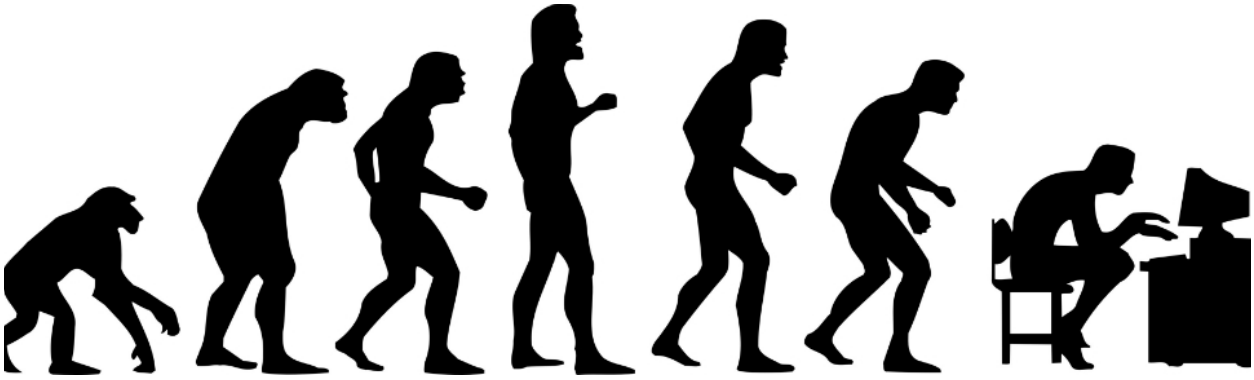
“Accountability in het tijdperk van de Homo Digitalis”

Een onderzoeksrapport over de verantwoordingsplicht van VECOZO onder de Algemene Verordening Gegevensbescherming



VECOZO

Y. (Yorick) van Houts

“Accountability in het tijdperk van de Homo Digitalis”

Een onderzoeksrapport over de verantwoordingsplicht van VECOZO onder de Algemene Verordening Gegevensbescherming

Auteur:	Yorick van Houts
Studentnummer:	2017955
Opleiding:	HBO Rechten, Jurdische Hogeschool Avans- Fontys te Tilburg
Afstudeeradres:	VECOZO Dr. Anton Philipsweg 35 5026 RK Tilburg
Afstudeerperiode:	6 februari 2017 – 25 mei 2017
Afstudeermentor:	de heer M.R.H. (Marc) Hagemeijer
Eerste afstudeerdocent:	mevrouw mr. M. (Maud) van Remortel
Tweede afstudeerdocent:	mevrouw mr. C.A.M. (Caro) van der Voort
Classificatie:	Intern

VOORWOORD

Voor u ligt het onderzoeksrapport “Accountability in het tijdperk van de Homo Digitalis” welke geldt als sluitstuk van mijn studie HBO-Rechten aan de Juridische Hogeschool Avans-Fontys. Dit onderzoek is uitgevoerd tussen januari en juni 2017 en geschreven in opdracht van VECOZO.

Wie mij toen ik aan deze studie begon had verteld, dat ik zou afstuderen met een onderzoek binnen het privacyrecht, had ik ter plekke en met veel plezier voor gek verklaard. Privacyrecht had een lange periode mijn interesse niet en leek me een droog en overschat rechtsgebied. Dit onderzoek heeft echter mijn eigen ongelijk bewezen en zoiets geef ik gebruikelijk nooit toe.

We leven in een samenleving die gedreven wordt door gegevens en informatie. Die van de Homo Digitalis. Persoonsgegevens zijn het nieuwe goud en desondanks strooien we er meer mee, dan met zout in de winters van voor de klimaatverandering. We hebben geen besef hoe veel van onze persoonsgegevens er dagelijks verwerkt worden en hoeveel inbreuken op onze fundamentele mensenrecht daarmee worden gemaakt.

De Europese Unie heeft door de invoering van de AVG een sterk signaal afgegeven. Het heeft geen vertrouwen meer dat organisaties privacyrechten uit zichzelf waarborgen. In de korte periode dat ik bij VECOZO stage heb mogen lopen, ben ik van mening geraakt dat zij één van de weinigen zijn die privacy nog wel serieus nemen. Vandaar dat ik trots ben op het feit dat ik daar aan bij mag dragen middels mijn onderzoeksrapport.

Ten eerste wil ik daarom VECOZO bedanken voor deze kans en in het bijzonder Marc Hagemeijer. Je was een geweldige partij om mee te filosoferen, of het nu gaat over de mogelijkheden van het verwerkingsregister of drones boven Gelderland. Ik wens je alvast veel plezier met je nieuwe uitdaging bij de Isatis groep en ik hoop oprecht dat we elkaar nog een keer tegen mogen komen!

Daarnaast wil ik graag mijn begeleidend docent Maud van Remortel bedanken. Maud, je bent de beste afstudeerdocent die een lone wolf als ik kan wensen. Je gaf me de ruimte om alles in te delen zoals ik zelf wilde en was er voor me wanneer ik dat nodig had. Ook wil ik de overige docenten en medewerkers van de Juridische Hogeschool bedanken. In het bijzonder Pascal Jacobs, Tim Quispel, Ron Ritzen, Lonneke Broers en Sheila Adjiembaks. Of jullie er van bewust zijn of niet, jullie hebben op de juiste momenten mij op een positieve manier beïnvloed en gemotiveerd.

Tot slot wil ik enkele dierbaren bedanken die mij zo lang ondersteund hebben tijdens mijn gehele studie. Carlijn Timmermans, je hebt me bijna dagelijks en tevergeefs naar college moeten schoppen, ik ben blij dat het erop zit voor je. Julia Manders en Anthony van Houts, jullie hebben me altijd gesteund in de keuzes die ik maakte. Ook toen ik besloot om, voor wat bijna een eeuwigheid leek mijn studie te onderbreken, benadrukten jullie alleen maar de positieve kanten. Bedankt. Floran van Houts bedankt dat je last minute gewoon weer voor me klaarstaat. En tenslotte Janice Richardson, bedankt voor de kansen die je me bied, ze waren op de juiste momenten een bron van motivatie om door te gaan als jurist.

SAMENVATTING

VECOZO is dienstverlener in de uitwisseling van administratieve gegevens binnen de zorgsector. In 2015 wisselden de verschillende ketenpartijen in de zorg meer dan twee miljard berichten uit via VECOZO.

Om de uitwisseling van gegevens plaats te laten vinden, worden op grote schaal persoonsgegevens verwerkt. Niet alleen van cliënten in de zorg, maar bijvoorbeeld ook van medewerkers van de ketenpartijen. In het kader van deze gegevensverwerking heeft VECOZO te maken met wet- en regelgeving op het gebied van privacy. In Nederland was dit lange tijd geregeld in de Wet bescherming persoonsgegevens maar hier komt verandering in. Op 25 mei 2016 is de Europese Algemene Verordening Gegevensverwerking (AVG) in werking getreden. Organisaties kregen van de Europese wetgever twee jaar de tijd om hun werkwijze aan te passen aan de nieuwe verordening. Over bijna precies een jaar is het zover en zal de Nederlandse Autoriteit Persoonsgegevens, met zware sancties en boetes (oplopend tot wel **€** 10 miljoen) in de hand, de naleving van de verordening gaan handhaven.

Een van de belangrijkste veranderingen voor organisaties is de introductie van de verantwoordingsplicht. Organisaties moeten bij de Autoriteit Persoonsgegevens kunnen aantonen dat zij de verordening naleven. De AVG heeft een aantal verplichte activiteiten opgenomen die bijdragen aan de verantwoordingsplicht. Zo zal VECOZO in bepaalde situaties een Privacy Impact Assessment moeten uitvoeren, dit is een instrument om de privacyrisico's van je verwerkingen in kaart te brengen. Daarnaast zullen er passende beveiligingsmaatregelen getroffen moeten worden en zal VECOZO een register moeten bijhouden, waarin alle verwerkingsactiviteiten die worden verricht zijn opgenomen.

Dit onderzoeksrapport geeft aan hoe dit register kan worden aangelegd en aan welke vereisten het moet voldoen en hoe dit samenhangt me de overige verantwoordingsinstrumenten.

Om dit register op te kunnen stellen is alvast voor een aantal VECOZO-diensten in kaart gebracht welke verwerkingsactiviteiten er plaatsvinden. Voor deze verwerkingsactiviteiten is uitgezocht wat VECOZO moet doen om ze conform de AVG vast te leggen in het register.

Een van de aanbevelingen van dit onderzoeksrapport is het creëren van bewustzijn en draagvlak omtrent de verantwoordingsplicht door middel van het informeren en opleiden van de hiervoor relevante werknemers. Daarnaast wordt aanbevolen om bij het aanleggen van het register niet 'slechts' te voldoen aan de juridische eisen, maar zelfs meer in het register op te nemen. Niet alleen voldoe je dan beter aan je verantwoordingsplicht dan minimaal vereist is maar kan het register een aanwinst voor je organisatie zijn.

Om VECOZO niet enkel te voorzien van een advies over de juridische eisen van het register en aanbevelingen te doen over een uitgebreider register, is een template ontwikkeld in Excel. In dit template register zijn de drie in dit onderzoek geanalyseerde VECOZO-diensten alvast opgenomen.

LIJST VAN AFKORTINGEN

AP	–	Autoriteit Persoonsgegevens
Art.	–	Artikel
AVG	–	Algemene verordening gegevensbescherming óf Aanlevering Verzekerdengegevens
BSN	–	Burgerservicenummer
BW	–	Burgerlijk Wetboek
COV	–	Controle op verzekering
cv	–	curriculum vitae
EG	–	Europese Gemeenschap
eIDAS	–	Electronic Identification and Signature
EU	–	Europese Unie
FG	–	Functionaris Gegevensbescherming
Handvest EU	–	Handvest van de grondrechten van de Europese Unie
ISO	–	International Standardization Organization
jo.	–	Juncto
NAW	–	Naam Adres Woonplaats
NEN	–	Nederlandse Norm
PIA	–	Privacy Impact Assessment
SSO	–	Single Sign On
TCA	–	Trusted Certification Authority
UAVG	–	Uitvoeringswet Algemene Verordening Gegevensbescherming
VECOZO	–	Veilige internet Communicatie in de Zorg
VWEU	–	Verdrag omtrent de werking van de Europese Unie
Wbp	–	Wet bescherming persoonsgegevens
Wet BSN-z	–	Wet gebruik Burgerservicenummer in de zorg
WGBO	–	Wet op de geneeskundige behandelovereenkomst
WP 29	–	Working Party 29

BEGRIPPENLIJST

Certificaat: een elektronische bevestiging die gegevens voor het verifiëren van een elektronische handtekening met een bepaalde persoon verbindt en de identiteit van die persoon bevestigt.

Diensten: Software-applicaties inclusief bijbehorende documentatie in de productieomgeving van VECOZO, ontsloten via webportaal of via webservices, waarvan VECOZO de (intellectuele) eigendomsrechten bezit.

Encryptie en decryptie: het coderen (versleutelen) van gegevens volgens een bepaald algoritme en het ontcijferen van versleutelde gegevens om de originele informatie weer terug te krijgen.

Gebruikers: de eindgebruikers van de diensten van VECOZO. Dit kan zowel een persoon als een systeem zijn.

Ontvanger: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, aan wie/waaraan de persoonsgegevens worden verstrekt

Pseudonimisering: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld.

Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon

Verantwoordingsinstrumenten: Het geheel aan activiteiten dat een organisatie verplicht moet uitvoeren om te voldoen aan de verantwoordingsplicht van de AVG.

Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/ dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.

Verwerking: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

Verwerkingsverantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen.

INHOUDSOPGAVE

HOOFDSTUK 1 - INLEIDING

In 2002 is VECOZO door enkele zorgverzekeraars opgericht. Sindsdien is het uitgegroeid tot hét landelijk communicatiepunt in de zorg bij wie alle zorgverzekeraars en vrijwel alle zorgverleners zijn aangesloten.[1] In de zorgsector staat VECOZO bekend als een betrouwbare partner die – in haar verschillende diensten - de (digitale) gegevensuitwisseling tussen de ketenpartners faciliteert. Denk bijvoorbeeld aan huisartsen die declaraties naar de juiste zorgverzekeraar van hun patiënten willen sturen of zorgverleners die willen weten of iemand verzekerd is. Jaarlijks vinden er inmiddels meer dan 2 miljard uitwisselingen plaats, waaronder declaraties, controles op verzekering (COV's) en zorginkoop.[2]

Op het uitwisselen van zoveel gegevens is onvermijdelijk wet- en regelgeving van toepassing. Met name om de privacy van de betrokkenen van die gegevens te waarborgen. Jarenlang was in Nederland hier de Wet bescherming persoonsgegevens op van toepassing. Dat gaat veranderen per 25 mei 2018, wanneer die wet komt te vervallen en vervangen wordt door Europese regelgeving.

1.1 Probleembeschrijving

Op 27 april 2016 is de Algemene Verordening Gegevensbescherming (AVG) officieel in werking getreden, ter vervanging van de Richtlijn 95/46/EG (Privacyrichtlijn). Na inwerkingtreding heeft iedereen die onderworpen is aan de AVG twee jaar de tijd gekregen om aan de verordening te gaan voldoen (tot mei 2018), alvorens er sancties opgelegd gaan worden. Dat geldt dus ook voor VECOZO. De AVG is een uniforme Europese verordening omtrent verwerking en bescherming van persoonsgegevens.

Binnen VECOZO zijn er veel verschillende diensten en processen waarin verwerking van persoonsgegevens plaatsvindt. Dat kan ook bijna niet anders, wanneer gegevensuitwisseling je kerntaak is. Binnen VECOZO is men al druk bezig met de implementatie van deze verordening en wil graag zien dat het verwerkingsregister dat artikel 30 van de AVG hen verplicht bij te houden, vormgegeven wordt. Bij het maken van dit register moet rekening gehouden worden met alle vereisten van de AVG die betrekking hebben op het afleggen van verantwoording naar toezichthouders en betrokkenen. Iedere verwerking van persoonsgegevens binnen VECOZO dient in het register te worden bijgehouden, om tegenover toezichthouders aan te kunnen tonen dat VECOZO persoonsgegevens verwerkt in overeenstemming met de AVG.

Het register is een onderdeel van de algehele verantwoordingsplicht die is opgenomen in de AVG.[3] De verwerkingsregisters zorgen voor een grote administratieve last, zowel in het proces voorafgaand aan compliancy, als in de periode erna. VECOZO moet alle verwerkingen en verwerkingswijzen gaan inventariseren en vastleggen naar de vereisten uit artikel 30 AVG. Om het niet enkel te zien als een administratieve last, wil VECOZO graag dat onderzocht wordt in welke mate dit register kan helpen bij het geven van invulling aan de andere verantwoordingsplichten uit de AVG. Kan bijvoorbeeld informatie die nodig is voor het uitvoeren van een verplichte Privacy Impact Assessment (PIA), voor een deel

[1] Over VECOZO, vecozo.nl
[2] Over onze diensten, vecozo.nl
[3] Comijs, *P&I* 2016, afl. 6, p. 252.

informatie halen uit hetgeen al is vastgelegd in het verwerkingsregister? Daarvoor is het dus ook nodig om te onderzoeken wat de AVG allemaal vereist omtrent de PIA.

1.1.1 Afbakening

Omdat de implementatie van alle aspecten van de AVG een zeer breed onderzoek betreft en VECOZO toch een diepgaand onderzoek, met bijbehorend gedetailleerd product opgeleverd wil zien, is gevraagd te focussen op de hierboven genoemde verwerkingsregisters van artikel 30 AVG. Daarnaast is gevraagd om te onderzoeken hoe dit in samenhang met de andere verantwoordingsplichten (of: verantwoordingsinstrumenten) kan worden ingezet.

De verantwoording die VECOZO vanaf mei 2018 zal moeten afleggen aan de toezichthouder bestaat namelijk niet enkel uit het bijhouden van een verwerkingsregister op grond van artikel 30 AVG. De andere instrumenten die ingezet moeten worden om een correcte verwerking van persoonsgegevens te verantwoorden zijn de eerder genoemde Privacy Impact Assessment en een overzicht van getroffen beveiligings- en organisatorische maatregelen.[4]

De focus van dit onderzoek is om in kaart te brengen aan welke juridische vereisten van artikel 30 AVG het register minimaal moet voldoen. VECOZO is echter ook geïnteresseerd óf en op welke wijze, dit register de basis kan vormen voor een geïntegreerde aanpak van de verantwoordingsplicht. In dat opzicht is het register niet alleen bedoeld voor de uitvoering van de in de verordening verplicht gestelde inzage door de toezichthouder maar ook voor medewerkers van VECOZO om te kunnen raadplegen. Dit kan bijvoorbeeld bij het doen van een PIA of bij de serviceverlening aan een betrokkene die zich beroept op zijn rechten.

De maatregelen die naar aanleiding van dit onderzoek worden aanbevolen, hebben als doel om VECOZO een verwerkingsregister te bieden dat in overeenstemming is met de AVG. Organisaties hebben straks twee jaar de tijd gehad om dit register aan te leggen en vanaf mei 2018 zal de Autoriteit Persoonsgegevens (AP) hier ook op gaan handhaven. Daarnaast moet ook verder gekeken worden dan mei 2018. VECOZO wil graag duurzaamheid in haar verwerkingsregister incorporeren. De brede omschrijving van de registerplicht in de AVG biedt kansen om hier op innovatieve, kernachtige en duurzame wijze invulling aan te geven.

1.2 Doelstelling, centrale vraag en deelvragen

Naar aanleiding van de hieronder uitgewerkte centrale vraag, waarvan het antwoord een oplossing voor de probleembeschrijving moet gaan geven, is de volgende doelstelling geformuleerd: *'Op uiterlijk 29 mei 2017 wordt een adviesrapport overhandigd aan de CRO van VECOZO, Marc Hagemeijer, waarin aanbevelingen en overwegingen staan waarmee VECOZO door middel van verwerkingsregisters invulling kan geven aan de verantwoordingsplicht zoals vereist op grond van de AVG. Naast dit adviesrapport zal als product een template verwerkingsregister aan VECOZO worden opgeleverd. Dit template omvat een tweetal diensten en dient als basis voor de verdere invulling van de registerplicht voor andere diensten en kan direct in gebruik worden genomen.'*

[4] Comijs, *P&I* 2016, afl. 6, p. 253.

De centrale vraag van dit onderzoek luidt dan ook: ***''Op welke manier moet VECOZO haar verantwoordingsplicht, met betrekking tot de verwerkingsregisters van artikel 30 inrichten, mede met het oog op de andere verantwoordingsinstrumenten in de Algemene Verordening Gegevensbescherming, om per mei 2018, maar ook daarna, te voldoen aan de eisen van de verordening?''***

De deelvragen die de centrale vragen ondersteunen zijn als volgt:

1. Wat zijn de vereisten die uit artikel 30 AVG voortvloeien omtrent de registers van verwerkingen van persoonsgegevens en hoe moeten deze worden geïnterpreteerd?
2. Welke verwerkingen vinden er plaats binnen de processen van VECOZO en op welke wijze worden deze gedaan?
3. Op welke wijze moet het verwerkingsproces worden vastgelegd in het register om te voldoen aan de eisen uit de AVG?
4. Op welke wijze moet het verwerkingsregister, als basis voor de andere verantwoordingsinstrumenten van artikel 32 en 35 AVG, invulling geven aan de totale verantwoordingsplicht van VECOZO?

1.3 Strategie en verantwoording

Om de verschillende aspecten, methoden en fases van dit onderzoek correct te classificeren is gebruik gemaakt van het boek praktijkgericht juridisch onderzoek van Geertje van Schaijk.[5]

Bij dit onderzoek is gekozen voor een uitgebreid kwalitatief theorieonderzoek naar onder anderen de AVG, de totstandkoming ervan, de Uitvoeringswet AVG(concept), Wet BSN-z en de beschikbare literatuur en publicaties over dit onderwerp. Deze hebben gezamenlijk geleid tot een duidelijke conclusie over de vereisten van de verwerkingsregisters van artikel 30 AVG. Dit is met name gebruikt om de **eerste deelvraag** te kunnen beantwoorden. Ook de (te vervangen) Wet bescherming persoonsgegevens (Wbp) heeft een rol gespeeld in het onderzoek. Dit komt doordat de eis tot registers bijhouden, die is vastgelegd in artikel 30 van de AVG, in zeer algemene termen is omschreven. De exacte vorm en invulling van de registers is niet vastgesteld. Om toch in beeld te krijgen waarop de Autoriteit Persoonsgegevens zou kunnen gaan toetsen, heeft ook deze wet en de literatuur daarover kunnen bijdragen aan de conclusie van dit onderzoek.
Hoewel artikel 30 van de AVG leidend is in de vraag wanneer een register wettelijk voldoet aan de AVG en de andere verantwoordingsinstrumenten hun grondslag in andere artikelen kennen, kunnen deze registers ook bijdragen aan de uitvoering en invulling van de andere instrumenten. De registers kunnen zo worden uitgewerkt, dat zij de basis, achtergrond en/of grondslag vormen voor andere AVG gerelateerde proceswijzigingen binnen VECOZO.
Daarom is er gekozen om ook de artikelen in de AVG, die gaan over de gegevensbeschermingseffectbeoordeling, beter bekend onder de naam Privacy Impact Assessment (PIA) en de beveiligingsmaatregelen, beknopt te belichten.
De beantwoording van de **tweede deelvraag** ligt verankerd in de huidige processen en werkwijzen binnen VECOZO. Om erachter te komen hoe en welke gegevens momenteel worden verwerkt binnen VECOZO en in hoeverre hiervan enige vorm van notities van worden bijgehouden is er een *kwalitatieve, enkelvoudige casestudy* gedaan. Door middel van *interviews* zijn een aantal van de huidige processen in kaart gebracht, dit is gedaan voor de

[5] Van Schaijk 2015

diensten genaamd *Certificatenbeheer*, *Berichtenbox* en *Aanlevering Verzekerden Gegevens*, ironisch genoeg binnen VECOZO afgekort als *AVG*.
Daarnaast is er volop gebruik gemaakt van de gedeelde dataschijf van VECOZO, de zogenoemde *Q-schijf*, om helder in kaart te brengen hoe de diensten zijn ingericht en door wie zij worden uitgevoerd. Deze *documentanalyse* was ook nodig om in kaart te brengen welke medewerkers van VECOZO benaderd moesten worden voor de vraaggesprekken.
Deze twee onderzoeksmethoden hebben ook bijgedragen grondwerk voor het beantwoorden van de **derde deelvraag**. Tot slot is er in het algemeen gebruik gemaakt van onderzoek naar hoe andere bedrijven, ICT-specialisten en juridische- en privacy experts omgaan met het vraagstuk van de verwerkingsregisters.
Door de vereisten uit de AVG naast de resultaten van het praktijkonderzoek te leggen is een analyse uitgevoerd om te bepalen hoe de registers er uit moeten komen zien.

HOOFDSTUK 2 – UITEENZETTING JURIDISCH KADER

Dit hoofdstuk zet het juridisch kader van de AVG, De Uitvoeringswet AVG en andere belangrijke en relevante wet- en regelgeving (zoals de Wet op de Geneeskundige Behandelovereenkomst) uiteen. De focus bij de uiteenzetting van de AVG zal liggen op de verantwoordingsplicht en daarbij aanverwante verantwoordingsinstrumenten. In het bijzonder die van artikel 30 AVG: het register van de verwerkingsactiviteiten.

2.1 De AVG algemeen

Een korte beschrijving van de ontstaansgeschiedenis en algemene onderdelen van de AVG is van belang om zaken het juiste perspectief te plaatsen en dient als achtergrond voor dit onderzoeksrapport.

2.1.1 Oorsprong

De AVG vervangt de Richtlijn bescherming persoonsgegevens, die sinds 1995 privacy op Europees niveau reguleert. Tussen 1995 en nu is de maatschappij echter sterk gedigitaliseerd en is privacy een steeds belangrijker thema geworden.[6] Er is een enorme toename aan dataverkeer en dus ook in het verzamelen en delen van persoonsgegevens. Daarnaast is de vraag vanuit de burger om te weten wat er met zijn of haar gegevens gebeurt sterk toegenomen.[7]
Daarom is in 2012 de AVG voorgesteld door de Europese Commissie en is hier na veel amendementen, in december 2015 overeenstemming over bereikt. Uiteindelijk is de AVG op 25 mei 2016 officieel in werking getreden. Omdat deze verordening op grond van artikel 288 van het verdrag omtrent de werking van de Europese Unie (hierna: VWEU) rechtstreekse werking heeft, moeten alle organisaties en openbare lichamen in de EU compliant worden aan de AVG. Omdat zo'n verandering niet over één nacht ijs gaat, is gekozen voor een implementatieperiode van twee jaar. In mei 2018 dient iedere organisatie te voldoen aan de inhoud van de AVG.

2.1.2 Doel van de AVG

Het doel van de AVG luidt als volgt: "*De bescherming van natuurlijke personen bij de verwerking van persoonsgegevens*."[8] Dat is het uitgangspunt dat werd genomen bij het opstellen van de AVG. Dit is namelijk een grondrecht van burgers van de Europese Unie o.g.v. artikel 8 lid 1 van het Handvest van de grondrechten van de Europese Unie (hierna: Handvest EU) en artikel 16 lid 1 VWEU.
Als gevolg van de interne Europese markt is een niveau van economische en sociale integratie bereikt dat heeft geleid tot een sterke toename van (grensoverschrijdende) uitwisseling en verwerkingen van persoonsgegevens tussen publieke en private instellingen. Door de technologische ontwikkeling en globalisering van het afgelopen decennium is de bescherming van persoonsgegevens significant uitdagender geworden.[9]
Om deze enorme toename aan verwerkingen op een uniforme en consequente wijze te reguleren, is de AVG ontworpen. De regelgeving in de AVG biedt lidstaten ook de ruimte om eigen regels voor de toepassing op te stellen. Bijvoorbeeld over wat de verwerking van

[6] *Gegevensbescherming en de AVG*, Europa decentraal, 2016.
[7] Van der Meulen & van Zoonen 2015
[8] Raad 2012.
[9] Raad 2012.

bijzondere persoonsgegevens betreft, wat verder kort wordt besproken in paragraaf 2.6 over de Uitvoeringswet AVG (hierna: UAVG).

2.1.3 De beginselen van de AVG

Veel van de beginselen uit de AVG sluiten geheel of gedeeltelijk aan bij de (te vervallen)[10] Wet bescherming persoonsgegevens (Wbp) en de algemene beginselen van het gegevensbeschermingsrecht. Er moet sprake zijn van een gerechtvaardigd doeleinde,[11] de verwerking moet beperkt zijn tot wat noodzakelijk is voor die doeleinden,[12] de gegevens moeten juist zijn,[13] er moet sprake zijn van een opslagbeperking[14] en er moeten passende technische of organisatorische maatregelen worden getroffen.[15]

2.1.4 Toepassingsgebied van de AVG

Het materieel toepassingsgebied van de AVG is geregeld in art. 2 AVG. Omdat VECOZO voor haar partners in de zorg door middel van haar diverse (geautomatiseerde) diensten een centraal punt is de onderlinge uitwisseling van persoonsgegevens,[16] is de AVG op grond van artikel 2 lid 1 AVG van toepassing op VECOZO.

2.2 De verantwoordingsplicht

Onder de AVG komt de meldingsplicht van artikel 27 Wet bescherming persoonsgegevens (hierna: Wbp) te vervallen. Vanaf nu zullen organisaties moeten kunnen laten zien wat en hoe zij verwerken. De AVG spreekt in artikel 5 lid 2 dan ook van een *verantwoordingsplicht*. Hoewel de beginselen van artikel 5 lid 1 AVG grotendeels aansluiten bij de Wbp, is deze verantwoordingsplicht van artikel 5 lid 2 AVG wél nieuw. De formulering hiervan in artikel 5 lid 2 is van algemene strekking en benoemt enkel de verwerkingsverantwoordelijke. De verantwoordingsplicht geldt echter ook voor verwerkers en de AVG bepaalt verderop in de verordening hoe en aan wie, deze verantwoording moet worden afgelegd. Het gebruikt hiervoor een aantal *verantwoordingsinstrumenten*.[17] Hieronder volgt een uiteenzetting van de verantwoordingsplicht.

2.2.1 Verwerkingsverantwoordelijk of verwerker?

Het onderscheid tussen de verwerkingsverantwoordelijke en de verwerker is terug te vinden in artikel 4 van de AVG. Een verwerkingsverantwoordelijke is *een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.*[18]

De verwerker is op grond van artikel 4 lid 8 *een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.*
Het grote verschil zit hem dus in het bepalen van het doel van en de middelen voor de verwerkingen.

---

[10] Artikel 46 UAVG.
[11] Artikel 5 lid 1 sub b AVG.
[12] Artikel 5 lid 1 sub c AVG.
[13] Artikel 5 lid 1 sub d AVG.
[14] Artikel 5 lid 1 sub e AVG.
[15] Artikel 5 lid 1 sub f AVG.
[16] Over VECOZO, vecozo.nl
[17] Comijs, *P&I* 2016, afl. 6, p. 253.
[18] Artikel 4 lid 7 AVG.

De verhouding tussen beide partijen (wie er verantwoordelijk is voor een bepaalde verwerking) dient te worden vastgelegd. Dit gebeurt doorgaans middels een verwerkersovereenkomst.[19]

In de overeenkomst moet tenminste worden vastgelegd:[20]
- Het onderwerp en de duur van de verwerking
- De aard en het doel van de verwerking
- De soorten persoonsgegevens en categorieën van betrokkenen
- De rechten en plichten van de verwerkingsverantwoordelijke

In de AVG is per artikel vaak duidelijk uitgelegd of de desbetreffende verantwoordingsplicht geldt voor de verwerkingsverantwoordelijke, de verwerker of beiden. Wie er verantwoordelijk is voor een bepaalde verwerking is ook van belang voor de aansprakelijkheid. De verwerkingsverantwoordelijke is aansprakelijk jegens de betrokkene. De verwerker is dat slechts, indien de verwerking niet conform de specifiek tot verwerkers gerichte verplichtingen van de AVG is uitgevoerd.[21]. In geval van meerdere verwerkingsverantwoordelijken is op basis van artikel 85 lid 4 en 5 AVG iedere verantwoordelijke in zijn geheel aansprakelijk jegens de betrokkene.

2.2.2 De verantwoordingsinstrumenten

De AVG schrijft een aantal zaken (de instrumenten) voor die verwerkingsverantwoordelijken en verwerkers vanaf mei 2018 in stelling moeten hebben gebracht om inzicht te bieden of zij voldoen aan (onder andere) artikel 5 AVG.[22] Deze verantwoordingsinstrumenten zijn de volgende:

1. Een overzicht van getroffen organisatorische- en technische beveiligingsmaatregelen;[23]
2. een privacy impact assessment, ook wel PIA genoemd;[24]
3. een register van verwerkingsactiviteiten op grond van artikel 30.[25]

Om goed invulling te geven aan de verantwoordingsplicht van artikel 5 lid 2 AVG is het van belang om deze verplichte instrumenten samenhangend in te zetten.[26] Het verwerkingsregister van artikel 30 AVG kan hierin een centrale rol vervullen en deze zal dan ook later in dit hoofdstuk uitgebreid aan bod komen. Ook de andere twee worden kort onder de loep genomen.

2.2.3 De toezichthoudende autoriteit en Functionaris Gegevensbescherming

De verantwoordingsplicht die hierboven wordt uitgelegd geeft in artikel 5 lid 2 AVG niet in het bijzonder aan bij wie de verantwoordelijke en/of de verwerker deze verantwoording dient af te leggen. Uit de artikelen van de afzonderlijke verantwoordingsinstrumenten valt onder meer af te leiden dat dit moet gebeuren bij de toezichthoudende autoriteit. Op grond van artikel 51 AVG is elke lidstaat vereist om zelf een overheidsinstantie aan te wijzen die toezicht houdt op de naleving van de AVG. Dit begrip 'overheidsinstantie' uit de AVG is

[19] Artikel 28 lid 3 AVG.
[20] Artikel 28 lid 3 AVG.
[21] Artikel 82 lid 1 jo. artikel 82 lid 3 AVG.
[22] Comijs, *P&I* 2016, afl. 6, p. 253.
[23] Artikel 32 AVG.
[24] Artikel 35 AVG.
[25] Comijs, *P&I* 2016, afl. 6, p. 253.
[26] Comijs, *P&I* 2016, afl. 6, p. 253.

ruimer dan wat in het Nederlandse bestuursrecht wordt verstaan onder een bestuursorgaan.[27] Nederland heeft hier de Autoriteit Persoonsgegevens (AP) voor aangewezen in artikel 6 lid 2 UAVG.

Daarnaast moet de verwerker in sommige gevallen ook een Functionaris Gegevensbescherming (FG) aanstellen.[28] Tot de inwerkingtreding van de AVG is het aanstellen van een FG optioneel, de AVG stelt hem echter verplicht[29] voor organisaties waarbij het verwerken van bijzondere persoonsgegevens tot de kernactiviteiten van de organisatie behoort, zoals VECOZO.[30] Deze is onder meer verantwoordelijk voor het toezien op de naleving van de verordening op grond van artikel 39 lid 1 sub b AVG. Dus intern legt de verwerker als het ware verantwoording af aan de FG. De FG is binnen de organisatie onafhankelijk en wordt betrokken bij alle zaken die te maken hebben met de bescherming van persoonsgegevens.[31] De FG is vervolgens weer degene die medewerking verleent aan en contact onderhoudt met de toezichthoudende autoriteit (in Nederland en dus ook verder in dit rapport: de Autoriteit Persoonsgegevens).

2.2.3.1 De taken, bevoegdheden en sancties van de toezichthouder

Het takenpakket van de Autoriteit Persoonsgegevens (AP) bestaat in simpele bewoordingen uit het toezicht op de naleving van de AVG. De algemene taken van de AP zijn vastgelegd in artikel 57 AVG en zijn onder anderen het monitoren en handhaven van de toepassing van de AVG maar denk bijvoorbeeld ook aan het informeren en meer bekendheid creëren bij het publiek over de regels, waarborgen en rechten in verband met verwerkingen. Naast de algemene taken van art. 57 AVG kunnen aanvullende taken voortvloeien uit andere bepalingen in de AVG of de nationale wet, de Uitvoeringswet AVG.

De bevoegdheden van de AP zijn zéér uitgebreid en zijn opgesomd in art. 58 AVG. Globaal gezien bestaan deze uit onderzoeksbevoegdheden, corrigerende bevoegdheden, adviesbevoegdheden en autorisatiebevoegdheden. In de UAVG zijn enkele van deze bevoegdheden verder uitgelegd naar Nederlands recht. Artikel 14 UAVG bepaald bijvoorbeeld dat vrijwel alle bevoegdheden van artikel 58 een besluit zijn in de zin van de Algemene wet bestuursrecht (Awb).
Artikel 83 AVG bepaalt de boetebevoegdheid van de AP en de algemene voorwaarden die daar aan verbonden zijn. In artikel 83 lid 2 AVG staan bijvoorbeeld de zaken waarmee rekening gehouden moet worden bij het besluit tot het opleggen van een administratieve boete en de hoogte ervan. Met betrekking tot inbreuken op de AVG die niet onderworpen zijn aan een geldboete op grond van artikel 83 AVG kunnen lidstaten zelf sancties vaststellen, art. 84 AVG geeft hiertoe de mogelijkheid.

2.3 De registerplicht van artikel 30 AVG

Nu de achtergrond van de AVG en diens beginselen zijn besproken en een beeld is gevormd bij wat de nieuwe verantwoordingsplicht uit de AVG inhoudt, zullen de eerder genoemde verantwoordingsinstrumenten worden besproken. In deze paragraaf wordt begonnen met registerplicht.

---

[27] Jak 2014, p. 291.
[28] Artikel 37 AVG.
[29] Artikel 37 AVG.
[30] Comijs, *P&I* 2016, afl. 6, p. 252.
[31] *Functionaris voor gegevensbescherming*, Europa decentraal, 2016.

In artikel 30 AVG is de plicht opgenomen om een register bij te houden van alle verwerkingsactiviteiten die plaatsvinden. Dit geldt voor zowel de verwerkingsverantwoordelijke[32] als voor de verwerker[33] van de persoonsgegevens. Niet voldoen aan deze plicht kan een boete opleveren van de AP, die kan oplopen tot 10 miljoen euro of 2% van de jaaromzet, op grond van art. 83 lid 4 sub a AVG. De toezichthouder heeft op grond van artikel 30 lid 4 AVG het recht om medewerking van de verwerkingsverantwoordelijke of verwerker te vorderen met betrekking tot het ter beschikking stellen van hun register. Het belang van deze registerplicht lijkt dus evident. Het verwerkingsregister moet in schriftelijke vorm worden opgesteld, waarvan tenminste ook in elektronische vorm.[34] Het is mogelijk om uitgezonderd te worden van de registerplicht. Dat is met name bedoeld voor MKB bedrijven die incidenteel persoonsgegevens verwerken. De uitzondering van artikel 30 lid 5 AVG is er namelijk voor ondernemingen of organisaties die minder dan 250 personen in dienst hebben, wiens verwerkingen geen risico vormen voor de rechten van de betrokkenen en de verwerkingen slechts een incidenteel karakter hebben.

Wanneer het een verwerking van persoonsgegevens, als bedoeld in artikel 9 AVG (bijzondere persoonsgegevens) en artikel 10 AVG (justitiële gegevens) betreft, is de uitzondering niet van toepassing.[35]

2.3.1 Het register van de verwerkingsverantwoordelijke
Op grond van artikel 30 lid 1 AVG is iedere verwerkingsverantwoordelijke verplicht een register bij te houden van de verwerkingsactiviteiten die onder hun verantwoordelijkheid plaatsvinden. Hieronder zal worden uiteengezet welke gegevens zo'n register moet bevatten.

Artikel 30 lid 1 sub a AVG vereist het opnemen van de contactgegevens van de verwerkingsverantwoordelijke (of diens vertegenwoordiger) en de Functionaris Gegevensbescherming.

Artikel 30 lid 1 sub b AVG van vereist het opnemen van de verwerkingsdoeleinden in het register. Het is belangrijk om hierbij in het oog te houden dat, hoewel een en ander vrij kort en bondig wordt benoemd in dit lid, deze doeleinden zeer goed doordacht moeten zijn en uitdrukkelijk omschreven. Artikel 5 lid 1 sub b van de AVG stelt dat persoonsgegevens enkel voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden mogen worden verzameld en enkel op een met die doeleinden verenigbare wijze mogen worden verwerkt. Hoe gedetailleerd een doeleinde moet worden omschreven hangt af van de context van de manier waarop wordt verwerkt en welke gegevens er worden verwerkt. Wel is duidelijk dat vage of generale omschrijvingen als *"verbeteren van gebruiksvriendelijkheid"* en *"vanwege veiligheidsredenen"* niet volstaan om aan de eisen van de verordening te voldoen.[36]

[32] Artikel 30 lid 1 AVG.
[33] Artikel 30 lid 2 AVG.
[34] Artikel 30 lid 3 AVG.
[35] Artikel 30 lid 5 AVG.
[36] WP29 2013.

Artikel 30 lid 1 sub c AVG vereist een beschrijving van de categorieën van betrokkenen en de categorieën van persoonsgegevens die worden verwerkt. De AVG geeft op zichzelf niet aan wat categorieën van betrokkenen exact inhoudt, maar de Autoriteit Persoonsgegevens gaat uit van categorieën zoals werknemers, uitzendkrachten, leveranciers, sollicitanten, etc.[37]

Categorieën van persoonsgegevens is een wat onduidelijke term die om verschillende redenen anders geïnterpreteerd zou kunnen worden. Enige verheldering hiervan is dus op zijn plaats. Wat zijn persoonsgegevens volgens de AVG nou precies? Artikel 4 lid 1 AVG geeft een vrij breed geformuleerde omschrijving, namelijk:

"alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon"

In artikel 9 lid 1 AVG is aanvullend hierop een omschrijving van de categorie bijzondere persoonsgegevens te vinden. Bijzondere gegevens zijn onder anderen persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze overtuigen blijken. De verwerking van dit soort gegevens is in beginsel verboden met uitzondering van de op in artikel 9 lid 2 AVG genoemde voorwaarden.

Maar is het om te voldoen aan de registerplicht van artikel 30 AVG dan voldoende, om te volstaan met het onderscheid tussen algemene persoonsgegevens[38] en bijzondere persoonsgegevens[39] als categorieën? Nee dit is een te algemene conclusie die niet aansluit bij hetgeen vereist in artikel 30 lid 1 sub c.[40] Hoe gedetailleerd dit onderscheid dan wel moet zijn kan dus niet worden afgeleid uit artikel 30 lid 1 sub c.

Op grond van **artikel 30 lid 1 sub d AVG** moeten ook de categorieën van ontvangers worden bijgehouden in het register. Dat kan een natuurlijke persoon, rechtspersoon, overheidsinstantie, dienst of ander orgaan zijn aan wie of waaraan de persoonsgegevens worden verstrekt.[41]

Artikel 30 lid 1 sub e AVG gaat, indien van toepassing, over doorgifte van persoonsgegevens aan een derde land of internationale organisatie. Het doorgeven mag enkel plaatsvinden als zowel de verwerkingsverantwoordelijke als de verwerker voldoen aan de voorwaarden uit Hoofdstuk V van de AVG. Deze voorwaarden zijn er om het voor natuurlijke personen gewaarborgde beschermingsniveau in stand te houden.[42]

Artikel 30 lid 1 sub f AVG vereist dat in het register de beoogde termijnen worden geregistreerd waarbinnen de verschillende categorieën van gegevens moeten worden

[37] www.autoriteitpersoonsgegevens.nl (zoek op: meldingsprogramma).
[38] Artikel 4 lid 1 AVG.
[39] Artikel 9 lid 1 AVG.
[40] WP 29 2007.
[41] Artikel 4 lid 9 AVG.
[42] Artikel 44 AVG.

gewist, oftewel de bewaartermijn. De AVG geeft geen concrete bewaartermijn maar noemt in artikel 5 lid 1 sub e wel opslagbeperking. Het persoonsgegeven mag, zolang het identificeerbaar is, alleen worden bewaard voor zolang het noodzakelijk is voor de doeleinden waarvoor is verwerkt. Het is dus van belang om van elke verwerkt persoonsgegeven de beoogde bewaartermijn vast te leggen en ook rekening te houden met vanuit welke doelbinding dit gebeurt.[43]

Artikel 30 lid 1 sub g AVG gaat over de algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen als bedoeld in artikel 32 lid 1 van de AVG. In dit artikel is een van de andere verantwoordingsinstrumenten benoemt als onderdeel van het verwerkingsregister. Je moet in je register bij de verwerkingen aangeven op welke wijze deze verwerkingen beveiligd zijn of welke privacy waarborgen in acht zijn genomen. Omdat het hier een van de andere verantwoordingsinstrumenten betreft, is verdere toelichting te vinden in paragraaf 2.5.2 van dit onderzoek.

De verwerkingsverantwoordelijke hoeft in zijn register geen inzicht te tonen in de afwegingen die hij heeft gemaakt bij de keuze tussen middelen en doelen.[44] Er hoeft daarom niet opgenomen te worden op welke juridische grondslag van artikel 6 AVG de verwerking plaatsvindt.

2.3.2 Het register van de verwerker

De verwerker van persoonsgegevens is op grond van artikel 30 lid 2 ook verplicht een register van verwerkingsactiviteiten bij te houden. Het register van de verwerker toont op enkele punten overeenkomsten maar heeft ook verschillen met die van de verwerkingsverantwoordelijke.

Op grond van **artikel 30 lid 2 sub a AVG** is de verwerker verplicht om de naam en de contactgegevens van de verwerkers en iedere verwerkingsverantwoordelijke voor rekening waarvan het gegevens verwerkt op te nemen. Daarnaast ook de naam en contactgegevens van de FG. De inhoud van dit vereiste is vrijwel identiek aan die van artikel 30 lid 1 sub a AVG. Voor een verwerker die ten behoeve van veel verschillende verwerkingsverantwoordelijken verwerkt, is de lijst met contactgegevens uiteraard vrij lang.

Artikel 30 lid 2 sub b AVG stelt de eis om de categorieën van verwerkingen die voor rekening van iedere verwerkingsverantwoordelijke zijn uitgevoerd op te nemen. Dit zijn alle soorten verwerkingen zoals genoemd in artikel 4 lid 2 AVG, zoals onder anderen verzamelen, opvragen, wijzigen en vernietigen van gegevens.

Artikel 30 lid 2 sub c AVG is identiek aan sub e van lid 1 van artikel 30 AVG. Dit gaat over de doorgifte van persoonsgegevens aan een derde land of internationale organisatie.

Tot slot moet ook de verwerker een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen (als bedoeld in artikel 32 lid 1 AVG) opnemen in het register, op grond van **artikel 30 lid 2 sub d AVG**. Ook dit is identiek aan de bepaling die geldt voor verwerkingsverantwoordelijken.

---

[43] Eding 2017.
[44] Comijs, *P&I* 2016, afl. 6, p. 253.

Hoewel het lijstje met verplichtingen voor verwerkers duidelijk korter is dan die voor verwerkingsverantwoordelijken, lijken de verschillen in eerste opzicht klein. Enkele van deze verschillen zijn echter op zijn minst opmerkelijk te noemen.

Een verschil tussen beiden is dat de verwerker geen categorieën van betrokkenen op hoeft te nemen in zijn register. Eveneens is de eis om de verwerkingsdoeleinden op te nemen (artikel 30 lid 1 sub b) voor een verwerker niet verplicht. Tot zover niets bijzonders.

Opvallender is dat de verwerkingsverantwoordelijke niet in zijn register hoeft op te nemen welke categorieën van verwerkingen er onder hun verantwoordelijkheid plaatsvinden. Hij moet dus wél verantwoorden/aantonen dat er onder zijn verantwoordelijkheid (bijv.) BSN-nummers verwerkt worden, maar niet of deze alleen verzameld worden of ook opgeslagen, vernietigd, doorgezonden, etc.

Andersom hoeft een verwerker enkel aan te tonen welke verwerkingen hij ten behoeve van de verwerkingsverantwoordelijke doet maar hoeft geen categorie van persoonsgegevens te benoemen. Ofwel: hij moet aangeven dat hij persoonsgegevens opslaat, verwijdert en doorzendt voor "Verantwoordelijke X", maar niet of het gaat om BSN-nummers, NAW-gegevens of telefoonnummers.

De wetgever geeft hierover nergens ook maar enige vorm van uitleg of motivatie over.

2.4 De interpretatie en invulling van de Artikel 30-vereisten

In artikel 30 AVG staan enkele begrippen die openstaan voor interpretatie: *"Indien mogelijk"*, "*de categorieën"*, "*algemene beschrijving"*, noem maar op.[45] Daarnaast is de opmaak van het register is grotendeels vrij te bepalen. Het enige over de opmaak dat verplicht wordt, is dat het in schriftelijke vorm, waaronder tenminste elektronische vorm moet.[46]

De wetgever zegt weinig over de invulling van artikel 30 AVG en rekent op de creativiteit van de verwerkingsverantwoordelijken en verwerkers.[47]

Desondanks zijn de boetes wanneer de AP je compliancy met artikel 30 AVG als onvoldoende beoordeelt niet gering. Deze paragraaf benoemt een aantal zaken waar rekening mee gehouden moet worden bij het correct opstellen van het verwerkingsregister, om te voorkomen dat je niet voldoet aan artikel 30. Of, om in de geest van de verantwoordingsplicht te blijven: aan te tonen dat je zoveel mogelijk hebt ondernomen om te voldoen aan artikel 30 AVG.

2.4.1 De beginselen van het gegevensbeschermingsrecht

Enkele belangrijke aspecten om rekening mee te houden bij het opstellen van het verwerkingsregister zijn de algemene beginselen van het gegevensbeschermingsrecht. Deze zijn er al sinds 1985 en zijn vastgelegd in Verdrag 108 van de Raad van Europa inzake de bescherming van personen met betrekking tot de geautomatiseerde verwerking van

[45] Felz 2016.
[46] Artikel 30 lid 3 AVG.
[47] Holvast, *P&I 2016 afl. 6,* p. 237.

persoonsgegevens. Later zijn deze beginselen geïmplementeerd in de Richtlijn 95/46/EG.[48] Deze beginselen zijn nu identiek overgenomen in de AVG en zijn als volgt:[49]

- Beginsel van rechtmatige verwerking (artikel 5 lid 1 sub a AVG)
- Beginsel van doelbinding (artikel 5 lid 1 sub b AVG)
- Relevantie van de gegevens (artikel 5 lid 1 sub c AVG)
- Nauwkeurigheidsbeginsel (artikel 5 lid 1 sub d AVG)
- Beperkte bewaring (artikel 5 lid 1 sub e AVG)

Als deze bekend voorkomen, is dan omdat ze destijds bijna letterlijk zijn overgenomen in de Wbp.[50] In de AVG is daar een belangrijk beginsel aan toegevoegd waar rekening mee gehouden moet worden: het transparantiebeginsel.[51] Dit beginsel is apart en tot twee keer toe opgenomen in de artikelen 5 lid 1 sub a en 12 van de AVG. Bovenop het feit dat deze twee artikelen in de AVG enkele concrete rechten en plichten in het leven roepen is het duidelijk dat de wetgever het bereiken van transparantie ziet als een van de hoofddoelen van de verantwoordingsplicht.[52]

2.4.2 De meldplicht van de wet bescherming persoonsgegevens

De registerplicht van artikel 30 lijkt nog het meest op de meldplicht uit de Wbp.[53] Onder de meldplicht zijn bedrijven verplicht om bij de Autoriteit Persoonsgegevens melding te maken van een gegevensverwerking. Echter waren hier de meest gangbare zaken zoals o.a. personeelsadministratie en klantenbestanden van vrijgesteld en werd dit niet tot nauwelijks gehandhaafd.[54] De vereisten aan deze meldplicht kunnen echter wel meegenomen worden bij het bepalen van de detailgraad van artikel 30 AVG.
Omdat artikel 30 AVG geen richtlijn geeft over wat nu precies een 'categorie van persoonsgegevens' is kan er gebruik gemaakt worden van de wijze waarop de AP hier onder de meldplicht van de Wbp mee om is gegaan. Zo wordt uit de toelichting bij het Wbp-meldingsformulier duidelijk dat de AP bij het gebruik van een persoonlijk identificatienummer, dit graag apart benoemd wil zien.[55]

2.5 De overige verantwoordingsinstrumenten belicht

Artikel 30 AVG geeft een op zichzelf staande verplichting tot een uitgebreide boekhouding van alle persoonsgegevens die de revue passeren binnen de onderneming. De AVG heeft daarnaast nog enkele andere artikelen die aan de verantwoordingsplicht voor verwerkingsverantwoordelijke en verwerker concrete verplichtingen verbinden. Dit zijn allemaal op zichzelf staande verplichtingen die desondanks nauw samenhangen. Daarom dat in deze paragraaf kort een licht wordt geworpen op de Privacy Impact Assessment (PIA) en de organisatorische- en technische beveiligingsmaatregelen.

2.5.1 De Privacy Impact Assessment (PIA)

Op grond van artikel 35 AVG moet onder bepaalde voorwaarden een gegevensbeschermingseffectbeoordeling uitgevoerd worden. Meer gebruikelijk is de van oorsprong Engelse term PIA, in dit rapport zal die term dan ook worden gebruikt. De PIA is

[48] Artikel 6 Richtlijn 95/46/EG.
[49] Raad van Europa, *Handboek Europese gegevensbeschermingswetgeving*, april 2014 p. 71.
[50] Kamerstukken II, 1997-1998, 25-892, nr.3 p.20.
[51] *Rechtmatigheid en Transparantie*, Europa decentraal, 2016.
[52] De Jong, Regelmaat 2015, afl. 1, p.11.
[53] Artikel 27 Wbp.
[54] Hennekens 2017.
[55] Meldingsprogramma AP, autoriteitpersoonsgegevens.nl.

een instrument om vooraf de (privacy)risico's van een bepaalde gegevensverwerking in kaart te brengen en in te schatten. Daar hoort ook bij het nemen van maatregelen om deze risico's te verkleinen.[56] Deze maatregelen manifesteren zich in de technische- en organisatorische beveiligingsmaatregelen die in de volgende paragraaf worden besproken. Een PIA is alleen verplicht als een verwerking een hoog privacy risico oplevert voor de betrokkenen.[57] Artikel 35 lid 3 AVG benoemt drie specifieke situaties waar in ieder geval een PIA uitgevoerd moet worden:

1. Systematisch en uitvoerige beoordeling van persoonlijke aspecten van natuurlijke personen;
2. Op grote schaal bijzondere persoonsgegevens verwerken;
3. Op grote schaal en systematisch mensen volgen in een publiek toegankelijk gebied.

Daarnaast heeft de werkgroep van Europese privacy toezichthouders (WP 29) een lijst met criteria opgesteld om te bepalen wanneer er sprake is van een hoog risico. De drie in de AVG benoemde situaties vallen daaronder, maar bijvoorbeeld ook: "het combineren van bepaalde gegevenssets" en "grootschalige gegevensverwerking". In het laatste voorbeeld geeft de WP 29 aan dat dus niet alleen het verwerken van bijzondere persoonsgegevens op grote schaal een hoog risico oplevert (zoals de AVG zelf benoemt). De volledige lijst is opgenomen in bijlage I.

2.5.2 De organisatorische- en technische beveiligingsmaatregelen

Wanneer na het uitvoeren van een PIA of anderszins blijkt dat er voor bepaalde verwerkingen een hoog risicogehalte is, moet hier natuurlijk ook iets mee gedaan worden. Daarom heeft de AVG in de artikelen 25 en 32 verplicht gesteld om technische- en organisatorische beveiligingsmaatregelen te nemen.

In artikel 32 wordt een viertal zaken opgesomd die bereikt moeten worden door middel van het treffen van de verplichte beveiligingsmaatregelen. Zo moeten de maatregelen er voor zorgen dat:

- persoonsgegevens waar mogelijk versleuteld of gepseudonimiseert zijn;[58]
- op permanente basis de vertrouwelijkheid, integriteit en beschikbaarheid van de systemen en diensten gegarandeerd kunnen worden;[59]
- in gevallen van incidenten er tijdig herstel kan plaatsvinden;[60]
- de kwaliteit van de maatregelen op routinebasis beoordeelt en geëvalueerd worden.[61]

Lid 3 beschrijft dat aansluiten bij een goedgekeurde gedragscode[62] of het gebruikmaken van goedgekeurde certificeringsmechanismen[63] als element geldt om aan te tonen dat wordt voldaan aan de vereisten van artikel 32 lid 1.

[56] www.autoriteitpersoonsgegevens.nl (zoek op Europese privacyverordening, Privacy Impact Assessment).
[57] WP 29 2017.
[58] Artikel 32 lid 1 sub a AVG.
[59] Artikel 32 lid 1 sub b AVG.
[60] Artikel 32 lid 1 sub c AVG.
[61] Artikel 32 lid 1 sub d AVG.
[62] Artikel 40 AVG.
[63] Artikel 42 AVG.

2.5.2.1 Privacy by default en privacy by design

In artikel 25 eist de AVG dat rekening wordt gehouden met *privacy by design* en *privacy by default*. Deze twee termen bestaan al een stuk langer, maar hebben nu dus een formeel karakter gekregen door ze te gebruiken in de AVG.[64] Privacy by default wil zeggen dat de standaardinstelling van een systeem een zo hoog mogelijk privacy-gehalte tracht te behalen. Privacy by design is de methode waarbij tijdens de ontwikkeling van een proces of systeem, privacy-verhogende maatregelen worden genomen.[65] Dataminimalisatie is een voorbeeld hiervan.
De verwerkingsverantwoordelijke zal iets moeten uitleggen wanneer deze meer gegevens verwerkt dan strikt noodzakelijk is, dit hangt ook sterk samen met de beginselen van het gegevensbeschermingsrecht en de vereisten van artikel 5 AVG.

Ook versleuteling van de persoonsgegevens is een vorm van privacy by design. Dit betekent dat de gegevens zijn gecodeerd en alleen toegankelijk zijn door gebruik te maken van een specifieke decryptiesleutel.[66]
Een ander voorbeeld van privacy by design dat specifiek genoemd wordt in de AVG is pseudonimisering. Dat is een proces waarin de identiteit van een persoon door een algoritme wordt omgezet in een unieke code of iets anders vergelijkbaars, de persoonsgegevens zijn dan niet meer te herleiden naar de betrokkene.[67]

Het mag na het lezen van deze paragraaf duidelijk zijn dat deze drie verantwoordingsinstrumenten (het verwerkingsregister, de PIA en de beveiligingsmaatregelen) nauw samenhangen. De PIA is er om risico's van verwerkingen te meten, daaruit volgen de te nemen maatregelen en welke dat zijn moet weer (onder anderen) worden vastgelegd in het register. Bepaalde gegevens uit het register kunnen weer gebruikt worden voor de uitvoering van een PIA en zo begint de cirkel opnieuw.

2.6 De Uitvoeringswet AVG

Op 25 mei 2018 vervalt de Wbp en wordt effectief vervangen door de Uitvoeringswet AVG. De AVG laat namelijk in een behoorlijk aantal gevallen aan lidstaten de mogelijkheid om de toepassing van de AVG verder uit te werken of aan te vullen middels een nationale wet. De UAVG is ten tijden van dit schrijven nog altijd een wetsvoorstel. Deze zou dus nog kunnen wijzigen maar in dit rapport wordt uitgegaan van de versie die er ligt op 26 mei 2017. De systematiek van de UAVG sluit grotendeels aan bij die van de verordening en is zodoende eenvoudig te lezen.[68] Een van de belangrijkste functies van de UAVG is het aanwijzen van de AP als toezichthoudende autoriteit.[69]

De UAVG maakt bij een aantal andere zaken ook gebruik van de mogelijkheden die de AVG biedt tot regulering op nationaal niveau. Hieronder worden enkele daarvan die direct of indirect in relatie staan tot de verantwoordingsplicht uiteengezet.

---

[64] Mahmood 2016.
[65] Comijs, *P&I* 2016, afl. 6, p. 254.
[66] Definition of encryption, kaspersky.com.
[67] FAQ, pseudonimiseer.nl.
[68] Jansen 2017
[69] Artikel 6 lid 2 Uitvoeringswet AVG.

Artikel 84 AVG biedt lidstaten de mogelijkheid om sancties vast te stellen voor inbreuken op de verordening die niet al onderworpen zijn aan de administratieve geldboeten van artikel 83 AVG. Nederland heeft hier gebruik van gemaakt door op inbreuk op artikel 10 AVG een boete te verbinden. Het gaat in dit artikel om de monopolie van de overheid op het verwerken van strafrechtelijke gegevens.[70]

Artikel 9 AVG biedt de ruimte aan lidstaten om in het nationale recht de uitzonderingen voor verwerking van bijzondere persoonsgegevens te reguleren, door het opnemen van een wettelijke verplichting of uitzonderingsgrond. De UAVG heeft hier gebruik van gemaakt in een groot aantal artikelen (artikelen 23 t/m 30 UAVG). Dit is gedaan zodat er minder verandert ten opzichte van de huidige situatie onder de Wbp. Met andere woorden, veel van de uitzonderingen op verwerkingsverboden die Nederland heeft blijven van kracht.

Ook is er in de UAVG gekozen op gebruik te maken van artikel 23 AVG. Dit geeft lidstaten de mogelijkheid om de rechten van betrokkenen[71] enigszins te beperken. Dit is geregeld in artikel 39 UAVG en heeft met name betrekking in gevallen van bedreiging voor nationale veiligheid en de openbare orde. Verder wordt er in de UAVG nauwelijks gebruik gemaakt van de opties die de AVG biedt aan de lidstaten.

2.7 Overige relevante wet- en regelgeving

In deze paragraaf worden enkele andere wetten en regelingen besproken die direct of indirect invloed hebben op de verantwoordingsplicht van de AVG. Zij hebben betrekking op verwerkingsactiviteiten in de zorg en zijn daarom een belangrijke achtergrond voor de werkzaamheden van VECOZO.

2.7.1 Wet op geneeskundige behandeling (WGBO)

Omdat VECOZO diensten verleent in de zorgsector zal ten alle tijden rekening gehouden moeten worden met de WGBO, opgenomen in boek 7 van het Burgerlijk Wetboek. Zorgverleners zijn op grond van deze wet gehouden aan hun beroepsgeheim.[72]In het kader van de bescherming van persoonsgegevens is dit beroepsgeheim van groot belang. Het medisch beroepsgeheim is geregeld in art. 7:457 van het Burgerlijk Wetboek en bepaalt dat geen inlichtingen over de patiënt mogen worden verstrekt dan na uitdrukkelijke toestemming van hem/haar. Hier zijn echter enkele uitzonderingen op. In de volgende gevallen zou het verstrekken van patiëntgegevens, zonder dienst uitdrukkelijk toestemming, wel zijn toegestaan:

- Indien de inlichtingen worden verstrekt aan diegene die rechtstreeks zijn betrokken bij de uitvoering van de behandelovereenkomst;[73]
- Aan de vervanger van de hulpverlener;[74]
- Aan degene die in artikel 7:450 en 7:465 BW is aangewezen als wettelijk vertegenwoordiger van de patiënt;[75]
- Onder bepaalde voorwaarden mogen in het kader van wetenschappelijk onderzoek inlichtingen verstrekt worden.[76]

[70] MvT Concept UAVG, paragraaf 3.2.3, p. 39.
[71] Hoofdstuk III AVG.
[72] WGBO, dwangindezorg.nl
[73] Artikel 7:457 lid 2 BW.
[74] Artikel 7:457 lid 2 BW.
[75] Artikel 7:457 lid 3 BW.

Ook artikel 7:450 BW is in dit geval van belang. Het uitwisselen van informatie over een patiënt, als verrichting ter uitvoering van de behandelingsovereenkomst, kan namelijk alleen na nadrukkelijke toestemming van de patiënt.

2.7.2 Wet gebruik Burgerservicenummer in de zorg (BSN-z)

Regelgeving omtrent de verwerking van een nationaal identificatienummer mogen van de AVG door lidstaten zelf worden vastgesteld.[77] De wet BSN-z bepaalt dat zorgaanbieders en zorgverzekeraars in het kader van het aanbieden van zorg, het BSN-nummer van personen mogen verwerken.[78] De doelbinding daarvan moet wel zijn grondslag hebben in de wet.

[76] Artikel 7:458 BW.
[77] Artikel 87 AVG.
[78] Artikel 4 jo. artikel 13 Wet BSN-z.

HOOFDSTUK 3 – DE GEGEVENSVERWERKINGEN VAN VECOZO

In dit hoofdstuk komt de gegevensverwerking die plaatsvindt binnen VECOZO aan bod. Om het overzichtelijk te houden is er gekozen voor het analyseren van drie diensten binnen VECOZO, namelijk:

- Certificatenbeheer (paragraaf 3.1);
- Aanlevering Verzekerdengegevens (paragraaf 3.2);
- Berichtenbox (paragraaf 3.3)

Er wordt ingezoomd op de werking en inhoud van de dienst en zijn juridische grondslag. Daarnaast komt uiteraard aan bod welke verwerkingen er plaatsvinden en welke organisatorische- en technische beveiligingsmaatregelen er zijn getroffen.

Er wordt binnen VECOZO gebruik gemaakt van verschillende interne documenten om het beleid van diensten vast te leggen en informatie te verschaffen. Om de gegevensverwerking van VECOZO in kaart te brengen is gebruik gemaakt van deze 'dienstbeschrijvingen' en/of beleidstukken (VECOZO policies). De aard en strekking van deze documenten loopt vaak door elkaar. Zo kan een dienstbeschrijving evenwel een (deel van de) omschrijving van het beleid van die dienst bevatten of staat er technische informatie in het Policy document.

Eveneens zijn er enkele interviews afgenomen met de mensen die directe zeggenschap over, of kennis en kunde hebben van de hierboven genoemde diensten. Wanneer bepaalde informatie uit een intern document voortkomt wordt hier in de tekst of in een voetnoot naar verwezen. Wanneer iets voortkomt uit een van de interviews wordt dit in de tekst vermeld of wordt in een voetnoot verwezen naar een interview transcript dat is opgenomen in de bijlagen. Bij sommige bevindingen wordt er verwezen naar de verwerkersovereenkomst die VECOZO heeft afgesloten met Zilveren Kruis (al zijn de verwerkersovereenkomsten met de overige verzekeraars identiek). Deze zijn vertrouwelijk en zodoende niet opgenomen in de bijlagen.

3.1 Certificatenbeheer

Wanneer aangesloten instanties of hun medewerkers gebruik willen maken van de diensten van VECOZO dienen zij zich in te loggen en te authentiseren. Om de diensten van VECOZO binnen een beveiligde omgeving te laten gebruiken, worden certificaten uitgegeven aan de gebruikers van de dienst.

Zo'n certificaat dient als een token in een twee-factor-authenticatie, namelijk:
- je hebt iets, de token ofwel certificaat
- en je weet iets, je wachtwoord.[79]

Het certificaat is een digitaal document dat op de hardware van de gebruiker wordt geïnstalleerd om zijn identiteit en authenticiteit vast te stellen.[80] VECOZO maakt voor haar certificering gebruik van de X.509 standaard. De X.509 standaard is een aanbevolen

[79] Dienstenbeschrijving Certificatenbeheer VECOZO, bijlage II.
[80] VECOZO Certificate Policy/Certificate Practice Statement.

certificaat dat er op gericht is een beveiligde verbinding te garanderen tussen twee partijen.[81]

3.1.1 Juridische grondslag en doelbinding van Certificatenbeheer

Voor de dienst Certificatenbeheer is VECOZO verwerkingsverantwoordelijke op grond van artikel 4 lid 7 AVG. VECOZO heeft namelijk het doel en de middelen bepaald. Het doel is ervoor te zorgen dat klanten en partijen aan wie VECOZO diensten verleend gebruik kunnen maken van een veilige omgeving waarin VECOZO kan garanderen dat de (andere) gebruikers rechtmatig gebruik maken van de diensten.[82]

Binnen Certificatenbeheer worden de gegevens van de certificaatgebruikers geregistreerd op basis van wat nu artikel 8 sub a en artikel 8 sub b van de Wbp zijn. Dat zijn de "toestemming van de betrokkene" (de gebruiker) en "vanwege de uitvoering van een overeenkomst", in dit geval de verwerkersovereenkomst die contractant heeft gesloten met VECOZO.
In de AVG blijven deze twee juridische grondslagen intact. De toestemming is geregeld in art. 6 lid 1 sub a jo. art. 7 AVG. De inhoud en strekking van dit artikel blijft onveranderd, met de opmerking dat er een verzwaarde bewijslast ligt bij de verwerkingsverantwoordelijke als het gaat om toestemming.[83] In de AVG is namelijk toegevoegd dat de *"vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting"* daarnaast ook te bewijzen moet zijn door middel van een *"verklaring of een ondubbelzinnige actieve handeling"*
Het aanvragen van het certificaat en daarna zelf verschaffen van je persoonsgegevens kan worden gezien als zo'n ondubbelzinnige actieve handeling.[84] Het initiatief komt immers van de gebruiker
De grondslag op basis van de uitvoering van een overeenkomst is geregeld in art. 6 lid 2 AVG en is ten aanzien van de Wbp onveranderd.

3.1.2 Voor wie en wat?

Wie zijn de gebruikers die een certificaat succesvol kunnen aanvragen bij VECOZO? Het is namelijk niet de bedoeling dat iedereen toegang kan krijgen tot de beveiligde omgeving en diensten van VECOZO. Om die reden stelt VECOZO een zeer beperkte gebruikersgemeenschap vast, die gebruik mag maken van haar diensten. De partijen binnen deze gebruikersgemeenschap zijn *Contractanten*, *Contactpersonen*, *Gebruikers* en *Vertrouwende partijen*.[85]

Contractanten zijn rechtspersonen binnen het zorgveld in Nederland die diensten verlenen op grond van één of meerdere zorgwetten. Daarnaast worden ook zorgverzekeraars en gemeenten aangemerkt als contractanten waar VECOZO diensten aan verleent.

Een *Contactpersoon* is een door contractant gemachtigde medewerker binnen de organisatie van contractant die als eerste aanspreekpunt voor VECOZO geldt en bepaalde rechten en plichten heeft. De Contactpersoon treedt namens Contractant op in de communicatie met VECOZO.

---

[81] X-505, forumstandaardisatie.nl.
[82] Dienstenbeschrijving Certificatenbeheer VECOZO, bijlage II.
[83] Berkvens 2016.
[84] Bijron, 2016.
[85] VECOZO Certificate Policy/Certificate Practice Statement.

Gebruikers zijn natuurlijke personen die deel uitmaken van de organisatie van de contractant en via een certificaat gebruik kan maken van de diensten van VECOZO.

Een *vertrouwende partij* is een partij die handelt in vertrouwen op een door VECOZO uitgegevens Single Sign On (SSO) certificaat.

VECOZO onderscheidt twee soorten certificaten die worden uitgegeven. *Persoonlijke certificaten* zijn gebonden aan één specifieke gebruiker en bedoeld om deze te authentiseren. *Systeemcertificaten* zijn verbonden aan de applicaties en/of systemen van de contractant en zijn bedoeld om gebruik te maken van de web services. Technisch gezien zijn deze certificaten precies hetzelfde. In de praktijk komt dit verschil er op neer dat persoonlijke certificaten zijn gebonden aan een individu en de systeemcertificaten gebruikt kunnen worden door iedereen die toegang heeft tot de applicaties, computersystemen etc. van de contractant.[86]

Voorbeeld: Zilveren Kruis maakt binnen hun organisatie gebruik van een intranet. Binnen dit intranet is aan de account van iedere medewerker een autorisatielevel gekoppeld. Medewerker X heeft op zijn account vrijwel alle autorisaties aan staan, ofwel hij is gemachtigd om overal bij te kunnen. Op het intranetsysteem van Zilveren Kruis is een systeemcertificaat van VECOZO geïnstalleerd. Medewerker X kan nu via het intranet van zijn werkgever, Zilveren Kruis, gebruik maken van de diensten van VECOZO. Hij hoeft niet apart in te loggen via een door VECOZO geleverde gebruikersnaam en een eigen ingesteld wachtwoord.

3.1.3 Aanvraag en geldigheid van het certificaat

Alleen de contactpersoon van een contractant kan een nieuwe gebruiker aanmelden en aangeven welk autorisatieniveau[87] de gebruiker moet krijgen. Een certificaat moet binnen 60 dagen na verlening van het gebruikersnummer en pincode aan de contactpersoon, worden opgehaald en geïnstalleerd. Het ophalen van het certificaat is een digitale handeling. Wanneer de gebruiker het certificaat probeert op te halen, controleert VECOZO of de juiste (eenmalige) pincode, gebruikersnaam en daar aan gekoppelde unieke naam (voor- en achternaam van de gebruiker) voor het certificaat met elkaar matchen. Dit laatste is een verwerking van een persoonsgegeven en zal verderop aan bod komen.

Wanneer het certificaat succesvol is opgehaald, is deze 2 jaar en 1 maand geldig (1 maand i.v.m. de aanvraag van een nieuw certificaat). Wanneer er wordt ingelogd bij de beveiligde VECOZO omgeving wordt nogmaals de geldigheid van het certificaat gecontroleerd aan de hand van een controle van de overeenkomst tussen het certificaat, het gebruikersnummer en het wachtwoord dat de gebruiker heeft aangemaakt.[88] Er wordt op dit punt geen koppeling meer gemaakt met de voor- en achternaam van de gebruiker.[89] Daarnaast is er

[86] Deze informatie vloeit voort uit gesprekken met Johan Boons, product owner van de dienst Certificatenbeheer, bijlage III.
[87] Dit is een toegangslevel om bepaalde gebruikers af te schermen van bepaalde data waar zij geen toegang tot behoren te hebben, de verschillende levels zijn door VECOZO vastgelegd in een autorisatiematrix.
[88] Dienstenbeschrijving Certificatenbeheer VECOZO, bijlage II.
[89] Deze informatie is verkregen uit een interview met Johan Boons, product owner van de dienst Certificatenbeheer en leden van het zogenoemde Team Blauw, ontwikkelaars van de dienst, bijlage III.

sprake van een automatisch gegenereerd gebruikersnummer en daarom is hier succesvol pseudonimisering toegepast.[90]

3.1.4 Gegevensverwerking en bewaartermijn

De gegevens die worden vastgelegd voor gebruikers waar een certificaat voor wordt aangevraagd zijn de volgende:

- Voor- en achternaam van de gebruiker wanneer het een persoon betreft
- E-mailadres van de gebruiker bij een persoonlijk certificaat en bij een systeemcertificaat het e-mailadres van de beheerder van dat certificaat, namelijk de contactpersoon van de contractant
- Gebruikersnummer (14-cijferig en automatisch gegenereerd)
- Wachtwoord (zelf bedacht door de gebruiker om in te loggen bij VECOZO)

Ook een wachtwoord dat zelf is aangemaakt is een verwerking van persoonsgegevens. Het wachtwoord, dat in gehashte[91] vorm is opgeslagen, bij VECOZO is in beginsel geen persoonsgegeven, omdat het niet herleidbaar meer is tot een specifiek persoon. Het wachtwoord zelf (de tekens die de gebruiker invoert) is echter wél een persoonsgegeven. Het met elkaar in verband brengen/combineren (van wachtwoord en gebruikersnaam) is desondanks ook een verwerking van een persoonsgegeven.[92]

Bij het aanvragen van een certificaat worden de gegevens van de aanvrager **verzameld**, **opgeslagen**, **verstrekt** aan de dienst Relatiebeheer, **gecombineerd** (gebruikersnummer en wachtwoord) en uiteindelijk bij afloop van een certificaat **vernietigd**. Bij de aanvraag van een certificaat door een contactpersoon wordt ook gecontroleerd of diegene daadwerkelijk door de tekenbevoegde van contractant is aangemerkt als contactpersoon. Dit gebeurt door het **opvragen** van diens gegevens bij de dienst Relatiebeheer.
Via een beveiligde lijn worden alleen de voor- en achternaam van de gebruiker naar de Trusted Certification Authority (TCA) KPN **doorgezonden**.[93] Daarnaast worden de namen opgeslagen binnen de interne VECOZO-dienst relatiebeheer.
Nogmaals ter verduidelijking, het gebruikersnummer wordt eenmalig als persoonsgegeven verwerkt tijdens het aanvragen en ophalen van het certificaat. Om dit succesvol te doen wordt hier op gecontroleerd in combinatie met de voor- en achternaam. Daarna, bij bijvoorbeeld inloggen of een nieuwe pincode aanvragen, wordt er geen koppeling meer tussen de twee gelegd om pseudonimisering toe te passen. Een succesvol voorbeeld van privacy by design.[94]

De bewaartermijn bedraagt twee jaar en één maand, of korter wanneer er een nieuw certificaat wordt aangevraagd of het certificaat wordt ingetrokken.

3.1.5 De beveiligingsmaatregelen van Certificatenbeheer

Het gebruik van KPN als TCA is probleemloos te verantwoorden. Zij voldoen aan de strenge ISO27001:2013-certificering, wat bewijst dat zij een veilige omgeving kunnen garanderen.[95]

---

[90] Comijs, *P&I* 2016, afl. 6, p. 254.
[91] Byte 2015.
[92] Dammers 2013.
[93] Een TCA is een dienstverlener die digitale certificaten verstrekt en hierbij optreed als Trusted Third Party.
[94] Deze informatie is verkregen uit een interview met Johan Boons, product owner van de dienst Certificatenbeheer en leden van het zogenoemde Team Blauw, ontwikkelaars van de dienst, bijlage III.
[95] VECOZO Certificate Policy/Certificate Practice Statement.

VECOZO maakt waar mogelijk gebruik van een twee-factor authenticatie om zoveel mogelijk beveiliging van het gebruik te garanderen. Waar nodig – denk bijvoorbeeld aan opvallende excessen in het gebruik van een certificaat– wordt gecontroleerd op het gebruik. Ter illustratie: Een systeemcertificaat wordt normaal gebruikt op één of twee IP-adressen, en ineens veranderd dit naar 25. Waarschijnlijk heeft de systeembeheerder van contractant dit dan gewoon gekopieerd, dan gaat VECOZO op onderzoek uit.
Zo'n onderzoek vind plaats na een melding of proactief. Daarnaast gaat men per 1-1-2018 naar een geautomatiseerd systeem dat wekelijks deze excessen herkent en rapporteert aan het team Ongepast Gebruik.[96]

Waar VECOZO momenteel niet op controleert is of de gebruikers van de certificaten nog steeds dezelfde zijn. Stel een bedrijf is ooit failliet gegaan of verkocht, en ze hebben het certificaat gewoon doorgegeven als onderdeel van de inboedel, dat mag niet. Hierop zou VECOZO wel moeten controleren op grond van art. 24 van de eIDAS verordening, maar dat doen ze niet.[97]

De technische beveiligingsmaatregelen van VECOZO voldoen allemaal aan de NEN 7510:2011-standaard voor medische informatica – informatiebeveiliging in de zorg.[98]

3.2 Aanlevering Verzekerdengegevens (AVG)

Om een en ander makkelijker te maken zal, wanneer de dienst Aanlevering Verzekerdengegevens bedoeld wordt, gesproken worden van de dienst AVG, in tegenstelling tot de AVG, waarmee de verordening bedoeld wordt.

In de dienst AVG worden bij VECOZO dagelijks verzekerdengegevens aangeleverd door zorgverzekeraars. Deze gegevens zijn bedoeld als bron van informatie voor diverse andere diensten.[99] Een voorbeeld hiervan is de VECOZO-dienst Controle Op Verzekering (COV). COV is een dienst waarin zorgaanbieders gegevens kunnen raadplegen omtrent patiënten die bij hen binnenlopen. Zo kunnen ze controleren of een patiënt verzekerd is, bij welke verzekeraar en waarvoor hij verzekerd is.[100] De dienst COV zou niet over deze gegevens beschikken indien de verzekeraars ze niet eerst zouden aanleveren in de dienst AVG.

3.2.1 Juridische grondslag Aanlevering Verzekerdengegevens

Voor de dienst Aanlevering Verzekerdengegevens is VECOZO verwerker zoals bedoeld in art. 4 lid 8 AVG. Aan de rol van verwerker moet op grond van artikel 28 lid 3 AVG een verwerkersovereenkomst met een verwerkingsverantwoordelijke ten grondslag liggen. VECOZO heeft voor de dienst AVG afzonderlijke overeenkomsten afgesloten met alle zorgverzekeraars voor wie zij verwerkt.[101] De doelbinding van de verwerking wordt dus bepaald door de zorgverzekeraars.

[96] Deze informatie is verkregen uit een interview met Johan Boons, product owner van de dienst Certificatenbeheer, bijlage III.
[97] De eIDAS verordening reguleert het gebruik van elektronische identificatie binnen de EU.
[98] Dienstenbeschrijving Certificatenbeheer VECOZO, bijlage II.
[99] Dienstenbeschrijving Aanlevering Verzekerdengegevens VECOZO, bijlage IV.
[100] Deze informatie is verkregen uit een interview met Ilse Schreurs, functioneel beheerder van de dienst AVG, bijlage V.
[101] Vanwege het bevatten van vertrouwelijke informatie zijn de overeenkomsten uitgesloten van de bijlagen.

3.2.2 Werking van de dienst Aanlevering Verzekerdengegevens

Dagelijks leveren zorgverzekeraars een Excelbestand met verzekerdengegevens aan. Dit is géén mutatiebestand maar een compleet bestand. Het komt er op neer dat iedere dag opnieuw, de gegevens van iedere verzekerde door de verzekeraars worden verzonden en door VECOZO ontvangen.[102] Deze gegevens zijn vervolgens te raadplegen via diverse andere diensten van VECOZO, waarvan Controle op Verzekering (COV) de grootste 'afnemer' is.

Betrokkenen kunnen bij hun verzekeraar aangeven dat zij niet in zo'n COV systeem willen staan, een zorgaanbieder kan dan niet zien óf en waar iemand verzekerd is. Dat kan. VECOZO ontvangt de gegevens dan wel van de zorgverzekeraar maar met een bepaalde code erbij, zij worden dan niet ter beschikking gesteld in de dienst COV.[103]

Dat verzoek om niet getoond te worden aan zorgaanbieders kan niet ook worden toegepast als het gaat om de raadpleging door De Belastingdienst. Om te bepalen of iemand recht heeft op zorgtoeslag, levert De Belastingdienst een lijst met BSN-nummers. Die lijst wordt dan met de gegevens uit de dienst AVG vergeleken om te controleren of iemand een basisverzekering heeft of niet.[104] Hierin worden deze mensen dus wel aan de Belastingdienst getoond. Dit raadplegen gaat via Trusted Partner Vektis[105], die dit soort zaken al jaren regelt voor o.a. de Belastingdienst. Eind van het jaar zal deze controle echter volledig overgedragen worden aan VECOZO.

Het aanleveren van persoonsgegevens in de dienst AVG verloopt via een geautomatiseerd proces. De aanlevering van de gegevens kan ook worden afgekeurd. Er zijn twee soorten afkeuring te onderscheiden:

1. Het hele bestand wordt afgekeurd. Dit gebeurt bijvoorbeeld omdat er in het verkeerde format is aangeleverd. De verzekeraar moet dan het hele bestand opnieuw aanleveren;
2. Er staan kleine fouten in specifieke subjecten.[106] In dat geval worden alleen de gegevens van die verzekerde niet geüpload en blijven zijn/haar gegevens van de dag ervoor staan.[107]

Omdat het wettelijk van belang is dat de gegevens die VECOZO in haar diensten aanbiedt juist en actueel zijn, op grond van artikel 5 lid 1 sub d AVG, zit er een tolerantiegrens van 0,1% op het aantal fouten. Als het aantal fouten boven die grens uit komt wordt het hele bestand alsnog afgekeurd.[108] In beide gevallen wordt er door VECOZO een geautomatiseerde foutenrapportage opgesteld. Bij afkeuring van het gehele bestand wordt deze rapportage ook naar de indiener (de verzekeraar) verzonden.

---

[102] Deze informatie is verkregen uit een interview met Ilse Schreurs, functioneel beheerder van de dienst AVG, bijlage V.
[103] Deze informatie is verkregen uit een interview met Ilse Schreurs, functioneel beheerder van de dienst AVG, bijlage V.
[104] Deze informatie is verkregen uit een interview met Ilse Schreurs, functioneel beheerder van de dienst AVG, bijlage V.
[105] Over Vektis, vektis.nl.
[106] Subjecten zijn in deze context natuurlijke personen, de verzekerden.
[107] Deze informatie is verkregen uit een interview met Ilse Schreurs, functioneel beheerder van de dienst AVG, bijlage V.
[108] Deze informatie is verkregen uit een interview met Ilse Schreurs, functioneel beheerder van de dienst AVG, bijlage V.

3.2.3 Gegevensverwerking en bewaartermijn

Wanneer de gegevens succesvol zijn aangeleverd, worden ze door diverse andere VECOZO-diensten opgehaald en geraadpleegd vanuit de dienst AVG. Omdat dagelijks een nieuw bestand wordt aangeleverd, worden de oude gegevens op moment van aanleveren van het nieuwe bestand automatisch verwijderd.

De gegevens die dagelijks door verzekeraars worden geleverd zijn de volgende:

- De verzekeraar en het label waarbij de verzekerde een pakket heeft
- Verzekerdennummer
- NAW-gegevens
- Postcode en huisnummer
- Geboortedatum
- BSN
- Premieachterstand J/N
- Ingangs- en einddatum van de verzekering
- Opschorting premie J/N
- Metadata

De gegevens worden in eerste instantie **verzameld** en daarna **opgeslagen**. De dienst AVG **stelt** deze gegevens vervolgens **ter beschikking** aan de VECOZO diensten die dat behoeven. Bij de aanlevering van een nieuw bestand worden de oude persoonsgegevens **vernietigd**. Het opvragen van de gegevens vind natuurlijk ook op grote schaal plaats, maar gebeurt binnen andere VECOZO diensten.[109] Met andere woorden, de verwerkingsactiviteit *"raadplegen"* wordt niet uitgevoerd door de dienst AVG, omdat deze dienst juist als gegevensbron geldt.

Daarnaast **stelt** VECOZO de BSN-nummers en Verzekerdennummers **ter beschikking** aan De Belastingdienst, zoals in de vorige paragraaf staat beschreven.

Zoals eveneens in de vorige paragraaf is beschreven, worden aangeleverde bestanden in sommige gevallen afgekeurd. Wanneer er een fout in het bestand staat en daar een rapportage van komt, worden het BSN en het verzekerdennummer **geraadpleegd** door het rapportageprogramma en **verstrekt** aan de verzekeraar om hem te laten weten waar de fouten zitten.[110] Dit zijn de categorieën van verwerkingen[111] die plaatsvinden binnen de dienst AVG. Momenteel wordt er niets doorgezonden naar het buitenland. Inmiddels is bij VECOZO bekend geworden dat CZ een Belgische partij ter hand heeft genomen die de factuurcontrole gaat doen voor ze bij Belgische zorgaanbieders. Die moeten kunnen controleren of iemand bij CZ verzekerd is. Het zou kunnen dat deze direct AVG gaan raadplegen, maar dat lijkt niet aannemelijk. Meer aannemelijk is dat deze gebruik gaat maken van de dienst COV[112]

De bewaartermijn van gegevens in de dienst AVG bedraagt maximaal 24 uur, tot de aanlevering van het nieuwe bestand succesvol is afgerond. In een enkel geval zal er door

[109] Dienstenbeschrijving Aanlevering Verzekerdengegevens VECOZO, bijlage IV.
[110] Deze informatie is verkregen uit een interview met Ilse Schreurs, functioneel beheerder van de dienst AVG, bijlage V.
[111] Op grond van art. 4 lid 2 AVG.
[112] Deze informatie is verkregen uit een interview met Ilse Schreurs, functioneel beheerder van de dienst AVG, bijlage V.

een fout in de aanlevering, een bepaalde set gegevens (iets) langer worden bewaard.[113]De foutrapportages c.q. retourbestanden worden bewaard gedurende één jaar.

3.2.4 Beveiligingsmaatregelen van Aanlevering Verzekerdengegevens

Om verzekerdengegevens succesvol in de dienst AVG aan te kunnen leveren, is een geldig VECOZO-certificaat nodig. Daarnaast worden de bestanden encrypted aangeleverd. VECOZO decrypt de bestanden om technische controles uit te voeren maar de bestanden worden te allen tijde weer encrypted in de database opgeslagen.[114]

Het afkeuringsproces is volledig geautomatiseerd en VECOZO kan niet het aangeleverde bestand – met de verzekerdengegevens- inzien. Wel wordt er van eventuele fouten, zoals hierboven beschreven, een rapportage opgesteld wat men ook wel het 'retourbestand' noemt.[115] Dit is een rapportage die VECOZO terugstuurt naar de verzekeraar en waar men dus wel bij kan. Hier is wel een vorm van privacy by design toegepast in de vorm van dataminimalisatie. Alleen de foutcode in combinatie met het BSN-nummer en het verzekerdennummer gaan terug naar de verzekeraar.[116]

De technische beveiligingsmaatregelen van VECOZO voldoen ook voor de dienst AVG aan de NEN 7510:2011-standaard voor medische informatica – informatiebeveiliging in de zorg.[117]

3.3 De Berichtenbox

De dienst Berichtenbox biedt bij VECOZO aangesloten partijen de mogelijkheid om berichten met elkaar uit te wisselen over zaken waar nog geen gestructureerde VECOZO-dienst voor bestaat. Dat wil zeggen, wanneer er een VECOZO dienst bestaat die hetzelfde doel kan bereiken dient deze gebruikt te worden. Indien de behoefte bestaat om berichten uit te wisselen die niet binnen een specifieke dienst uitgewisseld kunnen worden, kan gebruikt worden gemaakt van de Berichtenbox.

3.3.1 Juridische grondslag Berichtenbox

VECOZO is in het kader van de Berichtenbox voor een deel als verwerker en voor een deel als verwerkingsverantwoordelijke aan te merken.[118]

VECOZO is verantwoordelijk voor de juistheid van de (contact)gegevens die noodzakelijk zijn om het berichtenverkeer tot stand te brengen. Deze gegevens worden door de Berichtenbox gehaald uit de database van de dienst Relatiebeheer. Relatiebeheer is een interne administratiedienst waar de gegevens van de bij VECOZO aangesloten instanties zijn opgenomen.[119] VECOZO bepaalt hiermee het doel van de verwerking, namelijk het mogelijk maken van berichtenuitwisseling tussen de instanties. De rechtmatigheid van dit verwerkingsdoel heeft zijn grondslag in de overeenkomst die VECOZO heeft met de

[113] Deze informatie is verkregen uit een interview met Ilse Schreurs, functioneel beheerder van de dienst AVG, bijlage V.
[114] Dienstenbeschrijving Aanlevering Verzekerdengegevens VECOZO, bijlage IV.
[115] Dienstenbeschrijving Aanlevering Verzekerdengegevens VECOZO, bijlage IV.
[116] Deze informatie is verkregen uit een interview met Ilse Schreurs, functioneel beheerder van de dienst AVG, bijlage V.
[117] Dienstenbeschrijving Aanlevering Verzekerdengegevens VECOZO, bijlage IV.
[118] Artikel 26 lid 1 AVG.
[119] Dienstenbeschrijving Relatiebeheer VECOZO.

aangesloten instanties.[120] Dit is een rechtmatig verwerkingsdoel op grond van art. 6 lid 2 AVG.

De gebruikers van de Berichtenbox zijn juridisch aan te merken als verwerkingsverantwoordelijke voor de inhoud van het bericht.[121] VECOZO bepaalt immers de doelbinding van die inhoud niet en kan er ook geen feitelijke macht over uitoefenen. Voor dit andere deel van de dienst is VECOZO verwerker van de in de zin van de verordening op grond van de overeenkomsten met de verwerkingsverantwoordelijken.[122]

Het is de gebruiker toegestaan om administratief-medische gegevens te verzenden via de Berichtenbox, deze vallen niet onder de scope van gegevens over gezondheid als benoemt in art. 4 lid 15 AVG.[123] Het verzenden van gegevens uit het medisch dossier van een individu is door VECOZO absoluut verboden.[124] Het verzenden van gegevens uit het medisch dossier is ook in strijd met het medisch beroepsgeheim.[125] Zie voor meer informatie hierover paragraaf 2.7.1.

3.3.2 Werking van de Berichtenbox
Zoals eerder beschreven is de Berichtenbox bedoeld om ongestructureerde berichten onderling uit te wisselen, die niet op een andere wijze door een VECOZO-dienst worden gefaciliteerd.

Het verzenden van gegevens is onderworpen aan de gebruikersvoorwaarden van de Berichtenbox.[126] De berichten worden via een encryptiesleutel (dus beveiligd) naar de VECOZO server verzonden, waar de berichten tijdelijk decrypted worden om technische controles uit te voeren. Bij zo'n technische controle wordt gekeken of de door VECOZO voorgeschreven specificaties zijn aangehouden. Dat wil zeggen: VECOZO schrijft haar gebruikers een aantal verplichte invulvelden voor of heeft bijvoorbeeld een limiet op de bestandgrootte.[127] Voldoet het bericht hieraan, dan wordt deze encrypted weer doorgezonden naar de geadresseerde. Voldoet het bericht hier niet aan, wordt er automatisch een foutcode teruggezonden naar de indiener.[128] Behoudens de technische controle is het bericht encrypted en kan VECOZO op geen moment bij de inhoud van het bericht of de bijlagen.[129]

3.3.3 Gegevensverwerking en bewaartermijn
Binnen de dienst Berichtenbox wordt door VECOZO de verscheidenheid aan gegevens verwerkt. Het gaat vaak om de metadata die gekoppeld zijn aan de berichtformulieren. Deze worden **verzameld** en **opgeslagen**. De metadata worden tenminste **geraadpleegd** voor

[120] De overeenkomsten zijn vanwege het bevatten van vertrouwelijke informatie niet opgenomen in de bijlagen.
[121] Kamerstukken II, 1997-1998, 25-892, 3 p.59.
[122] Artikel 28 lid 3 AVG.
[123] Verordening (EU) 2016/679, overwegingen 30-36, nr. 35.
[124] Artikel 4.5 sub h Gebruiksvoorwaarden Berichtenbox VECOZO, bijlage VII.
[125] Artikel 7:457 lid 1 BW.
[126] Gebruiksvoorwaarden Berichtenbox VECOZO, bijlage VII.
[127] Resultaatcodes VECOZO Berichtenbox, bijlage IX.
[128] Deze informatie is verkregen uit een interview met Paul Vermeulen, product owner van de dienst Berichtenbox, bijlage VIII.
[129] Deze informatie is verkregen uit een interview met Paul Vermeulen, product owner van de dienst Berichtenbox, bijlage VIII.

het samenstellen van foutenrapportages. De metadata worden gelijktijdig met het bericht (inclusief bijlagen) na twee maanden **verwijderd**.[130]

Het adressenboek van de Berichtenbox wordt gevormd door de persoonsgegevens uit de bestanden van Relatiebeheer. Deze gegevens worden door Berichtenbox **geraadpleegd**.[131] Dit wordt gedaan om de uitwisseling van berichten operationeel te maken voor de gebruikers. Medewerker A van de zorgaanbieder moet een bericht sturen naar medewerker B van een verzekeraar, maar zij kennen elkaar niet. De Berichtenbox heeft dan de contactgegevens om toch berichten met elkaar te kunnen uitwisselen.

Alle persoonsgegevens die in het bericht staan worden wel door VECOZO verwerkt, maar zijn encrypted. Dat zorgt voor een gedegen beveiligingsmaatregel, maar zorgt er onbedoeld ook voor dat VECOZO geen zicht heeft op welke persoonsgegevens exact worden verwerkt. VECOZO kan zich enkel beroepen op het feit dat het in de gebruiksvoorwaarden van de Berichtenbox en de contractuele afspraken met de verwerkingsverantwoordelijke het delen van gegevens uit een medisch dossier niet toestaat. [132][133]Hier wordt echter niet actief op gecontroleerd mede omdat VECOZO, uit privacyoverwegingen, niet aan de inhoud van de berichten komt.[134]

3.3.4 Beveiligingsmaatregelen van de Berichtenbox

Zoals voor alle diensten van VECOZO dienen gebruikers te beschikken over een geldig persoonlijk- of systeemcertificaat. Zonder zo'n certificaat kun je geen gebruik maken van de Berichtenbox.[135] VECOZO heeft geen toegang tot de feitelijke inhoud van de Berichtenbox. Dat daar geen toegang tot is, mag gezien worden als een gezonde beveiligingsmaatregel in de zin van de AVG. Het zorgt er wel voor dat het onmogelijk is om te controleren op oneigenlijk gebruik van de dienst, ofwel of er conform de verwerkersovereenkomst wordt gehandeld door de gebruikers.[136]

In het geval van technische problemen raadpleegt VECOZO enkel de loggingbestanden en controleert op uitschieters (in de zin van foutmeldingen). In deze loggings staan verder geen persoonsgegevens. Dat is niet nodig om eventuele technische problemen op te lossen.[137] Ook deze vorm van privacy by design is een getroffen beveiligingsmaatregel in de zin van de AVG.

3.5 Conclusie over de verwerkingen

Over het algemeen verwerkt VECOZO, zowel in haar rol als verwerkingsverantwoordelijke als die van verwerker vrijwel uitzonderlijk niet-bijzondere persoonsgegevens. Een

---

[130] Dienstenbeschrijving Berichtenbox VECOZO, bijlage VI.
[131] Dienstenbeschrijving Berichtenbox VECOZO, bijlage VI.
[132] Dienstenbeschrijving Berichtenbox VECOZO, bijlage VI.
[133] Vanwege het bevatten van vertrouwelijke informatie zijn de overeenkomsten uitgesloten van de bijlagen.
[134] Deze informatie is verkregen uit een interview met Paul Vermeulen, product owner van de dienst Berichtenbox, bijlage VIII.
[135] Dienstenbeschrijving Berichtenbox VECOZO, bijlage VI.
[136] Deze informatie is verkregen uit een interview met Paul Vermeulen, product owner van de dienst Berichtenbox, bijlage VIII.
[137] Deze informatie is verkregen uit een interview met Paul Vermeulen, product owner van de dienst Berichtenbox, bijlage VIII.

uiteenzetting van de verwerkingen per dienst zijn terug te vinden in de bovenstaande paragrafen.

De verwerking van het BSN-nummer, zoals in de dienst AVG plaatsvindt, is een verwerking van een bijzonder persoonsgegeven en mag alleen verwerkt worden voor doeleinden bij wet bepaalt.[138]Omdat VECOZO voor deze dienst verwerker is en niet verantwoordelijk is voor de doelbinding heeft dit geen directe gevolgen voor de verantwoordingsplicht.

De verwerking van de persoonsgegevens "Opschorting verzekering J/N" en "Premieachterstand J/N" zijn strikt genomen geen bijzondere persoonsgegevens. Desondanks kunnen deze gegevens veelzeggende informatie geven over de detentie van een persoon respectievelijk hun financiële situatie.[139] In dit licht kunnen deze twee verwerkingen als verwerkingen van bijzondere persoonsgegevens worden aangemerkt. De Hoge Raad besliste in 2010 immers dat ook gegevens waaruit bijzondere persoonsgegevens kunnen worden afgeleid tot de bijzondere persoonsgegevens behoren.[140]Maar ook hier geldt: omdat VECOZO voor de dienst AVG verwerker is, heeft dit geen directe gevolgen voor de verantwoordingsplicht en hoeft de doelbinding niet opgenomen te worden in het register.[141]

Momenteel lijkt het erop alsof CZ een samenwerking aangaat met een Belgische partij, die de factuurcontrole gaat doen voor ze. Indien deze partij gebruik gaat maken van de diensten van VECOZO moet dit expliciet worden opgenomen in het verwerkingsregister, op grond van art. 30 lid 2 sub c AVG. Daarnaast moet voor die verwerkingen hoofdstuk V van de AVG in acht worden genomen.

Als het gaat om de verwerkingen die plaatsvinden binnen Certificatenbeheer, is VECOZO naast verwerker, ook verantwoordelijke voor de verwerkingen. Dat betekent dat ook de doelbinding in het register zal moeten worden opgenomen. Zoals in paragraaf 4.1 al wordt aangegeven, is dit "het nagaan of de gebruiker wel is wie hij zegt dat hij is." Deze maatregel is in het leven geroepen om te zorgen dat alleen personen die in het kader van hun beroep inzage nodig hebben in bepaalde persoonsgegevens, ook bij die gegevens kunnen komen. Het doel is dus gerechtvaardigd en in overeenstemming met art. 5 lid 1 sub AVG.

Tot slot, voor de Berichtenbox wordt er met name metadata verwerkt. Ook de versleutelde inhoud van de berichten wordt verwerkt (via VECOZO ter beschikking gesteld aan de ontvanger), maar VECOZO kan zelf niet bij de inhoud. Deze inhoud kán bijzondere persoonsgegevens bevatten. VECOZO is in deze gevallen verwerker van de persoonsgegevens en hoeft de doelbinding hiervan niet op te nemen in het register. Daarnaast is VECOZO wél verwerkingsverantwoordelijke voor de persoonsgegevens die gebruikt worden voor het adressenboek van de Berichtenbox, die het raadpleegt uit de dienst Relatiebeheer. De doelbinding hiervoor moet wel worden opgenomen in het verwerkingsregister.

---

[138] Artikel 44 UAVG.
[139] Deze informatie is verkregen uit een interview met Ilse Schreurs, functioneel beheerder van de dienst AVG, bijlage V.
[140] HR 23 maart 2010, ECLI:NL:PHR:2010:BK6331.
[141] Artikel 30 lid 2 AVG.

HOOFDSTUK 4 – EEN VERANTWOORD VERWERKINGSREGISTER

Nu het juridisch kader omtrent de verantwoordingsplicht en in het bijzonder het verwerkingsregister is uiteengezet (hoofdstuk 2) en er een beschrijving van de verwerkingen en processen heeft plaatsgevonden (hoofdstuk 3), is het tijd om een blik te werpen op hoe dit moet leiden tot een solide verwerkingsregister voor VECOZO. Daarnaast wordt in dit hoofdstuk besproken hoe dit op geïntegreerde wijze met de andere twee – reeds besproken- verantwoordingsinstrumenten kan worden ingezet.

De juridische vereisten zijn in hoofdstuk 2 besproken en daarom wordt er in dit hoofdstuk gekeken naar hoe privacy experts, juristen en andere professionals omgaan met dit vraagstuk.

4.1 De Autoriteit Persoonsgegevens

De AP is voor Nederland de autoriteit die op grond van artikel 51 AVG belast is met het toezicht op de toepassing van de verordening. Hoe zien zij de verantwoordingsplicht voor zich? Bieden zij VECOZO misschien hulpmiddelen en oplossingen voor dit vraagstuk?

4.1.1 Bewustwording

Een van de zaken die de AP in meerdere van hun gepubliceerde artikelen benadrukt is bewustwording. Het lijkt voor de hand liggend en is van algemene strekking maar daarom niet minder belangrijk, ook als het gaat om de verantwoordingsplicht. Het is van groot belang dat de relevante mensen inzicht krijgen in de vereisten rondom de verantwoordingsplicht. Zij kunnen inschatten wat voor invloed dit heeft op alle processen binnen de organisatie.[142] Binnen VECOZO zijn dit de product owners van de verschillende diensten, omdat zij het beleid van deze diensten voor een aanzienlijk deel (mede)bepalen. De implementatie van de AVG zal veel tijd en mankracht gaan kosten en inmiddels is er nog slechts een jaar te gaan voor deze zal worden gehandhaafd.

4.1.2 Inventariseer

Ook deze opmerking van de AP lijkt misschien een overvloedige maar het is van groot belang om tijdig in beeld te brengen welke verwerkingen er allemaal worden uitgevoerd binnen de organisatie. Houd ook rekening met zogenoemde 'unstructured data', er bestaat een kans op de aanwezigheid van persoonsgegevens waar weinig tot geen zicht op is.[143] Wanneer deze inventarisatie heeft plaatsgevonden moet ook alles samengebracht worden in het verplichte verwerkingsregister. Naast dat het kan dienen als interne informatievoorziening kan het register ook nodig zijn als betrokkenen hun privacyrechten uitoefenen. Als deze betrokkenen VECOZO vragen om bepaalde gegevens te corrigeren of verwijderen is VECOZO verplicht hier aan te voldoen en dit door te geven aan alle partijen met wie en voor wie zij de gegevens verwerkt.[144] Voor meer informatie over de rechten van betrokkenen en de implicaties daarvan voor VECOZO zie het adviesrapport "*Invulling rechten van betrokkenen*" van Yasamina Farahi.[145]

[142] Autoriteit Persoonsgegevens 2017.
[143] Tran 2017.
[144] Autoriteit Persoonsgegevens 2017.
[145] De naam van dit rapport is nog in concept.

4.1.3 PIA's en privacy by design

Indien je een nieuwe verwerking gaat introduceren, of zelfs een geheel nieuwe dienst met een hoog risicogehalte voor de privacy (voor richtlijnen hierover zie paragraaf 2.5.1 van dit onderzoek en bijlage I) moet een PIA worden uitgevoerd. Houd bij het ontwerpen van dit proces of deze dienst alvast rekening met hoe je privacy by design kunt toepassen.[146] Mocht je bij de uitvoering van de PIA concluderen dat het niet lukt om de benodigde organisatorische- en technische beveiligingsmaatregelen te treffen, moet je contact opnemen met de AP over een "voorafgaande raadpleging". De AP stelt dan een schriftelijk advies op over de voorgenomen verwerking en of deze in strijd is met de AVG.

Over het correct uitvoeren van een PIA zijn veel adviezen en modellen beschikbaar. Het AP beveelt op haar website echter de "handreiking voor de uitvoering van een PIA" van IT-auditors beroepsorganisatie NOREA aan.[147] Dit geeft een meer dan goede indicatie over wanneer volgens de AP voldaan wordt aan artikel 35 AVG.

Houd verder goed de publicaties van de AP in samenwerking met de andere Europese toezichthouders (Working Party 29) in de gaten. In de loop van 2017 publiceren zij onder andere nog richtlijnen met betrekking tot certificering en over het onderwerp transparantie.[148]

Daarnaast wordt mid-2017 een rapport verwacht van een werkgroep van Duitse privacyautoriteiten met daarin een verduidelijking van de term: "algemene beschrijving van beveiligingsmaatregelen".

4.2 Professionals in Privacy

Er zijn al verschillende privacy professionals en juristen bezig geweest met het vraagstuk van het verwerkingsregister. In sommige opzichten is de AVG specifiek en in sommige opzichten laat het ruimte voor de creativiteit van de verwerkingsverantwoordelijke en verwerker.[149] In het kader van de detailgraad van de verschillende categorieën (persoonsgegevens, betrokkenen, verwerkingen, ontvangers) die in het verwerkingsregister moeten worden opgenomen is dit bijvoorbeeld het geval.

Zo gaat het vooraanstaande advocatenkantoor Squire Patton Boggs voor hun afdeling Personeel bijvoorbeeld uit van categorieën van persoonsgegevens zoals[150]:

- Opleidingsgegevens;
- cv;
- bankgegevens;
- NAW-gegevens.

Dit wil zeggen dat zij in het register enkel zullen aangeven dat er van de categorie van betrokkenen genaamd "Werknemers", opleidingsgegevens worden verwerkt. Dat dit zowel een registratie van het niveau en een kopie van een diploma kan bevatten, hoeft niet verder te worden toegelicht.

---

[146] Autoriteit Persoonsgegevens 2017.
[147] autoriteitpersoonsgegevens.nl (zoek op: Zelf doen, Privacycheck, PIA)
[148] autoriteitpersoonsgegevens.nl (zoek op: Europese Privacywetgeving,voorbereiding op de AVG).
[149] J. Holvast, *P&I Aflevering 6 Redactioneel*, December 2016 p. 237.
[150] Demmel 2016

Wat betreft de categorieën van ontvangers wordt door hen aanbevolen om het per afdeling te benoemen, indien het ontvangers binnen de eigen organisatie betreft. Indien het ontvangers buiten de organisatie betreft, moeten deze apart benoemt worden.[151]

Daarnaast wordt aangeraden om allerlei aanvullende gegevens in het register op te nemen, die niet verplicht worden door artikel 30 AVG. Door het opnemen van deze zaken kunnen de verantwoordingsinstrumenten geïntegreerd worden ingezet. Eveneens kan verdere invulling gegeven worden aan het transparantiebeginsel door deze zaken in één bestand samen te voegen.[152] Enkele voorbeelden van zaken die opgenomen kunnen worden in het verwerkingsregister zijn:

- Is de verwerking op basis van toestemming? Dit kan handig zijn om per verwerking in beeld te krijgen nu de voorwaarden voor toestemming zijn aangescherpt en de toestemming makkelijker kan worden ingetrokken.[153] (zie ook paragraaf 3.1.1.)
- Is er informatie verschaft aan de betrokkene en zo ja, hoe? De rechten van betrokkenen zijn flink uitgebreid in de AVG.[154] Als je in het register opneemt op welke wijze invulling wordt gegeven aan de informatieplicht kun je meteen aantonen bij de AP dat je op dit terrein ook voldoet aan je verantwoordingplicht.
- Je kunt ook opnemen of een PIA vereist is of niet. Zo ja kun je ook opnemen in je register of deze al is uitgevoerd, gekoppeld aan een datum.

De opinie dat het veel voordelen voor een organisatie oplevert wanneer er meer gegevens worden opgenomen dan juridisch strikt noodzakelijk is, wordt ook ondersteunt door Tim Gough, CEO van Privacy Arts Ltd. en expert op het gebied van gegevensbescherming. Hij stelt voor om zaken op te nemen zoals de afdeling waar de verwerkingen plaatsvinden, de locatie waar het is opgeslagen (de server), een check of desbetreffende verwerking op de juiste manier is vastgelegd in de verwerkersovereenkomst en of de verwerking op basis van toestemming is gedaan. Daarnaast raadt hij aan om zaken als categorieën van persoonsgegevens en verwerkingsdoelen altijd op te nemen, ongeacht of dit verplicht is in artikel 30 AVG.[155]

Het opnemen van deze 'extra' zaken in je verwerkingsregister, lijkt een tijdrovende en overbodige onderneming, maar het levert je uiteindelijk erg veel op. Het zorgt er namelijk niet alleen voor dat je voldoet aan je verantwoordingsplicht en artikel 30 AVG, maar ook dat je bijvoorbeeld:

- Precies weet in welke gevallen je afhankelijk bent van gegeven toestemming. In dat geval weet je ook precies in welke gevallen je moet controleren of je voldoet aan de eisen van artikel 7 AVG (voorwaarden voor toestemming);
- Inzicht krijgt of je verwerkersovereenkomsten in overeenstemming zijn met artikel 28 AVG;

[151] Demmel 2016
[152] Demmel, 2016
[153] Artikel 7 AVG
[154] Hoofdstuk III AVG
[155] Gough, 2016

- Weet wanneer je gerechtvaardigde belangen als grondslag voor je verwerking hebt en hier dus bijvoorbeeld rekening mee moet houden in het kader van je informatieplicht aan de betrokkene, op basis van artikel 13 lid 1 sub d AVG.[156]

Dit zijn slechts enkele voorbeelden van zaken die opgenomen kunnen worden in het verwerkingsregister. Dit is natuurlijk ook volledig aan te passen aan de organisatie. Zo kan het voor organisaties die op grote schaal persoonsgegevens verwerken bijvoorbeeld interessant zijn om een risicoclassificatie op te nemen in het verwerkingsregister.

4.3 Een slim register

Dat het opstellen van het register en het verzamelen van de benodigde informatie om dat te bewerkstelligen een enorme administratieve last is, zal door niemand worden betwist.[157] Maar dit is nu eenmaal verplicht in artikel 30 AVG. Als het dan toch moet, is het misschien verstandig om van het register een handig hulpmiddel voor je organisatie te maken, in plaats van een onderhoudspost. Hoewel de enkele beschikbare voorbeelden van verwerkingsregisters allemaal in Excelbestanden zijn aangelegd, is het ook denkbaar om in overleg met de IT-afdeling een aantrekkelijk ogend systeem aan te leggen. Een systeem dat bijvoorbeeld melding geeft wanneer er in bepaalde diensten een nieuwe verwerking wordt gedaan, een die niet eerder plaatsvond.[158]

Een systeem dat bijvoorbeeld melding geeft wanneer er in bepaalde diensten een nieuwe verwerking wordt gedaan, een die niet eerder plaatsvond. Je kunt zelfs zover gaan dat als het een persoonsgegeven betreft met een hoog risicogehalte, het register dit automatisch herkent en een notificatie stuurt dat een PIA moet worden uitgevoerd. Nogmaals: 'the sky is the limit'. Enkele mogelijkheden op dit onderwerp worden voorgesteld in hoofdstuk 6.

[156] Gough, 2016
[157] Comijs, *P&I* 2016, afl. 6, p. 254
[158] Talen, 2017

HOOFDSTUK 5 - CONCLUSIES

In dit hoofdstuk worden de conclusies van dit onderzoek uiteengezet door middel van het beantwoorden van de centrale vraag. Deze conclusie zijn bedoeld ter ondersteuning van de aanbevelingen aan VECOZO naar aanleiding van dit onderzoek (hoofdstuk 6).

De centrale vraag is:
''Op welke manier moet VECOZO haar privacy boekhouding, met betrekking tot de verwerkingsregisters van artikel 30 inrichten, mede met het oog op de andere verantwoordingsinstrumenten in de Algemene Verordening Gegevensbescherming, om per mei 2018, maar ook daarna, te voldoen aan de eisen van de verordening?''

Voor de uiteenzetting van de conclusies van de juridische vereisten aan het verwerkingsregister is gekozen voor een schematische weergave.

5.1 Conclusie ten aanzien van verwerkingen en doeleinden

In artikel 30 van de AVG worden eisen gesteld omtrent de inhoud en vorm van het verwerkingsregister. Op basis van het onderzoek naar de verordening kan worden geconcludeerd dat de volgende gegevens in het verwerkingsregister van VECOZO moeten worden opgenomen:

Voor de verwerkingsverantwoordelijke (art. 30 lid 1 AVG)	**Voor de verwerker (art. 30 lid 2 AVG)**
De naam en contactgegevens van de (vertegenwoordiger van de) verwerkingsverantwoordelijke en van de FG (art. 30 lid 1 sub a AVG)	De naam en contactgegevens van de verwerker en iedere verwerkingsverantwoordelijke waar zij voor handelt en van de FG (art. 30 lid 2 sub a AVG)
De verwerkingsdoeleinden (art. 30 lid 1 sub b AVG)	De categorieën van verwerkingen die voor rekening van iedere verwerkingsverantwoordelijke zijn uitgevoerd (art. 30 lid 2 sub b AVG)
Een beschrijving van de categorieën van betrokkenen en categorieën van persoonsgegevens (art. 30 lid 1 sub c AVG)	Een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen (art. 30 lid 2 sub c AVG).
De categorieën van ontvangers (art. 30 lid 1 sub d AVG)	
De bewaartermijn (art. 30 lid 1 sub f AVG)	
Een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen (art. 30 lid 1 sub g AVG)	

Daarbij moeten de volgende verplichtingen worden nageleefd:

- Het register moet op schrift beschikbaar zijn, waarvan tenminste in digitale vorm (art. 30 lid 3 AVG);
- De verwerkingsdoeleinden moeten welbepaald zijn en uitdrukkelijk omschreven worden (art. 5 lid 1 sub b AVG);
- De categorieën van persoonsgegevens volstaan niet met een enkel onderscheid tussen algemeen en bijzonder;
- Het register moet desgevraagd ter beschikking van de AP worden gesteld.

Uit het onderzoek naar de verwerkingsactiviteiten binnen de VECOZO-diensten Certificatenbeheer, Aanlevering Verzekerdengegevens en Berichtenbox is gebleken dat VECOZO enkel voor Certificatenbeheer en voor een klein onderdeel van de Berichtenbox als verwerkingsverantwoordelijke kan worden aangemerkt. Voor deze diensten zal VECOZO moeten voldoen aan de eisen uit artikel 30 lid 1 AVG (zie kader hierboven).

Voor het overige van deze diensten is VECOZO verwerker en volstaat juridisch gezien de beperktere registerplicht van artikel 30 lid 2 AVG (zie kader hierboven).

Voor de drie onderzochte diensten zou de uiteenzetting van de categorieën van persoonsgegevens, categorieën van verwerkingen en de doeleinden er als volgt uit moeten komen zien. Voor de diensten waar VECOZO verwerker is, moet er per dienst benoemt worden voor welke verwerkingsverantwoordelijke de verwerkingen gedaan worden.

De categorieën van persoonsgegevens moeten in algemeen duidelijke termen worden geformuleerd en mogen niet té generaal zijn. Bijzondere persoonsgegevens kunnen in het geval van VECOZO het best apart genoemd worden. In dit geval het BSN-nummer.

	Categorie voor persoonsgegevens	**Soort verwerking**	**Verwerkingsdoel**
Certificatie beheer	- Voor- en achternaam - Contactgegevens (e-mailadres) - Gebruikersgegevens (gebruikersnummer en wachtwoord) - Metadata	- Verzamelen - Opslaan - Combineren - Vernietigen - Opvragen - Doorzenden	Authenticiteit van de persoonlijke gebruiker of systeemgebruiker controleren
AVG	- BSN - Verzekerdengegevens - NAW-gegevens - Geboortedatum - Gevoelige gegevens (Premieachter-stand/opschorting verzekering) - Metadata	- Verzamelen - Opslaan - Ter beschikking stellen - Vernietigen - Raadplegen	N.V.T.
Berichtenbox als verwerker	- Metadata - Berichtinhoud	- Verzamelen - Opslaan - Raadplegen - Verwijderen	N.V.T.
Berichtenbox als verantwoordelijke	Contactgegevens	Raadplegen	maken van berichten-uitwisseling tussen zorgpartijen

- Indien de dienst AVG (of een andere dienst) in de toekomst persoonsgegevens ter beschikking gaat stellen aan bijvoorbeeld de in paragraaf 3.2.3 genoemde Belgische partij of een andere buitenlandse partij, moet dit worden opgenomen in de registers.

5.2 Conclusie ten aanzien van beveiligingsmaatregelen

De getroffen technische en organisatorische beveiligingsmaatregelen die binnen VECOZO worden gehanteerd zijn voor beide varianten van het register verplicht en zullen dus voor elke dienst geregistreerd moeten worden. Per dienst zijn deze tenminste als volgt:

Certificatiebeheer	AVG	Berichtenbox
- Gebruik van een ISO27001:2013 gecertificeerde TCA (KPN) - Twee factor authenticatie (privacy by design) - Uitgifte van Certificaten - Hantering NEN 7510:2011 - Pseudonimisering gebruikers	- Certificering - Versleuteling van persoonsgegevens - Dataminimalisatie (privacy by design) - Hantering NEN 7510:2011 - Technische controles - Hanteren tolerantiegrens op fouten van 0,1%	- Versleuteling van persoonsgegevens - Technische controles - Certificering - Pseudonimisering in de logging bij oplossen technische incidenten

In het kader van de getroffen maatregelen zijn tijdens het onderzoek de volgende bijzonderheden geconstateerd:

- VECOZO is met de gebruikers van de Berichtenbox overeengekomen dat persoonsgegevens die onderhevig zijn aan het medisch beroepsgeheim niet uitgewisseld mogen worden. Er wordt hier niet op gecontroleerd en dit kán ook niet, omdat de inhoud van de verstuurde berichten versleuteld is. Daarnaast is het niet expliciet opgenomen in de gebruiksvoorwaarden, toch het meest eenvoudig te raadplegen document voor gebruikers maar wel in de dienstbeschrijving.
- VECOZO controleert niet of de huidige gebruiker van een certificaat nog steeds dezelfde is als de oorspronkelijke aanvrager. Dit zou wel moeten op basis van artikel 24 van de eIDAS-verordening en zou bijdragen aan het vervullen van de eisen van artikel 32 AVG, met name sub b en d.

5.3 Conclusie ten aanzien van bewaartermijnen

Voor Certificatenbeheer en het stukje Berichtenbox waarvoor VECOZO verwerkingsverantwoordelijke is, moeten de bewaartermijnen worden vastgelegd in het register. Voor de Berichtenbox is geen bewaartermijn van toepassing, omdat die zijn gegevens rechtstreeks ophaalt uit de database van Relatiebeheer en niet binnen de dienst bewaart. Voor Certificatenbeheer bedraagt dit maximaal 2 jaar en één maand.

Voor de dienst AVG en het deel Berichtenbox waar VECOZO verwerker van is, is het niet verplicht om bewaartermijnen op te nemen in het register.

5.4 Conclusie ten aanzien van categorieën ontvangers

Deze registerplicht valt ook alleen op verwerkingsverantwoordelijken en hoeft dus alleen bij Certificatenbeheer en een deel van Berichtenbox te worden uitgevoerd. Het gaat hier enkel om diegenen die persoonsgegevens ontvangen waar VECOZO verwerkingsverantwoordelijke voor is.

Certificatiebeheer	Berichtenbox
- Dienst Relatiebeheer - KPN (TCA) - Andere VECOZO-diensten	- Gebruikers

5.5 Conclusie ten aanzien van categorieën van betrokkenen

Deze categorie hoeft eveneens enkel door de verwerkingsverantwoordelijke te worden geregistreerd. De categorieën van betrokkenen waar VECOZO binnen Certificatenbeheer en Berichtenbox persoonsgegevens van verwerkt zijn:

Certificatiebeheer	Berichtenbox
- Gebruikers	- Gebruikers

5.6 Algemene conclusie ten aanzien van het register in samenhang met de verantwoordingsplicht

Alle hierboven uitgewerkte onderdelen moeten geïntegreerd worden in één (schriftelijk) register. Echter is het, om alle verantwoordingsinstrumenten op een effectieve wijze samenhangend in te zetten, verstandig om niet vast te houden aan de juridische ondergrens.

Een verwerker hoeft, strikt juridisch gezien, niet op te nemen welke persoonsgegevens hij verwerkt maar slechts welke verwerking hij daarmee doet (verzamelen, opslaan, vernietigen). Andersom hoeft een verwerkingsverantwoordelijke alleen maar te registreren welke persoonsgegevens hij verwerkt, maar niet wat hij daar mee doet.

Dat is niet in lijn met het transparantiebeginsel van de AVG, noch geeft het een compleet beeld wanneer de Autoriteit Persoonsgegevens inzicht wil verkrijgen in welke persoonsgegevens er allemaal worden verwerkt binnen een organisatie.

Daarnaast is het voor een bedrijf als VECOZO niet praktisch om een register bij te houden waarin halve waarheden staan. Zo zal men bij het uitvoeren van een op grond van de AVG verplichte PIA, alsnog in alle hoeken van de organisatie op zoek naar de benodigde informatie moeten.

Als men nèt iets meer opneemt in het verwerkingsregister dan wettelijk verplicht, kan een

medewerker die een (voorgestelde) nieuwe verwerking wil implementeren, het register raadplegen of de betreffende verwerking in een dergelijke samenstelling misschien al wordt gedaan. Na advies van de FG kan deze nieuwe verwerking dan wellicht zonder dat een PIA verplicht is worden geïmplementeerd. Andersom bekeken, indien de conclusie dat een PIA toch moet worden uitgevoerd, kan de uitkomst van de PIA rechtstreeks worden opgenomen in het verwerkingsregister.

Concluderend zijn er drie duidelijke redenen waarom het verstandig is om méér in het register op te nemen dan verplicht:

- Het sluit meer aan bij het in de AVG belangrijk geachte transparantiebeginsel;
- Het geeft een completere invulling aan de verantwoordingsplicht van de AVG;
- Het is praktisch en overzichtelijk voor de organisatie zelf om informatie op een plaats onder te brengen.

In paragraaf 4.2 van dit onderzoek worden al enkele suggesties gedaan die het verwerkingsregister tot een aanwinst voor de organisatie kunnen verheffen, maar “the sky is the limit.” Zolang het de inzichtelijkheid van het register maar niet beperkt. Want let wel, dan zou de AP zomaar eens niet tevreden kunnen zijn en dat wil je voorkomen (iets met tien miljoen euro).

Tot slot is het samenvoegen van de op grond van artikel 30 lid 1 en lid 2 AVG verplichte gegevens, een kleine moeite. Voor de benodigde informatie moet men vaak op exact dezelfde plaatsen zoeken en vaak is deze al in een geïntegreerde vorm beschikbaar.

HOOFDSTUK 6 - AANBEVELINGEN

Hieronder volgt een uiteenzetting van de aanbevelingen die worden gegeven op basis van hetgeen dit rapport concludeert. Deze aanbevelingen zijn gedaan tegen een juridische achtergrond en met als doel een praktische en efficiënte invulling te geven aan de verantwoordingsplicht van VECOZO en meer specifiek de registerplicht van artikel 30 AVG.

6.1 Algemene aanbevelingen ten aanzien van de verantwoordingsplicht

1. Indien de dienst Aanlevering Verzekerdengegevens (of een andere dienst) in de toekomst persoonsgegevens ter beschikking gaat stellen van een buitenlandse partij (zie paragraaf 3.2.3, hierin wordt gesproken van een mogelijke Belgische partner), moet VECOZO dit nadrukkelijk verwerken in de registers. Dit is een harde, minimale eis in artikel 30 AVG. Daarnaast moet VECOZO voor deze verwerkingen hoofdstuk V van de AVG in acht houden.

2. Neem het verbod op het uitwisselen van persoonsgegevens die onderhevig zijn aan het medisch beroepsgeheim, expliciet op in de gebruiksvoorwaarden van de Berichtenbox. Door dit te doen roept VECOZO een extra waarborg in het leven voor de privacy van de betrokkenen. Dit is een vorm van privacy by design dat bijdraagt aan de verantwoordingsplicht van VECOZO.

3. Voer actieve controle, op routinebasis uit op het gebruik van VECOZO-certificaten en of deze nog wel gebruikt worden door de oorspronkelijke aanvrager. Bouw eventueel een herinnering bij het register in die waarschuwt wanneer weer een controle uitgevoerd moet worden. Momenteel voldoet VECOZO niet aan deze verplichting uit de eIDAS-verordening en dat valt evengoed onder de verantwoordingsplicht.

4. Ga na welke verwerkingen er gebaseerd zijn op de toestemming van de betrokkenen. De AVG stelt strengere eisen aan toestemming. Evalueer daarom de manier waarop u toestemming vraagt, krijgt en registreert. Pas deze wijze indien nodig aan. Nieuw is dat u moet kunnen aantonen dat u geldige toestemming van mensen heeft gekregen om hun persoonsgegevens te verwerken. En dat het voor mensen net zo makkelijk moet zijn om hun toestemming in te trekken als om die te geven.

6.2 Aanbevelingen ten aanzien van het beleid rondom het register

1. Wijs een verantwoordelijke aan die er voor moet zorgen dat het verwerkingsregister compliant is en blijft aan de AVG. Deze “Register eigenaar” moet worden aangesteld of intern worden opgeleid en bekend zijn/worden met alles dat te maken heeft met de verantwoordelijkheidsplicht uit de AVG. Hij of zij is eindverantwoordelijk en neemt de benodigde maatregelen in het kader van compliancy maar hoeft het niet te doen zonder ondersteuning.

2. Wijs voor iedere dienst een verantwoordelijke, idealiter de product owners, aan die zorgt dat vernieuwingen in processen of verwerkingen op de juiste manier in het verwerkingsregister worden geïmplementeerd. De product owners zijn het meest geschikt voor deze rol omdat zij het best kunnen inschatten wat voor gevolgen wijzigingen hebben voor de processen en de organisatie van hun dienst.
   Zij moeten wel bewust worden gemaakt van de verantwoordingsplicht en worden getraind

in het herkennen van de implicaties van deze plicht op hun dienst. Dit rapport kan daarvoor als een goede start dienen. Daarnaast zijn in dit rapport diverse organen, andere rapporten en bronnen genoemd die kunnen bijdragen aan verdere opleiding. Tot slot zorgt de grote impact van de AVG op het Europese privacylandschap ervoor dat er talloze trainingen op dit gebied worden aangeboden. Zijn of haar eerste taak wordt het inventariseren van alle verwerkingen binnen zijn of haar dienst en deze op de juiste wijze implementeren in het template register dat bij dit rapport wordt aangeboden.

3. Start per direct met het hierboven genoemd inventarisatieproces! Per dienst is al redelijk veel informatie beschikbaar in dienstbeschrijvingen maar controleer ook of dit allemaal nog kloppend is. Misschien is er iets over het hoofd gezien of is iets ten onrechte wel of niet als verwerking aangemerkt.

4. Creëer draagvlak. Het is belangrijk om diegenen die VECOZO op gaat leiden/aanstellen om de verantwoordingsplicht in goede banen te leiden, in te laten zien wat voor praktische voordelen het verwerkingsregister kan bieden, mits goed uitgevoerd.

5. Zorg ervoor dat het up-to-date houden van het verwerkingsregister wordt verplicht en neem dit op in het Privacybeleid van VECOZO. Op grond van de AVG moet VECOZO voldoen aan een verantwoordingsplicht, het register is daar een onderdeel van. Het opnemen van bovenstaande verplichting in het Privacybeleid is bedoeld als bewijs naar de Autoriteit Persoonsgegevens dat het register dat zij onder ogen krijgen ook actueel is en biedt continuïteit in je verantwoordingsplicht.

6.3 Aanbevelingen ten aanzien van de inrichting van het register

Een aantal van de onderstaande aanbevelingen bevatten onder meer voorstellen omtrent het ontwikkelen van een tool/mechanisme om de verantwoordingsinstrumenten uit de AVG samenhangend en geïntegreerd in te zetten. Dit zijn IT-oplossingen voorgesteld door een jurist en zijn niet voorzien van een haalbaarheidstoets op het gebied van ontwikkeling/IT-design maar zijn puur gericht op de mogelijke inrichting.

- Scheidt de categorieën van persoonsgegevens en categorieën van verwerkingen niet van elkaar. Dit is onduidelijk en geeft in iedere situatie een onvolledig beeld. Wat is het nut van het aantonen dat je een BSN-nummer verwerkt, als je niet aantoont of je dit opslaat, verwijdert of zelfs doorzend? Andersom is het nutteloos om aan te tonen dat je als verwerker ten behoeve van een verwerkingsverantwoordelijke persoonsgegevens verzameld als je niet ook aantoont welke persoonsgegevens dat dan precies zijn. Denk ook aan het transparantiebeginsel!

- Bij twijfel of een bepaald persoonsgegeven onder een bestaande categorie valt, of afzonderlijk moet worden opgenomen in het register, kies altijd voor het laatste. Er is geen bovengrens voor het verwerkingsregister, maar wel een wettelijke grens, daar wil je niet onder zitten. Een uitgebreider register is niet alleen meer in overeenstemming met het transparantiebeginsel en de verantwoordingsplicht, het integreren van veel informatie biedt ook praktische voordelen voor VECOZO.

- Creëer een register voor de activiteiten waarin VECOZO optreed als verwerker én een register voor de activiteiten waar VECOZO verwerkingsverantwoordelijke voor is. Plaats

deze registers wel in hetzelfde bestand maar zorg dat ze ook afzonderlijk toegankelijk zijn.

- Er kan van de vorige aanbeveling worden afgeweken indien een volledig geïntegreerd verwerkingsregister de voorkeur van VECOZO geniet. Dit kost in de implementatiefase aanzienlijk meer middelen, maar levert op den duur wel meer praktische voordelen op. De aanbevelingen/suggesties voor zo'n geïntegreerd verwerkingsregister staan hieronder.

- Het wordt aanbevolen om in Excel of een vergelijkbare tool alle vereiste onderdelen van het register aan te leggen. Aan de hand hiervan kan een gebruiksvriendelijke database of applicatie ontwikkeld worden die naast het register bijvoorbeeld ook de capaciteit heeft om reeds uitgevoerde PIA's en verwerkersovereenkomsten in op te nemen.

- Bovenstaande database moet een volledige integratie van deze bestanden kunnen ondersteunen. Ook moet de database interactief zijn. Dat wil zeggen dat een uitgevoerde PIA of een in de database geüploade verwerkersovereenkomst automatisch in het register verwerkt wordt. De database/applicatie geeft een melding wanneer verplichte velden in het register leeg blijven, op deze wijze wordt automatisch gecontroleerd of de verwerkersovereenkomst conform artikel 28 AVG is. Want: blijft een veld leeg, is er blijkbaar niks afgesproken over bijvoorbeeld de beveiligingsmaatregelen. Daarnaast kan, door te staven aan de in de database geïntegreerde beleidsregels van het AP, worden gecontroleerd of de PIA op een juiste wijze is uitgevoerd.

- Bouw in deze database een automatische klok die een melding geeft wanneer het tijd is om een controle uit te voeren of de organisatorische- en technische beveiligingsmaatregelen getest en geëvalueerd moeten worden (zoals: worden de uitgegeven certificaten nog wel gebruikt door de oorspronkelijke aanvrager?). Deze klok kan bijvoorbeeld ook melding geven over aflopende verwerkersovereenkomsten.

6.4 Een template verwerkingsregister

Tot slot is er ter concretisering van het bovenstaande een template ontwikkeld in Excel dat kan dienen als een eerste opzet van het verwerkingsregister. Deze templates zijn voor de onderzochte diensten en op schrift bijgevoegd in de bijlagen. Een digitaal bestand is eveneens beschikbaar voor VECOZO waar de drie templates zijn samengevoegd tot een bestand met twee tabbladen (een voor de activiteiten als verwerkingsverantwoordelijke en een voor de activiteiten als verwerker):

- De template voor VECOZO als verwerker van de dienst AVG is opgenomen in bijlage XI.
- De template voor VECOZO als verwerker voor de dienst Berichtenbox is opgenomen in bijlage XI.
- De template voor VECOZO als verantwoordelijke voor de dienst Certificatenbeheer is opgenomen in bijlage XII.

Naast de template is in bijlage X een tabel opgenomen die als richtlijn dient voor het indelen in categorieën van betrokkenen, ontvangers, persoonsgegevens en verwerkingen.

BRONNENLIJST

LITERATUUR

Autoriteit Persoonsgegevens 2017
Autoriteit Persoonsgegevens, In 10 stappen voorbereid op de AVG, 2017

Berkvens 2016
Prof. mr. J.M.A. Berkvens, *Transparantie, informatievoorzieningen en toestemming*, 2016

Bijron 2016
Z. Bijron, *Toestemming als grondslag voor gegevensverwerking*, 2016

Byte 2015
Whitepaper Byte, *Hoe houd je hackers buiten?*, 2015

Comijs, P&I 2016, afl. 6, p.252
D.E. Comijs, 'Accountability in de AVG: Betere processen en een sterkere positie van betrokkenen', *P&I* 2016, afl. 6, p. 252

Dammers 2013
Mr. W. Dammers, *Is een (gehasht) wachtwoord een persoonsgegeven?*, 2013

Demmel, 2016
Dr. A. Demmel, *Maintaining a record of data processing activities under the GDPR*, 2016

Eding 2017
J. Eding, *Privacy: Bewaartermijnen uitgelegd*, 2017

Europa Decentraal 2016
Europa Decentraal, *Gegevensbescherming en de AVG*, 2016

Felz 2016
D. Felz, *German DPA's to create model processing records for GDPR compliance*, 2016

Hennekens 2017
M. Hennekens, *Tien dingen die u niet wilt, maar wel moet weten over de Privacy-verordening*, 2017

Holvast, P&I 2016, afl. 6, p.237
J. Holvast, 'Redactioneel' P&I 2016, afl. 6 p.237

Jak 2014
N. Jak, *Semipublieke instellingen. De juridische positie van instellingen op het snijvlak van overheid en samenleving,* Den Haag: Boom Juridische uitgevers 2014

Jansen 2017
Mr. M. Jansen, *Onbedoelde introductie lastige puzzels vanwege extraterritoriale werking Nederlands privacyrecht in Uitvoeringswet AVG*, 2017

De Jong, Regelmaat 2015, afl. 1, p.11
Mr. dr. J.P. de Jong, 'De Algemene verordening gegevensbescherming', Regelmaat 2015, afl.1, p. 11

Mahmood 2016
Sabba Mahmood, *Getting to know the GDPR, Part 6 – Designing for compliance*, 2016

Van der Meulen & van Zoonen 2015
H. van der Meulen & Prof. Dr. E.A. van Zoonen, *"Meer controle door burgers over hun persoonsgegevens"*, Den Haag: Ministerie van Binnenlandse Zaken, 2015

Van Schaijk 2015
G. van Schaijk, Praktijkgericht juridisch onderzoek, Den Haag: Boom Juridische uitgevers, 2015

Talen, 2017
Mr. R. Talen, *Het verwerkingsregister*, 2017

Tran 2017
W. Tran, *De ins en outs van het verwerkingsregister (artikel 30 AVG)*, 2017

WP29 2017
Article 29 Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, 2017

WP29 2013
Article 29 Data Protection Working Party, *"Opinion on purpose limitation",* 2013

WP29 2007
Article 29 Data Protection Working Party,*"Opinion on the concept of personal data"*, 2007

RECHTSBRONNEN

Wetten, verordeningen en verdragen:

AVG
Algemene Verordening Gegevensbescherming
BW
Burgerlijk Wetboek
eIDAS
Verordening betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt
UAVG
Uitvoeringswet Algemene Verordening Gegevensbescherming (Wetsvoorstel)
VWEU
Verdrag omtrent de werking van de Europese Unie
Wbp
Wet bescherming persoonsgegevens
Wet BSN-z
Wet gebruik Burgerservicenummer in de zorg

Richtlijnen:
Richtlijn 95/46/EG (Privacyrichtlijn)
Overige:

Raad 2012
Interinstitutioneel dossier: "Standpunt van de Raad in eerste lezing op vaststellen AVG", 2012.
Kamerstukken II, 1997-1998, 25-892, nr.3 p.20.
MvT Concept UAVG, paragraaf 3.2.3, p. 39.

JURISPRUDENTIE

HR 23 maart 2010, ECLI:NL:PHR:2010:BK6331

WEBSITES

www.autoriteitpersoonsgegevens.nl
www.dwangindezorg.nl
www.forumstandaardisatie.nl
www.kaspersky.com
www.pseudonimiseer.nl
www.vecozo.nl
www.vektis.nl