbonden aan de door hen geleverde dienstverlening en daarbij alle relevante verplichtingen na te leven.

In die hoedanigheid neemt hij de vereiste en passende technische en organisatorische maatregelen om de persoonsgegevens te beschermen tegen toevallige of ongeoorloofde vernietiging, tegen toevallig verlies, evenals tegen de wijziging van of de toegang tot, en iedere andere niet toegelaten verwerking van persoonsgegevens. Deze maatregelen moeten beantwoorden aan de stand van de techniek op het vlak van veiligheid.

De aanbieder duidt een functionaris voor gegevensbescherming aan.

De aanbieder neemt geen kennis van de toepassingen waartoe de gebruiker door middel van het middel voor elektronische identificatie toegang verzoekt.

De aanbieder installeert een beveiligd controlespoor (*audit trail*) zodat de gegevens per specifieke transactie kunnen worden gereconstrueerd met het oog op de beveiliging van de gegevens en de bescherming van de persoonlijke levenssfeer. Hiertoe bewaart de aanbieder voor iedere aanmelding en poging tot aanmelding de volgende informatie gedurende een termijn van tien jaar te rekenen vanaf het moment van de aanmelding of de poging tot aanmelding in kwestie:

1. het unieke identificatienummer van de gebruiker;

2. de dienst voor elektronische identificatie van de aanbieder waarmee de gebruiker zich aanmeldt of tracht aan te melden; en

3. het tijdstip van de aanmelding of de poging tot aanmelding.

13. De aanbieder voldoet aan de volgende vereisten inzake informatie-uitwisseling met de FAS.

De aanbieder van het middel voor elektronische identificatie stuurt naar de FAS bij elke aanmelding het identificatienummer van de sociale zekerheid (INSZ) van de gebruiker, op basis waarvan de FAS de identiteit van de gebruiker vaststelt.

De informatie-uitwisseling tussen de aanbieder en FAS geschiedt overeenkomstig de technische protocollen zoals uiteengezet in de technische specificaties.

Bij iedere informatie-uitwisseling tussen de FAS en de aanbieder alsook tussen de aanbieder en de gebruiker voert de dienst voor elektronische identificatie controles uit om ten minste de onderstaande misbruiken tegen te gaan:

1. een nieuwe verzending van eenzelfde boodschap of aanmeldingspoging;

2. een wijziging van de inhoud van de uitgewisselde informatie; en

3. een derde partij die zich voordoet als de aanbieder.

Deze misbruiken worden gedetecteerd en leiden tot het falen van de aanmelding.

De aanbieder van het middel voor elektronische identificatie voorziet voldoende controlemechanismen om eventuele veiligheidsrisico's proactief op te sporen.

14. De aanbieder voldoet aan volgende voorwaarden op het vlak van dienstverleningsbeheer.

De dienstverlening is op maandbasis 99,9 % van de tijd beschikbaar.

De reactietijd bij de aanmelding van een gebruiker bedraagt niet meer dan:

1 seconde in 95 % van de aanmeldingen;

2 seconden in 98 % van de aanmeldingen; en

5 seconden in 99,5 % van de aanmeldingen.

De aanbieder bouwt mechanismen in die de dienstverlening op ononderbroken wijze kunnen garanderen tot het einde van de samenwerking.

15. De aanbieder verzorgt ondersteunende diensten, klachtenbehandeling, veiligheidsonderzoeken, problemen en incidenten met betrekking tot het middel als ook de communicatie betreffende het middel naar de gebruiker.

16. De FOD BOSA en het eHealth-platform zullen in geen enkel geval aansprakelijk zijn voor schade die rechtstreeks voortvloeit uit het niet respect door de aanbieder van de technische specificaties en de procedures verbonden met het elektronisch identificatiemiddel zoals omschreven in de bijlage van de uitvoeringsverordening (EU) nr. 2015/1502:

- aanvraag en registratie,
- bewijs en verificatie van de identiteit van de betrokkene,
- ontwerp en werking van het elektronisch identificatiemiddel,
- uitgifte, uitreiking en activering van het elektronisch identificatiemiddel,
- schorsing, herroeping en reactivering van het elektronisch identificatiemiddel,
- verlenging en vervanging van het elektronisch identificatiemiddel,
- authenticatiemechanisme

17. Elke eindgebruiker is verantwoordelijk voor de goede bewaring, beveiliging, geheimhouding en beheer van zijn digitale codes en gegevens eraan verbonden. De eindgebruiker is verantwoordelijk voor de keuze van een veilige geheime code.

18. Overeenkomstig artikel 5, §1, van de wet van 5 mei 2014 *houdende verankering van het principe van de unieke gegevensinzameling in de werking van de diensten en instanties die behoren tot of taken uitvoeren voor de overheid en tot vereenvoudiging en gelijkschakeling van elektronische en papieren formulieren*, is het Comité bevoegd om het gebruik van het Rijkregister toe te staan telkens als over een gegevensstroom of verwerking van persoonsgegevens wordt beslist. Het Comité stelt vast dat het elektronisch identiteitsmiddel, mits de aanbieder ervan voldoet aan de voorwaarden van deze beraadslaging, beschikbaar zal zijn via de basisdienst 'geïntegreerd gebruikers- en toegangsbeheer' van het eHealth-platform. Artikel 8 van de wet van 21 augustus 2008 *houdende oprichting en organisatie van het eHealth-platform en diverse bepalingen* stelt dat bij de mededeling van niet-gepseudonimiseerde persoonsgegevens aan en door het eHealth-platform uitsluitend de identificatienummers bedoeld in artikel 8 van de wet van 15 januari 1990 *houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid* (zijnde ofwel het Rijkregisternummer ofwel het identificatienummer van de Kruispuntbank van de sociale zekerheid) worden gebruikt. Het Comité staat dan ook toe dat de aanbieder van het elektronisch identificatiemiddel dat voldoet aan de voorwaarden van deze beraadslaging, het Rijksregisternummer van de betrokkene die met het middel wordt geïdentificeerd, gebruikt.

19. Het gebruik van het elektronisch identificatiemiddel dient te worden opgenomen in het 'Gebruikersreglement voor de toegang en het gebruik van het informatiesysteem van de federale overheid en de openbare instellingen van sociale zekerheid door burgers en hun lasthebbers' na goedkeuring door het Beheerscomité van de Kruispuntbank van de sociale zekerheid in uitvoering van artikel 3, §2, 1°, en §4, van de wet van 24 februari 2003 *betreffende de modernisering van het beheer van de sociale zekerheid en betreffende de elektronische communicatie tussen ondernemingen en de federale overheid* en het koninklijk besluit van 21 november 2006 *houdende uitbreiding van de toepassing van artikel 3 van de wet van 24 februari 2003 betreffende de modernisering van het beheer van de sociale zekerheid en betreffende de elektronische communicatie tussen ondernemingen en de federale overheid tot de burgers*.

20. Door deze samenwerking zal *single sign on* mogelijk zijn tussen de aanmeldingen gebaseerd op deze elektronische identificatiemiddelen en de aanmeldingen binnen de FAS van hetzelfde niveau voor de toepassingen binnen de gezondheidssector.

21. Alvorens de FOD BOSA het gebruik van het elektronisch middel via de FAS in productie kan stellen, dient de aanbieder van het elektronisch identificatiemiddel aan het eHealth-platform aan te tonen dat hij voldoet aan de voorwaarden die in deze beraadslaging worden opgenomen. Het eHealth-platform bepaalt autonoom de wijze waarop de conformiteit met de voorwaarden die in deze beraadslaging worden opgenomen, wordt geverifieerd.

22. Conform de modaliteiten bepaald door de FOD BOSA wordt er een overleg tussen de aanbieder van het elektronisch identificatiemiddel en de FOD BOSA georganiseerd (service

meetings) om alle mogelijke aspecten van het gebruik van het elektronisch identificatiemiddel en de samenwerking met de FAS te bespreken.

23. De aanbieder van het elektronisch identificatiemiddel is ertoe gehouden om indien ernstige incidenten zich voordoen dit zo spoedig mogelijk en uiterlijk binnen de 72 uren na het incident aan het eHealth-platform en in kopie aan de FOD BOSA te melden en een uitgebreid verslag met betrekking tot de incidenten, hun impact en de opvolging ervan over te maken, inclusief een omstandig advies van de functionaris voor de gegevensbescherming van de aanbieder van het elektronisch identificatiemiddel aangaande deze incidenten.

24. Wanneer de FOD BOSA vaststelt dat de aanbieder van het elektronisch middel niet langer voldoet aan de voorwaarden van deze beraadslaging, kan het gedetailleerde verklaringen vragen en zo nodig een controle opleggen.

25. Wanneer de FOD BOSA vaststelt dat de aanbieder van het elektronisch middel de voorwaarden van deze beraadslaging niet naleeft, kan het de samenwerking van de aanbieder van het elektronisch identificatiemiddel met de FAS eenzijdig en zonder vooropzeg beëindigen.

Om deze redenen besluit

de kamer sociale zekerheid en gezondheid van het informatieveiligheidscomité

dat het eHealth-platform het gebruik van elektronische identificatiemiddelen aangeboden door privéorganisaties kan toelaten wanneer die worden aangeboden voor toegang tot toepassingen binnen de gezondheidssector, in samenwerking met de Federale Authenticatiedienst ("FAS") van de FOD BOSA, voor zover wordt voldaan aan de in deze beraadslaging beschreven voorwaarden.

De aanbieder van een elektronisch identificatiemiddel dat voldoet aan de voorwaarden van deze beraadslaging, wordt gemachtigd om het Rijksregisternummer van de betrokkene die door het middel wordt geïdentificeerd, te gebruiken.

Bart VIAENE