Deloitte.
Legal

Gegevensbescherming door ontwerp

Project Start Architectuur Programma Gespecificeerde Toestemming Structureel

Amsterdam, augustus 2019 – PK/rp/19-178a

Deloitte.
Legal

Deloitte Legal B.V.
Gustav Mahlerlaan 2970
1081 LA Amsterdam
Postbus 58110
1040 HC Amsterdam
Nederland

Tel: +31 (0) 88 288 28 88
Fax: +31 (0) 88 288 97 11
www.deloitte.nl

Dit document is verstrekt aan Stichting Nationaal ICT Instituut in de Zorg (hierna: Nictiz) door Deloitte Legal B.V. (hierna: Deloitte). Onze voorwaarden, zoals beschreven in ons voorstel DPIA Project Start Architectuur programma Gespecificeerde Toestemming Structureel, met kenmerk PK/rp/19-178 van d.d. 08-03-2019 zijn van toepassing op dit document.

We willen benadrukken dat onze rapportages voortvloeiend uit onze werkzaamheden slechts bedoeld zijn voor intern gebruik door Nictiz ten behoeve van het in de offerte omschreven doel. Zonder uitdrukkelijke en voorafgaande schriftelijke toestemming van Deloitte is het niet toegestaan deze rapportage, dan wel delen daaruit, te gebruiken voor andere doeleinden dan overeengekomen, aan derden te verspreiden of openbaar te maken, aan de rapportage te refereren of uit de rapportages te citeren. Het is, uiteraard, toegestaan om de rapportage te delen met samenwerkingspartners binnen het programma.

Dit rapport bevat geen conclusies of een andere vorm van zekerheid over de financiële huishouding, interne beheersingsmaatregelen of het voldoen aan wet- en regelgeving van Nictiz en/of het programmateam GTS.

Managementsamenvatting

*Met de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (hierna: "**Wabvpz**") wordt het vereiste van gespecificeerde toestemming geïntroduceerd voor uitwisseling van gezondheidsgegevens van cliënten via een elektronisch uitwisselingssysteem (hierna: "**US**"). Het Programmateam Gespecificeerde Toestemming Structureel (hierna: "**GTS**") heeft een online toestemmingsvoorziening (hierna: "**Voorziening**") ontworpen om cliënten de mogelijkheid te bieden hun toestemmingen landelijk te geven en te beheren op overzichtelijke en transparante wijze.*

In het kader van gegevensbescherming door ontwerp (hierna: "**GdO**") heeft GTS Deloitte Legal B.V. (hierna: "**Deloitte**") gevraagd na de ontwerpfase van de Voorziening, waarin de architectuur van de Voorziening is vastgesteld, deze architectuur te toetsen aan de gegevensbeschermingsbeginselen die zijn neergelegd in de Algemene Verordening Gegevensbescherming (hierna: "**AVG**"). Versie 1.0, Februari 2019 van de Project Start Architectuur (hierna: "**PSA**") is als uitgangspunt genomen voor de in dit rapport geformuleerde observaties en aanbevolen maatregelen. Het AVG raamwerk dat Deloitte heeft gebruikt bij de beoordeling is afgestemd met GTS.
Dit rapport beperkt zich enkel tot de vraag of het ontwerp van de Voorziening kan leiden tot een Voorziening waarmee cliënten en zorgaanbieders hun nieuwe rechten en plichten kunnen uitoefenen, en daarbij recht doen aan de aspecten van gegevensbescherming die daarbij in overweging moeten worden genomen.

Geselecteerde GdO maatregelen

GdO houdt in dat GTS reeds in het vroegste stadium van de architectuur van de Voorziening de technische en organisatorische maatregelen moet (aan)duiden om de privacy en gegevensbescherming van de (uiteindelijk) betrokkenen te waarborgen. Ter voorbereiding op een Data Protection Impact Assessment (hierna: "**DPIA**") in een later stadium van de ontwikkeling van de Voorziening, is gebruik gemaakt van het Deloitte raamwerk waarin aan de vereisten van AVG kan worden getoetst. Wij hebben onderzocht of in het ontwerp van de Voorziening voldoende rekening is gehouden met de volgende beginselen uit de AVG: rechtmatigheid, behoorlijkheid, transparantie, informatiebeveiliging, juistheid, opslagbeperking, integriteit en vertrouwelijkheid. De beginselen die gezien de beperkte reikwijdte van de opdracht niet door ons zijn meegenomen in het onderzoek zijn doelbinding, noodzakelijkheid en evenredigheid.

Onderstaand hebben wij een samenvatting opgenomen van de belangrijkste GdO aandachtspunten die wij tijdens onze analyse hebben geconstateerd. We hebben deze punten gesplitst in punten specifiek betrekking hebbende op architectuur en op de vervolgfase/implementatiefase.

De belangrijkste geselecteerde GdO maatregelen die GTS, dan wel de partij(en) die de Voorziening gaa(t)(n) bouwen, moet nemen, zijn:

Maatregelen betrekking hebbende op de architectuur:

Overweeg een alternatieve rolverdeling

Het is aanbevolen om de voordelen van de gekozen rolverdeling af te wegen tegen de voordelen van een alternatieve rolverdeling waarbij de Beheerder-V (volledig) als verwerker ten behoeve van de bij een US aangesloten zorgaanbieders acteert. Op voorwaarde dat de Beheerder-V bij het uitwisselen van gegevens volledig kan kwalificeren als "verwerker" in de zin van de AVG heeft laatstgenoemde geen zelfstandige grondslag nodig in de vorm van toestemming, zoals dat in de huidige opzet wel het geval is.

Gebruik een juridisch raster als basis voor de gegevensverwerking

Parallel aan het verder concretiseren van het (technisch) ontwerp van de Voorziening moet een sluitend juridisch overzicht worden gemaakt waarin heldere kaders worden gesteld: welke toestemmingen zijn vereist, waarvoor, welke wettelijke grondslag is van toepassing, tot wie is de toestemming gericht, welke AVG vereisten zijn van toepassing, en indien dat het geval is, welke mogelijkheden om deze nader in te regelen, samenloop met andere wet- en regelgeving en indien dat het geval is,

welke betekenis komt daaraan toe – toegespitst op concrete *use cases*. De vereiste heldere informatieverschaffing jegens cliënten en zorgverleners (hierna ook: "**Betrokkenen**"), hetgeen in de volgende fase van de Voorziening moet worden uitgewerkt, volgt dit juridisch raster.

Regel een proces in m.b.t. het vragen van toestemming
Het is aanbevolen reeds in de architectuurfase een apart proces op te stellen met betrekking tot het vragen van toestemming als grondslag voor de Beheerder-V. Daarbij moet rekening worden gehouden met de AVG-vereisten voor toestemming.

Verzoek de wetgever om een grondslag te creëren voor de verwerking van het BSN van cliënten
Mocht er geen grondslag gevonden kunnen worden aan de hand van een alternatieve rolverdeling, dan zal er een wettelijke grondslag gecreëerd moeten worden voor toestemmingssystemen die de toestemmingen faciliteren conform de Wabvpz.

Maatregelen betrekking hebbende op de implementatiefase:

Informatievoorziening
Normaliter zien wij dat de kaders voor de informatievoorziening in de architectuur zijn uitgewerkt. Gezien de rolverdeling en de uitgangspunten binnen de architectuur is het verdedigbaar dat het projectteam GTS deze uitwerking in de implementatiefase van de Voorziening heeft geplaatst. Het is aanbevolen de informatievoorziening jegens Betrokkenen direct mee te nemen in de volgende fase van de Voorziening. Het juridisch raster kan als basis dienen voor de verdere uitwerking van de informatievoorziening. Belangrijk uitgangspunt moet daarbij zijn dat Betrokkenen de informatie moeten krijgen om te kunnen beoordelen of zij hun persoonsgegevens verwerkt willen hebben in deze Voorziening, en wat de consequentie is als van het onthouden van toestemming.

Pas security-by-design vervolgstappen toe
De AVG vereist toepassing van het privacy-by-design principe. Het is lastig en kostbaar om beveiligingsmaatregelen achteraf te implementeren binnen een softwareoplossing. De huidige versie van de PSA beschrijft de uitgangspunten die het gewenste niveau van informatiebeveiliging moeten gaan borgen voor de Voorziening. Het is belangrijk dat het *security-by-design* principe bij alle vervolgstappen consequent toegepast blijft worden. Informatiebeveiliging moet als integraal onderdeel van de ontwikkeling van de Voorziening worden meegenomen. Hiermee wordt voorkomen dat bij de oplevering van de Voorziening niet wordt voldaan aan de vereiste informatiebeveiligingsstandaarden waardoor additionele kosten zouden kunnen ontstaan.

Overkoepelende conclusie
Na heroverweging van de wenselijkheid van de gekozen rolverdeling en de impact die dat heeft op de inrichting van de Voorziening en het helder beschrijven van de impact, de strekking en de adressant van de verschillende toestemmingen kan met de PSA worden voorgesorteerd op een heldere informatievoorziening en transparante werkwijze rondom de Voorziening, zodat de gegevensbeschermingsbelangen worden gediend.

Zo wordt op microniveau voorgesorteerd op een rechtmatige en transparante gegevensverwerking ten behoeve van de inregeling van het gespecificeerde toestemmingsvereiste voor uitwisseling van gegevens middels een US tussen zorgaanbieders.

Adviesopdracht

Deze opdracht betreft een adviesdienst. Adviesdiensten worden niet uitgevoerd in het kader van een assurance opdracht en derhalve wordt geen zekerheid verstrekt omtrent de getrouwheid van de informatie. Het is de verantwoordelijkheid van de (geautoriseerde) gebruikers van ons rapport om te beoordelen of de uitgevoerde adviesdiensten in het perspectief van het geheel van de hen ter beschikking staande informatie en hun risicoperceptie aan de door hen te stellen eisen voldoen.

Verantwoordelijkheid

Het programmateam GTS is zelf verantwoordelijk voor, onder andere (a) het maken van keuzes en nemen van beslissingen en het dragen van alle verantwoordelijkheden die het management toebehoren, (b) het aanwijzen van een individu, bij voorkeur binnen het senior management, die verantwoordelijk is voor de besluiten van GTS en het toezien op de opdracht, (c) het toezien op de werkzaamheden en de evaluatie van de toereikendheid en uitkomsten van de opdracht, (d) het aanvaarden van de verantwoordelijkheid voor eventuele acties die voortvloeien uit de resultaten van de dienstverlening.

Inhoudsopgave

Uitgangspunten

Opdrachtgever

Nationaal ICT Instituut in de Zorg (hierna: "**Nictiz**") is de formele (juridisch) opdrachtgever van Deloitte ten aanzien van deze opdracht. Echter, de werkzaamheden zijn verricht ten behoeve van GTS. In dit rapport zullen wij enkel GTS als opdrachtgever benoemen.

Reikwijdte GdO rapport

In dit rapport hebben wij ons conform de opdracht beperkt tot een beoordeling van de architectuur van de Voorziening zoals omschreven in versie 1.0, Februari 2019 van de PSA. De PSA beschrijft alle kaders die worden meegenomen in de architectuur van de Voorziening. Onze observaties en aanbevolen maatregelen zien dus niet op verdere ontwikkeling – na versie 1.0 PSA – en implementatie van de Voorziening, met uitzondering van de in het document "Thema's in aanvulling PSA" omschreven feiten. Desalniettemin stellen wij wel maatregelen voor die later in het (ontwerp)proces kunnen worden doorgevoerd.

De reikwijdte van onderhavig rapport is als volgt: De architectuur van de Voorziening zoals omschreven in versie 1.0 van de Project Start Architectuur, de feiten zoals omschreven in versie 1.0 van document "Thema's in aanvulling PSA" en feiten zoals omschreven in de documenten die zijn opgenomen in de tabel in bijlage II, zijn in scope.

Buiten scope zijn alle aspecten van de implementatie van de Voorziening alsmede de onderwerpen 'register van de verwerkingsactiviteiten', 'doorgiften van persoonsgegevens', 'informatiebeveiliging', 'bewaring en vernietiging', 'transparantie en rechten van Betrokkenen', 'de impact van de migratie van toestemmingen', 'het aantal toestemmingsvragen', 'noodsituatie' en 'doelbinding, noodzakelijkheid en evenredigheid van de verwerking'.

Het is aanbevolen voorafgaand aan de livegang van de Voorziening een DPIA uit te (laten) voeren zodat in alle (ontwerp)fasen van de Voorziening integraal wordt getoetst aan (alle) vereisten en beginselen van privacy en gegevensbescherming.

Voorziening

De Voorziening biedt cliënten de mogelijkheid op één plek toestemming te geven dan wel te onthouden om gezondheidsgegevens (niet) te laten delen tussen zorgaanbieders via een US. Zorgaanbieders kunnen de Voorziening raadplegen om te achterhalen of zij toestemming hebben voor het delen van bepaalde gezondheidsgegevens. Het US waarop de zorgaanbieder is aangesloten, controleert dit.

Rolverdeling Voorziening

In de hiernavolgende hoofdstukken gaan wij uit van de volgende door GTS gekozen opzet van de Voorziening en daaruit voortvloeiende rolverdeling. In deze opzet is de Beheerder-V verwerkingsverantwoordelijke voor de verwerkingsactiviteiten 'aan de zijde van de cliënt', namelijk:

Verwerkingsverantwoordelijke verwerkingsactiviteiten Voorziening
1. Identificeren cliënt in de Voorziening
2. Identificeren zorgverlener bij toestemming invullen namens cliënt in de Voorziening
3. GTS account beheren
4. Beheer van toestemmingen (inclusief historie)
5. Notificeren cliënt
6. Vertegenwoordiging registreren
7. Het toepassen van logging

De Beheerder-V is verwerker van de bij een US aangesloten zorgaanbieders 'aan de zijde van de bij een US aangesloten zorgaanbieders', namelijk:

Verwerker verwerkingsactiviteiten Voorziening
1. Identificeren zorgverlener Voorziening
2. Het abonneren op notificaties door zorgaanbieders
3. Het notificeren van zorginstellingen
4. Beantwoorden autorisatievragen aan US

Tot slot hanteren wij als uitgangspunt dat de Beheerder-V verwerker is van de beheerder US. De Beheerder-V verwerkt immers óók toestemmingen ten behoeve van de beheerder US. Dit is geen aparte uitvraag maar betreft een clustering met de Wabvpz-toestemmingsvra(a)g(en).

Classificatie persoonsgegevens

De Beheerder-V verwerkt:

Omschrijving	Kwalificatie
Aanspreeknaam	De aanspreeknaam van de cliënt is een 'normaal' persoonsgegeven in de zin van artikel 4 lid 1 AVG.
Emailadres van cliënt voor een account in de Voorziening	Het e-mailadres van de cliënt is een 'normaal' persoonsgegeven in de zin van artikel 4 lid 1 AVG.
Telefoonnummer van cliënt voor een account in de Voorziening	Het telefoonnummer van de cliënt is een 'normaal' persoonsgegeven in de zin van artikel 4 lid 1 AVG.
Leeftijdscategorie van de cliënt	De leeftijdscategorie van de cliënt is een 'normaal' persoonsgegeven in de zin van artikel 4 lid 1 AVG.
BSN van de cliënt en eventueel diens (wettelijk) vertegenwoordiger	Het BSN is een nationaal identificatienummer ex. artikel 46 UAVG. Het BSN kan slechts worden gebruikt voor doeleinden die bij wet zijn bepaald. Gelet op de functie van het BSN betreft het een zeer gevoelig persoonsgegeven., De verwerking daarvan dient aan de hoogste beveiligingsstandaarden te voldoen.
"Toestemmingsinformatie" of "toestemmingsprofielen"	De toestemmingsinformatie of toestemmingsprofielen worden binnen het programma als bijzondere persoonsgegevens in de zin van artikel 4 lid 15 AVG aangemerkt. Het kan niet worden uitgesloten dat een specifieke toestemming voor een specifieke categorie zorgaanbieders informatie over de gezondheid weergeeft.
UZI-nummer van de aangesloten zorgverlener	Het UZI-nummer van de aangesloten zorgverlener is een 'normaal' persoonsgegeven in de zin van artikel 4 lid 1 AVG.
UZI-rolcode van de aangesloten zorgverlener	De UZI-rolcode van de aangesloten zorgverlener is een 'normaal' persoonsgegeven in de zin van artikel 4 lid 1 AVG.

Toestemmingen

In de gekozen opzet is de volgende set aan toestemmingen vereist:

Definitie	Wettelijke grondslag	Adressant	Toelichting
Wabvpz-toestemming of gespecificeerde uitwisselingstoestemming	Artikel 15a lid 1 en lid 2 Wabvpz	Zorgaanbieders	Uitdrukkelijke en gespecificeerde toestemming aan de dossierhoudende zorgaanbieder om gegevens van de cliënt ter beschikking te stellen via een US.
WGBO-toestemming	Artikel 7:457 lid 1 BW (WGBO)	Dossierhoudende zorgverlener	(Impliciete) toestemming ter doorbreking van het beroepsgeheim van de cliënt aan de dossierhoudende zorgaanbieder, op wie de plicht tot verificatie van deze toestemming rust. De dossierhoudende zorgaanbieder dient (veronderstelde) toestemming te verkrijgen van de cliënt vóór verstrekking van de gegevens, ongeacht de wijze van verstrekking en ongeacht wie de ontvanger is van de gegevens. Deze toestemming kan impliciet worden gegeven.
Verwerkingstoestemming Voorziening	Artikel 9 lid 2 sub a en artikel 6 lid 1 sub a AVG	Beheerder-V (indien verantwoordelijke)	Uitdrukkelijke toestemming voor de verwerking van de toestemmingsprofiel in de Voorziening. NB: Uit de ontvangen documentatie blijkt niet of deze toestemming apart wordt uitgevraagd door de Beheerder-V, of dat deze toestemming is meegenomen in de toestemmingsvragen op grond van de Wabvpz.
Verwerkingstoestemming US	Artikel 9 lid 2 sub a AVG en artikel 6 lid 1 sub a AVG	Beheerder US (indien verwerkingsverantwoordelijke)	Uitdrukkelijke toestemming voor de verwerking van de gegevens in/via het US. Uit de juridische documentatie van programmateam GTS blijkt dat deze toestemmingsvraag aan de beheerder US is inbegrepen bij de toestemmingsvragen op grond van de Wabvpz. De beheerder US vraagt dus geen separate toestemming aan de cliënt om zijn of haar persoonsgegevens te verwerken in/via het US.

Samenloop WGBO- en Wabvpz-toestemming

In de gekozen opzet van de Voorziening is sprake van geclusterde toestemmingen. Deze toestemmingen zijn niet verder benoemd in dit rapport. Desalniettemin willen wij graag benadrukken dat er rekening moet worden gehouden met de verschillende situaties die kunnen optreden, zoals dat het niet logisch is dat een cliënt (Betrokkene) bij wijze van voorbeeld wel toestemming geeft voor beschikbaarstelling van gegevens via een US, maar dan toch bezwaar heeft tegen het doorbreken van het medische beroepsgeheim. Wel logisch kan zijn dat een 'nee' in het systeem zich slechts beperkt tot een bezwaar tegen beschikbaarstelling via een US, maar dat een cliënt daarmee niet heeft uitgesloten wel akkoord te kunnen gaan met de doorbreking van het beroepsgeheim, maar uitwisseling wenst via andere wegen post, mail, fax. Dit model levert minder bezwaren op voor degenen die buiten de registratie middels de Voorziening (willen) blijven. Niet registreren levert immers ook een 'nee' op maar de raadplegende zorgaanbieder hoeft de zoektocht naar de noodzakelijke gegevens dan niet te staken. Hij weet dat de zoektocht kan worden voortgezet buiten het systeem om. De clustering van de drie toestemmingsvarianten bij een 'nee' is niet als uitgangspunt genomen in de PSA.

1. Onderzoeksopzet

1. Onderzoeksopzet

Onderhavige GdO rapportage is uitgevoerd aan de hand van een door Deloitte en GTS afgestemd AVG raamwerk. Middels deze analyse wordt inzicht verschaft aan betrokken partijen (waaronder Ministerie van Volksgezondheid, Welzijn en Sport (hierna: "VWS"), zorgkoepels en leveranciers) in de actiepunten om de Voorziening ("*by design*") op de meest passende en wenselijke manier in het licht van de AVG, UAVG, Wabvpz, WGBO, ISO 27001, NEN 7510, 7512 en 7513, OWASP en NIST in te richten.

Opdrachtgever heeft adviseurs van CGI gevraagd het proces te begeleiden. In overleg met GTS en CGI heeft de aanpak van onze werkzaamheden in hoofdlijnen uit de volgende stappen bestaan:

- Planning en voorbereiding
- Doornemen documentatie en uitvoeren interviews
- Uitvoeren GdO werkzaamheden
- Opstellen en afstemmen rapportages

Hieronder geven we de activiteiten weer die in de verschillende fasen zijn uitgevoerd.

Planning en voorbereiding

De planning en voorbereiding is in overleg en samenwerking met GTS en CGI uitgevoerd. Wij hebben tijdens de planningsfase operationele afspraken gemaakt over afstemmomenten, de interviews en het aanleveren van documentatie. Daarnaast hebben wij de informatie verzameld die als uitgangspunt voor onze GdO werkzaamheden is genomen..

Doornemen documentatie en uitvoeren interviews

Direct bij aanvang van onze werkzaamheden zijn wij gestart met het doornemen van de documentatie. Voor een overzicht van de documentatie, zoals wij deze tijdens onze werkzaamheden hebben gebruikt, verwijzen wij naar bijlage II.
Wij hebben naast het doornemen van de documentatie op verschillende momenten overleg gehad met de contactpersonen vanuit GTS en CGI. Belangrijke contactmomenten waren een kick-off overleg, een overleg met een algemene toelichting inzake de Voorziening en een tussentijds overleg na oplevering van tussenrapport nummer 1. Wij hebben tijdens deze contactmomenten informatie gekregen die voor ons de achterliggende motieven van de Voorziening helder hebben gemaakt en daardoor een goede basis voor onze GdO werkzaamheden hebben gelegd.

Uitvoeren GdO werkzaamheden

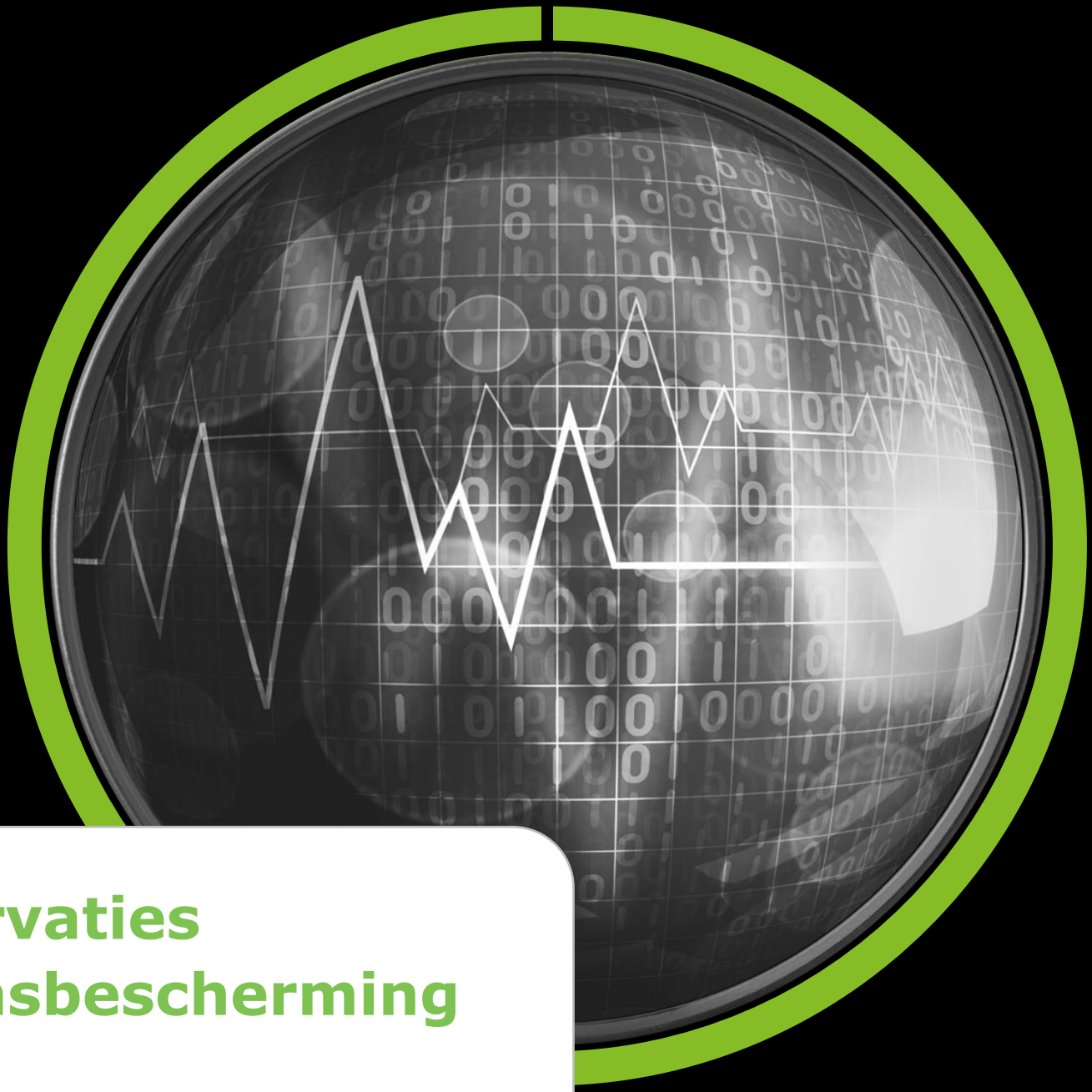
GdO is een proactieve benadering van gegevensbescherming omdat reeds in de architectuurfase wordt getoetst aan de gegevensbeschermingsbeginselen en vereisten uit de AVG. Tijdens de werkzaamheden is de Algemene Verordening Gegevensbescherming (AVG) niet als een 'silo' benaderd, maar is de AVG geplaatst in het volledige regelgevend kader waar de Voorziening aan moet voldoen. Ter voorbereiding van een DPIA in een later stadium van de ontwikkeling van de Voorziening, is gebruik gemaakt van het Deloitte raamwerk waarin aan de vereisten van AVG kan worden getoetst.

Opstellen en afstemmen rapportages

Allereerst hebben wij voldaan aan de drietal tussentijdse rapportageverplichtingen die in de opdrachtgunning waren opgenomen. Deze rapportages zijn rondom oplevering besproken met GTS. De tussentijdse rapporten waren zeer kort om geen projecttijd te verliezen en in die fase alleen de belangrijkste bespreekpunten tussen Deloitte en GTS inzichtelijk te maken.

Op 9 mei en 28 mei 2019 hebben er overleggen plaatsgevonden tussen GTS, CGI en Deloitte waarbij versie 0.9 van onderhavig rapport is besproken. Tijdens deze overleggen zijn vervolgstappen besproken. Tussen 28 mei en 15 augustus 2019 zijn de vervolgstappen uitgevoerd.

Het eindresultaat van de rapportagefase is het rapport dat hier voor u ligt. Wij hebben dit rapport met u besproken en zijn uiteraard beschikbaar voor een verdere toelichting omtrent de inhoud van het rapport.



2. Observaties gegevensbescherming

4.1 Gegevensbescherming door ontwerp maatregelen

Topic	Beginsel	Maatregel	Fase	Verwijzing PSA	Detailuitwerking
Rolverdeling	Rechtmatigheid	Overweeg een alternatieve rolverdeling	Architectuur	Algemene observatie	Hoofdstuk 2.2
Rolverdeling	Rechtmatigheid	Neem de grondslagen op in de PSA	Architectuur	Algemene observatie	Hoofdstuk 2.2
Rolverdeling	Transparantie	Informeer betrokkenen over de grondslagen	Architectuur	Algemene observatie	Hoofdstuk 2.2
Toestemming	Rechtmatigheid, behoorlijkheid, transparantie	Gebruik een juridisch raster als basis voor de gegevensverwerking	Architectuur	Algemene observatie	Hoofdstuk 2.3
Toestemming	Rechtmatigheid, behoorlijkheid, transparantie	Regel een proces in m.b.t. het vragen van toestemming	Architectuur	Algemene observatie	Hoofdstuk 2.3
Transparantie	Transparantie	Werk de informatievoorziening uit in de volgende fase	Implementatie	Algemene observatie	Hoofdstuk 2.4
Transparantie	Alle AVG beginselen	Toets de informatievoorziening in een DPIA voorafgaand aan livegang van de Voorziening	Implementatie	Algemene observatie	Hoofdstuk 2.4
Verwerking BSN	Rechtmatigheid	Overweeg een alternatieve rolverdeling	Architectuur	Pagina 34, 57, 79 PSA Overzicht juridische doc. nr. 33, p. 17	Hoofdstuk 2.5
Verwerking BSN	Rechtmatigheid	Verzoek de wetgever om een grondslag te creëren voor de verwerking van het BSN van cliënten	Architectuur	Pagina 34, 57, 79 PSA Overzicht juridische doc. nr. 33, p. 17	Hoofdstuk 2.5
Verwerking BSN	Rechtmatigheid	Toets of artikel 9 Wabvpz een rechtmatige wettelijke grondslag vormt voor de verwerking van het BSN van cliënten	Architectuur	Pagina 34, 57, 79 PSA Overzicht juridische doc. nr. 33, p. 17	Hoofdstuk 2.5
Verwerking BSN	Rechtmatigheid	Toets of artikel 8 Wabvpz een rechtmatige wettelijke grondslag vormt voor de verwerking van het BSN van cliënten	Architectuur	Pagina 34, 57, 79 PSA Overzicht juridische doc. nr. 33, p. 17	Hoofdstuk 2.5

2.2 Rolverdeling

Thema:	**Referentie:**
Rolverdeling: verwerkingsverantwoordelijke – verwerker	Algemene observatie

AVG vereiste

De rolverdeling en verantwoordelijkheden van de partijen die de persoonsgegevens van cliënten verwerken, moeten transparant zijn voor Betrokkenen.

Observatie

In de huidige architectuur is onderscheid gemaakt tussen gegevensverwerkingen aan de zijde van de cliënt enerzijds en de zorgaanbieder anderzijds. Voortbordurend op dit onderscheid is gekozen voor de opzet waarin de Beheerder-V verwerkingsverantwoordelijke is ten aanzien van de verwerkingen aan de zijde van de cliënt, en de zorgaanbieder verwerkingsverantwoordelijke is ten aanzien van de verwerkingen aan de zijde van de zorgaanbieder.

Als verwerkingsverantwoordelijke heeft de Beheerder-V een eigen grondslag nodig voor het verwerken van de gegevens ter identificatie van de Betrokkene en de toestemmingsinformatie in de Voorziening. Omdat deze persoonsgegevens als bijzondere persoonsgegevens kwalificeren, is als ontheffing op het verbod om deze gegevens te verwerken uitdrukkelijke toestemming vereist. Deze toestemming kan tegelijk dienst doen als verwerkingsgrondslag voor de Beheerder-V ex. artikel 6 lid 1 a AVG.

GdO maatregelen

- **Overweeg een alternatieve rolverdeling**: Het is aanbevolen om de voordelen van de gekozen rolverdeling af te wegen tegen de voordelen van een alternatieve rolverdeling waarbij de beheerder Voorziening (volledig) als verwerker ten behoeve van de bij een US aangesloten zorgaanbieders acteert. De Beheerder-V zal in voornoemde alternatieve rolverdeling geen zelfstandige grondslag nodig hebben. Als verwerker kan zij meeliften op de grondslag van de bij een US aangesloten zorgaanbieders.

- **Neem de grondslagen op in de PSA**: Indien de gekozen rolverdeling de voorkeur heeft, dan moet de grondslag voor de verwerking door de Beheerder-V worden opgenomen in de PSA.

- **Informeer Betrokkenen over de grondslagen:** Het is aanbevolen reeds in de architectuurfase na te denken over de wijze waarop deze toestemming moet worden verkregen, en hoe cliënten daaromtrent moeten worden geïnformeerd.

2.3 Toestemming als grondslag in de zin van de AVG

Thema:	**Referentie:**
Toestemming, transparantie	Algemene observatie

AVG vereiste

De juridische reikwijdte van de verschillende toestemmingen die kunnen worden gegeven in de Voorziening, moet worden opgenomen in het privacy beleid van de verwerkingsverantwoordelijke.

Observatie

In de huidige opzet is gekozen voor de rol van verwerkingsverantwoordelijke voor de Beheerder-V voor de gegevensverwerkingen aan de patiëntkant. Daardoor ontstaat de noodzaak voor het apart verzoeken om een ontheffing en grondslag voor de Beheerder-V in de vorm van aparte toestemming. Echter, in de PSA ontbreekt de constatering dat als gevolg van de gekozen rolverdeling aparte toestemming vereist is en een beschrijving van het voornemen deze toestemming apart uit te vragen.

Omdat deze toestemming een verwerkingsgrondslag in de zin van de AVG betreft, moet voldaan worden aan de specifieke toestemmingsvereisten die in de AVG worden gesteld.

Zoals onder 2.2 aangegeven is in de huidige PSA geen aparte uitvraag beschreven van de verkrijging van deze ontheffing en grondslag. Ook blijft daarom in de PSA de noodzaak onbesproken dat moet worden voldaan aan de toestemmingsvereisten van de AVG, met name:

- Dat de cliënt de toestemming aan de Beheerder-V moet kunnen intrekken, en op welke wijze gefaciliteerd kan worden dat het intrekken van de toestemming even eenvoudig is als het geven van de toestemming;
    - In het verlengde van het voorgaande: dat voorzien moet worden in het scenario dat de toestemming wordt ingetrokken. Wat zijn de consequenties van het niet geven en het intrekken van de toestemming?
- Dat de cliënt de toestemming duidelijk kan onderscheiden van de andere toestemmingsvragen: de toestemming voor de beheerder US in voorkomend geval en de toestemming voor de dossierhoudende zorgaanbieders;
- Dat de toestemming vrijelijk moet zijn gegeven en dat dit extra zorgvuldigheid vereist bij de inrichting van het proces en bij de informatievoorziening aan de cliënt.

GdO maatregelen

- **Grondslag**: Bij de afweging van een alternatieve rolverdeling zou de noodzaak om toestemming te vragen als grondslag voor gegevensverwerking, meegenomen moeten worden.

- **Gebruik een juridisch raster als basis voor de gegevensverwerking:** Ga werken met een "juridisch raster" dat als basis fungeert om aan de transparantievereisten te voldoen richting zowel de cliënt als de zorgverlener. Wij vragen met name aandacht voor het inzicht dat de Betrokkene moet hebben in de consequentie van het gekozen toestemmingsmodel. Betrokkenen moeten bijvoorbeeld worden geïnformeerd over de consequenties van het niet verlenen van toestemming in de Voorziening. Een 'nee' leidt niet noodzakelijkerwijs tot staking van de verstrekking van medische informatie van de betrokken cliënt. Mogelijk is uitwisseling buiten het systeem om immers wél mogelijk.

- **Regel een proces in m.b.t. vragen van toestemming**: Het is aanbevolen reeds in de architectuurfase een apart proces op te stellen met betrekking tot het vragen van toestemming als grondslag voor de Beheerder-V. Daarbij moet rekening worden gehouden met de AVG-vereisten voor toestemming.

2.4 Informatievoorziening

Thema:	**Referentie:**
Transparantie	Algemene observatie

AVG vereiste

De juridische reikwijdte van de verschillende toestemmingen die kunnen worden gegeven in de Voorziening moet transparant zijn voor Betrokkenen.

Observatie

Zoals onder 2.2 en 2.3 aangegeven is de Beheerder-V voor de gegevensverwerkingen 'aan de kant van de cliënt' verwerkingsverantwoordelijke. Dat betekent dat de Beheerder-V op grond van artikel 12 e.v. AVG de cliënt moet informeren over deze gegevensverwerkingen.
In de PSA zijn kaders geschetst waaruit blijkt dat de Beheerder-V de cliënt moet informeren over de verwerking in de Voorziening en de toestemmingsvarianten. Echter, een onderkenning van de verschillen tussen de toestemmingen en hun juridische reikwijdte ontbreekt terwijl dit (ook) impact heeft op de architectuur. Zonder systematische en gestructureerde omschrijving van dit toestemmingenmodel wordt niet voorgesorteerd op een transparante informatievoorziening.
In de informatievoorziening jegens Betrokkenen moet tevens de 'noodsituatie' waarin gegevens van de cliënt kunnen worden verwerkt, worden toegelicht. Blijkens de PSA gaat het bij noodsituaties niet om uitvoering te geven aan bijzondere in de wet bepaalde situaties (bijvoorbeeld 'vitaal belang' of 'levensbedreigende situaties') maar om de algemene notie dat er gegevens geraadpleegd kunnen worden ten behoeve van zorgverlening in een noodsituatie. 'Noodsituatie' is niet nader gedefinieerd in de PSA of de Wabvpz.

GdO maatregelen

- **Werk de informatievoorziening direct in de volgende fase uit**: Normaliter zien wij dat de kaders voor de informatievoorziening in de architectuur zijn uitgewerkt. Gezien de rolverdeling en de uitgangspunten binnen de architectuur is het verdedigbaar dat het projectteam GTS deze uitwerking in de implementatiefase van de Voorziening heeft geplaatst. Het is aanbevolen de informatievoorziening jegens Betrokkenen direct mee te nemen in de volgende fase van de Voorziening. Daaraan zou de definitie van een noodsituatie moeten worden meegenomen. Een belangrijke overweging is het toepassen van UX-design op de informatievoorziening.

- **Toets de informatievoorziening in een DPIA voorafgaand aan livegang van de Voorziening**: Het is tevens aanbevolen de nog uit te werken informatievoorziening in een DPIA te toetsen voorafgaand aan de livegang van de Voorziening.

2.5 Verwerking BSN door de Beheerder-V

Thema:	**Referentie:**
Verwerking BSN	Pagina 34, 57, 79 PSA

AVG vereiste

Voor het verwerken van een BSN is een wettelijke grondslag en doelomschrijving vereist.

Observatie

De Beheerder-V beoogt het BSN van de cliënt en eventueel diens (wettelijk) vertegenwoordiger te verwerken. Voor zover de Beheerder-V in de rol van verwerkingsverantwoordelijke het BSN van de cliënt en eventueel diens (wettelijk) vertegenwoordigt, heeft zij daarvoor geen wettelijke grondslag.
Uit de PSA volgt dat een aparte grondslag wordt geregeld door VWS voor de verwerkingsactiviteiten van de Beheerder-V 'aan de zijde van de cliënt'.

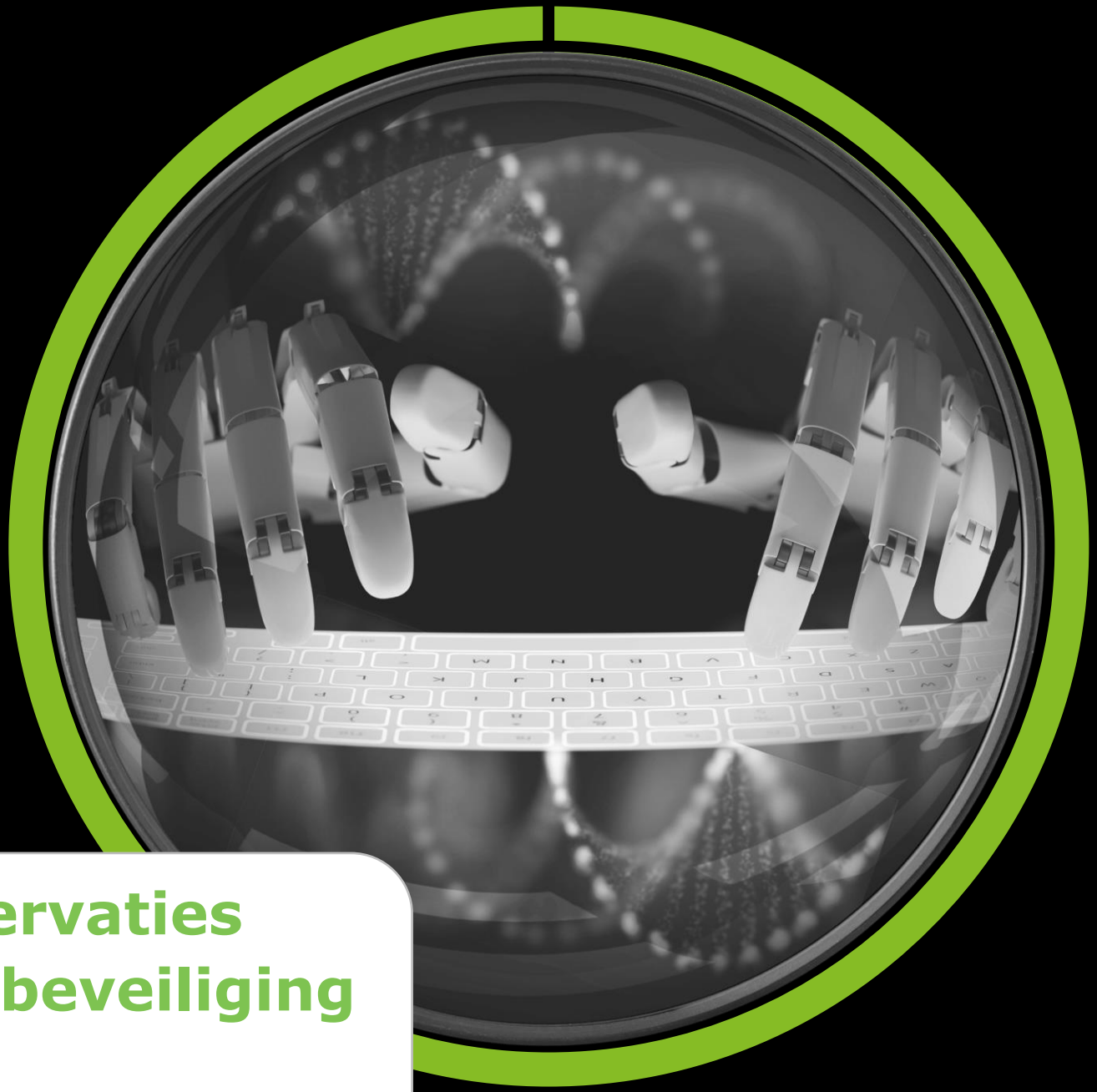
GdO maatregelen

- **Overweeg een alternatieve rolverdeling**: Zie 2.2. Het is aanbevolen om de voordelen van de gekozen rolverdeling af te wegen tegen de voordelen van een alternatieve rolverdeling waarbij de beheerder Voorziening (volledig) als verwerker ten behoeve van de bij een US aangesloten zorgaanbieders acteert. De Beheerder-V zal in voornoemde alternatieve rolverdeling geen zelfstandige grondslag nodig hebben voor de verwerking van het BSN van de cliënt.

- **Verzoek de wetgever om een grondslag te creëren voor de verwerking van het BSN van cliënten**: Mocht er geen grondslag gevonden kunnen worden aan de hand van een alternatieve rolverdeling, dan zal er een wettelijke grondslag gecreëerd moeten worden voor toestemmingssystemen die de toestemmingen faciliteren conform de Wabvpz.

- **Toets of artikel 9 Wabvpz een rechtmatige wettelijke grondslag vormt voor de verwerking van het BSN van cliënten**: Is een alternatieve rolverdeling niet mogelijk en wordt er geen separate grondslag gecreëerd door de wetgever, dan moet worden bekeken of de verwerking van de bij een US aangesloten zorgaanbieders in de Voorziening kan worden geschaard onder artikel 9 Wabvpz. Zo ja, dan kan de Beheerder-V in de rol van verwerker mogelijk 'meeliften' op deze grondslag voor de bij een US aangesloten zorgaanbieders.

- **Toets of artikel 8 Wabvpz een rechtmatige wettelijke grondslag vormt voor de verwerking van het BSN van cliënten**: Afhankelijk van de gekozen rolverdeling moet worden onderzocht of de verwerking in de Voorziening door de Beheerder-V in de rol van verwerkingsverantwoordelijke kan worden geschaard onder artikel 8 lid 2 Wabvpz.



3. Observaties informatiebeveiliging

3.1 Algemene toelichting informatiebeveiliging

Op grond van artikel 32 AVG moet de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen treffen ter bescherming van de persoonsgegevens. Voor de verwerking van bijzondere persoonsgegevens, zoals gegevens over iemands gezondheid, gelden extra strenge eisen. Daarnaast vereist de AVG toepassing van het *privacy-by-design* principe. Het is lastig en kostbaar om beveiligingsmaatregelen achteraf te implementeren binnen een softwareoplossing. Derhalve is het belangrijk om reeds in de architectuurfase van de voorgenomen verwerking maatregelen te specificeren (*security-by-design*). Een risicoanalyse verschaft inzicht in de (belangrijkste) beveiligingsrisico's waaraan de verwerkingen bloot staan.[1] Het ontwerp van de beveiligingsmaatregelen dient gebaseerd te zijn op beschikbare (inter)nationale beveiligingsstandaarden (zoals bijvoorbeeld NEN 7510-7513, ISO 27001, NIST en OWASP) en de Richtsnoeren bescherming persoonsgegevens van het College bescherming persoonsgegevens (thans: "**AP**")[2].
Daarnaast is het een verplichting om regelmatig te controleren of beveiligingsmaatregelen adequaat zijn en worden nageleefd. Een regelmatige analyse of de getroffen beveiligingsmaatregelen nog aansluiten bij de stand van de techniek is daarbij ook een verplichting.

Vertrouwen is de basis
De verschillende stakeholders hebben met elkaar geconcludeerd dat *vertrouwen in de Voorziening* door de gebruikers de belangrijkste voorwaarde betreft voor het succes van de Voorziening. Het is daarmee van evident belang dat binnen de Voorziening een vastgesteld minimumniveau (ofwel specifieke baseline) van beveiliging van persoonsgegevens moet worden gewaarborgd voor de omgeving zelf, maar ook richting de betrokken deelnemende partijen en ketenpartners. Beide partijen hebben hierin uiteraard hun eigen verantwoordelijkheid waarvoor een overeenkomst wordt opgesteld waarin de afspraken en het niveau van toetsen op waarborging met elkaar wordt afgesproken.
De huidige versie van de PSA beschrijft de uitgangspunten die het gewenste niveau van informatiebeveiliging moeten gaan borgen voor de Voorziening. Een aantal hiervan is als volgt:

- Ten aanzien van informatiebeveiliging moet voldaan worden aan de normen ISO 27001 en de NEN normen 7510, 7512 en 7513. Dit zijn de standaard normen voor veilige gegevensuitwisseling in de zorg. Compliance op deze normen zal normaliter door een externe partij moeten worden vastgesteld (paragraaf 9.2, PSA);
- De principes en uitgangspunten zijn geformuleerd ten aanzien van informatiebeveiliging (paragraaf 9.3, PSA);
- Ten aanzien van informatiebeveiliging is een risicoanalyse uitgevoerd waarvan de resultaten zijn opgenomen (paragraaf 9.4, PSA);
- De maatregelen, die ten aanzien van security-by-design zijn beschreven om in te voeren, zijn gebaseerd op eerder genoemde kaders maar ook op de maatregelen die binnen "Aorta" staan beschreven. De uitwerking hiervan is opgenomen binnen de PSA (globaal in paragraaf 9.5) en binnen de Programma's van Eisen;
- De Beheerder-V komt voorafgaand aan de aansluiting met een US een overeenkomst overeen met de beheerder US. In deze overeenkomst (die nog in concept opgesteld moet worden) worden afspraken opgenomen over het vertrouwen in de ketenpartner, de comformiteit aan de aansluiteisen, de testresultaten op koppelvlakken en de migratiestrategie (paragraaf 5.4.4, PSA).

Het is voor GTS belangrijk dat een strategie wordt gehanteerd die is gestaafd op de boodschap: ***Zeg wat je doet en doe wat je zegt*.** Door het verkrijgen, maar vooral ook behouden, van vertrouwen zal de bereidwilligheid van gebruikers toenemen om de Voorziening te gaan en blijven gebruiken. De gebruiker moet erop kunnen vertrouwen dat er verantwoord en veilig wordt omgegaan met zijn of haar data. De Beheerder-V zal maatregelen moeten nemen om het vertrouwen van deelnemers te verkrijgen en behouden.

[1] Blijkens paragraaf 9.4 van de PSA is hier reeds invulling aan gegeven.

[2] https://wetten.overheid.nl/BWBR0033572/2013-03-01.

3.2 Informatiebeveiliging door ontwerp maatregelen

Topic	Beginsel	Maatregel	Verwijzing
Informatie-beveiliging	Informatiebeveiliging	1. Neem informatiebeveiliging als integraal onderdeel op binnen iedere fase van de ontwikkeling van de Voorziening.	Pagina 34-36, 44, 77 PSA
	Informatiebeveiliging	2. Stel integraal de beveiligings- en overige vereisten voor externe koppelvlakken vast. Het is belangrijk beleid op te stellen met betrekking tot het testen van het systeem, inclusief de koppelvlakken. Daarmee wordt gewaarborgd dat externe ketenpartners voldoen aan tenminste de minimale set van eisen aan informatiebeveiliging	Pagina 56, 59, 73-74 PSA
	Informatiebeveiliging	3. Geef opvolging aan het opstellen en implementeren van beleid omtrent het toepassen en gebruik van sleutels binnen de Voorziening.	Algemene observatie
	Informatiebeveiliging	4. Neem maatregelen die afdwingen dat geen gebruik wordt gemaakt van productiedata (en data voorzien van persoonsgegevens) binnen test- en ontwikkelomgevingen.	Algemene observatie
	Informatiebeveiliging	5. Maak de informatiebeveiligingsbaseline zo specifiek mogelijk (uiteraard volgens een risicoanalyse gebaseerde benadering zoals in paragraaf 9.4 van de PSA een invulling aan is gegeven).	Pagina 76-79 PSA
	Informatiebeveiliging	6. Werk de algemene informatiebeveiligingsbeginselen in de PSA en onderliggende documentatie verder uit. Door het uitwerken van de principes en uitgangspunten in een paragraaf kan meer duiding, diepgang en reikwijdte worden gegeven.	Pagina 77 PSA

De bovenstaande maatregelen zijn allen maatregelen die vooral betrekking hebben op de implementatiefase van de Voorziening.

4. Bijlagen

4.1 Bijlage I: Het juridisch kader

Wabvpz

Artikel 15a lid 1 Wabvpz:
De zorgaanbieder stelt gegevens van de cliënt slechts beschikbaar via een elektronisch uitwisselingssysteem, voor zover de zorgaanbieder heeft vastgesteld dat de cliënt daartoe uitdrukkelijk toestemming heeft gegeven.

Artikel 15a lid 2 Wabvpz:
De in het eerste lid bedoelde toestemming betreft gespecificeerde toestemming voor het beschikbaar stellen van alle of bepaalde gegevens aan bepaalde door de cliënt aan te duiden zorgaanbieders of categorieën van zorgaanbieders.

Artikel 15g Wabvpz:
Indien de cliënt een wettelijk vertegenwoordiger heeft, worden de op grond van deze paragraaf aan de cliënt toekomende rechten uitgeoefend door deze vertegenwoordiger, met dien verstande dat in afwijking van artikel 5, eerste lid, van de Uitvoeringswet Algemene verordening gegevensbescherming toestemming voor het verwerken van persoonsgegevens, mede is vereist van de cliënt die de leeftijd van twaalf maar nog niet van zestien jaren heeft bereikt, tenzij de desbetreffende cliënt niet in staat kan worden geacht tot een redelijke waardering van zijn belangen ter zake.

WGBO

Artikel 7:457 lid 1 BW:
Onverminderd het in artikel 448 lid 3, tweede volzin, bepaalde draagt de hulpverlener zorg, dat aan anderen dan de patiënt geen inlichtingen over de patiënt dan wel inzage in of afschrift van de bescheiden, bedoeld in artikel 454, worden verstrekt dan met toestemming van de patiënt. Indien verstrekking plaatsvindt, geschiedt deze slechts voor zover daardoor de persoonlijke levenssfeer van een ander niet wordt geschaad. De verstrekking kan geschieden zonder inachtneming van de beperkingen, bedoeld in de voorgaande volzinnen, indien het bij of krachtens de wet bepaalde daartoe verplicht.

AVG

Artikel 6 lid 1 sub a AVG:
De verwerking is alleen rechtmatig indien en voor zover aan ten minste een van de onderstaande voorwaarden is voldaan: de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden; (…)

Artikel 6 lid 1 sub d AVG:
De verwerking is alleen rechtmatig indien en voor zover aan ten minste een van de onderstaande voorwaarden is voldaan; (…) de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;

Artikel 7 lid 2 AVG
Indien de betrokkene toestemming geeft in het kader van een schriftelijke verklaring die ook op andere aangelegenheden betrekking heeft, wordt het verzoek om toestemming in een begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal zodanig gepresenteerd dat een duidelijk onderscheid kan worden gemaakt met de andere aangelegenheden. Wanneer een gedeelte van een dergelijke verklaring een inbreuk vormt op deze verordening, is dit gedeelte niet bindend.

Artikel 9 lid 1 en lid 2 sub a AVG:
Verwerking van persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid zijn verboden.

Lid 1 is niet van toepassing wanneer aan een van de onderstaande voorwaarden is voldaan: de betrokkene heeft uitdrukkelijke toestemming gegeven voor de verwerking van die persoonsgegevens voor een of meer welbepaalde doeleinden, behalve indien in Unierecht of lidstatelijk recht is bepaald dat het in lid 1 genoemde verbod niet door de betrokkene kan worden opgeheven; (…)

Artikel 9 lid 1 en lid 2 sub c AVG
Verwerking van persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid zijn verboden.

Lid 1 is niet van toepassing wanneer aan een van de onderstaande voorwaarden is voldaan: (…) de verwerking is noodzakelijk ter bescherming van de vitale belangen van de betrokkene of van een andere natuurlijke persoon indien de betrokkene fysiek of juridisch niet in staat is zijn toestemming te geven.

Standaarden

NEN 7510
De verwerking van patiëntgegevens door Voorziening moet voldoen aan de NEN 7510. NEN 7510 geeft richtlijnen en uitgangspunten voor het bepalen, instellen en handhaven van maatregelen die moeten worden getroffen ter beveiliging van de informatievoorziening in de zorg. De grondslag van deze verplichting is gelegen in het Besluit elektronische gegevensverwerking door zorgaanbieders.

NEN 7512
De verwerking van patiëntgegevens door Voorziening moet voldoen aan NEN 7512. NEN 7512 heeft als doel het bieden van zekerheid bij partijen die onderling medische gegevens uitwisselen. De grondslag van deze verplichting is gelegen in het Besluit elektronische gegevensverwerking door zorgaanbieders.

NEN 7513
De verwerking van patiëntgegevens door Voorziening moet voldoen aan NEN 7513. Deze norm heeft betrekking op logging. De grondslag van deze verplichting is gelegen in het Besluit elektronische gegevensverwerking door zorgaanbieders.

4.2 Bijlage II: Overzicht belangrijkste gebruikte documentatie

Overzicht ontvangen documentatie		
Content van GTS	**Ontvangen**	**Toelichting**
RFP DPIA GTA – V1.1.pdf	05 maart 2019	Ontvangen van André Klappe
1) PSA GTS v10 wijzigingen doorgevoerd.pdf	05 maart 2019	Ontvangen van André Klappe
3) 20180913 GTS voor SAP ziekenhuizen TN.pdf	05 maart 2019	Ontvangen van André Klappe
4) VZVZ_OTV_1111_PvE_TAP_toestemmingsapplicatie v00.01.pdf	05 maart 2019	Ontvangen van André Klappe
4) VZVZ_OTV_1112_PvE_REG_toestemmingsregister_v00.01.pdf	05 maart 2019	Ontvangen van André Klappe
4) VZVZ_OTV_1113_PvE_BAP_beheerapplicatie_00.01.pdf	05 maart 2019	Ontvangen van André Klappe
4) VZVZ_OTV_1120_PvE_NF_Nonfuctionals_v00.01.pdf	05 maart 2019	Ontvangen van André Klappe
4) VZVZ_OTV_2000_PvE_ORG_Beheerorganisatie_OTV_v00.01.pdf	05 maart 2019	Ontvangen van André Klappe
4) VZVZ_OTV_2000_PvE_APP_Aansluiteisen_Patientportalen_v00.01.pdf	05 maart 2019	Ontvangen van André Klappe
4) VZVZ_OTV_Programma van Eisen Oplegger.pdf	05 maart 2019	Ontvangen van André Klappe
5) OTV modellen 00.30.pdf	05 maart 2019	Ontvangen van André Klappe
2) Overzicht juridische documentatie GTA (cocept).pdf	14 maart 2019	Ontvangen van André Klappe
OTV alg intro.pptx	27 maart 2019	Ontvangen van Albert Vlug
Voortgang-online-toestemmingsvoorziening-voor-gespecificeerde-toestemming-wet-aanvullende-bepalingen-verwerking-persoonsgegevens-in-de-zorg-art.-15a-lid-2.pdf	28 maart 2019	Openbare bron
PBLQ rapport gespecificeerde toestemming.pdf	28 maart 2019	Openbare bron
Email RE: Resterende vragen OTV nav gesprek gisteren	16 april 2019	Ontvangen van Albert Vlug
Thema's in aanvulling PSA	06 juni 2019	Ontvangen van Albert Vlug

4.3 Bijlage III: Overzicht afgenomen interviews

Overzicht afgenomen interviews		
Personen	**Functie**	**Tijd/plaats**
Albert Vlug	Lead architect OTV	27 april 2019, Deloitte kantoor Amsterdam
Albert Vlug André Klappe Pieter van Gemeren	Lead architect OTV Opdrachtmanagement vanuit CGI Enterprise architect VZVZ	4 april 2019, Nictiz kantoor Den Haag

4.5 Bijlage IV: Afkortingen

AVG	Algemene Verordening Gegevensbescherming
AP	Autoriteit Persoonsgegevens
Beheerder US	Beheerder van een elektronisch Uitwisselingssysteem
Beheerder-V	Beheerder van de Voorziening
BRP	Basisregistratie Personen
BSN	Burgerservicenummer
BW	Burgerlijk Wetboek
Cliënt	Cliënt in de zin van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg
DigiD	Digitale Identiteit
DPIA	Data Protection Impact Assessment
IGJ	Inspectie Gezondheidszorg en Jeugd
GTS	Gespecificeerde Toestemming Structureel
LSP	Landelijk Schakelpunt
MVP	Minimum Viable Product
PSA	Project Start Architectuur
UAVG	Uitvoeringswet Algemene Verordening Gegevensbescherming
US	Elektronisch uitwisselingssysteem
UZI	Unieke Zorgverlener Identificatie
Wabvpz	Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg
Wkkgz	Wet kwaliteit, klachten en geschillen zorg
WGBO	Wet op de Geneeskundige Behandelingsovereenkomst
Voorziening	Online toestemmingsvoorziening
VZVZ	Vereniging van Zorgaanbieders voor Zorgcommunicatie
NEN	Nederlandse Norm
ISO	Internationale Organisatie voor Standardisatie
NIST	National Institute of Standards and Technology
OWASP	Open Web Application Security Project