Verklaring op eer

(Circle-of-Trust - CoT)

Inleiding

In het kader van de toenemende communicatie van gezondheidsgegevens van en naar een organisatie actief in het domein van gezondheid, zorg- en hulpverlening is er de noodzaak aan garanties m.b.t. informatieveiligheid en wordt daarbij het principe van "**Circle of Trust - CoT**" voorzien.

Een "Circle-of-Trust" wordt toegekend aan een organisatie actief in het domein van gezondheid, zorg- en hulpverlening die, t.a.v. zijn gebruikers van gegevens, op verschillende niveaus maatregelen inzake informatieveiligheid neemt en toeziet op de naleving ervan, zodat andere organisaties en/of zorg- en hulpverleners en/of overheden en de betrokken burger er redelijkerwijze op kunnen vertrouwen dat deze veiligheidsmaatregelen nageleefd worden en ze die niet zelf dienen te organiseren of te controleren"[1]

Opdat een organisatie actief in het domein van gezondheid, zorg- en hulpverlening beschouwd wordt als een Circle-of-Trust dient deze te voldoen aan de 13 criteria die gevalideerd werden in een Reglement dat door het Beheerscomité van het eHealth-platform op 10 september 2019 en door het Informatieveiligheidscomité op 1 oktober 2019 (Beraadslaging 19/166) is goedgekeurd. Zij dienen de nodige maatregelen te nemen voor de naleving van deze criteria. Deze criteria kunnen worden geraadpleegd op het portaal van het eHealth-platform https://www.ehealth.fgov.be/ehealthplatform/nl/reglementen.

Het is de erkennende overheid of de overheid met wie er de organisatie actief in het domein van gezondheid, zorg- en hulpverlening een overeenkomst heeft (beheerder van de haar betreffende informatie in de referentie-bron CoBrHA) [2], die het "CoT-statuut" in CoBRHA[3] registreert van zodra een organisatie actief in het domein van gezondheid, zorg- en hulpverlening verklaart in overeenstemming te zijn met de 13 criteria die van toepassing zijn op het principe van de Circle-of-Trust.

---

[1] artikel 1 uit Beraadslaging nr. 19/166 van 1 oktober 2019 met betrekking tot het reglement tot vaststelling van de criteria voor de toepassing van een cirkel van vertrouwen door een organisatie actief in het domein van gezondheid, zorg- en hulpverlening in het kader van de uitwisseling van gezondheidsgegevens

[2] De administratie die een organisatie actief in het domein van gezondheid, zorg- en hulpverlening erkent of waarmee de organisatie actief in het domein van gezondheid, zorg- en hulpverlening een overeenkomst heeft en die uw hoedanigheid en gegevens publiceert in CoBRHA. Dit kan onder meer zijn : het RIZIV, FOD Volksgezondheid, VAZG, Iriscare, Aviq, DSL, …). Deze administratie registreert in CoBRHA de vlag "COT" als een zorgorganisatie verklaart dat het voldoet aan de 13 criteria.

[3] CoBRHA: unieke database van de federale en gefedereerde overheden, die de identificatie-gegevens bevat van alle individuele zorg- en hulpverleners en de zorgorganisaties en die gevoed wordt door alle unieke bronnen van het land en gehost wordt het eHealth-platform.

De controle op de naleving van het Reglement CoT en van de Beraadslaging nr. 19/166 van 1 oktober 2019 en in bijzonder de controle op de naleving van de algemene verordening gegevensbescherming[4] en de regelgeving betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens die de basis is van dit reglement, gebeurt door de toezichthoudende autoriteit (de Gegevensbeschermingsautoriteit of een andere toezichthoudende autoriteit).

De registratie van behoren tot een Circle-of-Trust, kan door een erkennende overheid op verzoek van een bevoegde toezichthoudende autoriteit ingetrokken worden als de opdrachten of verplichtingen die voortvloeien uit het reglement CoT, niet vervuld of niet nageleefd worden door de betrokken organisatie actief in het domein van gezondheid, zorg- en hulpverlening. De mogelijke impact is dat de organisatie actief in het domein van gezondheid, zorg- en hulpverlening niet langer toegang heeft voor lezen/schrijven van bepaalde informatie via één of meerdere eGezondheidsdiensten en de aanvraag voor behoren tot een Circle-of-Trust opnieuw moeten indienen.

Deze intrekking kan pas worden uitgevoerd nadat een toezichthoudende autoriteit inzake informatieveiligheid, na het doorlopen van een proces[5] dat daartoe werd uitgewerkt door deze overheid, bevestigt dat de organisatie actief in het domein van gezondheid, zorg- en hulpverlening niet langer beantwoordt aan de opgelegde voorwaarden inzake informatieveiligheid zoals bedoeld in het reglement van CoT.

[4] 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 de Richtlijn 95/46/EG (algemene verordening gegevensbescherming).

[5] Hierbij wordt voorzien dat de betrokken zorgorganisatie eerst de mogelijkheid krijgt om alsnog zijn verplichtingen na te komen en in geval van conflict kan gehoord worden

Verklaring

Door het ondertekenen van dit document verklaar ik dat de organisatie de regelgeving betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens naleeft, en in overeenstemming is met de 13 onderstaande criteria die van toepassing zijn op het principe van de Circle-of-Trust.

Ik ga akkoord dat een niet naleving van de 13 criteria door de organisatie een intrekking van de registratie van de Circle-of-Trust tot gevolg kan hebben.

De organisatie verbindt zich ertoe te zorgen voor voortdurende naleving van de elementen in de verklaring. Ze verbindt zich ertoe bij elke substantiële verandering in haar processen - in het bijzonder IT - te verifiëren dat alle criteria in dit document goed worden gerespecteerd en onmiddellijk te melden als ze niet langer aan deze criteria kunnen voldoen.

Naam van de organisatie actief in het domein van gezondheid, zorg- en hulpverlening:
……..

Adres: ……..

Contactgegevens van de verantwoordelijke: ……..

Contactgegevens van de functionaris voor gegevensbescherming: ……..

Nummer[6] waarmee uw instelling is gekend in CoBRHA:

HCO-nr.: ……..

Het KBO-nr. waartoe de organisatie actief in het domein van gezondheid, zorg- en hulpverlening behoort : ……..

Naam van uw erkennende overheid: ……

[6] Hier moet het nummer vermeld worden van de individuele organisatie actief in het domein van gezondheid, zorg- en hulpverlening : vb. van de dienst thuisverpleging, het ziekenhuis, de revalidatie-instelling, het woonzorgcentrum, het psychiatrisch verzorgingstehuis, de dienst voor gezinszorg, de dienst maatschappelijk werk van het ziekenfonds, … .

Enkel geregistreerde functiehouders van de organisatie actief in het domein van gezondheid, zorg- en hulpverlening, zoals gekend in de Kruispuntbank van Ondernemingen, kunnen dit document ondertekenen. Bij ontbreken van een handtekening of ondertekening door een niet geregistreerde functiehouder, wordt dit document onontvankelijk verklaard door de erkende overheid van hun organisatie actief in het domein van gezondheid, zorg- en hulpverlening.

Datum, naam, hoedanigheid en handtekening van de verantwoordelijke:

Dit formulier dient bezorgd te worden aan de erkennende overheid (registratie-autoriteit). De organisatie actief in het domein van gezondheid, zorg- en hulpverlening dient de naleving van de bescherming van de persoonlijke levenssfeer op elk moment te kunnen aantonen aan de bevoegde gegevensbeschermingsautoriteit.

De erkennende overheid is niet bevoegd voor het toezicht op de organisatie actief in het domein van gezondheid, zorg- en hulpverlening inzake de naleving van de regelgeving i.v.m. privacy, het oplossen van problemen en geschillen of het behandelen van klachten hierover. Wanneer een erkennende overheid een klacht ontvangt, zal deze worden overgemaakt een toezichthoudende autoriteit.

Gelieve voor elk van de 13 vakjes hieronder aan te duiden of uw organisatie actief in het domein van gezondheid, zorg- en hulpverlening daaraan beantwoordt. Indien u één of meerdere vakjes niet aanvinkt, wordt dit document onontvankelijk verklaard door de erkennende overheid van uw organisatie actief in het domein van gezondheid, zorg- en hulpverlening.

☐ CRITERIUM 1: REGISTER VAN DE VERWERKINGSACTIVITEITEN

De organisatie beschikt voor de verwerkingsactiviteiten m.b.t. gezondheidsgegevens over een register van de verwerkingsactiviteiten zoals bedoeld in artikel 30 van de Algemene Verordening Gegevensbescherming (AVG), waarin de rechtmatige verwerkingsdoeleinden van de verwerkingsactiviteiten staan vermeld[7].

☐ CRITERIUM 2: PRECISERING VAN DE RECHTSGRONDEN VOOR DE VERWERKING VAN BIJZONDERE CATEGORIEËN VAN PERSOONSGEGEVENS

Voor de verwerking van bijzondere categorieën van persoonsgegevens, bedoeld in artikel 9, 1. van de Algemene Verordening Gegevensbescherming (AVG) m.b.t. zorgvragenden, vermeldt het register van de verwerkingsactiviteiten de rechtsgrond(en) bedoeld in artikel 9, 2. van de AVG op basis waarvan de bijzondere categorieën van persoonsgegevens worden verwerkt.

☐ CRITERIUM 3: VERWERKINGSBEPERKING

De persoonsgegevens m.b.t. zorgvragenden, in het bijzonder de bijzondere categorieën van persoonsgegevens bedoeld in artikel 9, 1. van de Algemene Verordening Gegevensbescherming (AVG), kunnen enkel worden verwerkt door gebruikers die deze in hoofde van hun functie moeten kunnen verwerken voor de rechtmatige verwerkingsdoeleinden beschreven in het register van de verwerkingsactiviteiten. De verwerkingsmogelijkheden worden voldoende fijnmazig gemoduleerd, zodat elke gebruiker slechts de persoonsgegevens m.b.t. zorgvragenden kan verwerken waarvoor dit in hoofde van zijn functie nodig is en over de tijdsperiode waarvoor dit in hoofde van zijn functie nodig is.

☐ CRITERIUM 4: AUTHENTICATIE VAN DE IDENTITEIT VAN DE GEBRUIKER

De organisatie authentiseert de identiteit van de natuurlijke persoon die de bijzondere categorieën van persoonsgegevens bedoeld in artikel 9, 1. Van de Algemene Verordening Gegevensbescherming (AVG) verwerkt (de 'gebruiker').

Deze authenticatie geschiedt

- hetzij met een middel geïntegreerd in de Federal Authentication Service (FAS) van een niveau dat gelijk is aan of hoger is dan het niveau vastgesteld door het Beheerscomité van het eHealth-platform;
- hetzij door een authenticatiesysteem eigen aan de organisatie
  - mits een registratie van de identiteit geschiedt aan de hand van een eenmalig gebruik van een authenticatiemiddel geïntegreerd in de FAS van een niveau dat gelijk is aan of hoger is dan het niveau vastgesteld door het Beheerscomité van het eHealth-platform en
  - 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) en 2.4. 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.

[7] Hieronder vallen ook de andere persoonsgegevens die de organisatie actief in het domein van gezondheid, zorg- en hulpverlening moet kunnen uitwisselen om zijn opdracht te kunnen vervullen

Het minimumniveau, in de FAS vastgesteld door het Beheerscomité van het eHealth-platform, is niveau 400 voor natuurlijke personen handelend als zorgverstrekker en niveau 350 voor natuurlijke personen handelend als zorgvrager.

☐ CRITERIUM 5: VERIFICATIE VAN DE RELEVANTE KENMERKEN EN RELATIES VAN DE GEBRUIKER

Indien de elektronische verwerking van bijzondere categorieën van persoonsgegevens bedoeld in artikel 9, 1 van de Algemene Verordening Gegevensbescherming (AVG) de verificatie vereist van relevante kenmerken of relaties van de gebruiker, worden deze kenmerken of relaties geraadpleegd

- hetzij in de betrokken authentieke bronnen vastgelegd door het Beheerscomité van het eHealth-platform
- hetzij in een gegevensbank van de organisatie of van een gezondheidsnetwerk waarvan de organisatie deel uitmaakt en die, waar nodig, gesynchroniseerd is met kwaliteitsvolle informatie uit de authentieke bronnen vastgelegd door het Beheerscomité van het eHealth-platform.
  Het Beheerscomité heeft tot op heden het gebruik vastgelegd van de volgende authentieke bronnen:
  - CoBrHA
  - de gegevensbank bij de ziekenfondsen m.b.t. de houders van een Globaal Medisch Dossier.

☐ CRITERIUM 6: INTERNE LOGGING

De elektronische toegang tot persoonsgegevens wordt gelogd. Het logbeheer moet minimaal beantwoorden aan de volgende doelstellingen

- toelaten snel en eenvoudig te kunnen bepalen welke natuurlijke persoon, wanneer en op welke manier toegang heeft verkregen tot welke persoonsgegevens m.b.t. welke persoon;
- de persoon die persoonsgegevens heeft verwerkt en de persoon waarover persoonsgegevens zijn verwerkt eenduidig kunnen identificeren;
- de noodzakelijke tools ter beschikking hebben om toe te laten de loggegevens uit te baten door de geautoriseerde personen;
- de loggegevens minstens 10 jaar bewaren.

☐ CRITERIUM 7: AUDITTRAIL

Indien de elektronische verwerking van persoonsgegevens de toegang inhoudt tot persoonsgegevens verwerkt door derden, wordt ervoor gezorgd dat bij onderzoek, op initiatief van het eHealth-platform, of van een toezichtsorgaan, naar aanleiding van een klacht, een volledige reconstructie kan geschieden die ertoe strekt te bepalen welke natuurlijke persoon toegang heeft gehad tot welke soorten persoonsgegevens m.b.t. welke personen, wanneer en op welke manier. Onder coördinatie van het eHealth-platform worden methoden afgesproken die deze volledige reconstructie mogelijk maken.

☐ CRITERIUM 8: INFORMATIE, VORMING EN SENSIBILISERING

De organisatie stelt de nodige policies op om uitvoering te geven aan de criteria vermeld in dit document, stelt deze op een algemeen toegankelijke wijze ter beschikking van alle gebruikers die deel uitmaken van de cirkel van vertrouwen, biedt hierover een gepaste permanente vorming aan deze gebruikers en sensibiliseert hen voortdurend tot het naleven van de policies.

☐ CRITERIUM 9: INTERNE CONTROLE

De organisatie organiseert een regelmatige interne controle op de naleving van de criteria vervat in dit document en de policies die er uitvoering aan geven. De organisatie bewaart de resultaten van deze interne controle gedurende 2 jaar. De organisatie voorziet in afschrikwekkende sancties t.a.v. gebruikers die deel uitmaken van de cirkel van vertrouwen die de criteria of de policies die eraan uitvoering geven, niet naleven.

☐ CRITERIUM 10: NALEVING BERAADSLAGINGEN INFORMATIEVEILIGHEIDSCOMITÉ

De organisatie bevestigt alle maatregelen inzake informatieveiligheid en bescherming van de persoonlijke levenssfeer na te leven die zijn voorzien in de toepasselijke beraadslagingen van het Informatieveiligheidscomité.

☐ CRITERIUM 11: OPNAME IN DE AUTHENTIEKE BRON COBRHA ALS ORGANISATIE DIE EEN CIRKEL VAN VERTROUWEN ORGANISEERT

De organisatie meldt schriftelijk aan de beheerder van de haar betreffende informatie in de authentieke bron CoBRHA dat zij een cirkel van vertrouwen instelt overeenkomstig de voorwaarden vermeld in dit document, en bevestigt daarbij te voldoen aan elk van deze voorwaarden. In de authentieke bron CoBrHA wordt door deze beheerder geregistreerd dat de organisatie een cirkel van vertrouwen heeft ingesteld.

☐ CRITERIUM 12: OPENBARE DOCUMENTATIE

De organisatie publiceert op haar website, of op andere, publiek-beschikbare manier, op een begrijpbare wijze de verwerkingsdoeleinden waarvoor ze de gezondheidsgegevens van personen verwerkt en de policy waarmee uitvoering wordt gegeven aan het evenredigheidsbeginsel.

☐ CRITERIUM 13: EXTERNE CONTROLE

De organisatie houdt het verwerkingsregister en de documenten en policies die ze voor de naleving van deze voorwaarden uitwerkt, evenals de resultaten van de interne controle, ter beschikking van de toezichthoudende overheden inzake informatieveiligheid.