Bijlage 2 bij Privacyreglement NIVEL Zorgregistraties eerste lijn

Technische beschrijving pseudonimisatie gegevensverzameling NIVEL Zorgregistraties eerste lijn

Pseudonimisatie

Onder 'pseudonimisatie' verstaan wij het omzetten van een persoonsgegeven naar een niet-herleidbare code. De omzettingen zijn, in de door ZorgTTP gehanteerde variant, onomkeerbaar. Het is daarbij onmogelijk een pseudoniem terug te vertalen naar het oorspronkelijke persoonsgegeven.

De kerntaak van ZorgTTP is het depersonaliseren van bestanden om daarmee het uitwisselen van informatie op individueel niveau, conform de wettelijke vereisten, mogelijk te maken. De verzendende partij (de bron) en de ontvangende partij (het doel) maken gezamenlijk afspraken over welke informatie wordt uitgewisseld en welke gegevens daarbij dienen te worden geanonimiseerd. ZorgTTP zal een adviserende rol spelen bij deze afweging als onderdeel van de werkzaamheden die horen bij het inrichten van een pseudonimisatieketen.

De omzetting verloopt in twee stappen: de partij die in het bezit is van de te verzenden (persoons)gegevens (de bron) maakt gebruik van pseudonimisatiesoftware waarmee een persoonsgegeven wordt omgezet naar een zogenaamd pre-pseudoniem. Volgens wordt als tweede stap in het proces het pre-pseudoniem door de TTP, met behulp van software, omgezet naar een definitief pseudoniem. Dit pseudoniem, en de bijbehorende overige data, worden beschikbaar gesteld aan de ontvangende partij (het doel).

Alleen de TTP weet op welke wijze het definitieve pseudoniem is aangemaakt. Daarmee wordt een situatie bereikt waarbij het voor zowel de bron als het doel (de ontvangende partij) onmogelijk is om het oorspronkelijke persoonsgegeven met het aangemaakte pseudoniem in verband te brengen. Persoons-identificerende kenmerken zoals naam en BSN worden bij pseudonimisatie vervangen door een pseudoniem, zodanig dat voor ieder persoonsgegeven steeds hetzelfde pseudoniem wordt gegenereerd. Individuen worden op deze wijze koppelbaar in tijd en over verschillende bronnen heen zonder dat daartoe de oorspronkelijke persoonsgegevens verstrekt hoeven te worden. Door tussenkomst van de TTP zijn bron en doel niet in staat om persoonsgegeven en het daar uit resulterende pseudoniem aan elkaar te relateren.

De inzet van pseudonimisatie via ZorgTTP werkt via een gelaagd model. Hierin worden een aantal vormen van beveiliging gehanteerd. Het gaat om maatregelen op de volgende niveaus:

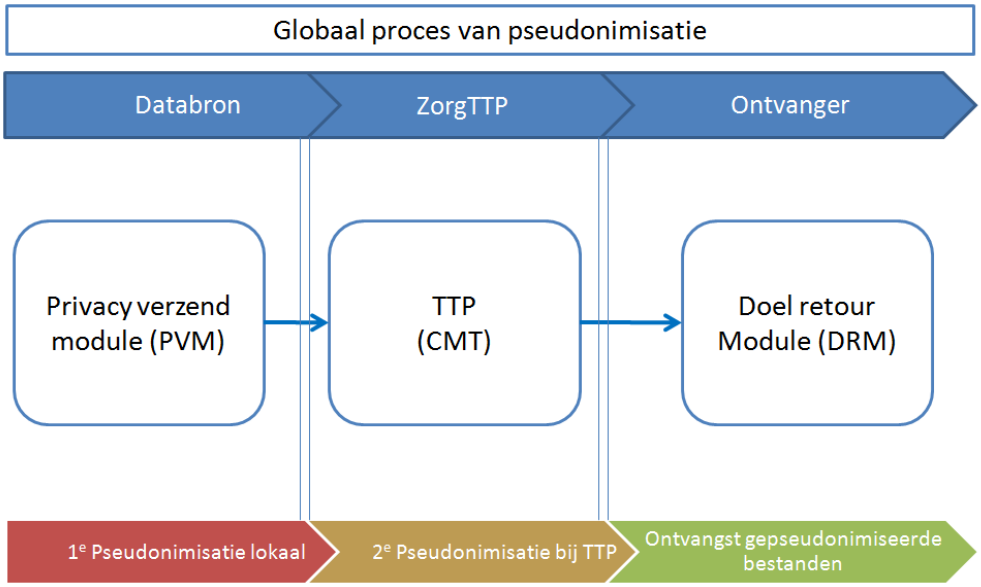
1) Pseudonimisatie op recordniveau
2) Versleuteling op bestandsniveau
3) Transportbeveiliging
4) Controle afzender middels certificaat

Op de volgende pagina wordt het pseudonimisatieproces schematisch weergegeven en toegelicht.

Beschrijving van het pseudonimisatieproces

De pseudonimisatieketen bestaat uit drie onderdelen:

1. Privacy- en Verzend Module (PVM) wordt door de informatiebron gebruikt om de bestanden te pseudonimiseren en te verzenden;
2. Centrale Module TTP (CMT) wordt door ZorgTTP gebruikt;
3. Doel- en Receive Module (DRM) wordt door het informatiedoel gebruikt om de bestanden vanaf de server van ZorgTTP te downloaden.



Het pseudonimisatieproces bestaat in het kort uit de volgende stappen:

1. Uitgangspunt is dat de verzendende partij (de zorgverlener) een bestand genereert dat voldoet aan vooraf vastgestelde specificaties;
2. Het bestand wordt verwerkt met de door ZorgTTP aan de databron beschikbaar gestelde software;
3. Na verwerking volgt beveiligd transport naar ZorgTTP voor het aanmaken van de definitieve pseudoniemen;
4. ZorgTTP voert met behulp van eigen pseudonimisatiesoftware centraal een tweede bewerking uit waarbij een voor de zender en ontvanger geheime ‘sleutel’ wordt gebruikt;
5. Het gepseudonimiseerde bestand wordt vrijgegeven en kan vervolgens worden opgehaald door de ontvangende partij met een daartoe beschikbaar gestelde ontvangstmodule.

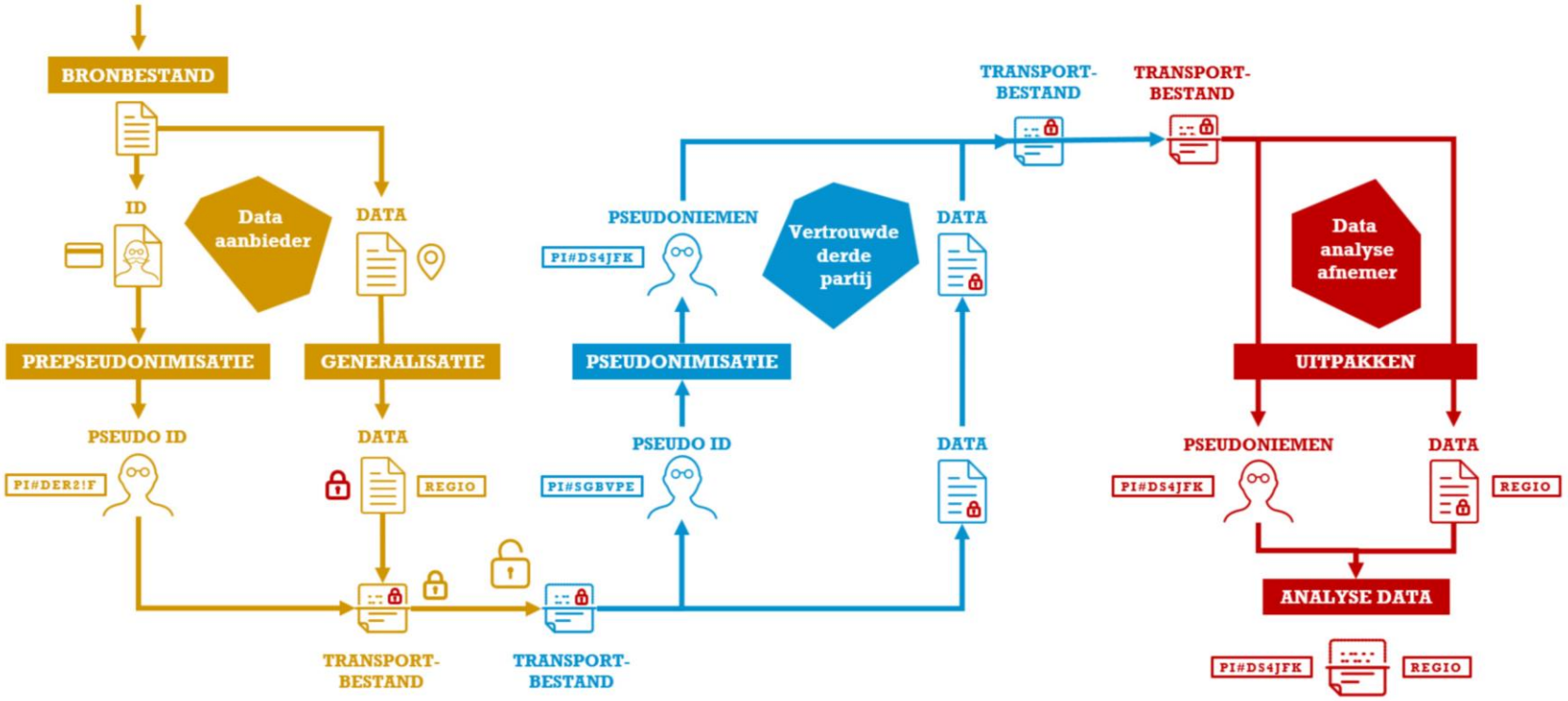
Op de volgende twee pagina’s wordt het pseudonimisatieproces schematisch weergegeven en gedetailleerder beschreven.

Beveiliging van informatie

ZorgTTP stelt de databron software ter beschikking voor de eerste bewerking. Daarbij worden persoonsgegevens omgezet naar pseudoniemen, ook wordt het bestand geanonimiseerd. Bijvoorbeeld door het omzetten van een geboortedatum naar een leeftijdscategorie. De medisch inhoudelijke informatie wordt vervolgens versleuteld, deze informatie is voor ZorgTTP gedurende het transport ontoegankelijk. Vanwege logistieke voordelen worden de pseudoniemen én inhoudelijke data in één levering via ZorgTTP aan de ontvanger aangeboden.

Uitwisseling van gegevens tussen de diverse partijen vindt plaats over beveiligde internetverbindingen (TLS). De identiteit van partijen wordt gevalideerd middels digitale certificaten (Public Key Infrastructure (PKI)).

In onderstaand figuur zijn de berichtstromen opgenomen en op de volgende pagina wordt een toelichting op het figuur gegeven.



Privacy- en Verzend Module (PVM)

Deze module wordt gebruikt door de bron en kent een aantal functies. Allereerst wordt een aantal controles uitgevoerd op de aangeboden gegevens. Daarna worden de identificerende persoonsgegevens omgezet in zogenaamde pre-pseudoniemen. Pre-pseudoniemen zijn persoonsgegevens waarop een eerste bewerking heeft plaatsgevonden. Vervolgens wordt een scheiding aangebracht tussen de pseudoniemen (sleuteldeel) en de bijbehorende data (datadeel). Beide delen worden vervolgens geëncrypteerd. Het sleuteldeel kan enkel worden gedecrypteerd door ZorgTTP, het datadeel enkel door de uiteindelijke ontvanger.

Voordat van een onomkeerbaar pseudoniem gesproken kan worden, dient de TTP een definitieve omzetting te doen op de voorbewerkte gegevens. De gegevens worden op beveiligde wijze naar de TTP verstuurd. Daarbij zijn de gegevens zodanig beveiligd dat deze slechts voor de TTP toegankelijk zijn voor verdere bewerking. De hiertoe benodigde op Java gebaseerde software wordt via het internet beschikbaar gesteld en maakt gebruik van door de TTP uitgegeven digitale certificaten. De digitale certificaten worden gebruikt voor ondertekening van de te verzenden berichten, het opbouwen van een beveiligde (HTTPS-) verbinding en encryptie van de te verzenden data.

Centrale Module TTP (CMT)

De centrale applicatie ontvangt een versleuteld bestand. Dit bestand bestaat uit twee onderdelen: een datadeel en een sleuteldeel. Het sleuteldeel bevat de pre-pseudoniemen, deze worden door de centrale applicatie omgezet tot de definitieve pseudoniemen.

De centrale applicatie heeft geen toegang tot het datadeel, deze is beveiligd en enkel door de ontvangstapplicatie te decrypteren. Voor de transportbeveiliging wordt ook weer gebruik gemaakt van een Public Key Infrastructure (PKI).

Doel- en Retour Module (DRM)

De ontvangstmodule wordt gebruikt door de ontvangende partij. De module ontvangt van de centrale applicatie de berichten. De berichten hebben een multipart-xml-indeling. Het is feitelijk een container met daarin bestanden. De module ontsleutelt allereerst het sleuteldeel, vervolgens het datadeel en voegt deze daarna weer samen. Afhankelijk van de grootte van het bestand kost dit proces enkele seconden tot een minuut.

Herleidbaarheid gepseudonimiseerde gegevens

Voor het verwerken van persoonsgegevens is de Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 (Algemene verordening gegevensbescherming) van toepassing.

Op het moment dat persoonsgegevens worden verwerkt stelt de AVG eisen aan het verwerken van die persoonsgegevens, zoals het treffen van passende organisatorische en technische beveiligingsmaatregelen. Privacy Enhancing Technology (PET) is een verzamelnaam voor die maatregelen. Een vorm van PET is het pseudonimiseren van persoonsgegevens. De opgeslagen gegevens blijven een zekere mate van gevoeligheid behouden, zeker in het geval van medische gegevens. Dit komt omdat door het koppelen van gepseudonimiseerde dataverzamelingen of door het toevoegen van aanvullende variabelen alsnog op indirecte wijze sprake kan zijn van tot persoonsgegevens herleidbare data. Door middel van pseudonimisatie wordt de directe herleidbaarheid van persoonsgegevens tegengegaan en is daarmee een sterke beveiligingsmaatregel om ongewenste herleiding tegen te gaan getroffen. Verder is het van verplicht om naast het inzetten van pseudonimisatie gegevens te verwerken op basis van een grondslag uit de AVG. Daarbij hoort ook het informeren van betrokkenen over het doel van de verwerking en de middelen die worden ingezet om misbruik tegen te gaan.

Om de kans op indirecte herleidbaarheid te minimaliseren adviseert ZorgTTP om:

- gegevens waar mogelijk op geaggregeerd niveau te verstrekken;
- per gepseudonimiseerde dataverzameling met een andere geheime sleutelwaarde te werken. Daarmee wordt directe koppeling op grond van de pseudoniemen onmogelijk;
- gepseudonimiseerde data op het laagste aggregatieniveau alleen op basis van een overeenkomst te verstrekken;
- gepseudonimiseerde data op het laagste aggregatieniveau uit andere gepseudonimiseerde dataverzamelingen alleen toe te voegen na analyse van het risico op directe op indirecte herleidbaarheid.

ISO Certificering 27001 voor Informatiebeveiligingsbeleid

ISO 27001 is gericht op het informatiebeveiligingsbeleid. Deze ISO norm stelt eisen voor het vaststellen, implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren van het Information Security Management Systeem (ISMS). ZorgTTP heeft een up to date ISMS en er heeft mei 2018 een certificerende audit plaatsgevonden. ZorgTTP is door de certificerende partij KIWA voorgedragen voor certificering, wat inhoudt dat ZorgTTP verwacht per juli 2018 officieel gecertificeerd te zijn.

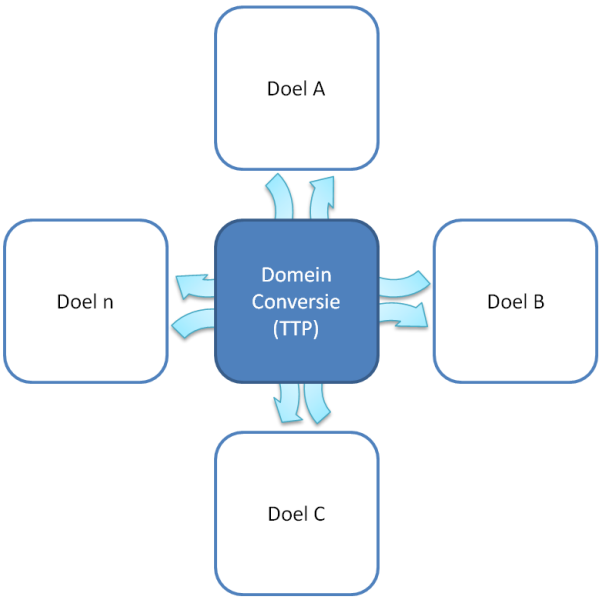
Domeinconversie

ZorgTTP verleent pseudonimisatiediensten aan diverse partijen. Deze en andere partijen die al dan niet over gepseudonimiseerde dataverzamelingen beschikken, hebben behoefte aan de mogelijkheid om – op gecontroleerde wijze – bestanden aan elkaar te kunnen koppelen. Daarom is een functie voor zogenaamde ‘domeinconversie’ ontwikkeld.

Domeinconversie maakt het mogelijk om een pseudoniem van een BSN van het ene domein (lees een gepseudonimiseerde dataverzameling) te converteren naar een pseudoniem, op grond van hetzelfde BSN, zoals bekend binnen een ander domein.
Het reguliere pseudonimisatieproces verloopt in twee stappen. De eerste versleuteling vindt plaats bij de bron, de tweede versleuteling bij ZorgTTP. Onderdeel van de tweede versleuteling is een domeinspecifieke encryptie. Dit betekent dat iedere gepseudonimiseerde dataverzameling van een specifieke serie pseudoniemen wordt voorzien. De kracht van deze domeinspecifieke encryptie is dat kan worden voorkomen dat gepseudonimiseerde dataverzamelingen eenvoudigweg op basis van pseudoniemen aan elkaar gekoppeld kunnen worden. Daarmee zou het risico op indirecte herleidbaarheid naar de oorspronkelijke persoonsgegevens onaanvaardbaar hoog worden.

Voor elke opdrachtgever kan daardoor voorzien worden in één of meer domeinen.
In de praktijk betekent dit dat gelijke input – bijvoorbeeld een bepaald BSN – in de verschillende domeinen verschillende pseudoniemen zal opleveren. Slechts met behulp van domeinconversie kunnen verschillende domeinen aan elkaar gekoppeld worden.

Model voor de functie Domeinconversie



NIVEL-ZorgTTP juli 2011

Aangezien het in specifieke gevallen mogelijk moet zijn om additionele informatie te verzamelen, wordt er gebruik gemaakt van een communicatiemechanisme. De reguliere pseudonimisatie wordt zoals eerder beschreven uitgevoerd. Voor het verzoek om additionele informatie zijn twee zaken noodzakelijk: een identificatie van de behandelaar en een lokaal patiëntnummer.

Als de onderzoeker tot de conclusie komt dat additionele informatie van grote meerwaarde zou zijn, dan kan gebruik worden gemaakt van de communicatiedatabase. Het is dan wel noodzakelijk dat er een gedeelde variabele is tussen beide domeinen. We maken daarvoor gebruik van een communicatiepseudoniem. Dit pseudoniem is zowel beschikbaar in het domein Onderzoek als in het domein Communicatie. Omdat het twee domeinen betreft, zal het pseudoniem – ondanks identieke input – een andere waarde opleveren. ZorgTTP kan het communicatiepseudoniem – onder strikte voorwaarden - converteren van het domein Onderzoek naar het domein Communicatie.

Het proces verloopt dan als volgt:

1. NIVEL bepaalt in welke gevallen er sprake is van grote meerwaarde van additionele informatie. Enkel in die gevallen wordt er gebruik gemaakt van het communicatiemechanisme;
2. De aanvraag betreft een zogenaamde ‘domeinconversie’. Deze moet technisch door twee medewerkers van ZorgTTP worden goedgekeurd;
3. Vanuit NIVEL wordt de zorgverlener gevraagd om de patiënt te benaderen met het verzoek om additionele informatie;
4. Door deel te nemen aan het onderzoek geeft de patiënt automatisch toestemming voor het gebruik van zijn of haar gegevens.
5. Bij het verstrekken van de informatie wordt gewerkt met een onderzoeksnummer, er zijn geen persoonsgegevens noodzakelijk.

Schematische weergave communicatiemodel