Privacy geldt waar gezondheid telt!

‘Een toetsing van het beleid en de werkwijze van de GGD Hart voor Brabant aan huidige- en in de toekomst in te voeren privacywet- en regelgeving’

GGD Hart voor Brabant

Marlin van Dinther

Den Bosch, 9 januari 2017

Privacy geldt waar gezondheid telt!

‘Een toetsing van de werkwijze van de GGD Hart voor Brabant aan huidige- en in de toekomst in te voeren privacywet- en regelgeving’

Auteur:	Marlin van Dinther
Onderwijsinstelling	Juridische Hogeschool Avans-Fontys te Tilburg
Afstudeerorganisatie	GGD Hart voor Brabant
Afstudeermentor	René van Kessel
1e docent	Mevrouw mr. M.E.R van Remortel
2e docent	Mevrouw mr. C.A.M van der Voort

Den Bosch, 9 januari 2017

Voorwoord

Voor u ligt het onderzoeksrapport ‘Privacy geldt waar gezondheid telt’, ‘Een toetsing van de werkwijze van de GGD aan huidige- en in de toekomst in te voeren privacywet- en regelgeving’’. Dit onderzoek is uitgevoerd in opdracht van de GGD Hart voor Brabant (hierna: de GGD).

In het kader van het afstuderen voor de opleiding HBO rechten aan de Juridische Hogeschool te Tilburg, heb ik gezocht naar een actueel onderwerp om praktijkgericht juridisch onderzoek naar te doen. Aangezien er in het privacyrecht een en ander is gewijzigd en er in de nabije toekomst nog meer wijzigingen volgen, vond ik dit een voldoende actueel onderwerp.

De keuze om te solliciteren bij de GGD heb ik gemaakt, omdat hier veel gewerkt wordt met bijzondere persoonsgegevens. Dit maakt het onderzoek voor mij interessanter en geeft diepgang aan het onderwerp.

Het was erg interessant om de medewerkers van de GGD te spreken over dit onderwerp en zelfstandig een onderzoek uit te voeren binnen een grote organisatie als deze. In de titel is de slogan van de GGD verwerkt. Op de interne website van de GGD staat de slogan: ‘Gezondheid telt!’.

Dit onderzoek is de afsluiting van mijn rechtenstudie. In dit onderzoek breng ik in de praktijk wat ik geleerd heb in de afgelopen jaren. Dit had ik nooit kunnen waarmaken zonder de hulp van verschillende mensen. In de eerste plaats wil ik René van Kessel bedanken voor de begeleiding vanuit de GGD. In het bijzonder voor het meedenken in het kader van dit onderzoek en de tijd die hij heeft gestoken in het bespreken van de resultaten. Daarnaast wil ik Maud van Remortel bedanken. Dankzij haar inhoudelijke feedback en de sturing die zij heeft gegeven vanuit de opleiding heb ik dit onderzoeksrapport op kunnen leveren. Daarnaast wil ik alle andere mensen bedanken die betrokken zijn geweest bij het tot stand komen van dit onderzoek.

Ik wens u veel plezier met het lezen van dit onderzoeksrapport.

Marlin van Dinther

Inhoudsopgave

Samenvatting

De GGD Hart voor Brabant (hierna: de GGD) is de gemeentelijke gezondheidsdienst voor 27 gemeentes in de regio Midden-Brabant en Brabant-Noord. Door de GGD wordt gewerkt aan de gezondheid van de inwoners van de regio. Hierbij is speciale aandacht voor bepaalde risicogroepen.

Bij de GGD vindt op grote schaal verwerking van persoonsgegevens plaats. Het gaat hierbij veelal om een bijzondere categorie persoonsgegevens, namelijk gegevens over de gezondheid van personen. De GGD heeft door de verwerking van deze gegevens te maken met wet- en regelgeving op het gebied van privacy. De voornaamste regeling in dat kader is op dit moment de Wet bescherming persoonsgegevens (hierna: Wbp). Deze regeling is gebaseerd op een Europese richtlijn die dateert uit 1995. Omdat de richtlijn, en daarom ook de daarop gebaseerde Wbp is verouderd, heeft de Europese Unie een Verordening gemaakt, de Algemene Verordening Gegevensbescherming (hierna: AVG). Aan deze verordening moet de GGD vanaf 25 mei 2018 voldoen, omdat de AVG de Wbp zal gaan vervangen.

Dit onderzoek geeft een overzicht van het beleid en de werkwijze van de GGD op het gebied van de verwerking van persoonsgegevens binnen 6 systemen die gebruikt worden door de GGD. HP Zone, Kidos, Tubis, Orion Globe, Orion Forensisch en Topdesk Klantcontactcentrum zijn de systemen die in dit onderzoek zijn betrokken. Daarnaast bevat het onderzoek een toetsing aan zowel huidige als in de toekomst in te voeren wet- en regelgeving.

Om aan de Wbp te voldoen moet er door de GGD een aantal wijzigingen worden doorgevoerd. In de eerste plaats moet er beleid worden opgesteld dat alle aspecten van de verwerking van persoonsgegevens bevat. Op dit moment is er niet voldoende geformuleerd beleid. Bovendien is het bewustzijn van medewerkers niet voldoende. Voor het systeemTopdesk KCC moet bijvoorbeeld een concreet doel worden geformuleerd op basis waarvan de persoonsgegevens worden verwerkt. De wettelijke grondslag voor de verwerking van persoonsgegevens is in de meeste gevallen de wettelijke plicht. In de gevallen dat echter de veronderstelde toestemming wordt gebruikt als grondslag voor de verwerking, moet deze toestemming daadwerkelijk worden gevraagd aan klanten. Daarnaast moet voor de verschillende systemen een bewaartermijn worden geformuleerd en moet er een manier worden gevonden om deze bewaartermijn daadwerkelijk te handhaven. Wat betreft de beveiliging van persoonsgegevens ligt er een grote taak bij de medewerkers. Zij moeten verantwoord omgaan met de verwerking van persoons-gegevens. Bovendien moet er bij het klantcontactcentrum, waar gewerkt wordt met het systeem Topdesk KCC, gezorgd worden voor extra accounts voor het onderdeel reizigers. Op die manier kan iedere werknemer op een eigen account inloggen. Om aan het recht op informatie dat de betrokkene heeft, tegemoet te komen, hoeft de GGD juridisch gezien geen actie te ondernemen. Wel kan er voor de systemen Orion Globe en HP Zone een standaard manier worden ontwikkeld om aan dit recht tegemoet te komen. Voor de andere systemen is een dergelijke procedure al aanwezig. De GGD voldoet aan de eisen voor het verwerking van bijzondere persoonsgegevens. Op dat punt hoeft niets te veranderen. Om aan de meldplicht datalekken te voldoen moeten medewerkers goed geïnformeerd worden over wanneer er sprake is van een datalek. Bovendien moet de Functionaris Gegevensbescherming (hierna: functionaris) telkens de afweging maken of dit datalek gemeld moet worden aan de Autoriteit Persoonsgegevens en de betrokkene. De rol van de functionaris binnen de GGD moet meer actief worden.

Om aan de AVG te voldoen moet de GGD voor 25 mei 2018 een aantal wijzigingen doorvoeren. Daar waar de verwerking van persoonsgegevens zijn grondslag vindt in de veronderstelde toestemming moet, voor de AVG de Wbp vervangt, een verandering

plaatsvinden. De toestemming van klanten voor de verwerking van persoonsgegevens moet door een actieve handeling worden gegeven. De GGD moet een standaardformulier opstellen aan de hand waarvan de toestemming van klanten wordt gevraagd. Daarnaast moet er een documentatie worden gemaakt van alle verwerking van persoonsgegevens die plaatsvindt. Op de GGD rust op grond van de AVG bovendien een informatieplicht. Om aan deze plicht te voldoen moet de GGD in het zojuist genoemde standaardformulier tevens de aspecten opnemen die zorgen dat aan de informatieplicht wordt voldaan. De organisatie moet bovendien een gegevensbeschermingseffectenbeoordeling laten uitvoeren door specialisten. Middels deze beoordeling moet tevens worden nagegaan of de bescherming van persoonsgegevens optimaal is binnen de organisatie.

De rol van de functionaris wordt door de invoering van de AVG uitgebreid. Er zijn meer taken die de functionaris moet uitvoeren dan bij de Wbp het geval was. Ook wat betreft de meldplicht datalekken is een wijziging van belang voor de GGD. De GGD is op grond van de AVG verplicht om een documentatie bij te houden van alle datalekken. Dit is anders dan bij de Wbp, waar het enkel verplicht was om meldingsplichtige datalekken te documenteren.

Lijst van afkortingen

Wbp	Wet bescherming persoonsgegevens
WGBO	Wet op de geneeskundige behandelingsovereenkomst
EU	Europese Unie
AVG	Algemene Verordening Gegevensbescherming
EVRM	Europees Verdrag voor de Rechten van de Mens
VWEU	Verdrag betreffende de werking van de Europese Unie
UVRM	Universele Verklaring van de Rechten van de Mens
IVBPR	Internationaal verdrag inzake burgerrechten en politieke rechten
Wet BIG	Wet op de beroepen in de individuele gezondheidszorg
JGZ	Jeugdgezondheidzorg
AP	Autoriteit Persoonsgegevens
TBC	Tuberculose
FG	Functionaris voor de gegevensbescherming
PIA	Privacy Impact assessment
KCC	Klantcontactcentrum

Begrippenlijst

Persoonsgegeven
Alle gegevens betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Een persoon is identificeerbaar wanneer de identiteit van de betrokken persoon zonder onevenredige inspanning kan worden vastgesteld.[1]

Verwerking
Dit begrip heeft betrekking op het hele proces dat een persoonsgegeven doormaakt vanaf het moment van verzamelen van een gegeven tot aan het moment van vernietigen.[2]

Bestand
Een bestand is 'elk gestructureerd geheel van persoonsgegevens dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen'. Er moet een samenhang zijn tussen gegevens en het systeem moet systematisch toegankelijk zijn. Bij niet-geautomatiseerde verwerking van persoonsgegevens vallen enkel bestanden onder de Wbp.[3]

Betrokkene
De persoon op wie een persoonsgegeven betrekking heeft.

Verantwoordelijke
De persoon die in juridische zin bevoegd is om doel en middelen van gegevensverwerking vast te stellen. Het is de natuurlijke persoon of rechtspersoon die verantwoordelijk is voor de verwerking.

Bewerker
Degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt. Dit is niet iemand die in hiërarchische verhouding staat tot de verantwoordelijke. De bewerker handelt in overeenstemming met instructies van de verantwoordelijke.[4]

Derde
Iedereen die niet valt onder de categorieën genoemd in artikel 1 van de Wbp.

De Autoriteit Persoonsgegevens
Een bestuursorgaan dat toezicht houdt op de naleving van de wettelijke regels voor bescherming van persoonsgegevens.[5]

De GGD
De gemeentelijke gezondheidsdienst. In het kader van dit onderzoek wordt met de GGD gedoeld op de GGD Hart voor Brabant.

Richtlijn
Een richtlijn wordt op Europees niveau vastgesteld en heeft geen rechtstreekse werking in Nederland. Het doel van een richtlijn is het harmoniseren van wetgeving binnen de EU. Een richtlijn moet worden omgezet naar nationaal recht voordat het werking heeft binnen een lidstaat.

Verordening
Een verordening heeft rechtstreekse werking in lidstaten van de EU. Een verordening

[1] H. Kranenborg 2011, p. 60.
[2] H. Kranenborg 2011, p. 61.
[3] H. Kranenborg 2011, p. 67.
[4] H. Kranenborg 2011, p. 78.
[5] www.autoriteitpersoonsgegevens.nl

maakt dus direct deel uit van de rechtsorde van Nederland zonder dat hiervoor omzetting is vereist. Het doel van een verordening is eenmaking van wetgeving binnen de lidstaten van de EU. Bij strijdigheid gaat een verordening boven nationale wetten.

Hoofdstuk 1. Inleiding

1.1 Organisatie

Gemeentes in Nederland zijn op grond van de Wet publieke gezondheid verplicht om middels gemeentelijke regeling een GGD in te stellen.[6] De GGD Hart voor Brabant is een organisatie waarin gewerkt wordt aan de gezondheid van inwoners binnen de regio. Hierbij heeft hij speciale aandacht voor risicogroepen. Het werkgebied van de GGD Hart voor Brabant bestaat uit 27 gemeentes binnen regio Midden-Brabant en Brabant-Noord.

Waar bij de GGD in de eerste plaats gedacht wordt aan de jeugdgezondheidszorg, reizigersvaccinaties en soa testen, is de GGD veel meer dan dat. De GGD richt zich op de publieke gezondheid in zijn geheel. Ook wanneer er rampen plaatsvinden, wanneer een arrestant medische zorg nodig heeft of wanneer er epidemieën uitbreken staat de GGD voorop met het bieden van de nodige zorg.

1.2 Probleemomschrijving

Met regelmaat schrijven de kranten over datalekken bij grote bedrijven. Een recent voorbeeld is het bericht van 2 mei 2016 over de GGD IJsselland.[7] Een onbeveiligde USB-stick met daarop persoonsgegevens was zoek geraakt tijdens het versturen per post, een datalek. Voor de GGD IJsselland was dit incident reden om het beleid rond privacy nog eens tegen het licht te houden. Het is mogelijk dat het beleid en de werkwijze niet voldoen aan de huidige wet- en regelgeving in het kader van het recht op privacy.

De GGD Hart voor Brabant (hierna: de GGD), de opdrachtgever van dit onderzoek, voert de publieke gezondheidszorg uit voor de gemeenten in zijn werkgebied en die gemeenten betalen de GGD daarvoor. Als de gezondheidsadviseur van de overheid geeft de GGD advies over het opstellen van beleid om de gezondheid van de bevolking te kunnen verbeteren.[8]
Binnen de GGD wordt veel gewerkt met persoonsgegevens. Het gaat hierbij vaak om medische gegevens. Deze gegevens betreffende de gezondheid van personen zijn zogenaamde “bijzondere persoonsgegevens”.[9] Voor deze gegevens gelden op grond van de Wet bescherming persoonsgegevens (hierna: Wbp) strengere eisen als het gaat om de bevoegdheid deze te verwerken. Daarnaast is de Wet op de Geneeskundige Behandelings-overeenkomst (hierna: WGBO) van toepassing op deze medische gegevens, waardoor onder andere een geheimhoudingsplicht geldt voor bepaalde zorgverleners.

De huidige Wbp is gebaseerd op een Europese richtlijn die dateert uit 1995.[10] Op het moment dat deze richtlijn werd opgesteld, was het internet nog maar sinds kort toegankelijk voor commerciële doeleinden. Inmiddels is in de Wbp per januari 2016 een aantal aanpassingen gedaan om vooruit te lopen op een verordening die op Europees niveau is vastgesteld. Deze verordening zal in de toekomst de Wbp gaan vervangen. De verordening zal vanaf 25 mei 2018 rechtstreeks van toepassing zijn in alle EU-lidstaten.[11] De Verordening moet een hoger niveau van bescherming gaan bieden aan

[6] Artikel 14 Wet publieke gezondheid.
[7] Verdwenen USB-stick brengt GGD in verlegenheid, *Algemeen Dagblad* 2 mei 2016, ad.nl.
[8] Missie en visie, intranet de GGD Hart voor Brabant.
[9] Artikel 16 Wet Bescherming Persoonsgegevens.
[10] *PbEG* 1995, C 93/1.
[11] Autoriteitpersoonsgegevens.nl (zoek op *Europese privacywetgeving*).

persoonsgegevens. Een mogelijk gevolg daarvan is dat er zwaardere plichten zullen zijn voor de verwerkers van de persoonsgegevens.[12]

Binnen de GGD is behoefte aan duidelijkheid over het te voeren privacybeleid. Op dit moment wordt er binnen de verschillende afdelingen op verschillende wijze omgegaan met de verwerking van persoonsgegevens. Er wordt hard gewerkt aan het op orde stellen van het privacybeleid. Dat blijkt onder andere uit het beleidsplan onderdeel informatieveiligheid 2015-2017 (zie bijlage I).[13] Er is geen duidelijk, eenduidig beleid dat door medewerkers kan worden geraadpleegd als het gaat om de verwerking van persoonsgegevens.

Doordat er onlangs wettelijk een en ander gewijzigd is en er in de toekomst een nieuwe verordening in werking zal treden, is het zaak om het te voeren beleid op het gebied van privacy up-to-date te maken. Er is behoefte aan een toetsing van het huidige beleid en de huidige werkwijze aan wet- en regelgeving.

In dit onderzoek richt ik mij meer specifiek op het verwerken van al dan niet medische gegevens van klanten van de GGD. Binnen de GGD wordt gewerkt met veel verschillende systemen waarmee persoonsgegevens worden verwerkt. In dit onderzoek zal aandacht worden besteed aan de verwerking van persoonsgegevens van klanten binnen de systemen Kidos, Orion Globe, Orion Forensisch, Tubis, HP Zone en Topdesk klantcontactcentrum. Op dit moment is het voor de GGD belangrijk om te inventariseren hoe het in de verschillende systemen is gesteld met de omgang met de persoonsgegevens. Het onderzoek richt zich daarom op sommige werknemers van de GGD, onder andere de functioneel beheerders van deze systemen. Daarnaast zal onderzocht worden hoe er door de medewerkers binnen deze systemen om wordt gegaan met persoonsgegevens.

Voor de GGD is de heersende onduidelijkheid een probleem, omdat hij niet voldoende specialistische kennis in huis heeft op het gebied van verwerking van persoonsgegevens. Daarnaast is er op internet nog onvoldoende informatie te vinden, omdat de regelgeving relatief nieuw en onduidelijk is. Deze kennis hebben de medewerkers van de GGD nodig om het beleid in overeenstemming te krijgen met huidige en in de toekomst in te voeren wet- en regelgeving.

Het is merkbaar dat het beleid voor de werknemers van de GGD Hart voor Brabant niet duidelijk is. Meerdere mensen geven aan het lastig te vinden om beslissingen te nemen over het al dan niet doorzenden van informatie over klanten. Het gaat hierbij zowel om het intern als extern delen van informatie. Het zou goed zijn om hier duidelijkheid in te kunnen scheppen voor de organisatie en haar werknemers.

Kortom: ik onderzoek de Nederlandse en Europese wet- en regelgeving op het gebied van bescherming van persoonsgegevens, omdat ik wil weten of het door de GGD gevoerde privacybeleid en de gehanteerde werkwijze conform huidige en in de toekomst in te voeren wet- en regelgeving is. Daardoor kan ik een advies geven, zodat de opdrachtgever haar beleid aan kan passen aan wet- en regelgeving.

1.3 Centrale vraag

Welke aanbevelingen kunnen worden gedaan aan de GGD Hart voor Brabant om het privacy-beleid en de werkwijze omtrent de verwerking van persoonsgegevens in overeenstemming te krijgen met de huidige en in de toekomst in te voeren wet- en regelgeving?

[12] De Vries, *NJB* 2016/1077.
[13] Bijlage I, Beleidsplan 2015-2017.

1.4 Deelvragen

- Wat is het huidige juridische kader voor het verwerken van persoonsgegevens binnen de GGD?
- Wat houdt het huidige beleid bij de GGD in omtrent de verwerking van persoonsgegevens?
- Wat is de huidige werkwijze binnen de GGD met betrekking tot de verwerking van persoonsgegevens?
- In hoeverre komen de werkwijze en het gevoerde beleid overeen met huidige en in de toekomst in te voeren wet- en regelgeving?

1.5 Doelstelling

Voor 9 januari wil ik in kaart brengen welke eisen de huidige en in de toekomst in te voeren wet- en regelgeving stelt voor de GGD Hart voor Brabant wat betreft de bescherming van persoonsgegevens. Voor de GGD zal ik dan ook conclusies opstellen waarin wordt geoordeeld over de vraag of het huidige beleid en de huidige werkwijze conform wet- en regelgeving is en zal ik aanbevelingen doen over eventuele aanpassingen in het te voeren beleid en de huidige werkwijze, zodat de organisatie haar beleid en de werkwijze hierop aan kan passen.

1.6 Methoden

Wat is het huidige juridische kader waarnaar onderzoek gedaan moet worden?
Om deze vraag te beantwoorden zal ik gebruik maken van de onderzoeksmethode inhoudsanalyse. Ik zal rechtsbronnen en juridische literatuur gaan bestuderen en inhoudelijk analyseren.

Wat verandert er met de Vordering in 2018, wat moet er binnen de GGD aangepast worden om hieraan te voldoen?
Ook hier volgt een inhoudsanalyse. Ten eerste zal ik aan de hand van rechtsbronnen en juridische literatuur uitzoeken wat er verandert met de nieuwe Vordering ten opzichte van de huidige situatie.

Wat is het huidige beleid bij de GGD Hart voor Brabant?
Om het beleid te achterhalen pas ik de inhoudsanalyse toe op documenten over het beleid dat wordt gevoerd omtrent de verwerking van persoonsgegevens.

Is het huidige beleid conform huidige Nederlandse wet- en regelgeving omtrent bescherming *van persoonsgegevens?*
Deze vraag ga ik beantwoorden, deels doormiddel van een inhoudsanalyse en deels door praktijkonderzoek. Ik zal gebruik maken van half gestructureerde interviews. De informatie die voortkomt uit de interviews ga ik analyseren en vergelijken met de bestaande wet- en regelgeving. Op die manier kan ik tot een conclusie komen voor deze deelvraag. Daarnaast zal ik uitzoeken hoe het beleid dat door de GGD gevoerd wordt, moet worden aangepast om conform in de toekomst in te voeren wetgeving te zijn. Dit zal ik doen door een inhoudsanalyse uit te voeren.

Wat is de werkwijze binnen de GGD Hart voor Brabant bij de verwerking van persoonsgegevens?
Dit praktijkonderzoek zal ik doen door middel van interviews met mensen die zelf het beleid opstellen en hier ook mee bezig zijn. Zij hebben het beste overzicht binnen de organisatie als het gaat om het beleid en de uitvoering daarvan. Daarnaast zal ik interviews houden met de functioneel beheerders van de verschillende systemen waarmee gewerkt wordt binnen de GGD. Als dit niet de personen zijn die dagelijks met de systemen werken, zal ik ook informatie inwinnen bij personen die wel dagelijks met deze systemen werken.

1.7 Verantwoording van bronnen

Het te verrichten onderzoek is een praktijkgericht juridisch onderzoek. Om de juridische aspecten van deze scriptie op een juiste manier te onderzoeken, is de inhoudsanalyse een geschikt instrument. Met deze analyse kan ik rechtsbronnen en juridische literatuur analyseren. Naast het juridische deel van de scriptie is het onderzoek ook praktijkgericht. Om dit praktische onderdeel goed te kunnen onderzoeken is het interviewen van werknemers een goede methode, omdat zij het inzicht en de kennis hebben om mij te informeren over de gang van zaken binnen de organisatie. Zij weten als geen ander hoe er binnen hun organisatie met verschillende regels wordt omgegaan en of deze regels bekend zijn bij andere medewerkers.

Hoofdstuk 2. Juridisch kader

Om tot een compleet beeld te komen van het juridisch kader dat nodig is voor dit onderzoek, volgt hieronder een uiteenzetting van zowel de internationale als de nationale wet- en regelgeving. Hierbij komt eerst het internationale recht aan bod, dan het nationale en ten slotte de te verwachten veranderingen ten opzichte van de nationale wet op het moment dat de Algemene Verordening Gegevensbescherming (AVG) rechtstreeks van toepassing zal zijn vanaf 25 mei 2018.

2.1 Internationaal juridisch kader

Het privacyrecht is internationaal vastgelegd in verschillende regelingen. Artikel 8 van het EVRM waarborgt het recht op eerbiediging van de privésfeer. Dit recht is verankerd in verschillende andere internationale regelingen: zoals artikel 16 VWEU, artikel 8 EVRM, artikel 12 UVRM, artikel 17 IVBPR en artikel 8 van het Handvest van de grondrechten van de Europese Unie. Naast deze artikelen is er door de Europese Unie een Richtlijn opgesteld in 1995 die voor het Nederlandse privacyrecht van groot belang is. De belangrijkste nationale wetgeving over de verwerking van persoonsgegevens, de Wbp, is gerealiseerd op basis van Richtlijn 95/46/EG. De Europese richtlijn is door Nederland dus geïmplementeerd middels de Wbp.

In artikel 8 van het EVRM is 'het recht op eerbiediging van privé-, familie-, en gezinsleven' als grondrecht vastgelegd.[14] Dit is de basis van de bescherming van persoonsgegevens binnen Europa. Het betreft hier geen absoluut recht, inmenging op grond van de wet is volgens dit artikel mogelijk.

Artikel 8 van het Handvest noemt in tegenstelling tot het EVRM uitdrukkelijk de bescherming van persoonsgegevens. Hier is het dus een zelfstandig recht, naast de eerbiediging van privé-, familie-, en gezinsleven uit artikel 7 van het Handvest.

Artikel 16 VWEU vormt de specifieke rechtsgrondslag voor Europese regels voor gegevensbescherming voor alle activiteiten die binnen toepassingsgebied van de Unie vallen.[15] Het vormt de basis voor Richtlijn 95/46/EG en indirect dus ook de basis voor de Wbp.

2.2 Nationale wetgeving

In het kader van dit onderzoek, waarbij ik kijk naar het verwerken van persoonsgegevens binnen de organisatie en het verstrekken van persoonsgegevens aan derden, is een aantal wetten van belang om tot een compleet juridisch kader te komen. Hierna zal ik uitsluitend in gaan op wet- en regelgeving die in het kader van dit onderzoek relevant is.

2.2.1 Grondwet

In artikel 10 van de Grondwet is het recht op privacy opgenomen. Dit is een klassiek grondrecht.[16] Omdat het een klassiek grondrecht is, moet de overheid zich onthouden van inmenging in dit recht, tenzij er een beperkingsgrond van toepassing is.

2.2.2 Wet op geneeskundige behandelingsovereenkomst (WGBO)

Omdat er binnen de organisatie veel wordt gewerkt met medische gegevens is de WGBO van belang. Deze wet is opgenomen in Burgerlijk Wetboek 7. Zorgverleners zijn op grond van deze wet verplicht om vertrouwelijke gegevens geheim te houden.[17] Daarnaast regelt

[14] Artikel 8 Europees Verdrag betreffende de Rechten van de Mens.
[15] H.R. Kranenborg 2013, p. 310.
[16] Europa-nu.nl (zoek op *Klassieke grondrechten*).
[17] Artikel 7:457 Burgerlijk Wetboek.

deze wet onder andere het recht op informatie, toestemming voor een medische behandeling en inzage in het medische dossier.[18]

In het kader van de bescherming van persoonsgegevens is een aantal rechten en plichten uit deze wet van belang. Zo kent de WGBO de inlichtingenplicht over voorgenomen onderzoek.[19] Dankzij deze plicht is de hulpverlener verplicht de patiënt op duidelijke wijze in te lichten over voorgenomen onderzoek en behandeling. Voor verrichtingen ter uitvoering van een behandelovereenkomst is toestemming van de patiënt vereist.[20] De hulpverlener moet over de behandeling een dossier opstellen.[21] De patiënt heeft recht op inzage en een afschrift van dit dossier.

Artikel 457 boek 7 van het Burgerlijk Wetboek geeft wellicht de belangrijkste plicht voor de hulpverlener in het kader van bescherming van persoonsgegevens. Dit is de geheimhoudingsplicht. De hulpverlener moet ervoor zorgen dat niemand, anders dan de patiënt over wie het dossier gaat, inlichtingen kan krijgen over de patiënt of inzage krijgt in het dossier, zonder toestemming van de patiënt.

In de volgende gevallen kunnen inlichtingen worden verstrekt over medische gegevens van de patiënt zonder daartoe uitdrukkelijk toestemming te ontvangen van patiënt:

- aan patiënt zelf (7:457 lid 1);
- aan degene die rechtstreeks betrokken zijn bij de uitvoering van de behandelovereenkomst en degene de optreedt als de vervanger van deze rechtstreeks betrokkene (7:457 lid 2);
- aan degene die wettelijk vertegenwoordiger is van de patiënt op grond van artikel 7:450 of 7:465 BW (7:457 lid 3);
- onder voorwaarden voor wetenschappelijk onderzoek, en;
- als er een wettelijke plicht geldt. De hulpverlener heeft dan een wettelijke plicht om informatie over zijn patiënt te verstrekken. Hij verbreekt dan zijn beroepsgeheim, omdat de wet dit van hem eist. Bijvoorbeeld het melden van bepaalde besmettelijke infectieziektes bij de gemeentelijke gezondheidsdienst. Dit ter voorkoming van verdere verspreiding van de infectie.[22]

Conflict van plichten

Naast deze in artikel 7:457 genoemde uitzonderingen is er nog de uitzondering “conflict van plichten”. De hoofdregel is dat als er geen sprake is van een van de vijf uitzonderingen zoals hierboven vermeld, de hulpverlener geen gegevens over patiënt mag verstrekken aan anderen zonder uitdrukkelijke toestemming van de patiënt. In het geval van conflict van plichten staat tegenover de plicht van de hulpverlener om te zwijgen, een ander, zwaarwegend belang. Dit zwaarwegende belang kan dan een doorbreking van het beroepsgeheim rechtvaardigen.[23] De hulpverlener breekt zijn zwijgplicht om een zwaar-wegender belang te dienen.

Om tot de beslissing te komen het beroepsgeheim te doorbreken op grond van een conflict van plichten, moet de hulpverlener een vijftal vragen beantwoord hebben:[24]

1. Welk zwaarwegend belang van de patiënt (of van zijn gezinslid) wil ik dienen met het geven van informatie?

[18] Dwangindezorg.nl (zoek op *WGBO*).
[19] Artikel 7:448 Burgerlijk Wetboek.
[20] Artikel 7:450 Burgerlijk Wetboek.
[21] Artikel 7:454 Burgerlijk Wetboek.
[22] L. Janssen 2015, par. 4.3.
[23] J. Legemaate, *NJB* 2011/2097.
[24] L. Janssen 2015, par. 4.4.

2. Kan dit zwaarwegende belang ook worden gediend zonder dat ik informatie aan een ander verstrek?
3. Is het, gelet op de situatie, mogelijk om toestemming van de patiënt te vragen en zo ja, heb ik alles gedaan om die toestemming daadwerkelijk te krijgen?
4. Weegt het belang van de patiënt dat ik met de gegevensverstrekking wil dienen op tegen het belang dat de patiënt heeft bij geheimhouding?
5. Welke informatie heeft de ander nodig om het belang van de patiënt te dienen of het gevaar voor hem af te wenden?

2.2.3 Wet op de beroepen in de individuele gezondheidszorg (Wet BIG)

Naast het beroepsgeheim dat is vastgelegd in de WGBO geldt ook een beroepsgeheim uit artikel 88 van de Wet BIG. De hulpverlener is op grond van dit artikel verplicht geheimhouding in acht te nemen ten opzichte van al datgene wat hem bij het uitoefenen van zijn beroep op het gebied van de individuele gezondheidszorg als geheim is toevertrouwd, of wat daarbij als geheim te zijner kennis is gekomen of waarvan hij het vertrouwelijke karakter moest begrijpen.

2.2.4 Archiefwet

Voor de bewaartermijnen van gegevens is onder andere de archiefwet van belang voor de GGD. Op deze wet zal dit onderzoek echter niet nader ingaan. Binnen de GGD is een persoon werkzaam die zich inspant om de bewaartermijnen conform wet- en regelgeving te maken. Deze persoon is uitstekend op de hoogte van de inhoud van de Archiefwet. Voor dit onderzoek is het daarom niet van belang deze nader uit toe te lichten. Hierbij dient wel opgemerkt te worden dat de GGD de gegevens moet vernietigen indien de gegevens niet langer noodzakelijk zijn.[25] De gegevens mogen enkel gearchiveerd worden als de gegevens bestemd zijn voor historische, statistische of wetenschappelijke doeleinden.[26]

2.2.5 Ambtenarenwet

Op een groot deel van de medewerkers van de GGD is de Ambtenarenwet van toepassing. Op grond van artikel 125a van deze wet geldt voor de ambtenaren een geheimhoudingsplicht.[27]

2.2.6 Wet bescherming persoonsgegevens (Wbp)

De Wbp geeft de overheid, organisaties en bedrijven regels voor de verwerking van persoonsgegevens.[28] Er wordt onder andere bepaald wanneer ze mogen worden verwerkt en voor welke doeleinden.

Onder *persoonsgegevens* vallen alle gegevens betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.[29] Onder gegevens valt niet alleen geschreven tekst. Het begrip moet breed worden uitgelegd. Om te bepalen of het gegevens zijn over een identificeerbaar persoon geldt dat daarvan sprake is wanneer de identiteit van de betrokken personen zonder onevenredige inspanning kan worden vastgesteld.[30]

Het begrip *verwerking* is in de Wbp eveneens een breed begrip. Verwerking heeft betrekking op het hele proces dat een persoonsgegeven doormaakt vanaf het moment van verzamelen van een gegeven tot aan het moment van vernietiging.[31] Het gaat hierbij zowel om geautomatiseerde als handmatige verwerking. Onder verwerking valt het

[25] Artikel 10 lid 1 Wet bescherming persoonsgegevens.
[26] Autoriteitpersoonsgegevens.nl (zoek op bewaren persoonsgegevens).
[27] Artikel 125a Ambtenarenwet.
[28] L. Janssen 2012, p. 12.
[29] H. Kranenborg 2011, p. 60.
[30] H. Kranenborg 2011, p. 61.
[31] H. Kranenborg 2011, p. 65.

verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken doormiddel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.[32]

Een aantal andere begrippen dat nog uitleg verdient, zijn de verschillende actoren die in de wet worden genoemd.

- Ten eerste is de *betrokkene* van belang. Dit is de persoon op wie een persoonsgegeven betrekking heeft.[33] Als een individu wordt aangemerkt als betrokkene kan zij beroep doen op verschillende rechten uit de Wbp.

- De *verantwoordelijke* is de persoon die in juridische zin bevoegd is doel en middelen van gegevensverwerking vast te stellen.[34] Het is dus de natuurlijke persoon of rechtspersoon die verantwoordelijk is voor de verwerking van persoonsgegevens. Waar de feitelijke zeggenschap ligt doet er in dat geval niet toe.

- De *bewerker* is degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt.[35] Dit is niet iemand die in hiërarchische verhouding staat tot de verantwoordelijke. De bewerker handelt in overeenstemming met instructies van de verantwoordelijke. Hij is niet de persoons die beslist over de verwerking van de persoonsgegevens.[36]

- De *derde* is iedereen die niet valt onder de categorieën genoemd in de wet in artikel 1 Wbp. Ten slotte kent de wet nog de ontvanger. Dit is degene aan wie persoonsgegevens worden verstrekt. Dit kan zowel een persoon binnen als buiten de organisatie van de persoon die verantwoordelijk is zijn.

Nu er duidelijkheid is over de begrippen zoals gebruikt in de Wbp kan de wet nader worden toegelicht. Hierbij is het in de eerste plaats van belang om de algemene bepalingen van de Wbp toe te lichten, daarna volgt een uiteenzetting van de bijzondere bepalingen van deze wet.

De GGD verwerkt persoonsgegevens. Via verschillende kanalen komen persoonsgegevens binnen bij de organisatie. Enkele voorbeelden hiervan zijn:

- Het Klantcontactcentrum met het systeem Topdesk KCC, waar mensen naartoe bellen met een hulpvraag;
- Het team Jeugdgezondheidszorg (JGZ) met het systeem KIDOS, waar gegevens van kinderen worden geïmporteerd door de gemeente en waar medewerkers zelf gegevens in kunnen verwerken;
- Het team Reizigerszorg met het systeem Orion Globe, waar reizigers komen voor vaccinaties;
- Ook komen er gegevens binnen van politie en gemeenten bij het team Forensische geneeskunde dat werkt met het systeem Orion Forensisch, hierbij gaat het bijvoorbeeld om een verzoek om verplichte DNA-testen af te nemen of een hulpvraag voor arrestanten die medische hulp nodig hebben. Deze gegevens worden door de GGD verwerkt.

[32] Artikel 1 onder b Wet bescherming persoonsgegevens.
[33] Artikel 1 onder f Wet bescherming persoonsgegevens.
[34] Artikel 1 onder d Wet bescherming persoonsgegevens.
[35] Artikel 1 onder e Wet bescherming persoonsgegevens.
[36] H. Kranenborg 2011, p. 78.

De Wbp is daarom in vele opzichten van toepassing op de werkzaamheden binnen de GGD.

Na het binnenkomen van de gegevens onderneemt de GGD nog verschillende acties met de gegevens. Ook hierop is de Wbp dus van toepassing. Wat nog bijzonder is binnen de GGD is dat er veel wordt gewerkt met gegevens betreffende de gezondheid, namelijk medische gegevens. Hierop zijn de bijzondere bepalingen uit de Wbp van toepassing.

2.2.6.1 Algemene bepalingen Wbp.

Om tot rechtvaardige verwerking van persoonsgegevens te komen moet volgens het algemene hoofdstuk aan een aantal voorwaarden zijn voldaan. Op grond van artikel 6 Wbp dienen persoonsgegevens in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt te worden. Dit wordt het rechtmatigheidsbeginsel genoemd.[37]

Doelbinding

Artikel 7 Wbp geeft vervolgens het beginsel van doelbinding. Persoonsgegevens mogen enkel worden verwerkt voor een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doeleinde. Het doel van de verwerking moet dus voordat de verwerking van start gaat al duidelijk zijn en ook uitdrukkelijk zijn omschreven. Dit is medebepalend voor een eventuele beoordeling van de rechtmatigheid van deze gegevensverwerking.[38] De doeleinden moeten gerechtvaardigd zijn, wat betekent dat men de doeleinden moet kunnen bereiken met inachtneming van de regels gesteld in artikel 8 Wbp.

Gronden

De verwerking van een persoonsgegeven moet op een bepaalde grond worden gebaseerd. Artikel 8 Wbp geeft een limitatieve en alternatieve opsomming van de wettelijke gronden. Elke verwerking van persoonsgegevens moet dus zijn gebaseerd op een van de gronden genoemd in dit artikel. Persoonsgegevens mogen slechts worden verwerkt indien:

a) De betrokkene voor de verwerking zijn ondubbelzinnige toestemming heeft verleend;
b) De gegevensverwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die noodzakelijk zijn voor het sluiten van een overeenkomst;
c) De gegevensverwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is;
d) De gegevensverwerking noodzakelijk is ter vrijwaring van een vitaal belang van de betrokkene;
e) De gegevensverwerking noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan aan wel het bestuursorgaan waaraan de gegevens worden verstrekt, of
f) De gegevensverwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt.

Voor bijzondere persoonsgegevens geldt naast deze algemene regels een strikter regime. De verwerking van die bijzondere persoonsgegevens dient te voldoen aan zowel de algemene bepalingen, als aan artikel 16 tot en met 23.[39] Hierop wordt later nader ingegaan.

[37] H.H. de Vries 2001, p. 22.
[38] Kamerstukken II 1997-1998, 25 892, nr. 3, p. 20.
[39] Kamerstukken II 1997-1998, 25 892, nr. 3, p. 21

Naast de limitatieve gronden geldt op basis van artikel 8 nog de eis van zowel proportionaliteit als subsidiariteit bij elke verwerking van persoonsgegevens. Het proportionarliteitsbeginsel houdt in dat de verwerking van persoonsgegevens niet onevenredig mag zijn ten opzichte van het te dienen doel.[40] Het subsidiariteitsbeginsel betekent dat het minst nadelige middel om het doel te bereiken gebruikt moet worden.

De gronden voor verwerking nader toegelicht

a) **Ondubbelzinnige toestemming**
Bij verwerking op grond van ondubbelzinnige toestemming, moet bij de verantwoordelijke elke twijfel zijn uitgesloten over de vraag of de betrokkene zijn toestemming heeft gegeven. Als er twijfel bestaat over de vraag of betrokkene zijn toestemming heeft verleend, moet de verantwoordelijke nagaan of hij er terecht vanuit gaat dat deze toestemming door betrokkene is verleend.

b) **Uitvoering van een overeenkomst**
Als gebruik wordt gemaakt van de grond “uitvoering van een overeenkomst” is van belang dat de betrokkene partij is in die overeenkomst. De betrokkene moet bewust partij zijn bij de overeenkomst. Het moet geen overeenkomst zijn met als doel de verwerking van persoonsgegevens, maar waarbij deze verwerking een noodzakelijk uitvloeisel daarvan is.

c) **Wettelijke plicht**
Grond c heeft 2 toetsingscriteria. In de eerste plaats moet de verwerking van de persoonsgegevens noodzakelijk zijn voor de uitvoering van een wettelijke plicht. Daarnaast moet de verantwoordelijke zijn belast met de uitvoering van een wettelijke verplichting. Dus zonder de verwerking van de persoonsgegevens is het in redelijkheid niet mogelijk om de wettelijke verplichting na te komen.

d) **Dringende medische noodzaak**
Om gegevens te kunnen verwerken op grond d moet sprake zijn van een dringende medische noodzaak.[41] Het moet gaan om een zaak van leven of dood. Het subsidiariteitsbeginsel brengt in dit geval met zich mee dat als het mogelijk is om toestemming te vragen, dit de voorkeur krijgt. Dit is in gevallen van leven of dood niet mogelijk. Maar ook in gevallen dat het onmogelijk is alle betrokkene te informeren en toestemming te vragen voordat er hulpverlening gestart wordt kan een beroep worden gedaan op deze grond. Denk hierbij aan grootschalige rampen. Deze eis moet eng worden uitgelegd. Slechts zelden zal er bij deze organisatie gebruik kunnen worden gemaakt van deze grond.

e) **Publiekrechtelijke taak**
Van verwerking die noodzakelijk is voor de vervulling van een publiekrechtelijke taak (onderdeel e) is sprake als het gaat om zowel een bestuursorgaan als een publiekrechtelijke taak. Wanneer een bestuursorgaan een privaatrechtelijke handeling verricht kan dus geen beroep worden gedaan op onderdeel e. De begrippen publiekrechtelijk en bestuursorgaan worden in de Wbp het zelfde uitgelegd als in de Algemene wet bestuursrecht (Awb). De GGD is geen bestuursorgaan. Om die reden is deze grond dan ook niet van toepassing voor de organisatie.

f) **Gerechtvaardigd belang**
Onderdeel f is als het ware een soort restcategorie. Van een gerechtvaardigd

[40] Kamerstukken II 1997-1998, 25 892, nr. 3, p. 80
[41] Kamerstukken II 1997-1998, 25 892, nr. 3, p. 84

belang is sprake indien de verwerking voor de verantwoordelijke noodzakelijk is om zijn reguliere bedrijfsactiviteiten voort te zetten.[42] Bijvoorbeeld de schadeverzekeraar die de gegevens van zowel cliënt als tegenpartij nodig heeft om een schadeclaim te verwerken. De richtlijn begrenst deze verwerking door een motiveringsplicht te impliceren voor de verantwoordelijke. De verantwoordelijke moet voor zichzelf de volgende vragen kunnen beantwoorden:

- Is er werkelijk een belang dat verwerking van persoonsgegevens rechtvaardigt?
- Wordt met de verwerking een inbreuk gemaakt op belangen of fundamentele rechten van degene wiens gegevens worden verwerkt en zo ja, dient dan –afhankelijk van de ernst van de inbreuk- gegevensverwerking niet achterwege te blijven?
- Kan het doel dat met de verwerking wordt nagestreefd ook langs andere weg – zonder verwerking- worden bereikt?
- Is de verwerking in de mate die is beoogd evenredig aan het nagestreefde doel?

Verenigbaar gebruik

Artikel 9 Wbp geeft de eis van verenigbaar gebruik. Binnen de organisatie van de verantwoordelijke kunnen de persoonsgegevens voor andere doeleinden worden gebruikt dan waarvoor zij zijn vergaard, mits deze doeleinden verenigbaar zijn met het oorspronkelijke doel waarvoor zij werden verwerkt.[43]

Overige eisen van belang uit de Wbp

Bewaartermijn

Artikel 10 Wbp bepaalt dat persoonsgegevens niet langer mogen worden bewaard in een vorm die het mogelijk maakt de betrokkene te identificeren dan noodzakelijk is voor de verwerking van de doeleinden waarvoor zij worden verzameld of vervolgens worden opgeslagen. De wet geeft hiervoor geen termijn. De verantwoordelijke dient zich dus af te vragen of er redenen zijn op grond waarvan gegevens vastgelegd kunnen blijven.[44]

Soms geeft bijzondere wetgeving een termijn voor bewaring. Zo mogen medische gegevens op grond van artikel 7:454 lid 3 BW in de regel 10 jaar worden bewaard.

Als de termijn is verlopen, mogen de gegevens niet meer worden verwerkt, tenzij voor een ander, daarmee verenigbaar doel. Bijvoorbeeld voor statische archivering.

Beveiliging persoonsgegevens

De verantwoordelijke is verplicht passende maatregelen te treffen ter beveiliging van persoonsgegevens. Wat deze passende maatregelen zijn hangt af van de omstandigheden van het geval. De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer, om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking.[45] De beveiliging moet in overeenstemming zijn met de stand van de techniek.[46] Technische en organisatorische maatregelen dienen cumulatief te worden getroffen.[47]

[42] Kamerstukken II 1997-1998, 25 892, nr. 3, p. 86.
[43] Kamerstukken II 1997-1998, 25 892, nr. 3, p. 89.
[44] Kamerstukken II 1997-1998, 25 892, nr. 3, p. 95.
[45] Artikel 13 Wet bescherming persoonsgegevens.
[46] Richtsnoer Beveiliging van persoonsgegevens 2013.
[47] Kamerstukken II 1997-1998, 25 892, nr. 3, p. 99.

Als er sprake is van verwerking door een verwerker is de verantwoordelijke verantwoordelijk voor voldoende waarborgen wat betreft beveiliging. De te treffen beveiligingsmaatregelen worden vastgelegd in een bewerkersovereenkomst.[48]

Informatie
De betrokkene heeft op grond van artikel 35 recht op kennisneming. Dit houdt in dat de betrokkene de verantwoordelijke kan vragen of er persoonsgegevens van hem worden verwerkt. Daartegenover staat de plicht van de verantwoordelijke om informatie te verstrekken.[49] Dit recht en deze plichten samen zorgen voor een uitwerking van het transparantiebeginsel.[50] Als de persoonsgegevens bij betrokkene zelf worden verkregen is artikel 33 Wbp van toepassing. Als de persoonsgegevens worden verkregen bij een derde is artikel 34 van toepassing. Uitgangspunt bij beide artikelen is dat de verantwoordelijke zijn identiteit en de doeleinden van de verwerking aan betrokkene mededeelt. De verantwoordelijke verstrekt bovendien 'nadere informatie voor zover dat gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen'.[51]

2.2.6.2 Verwerking bijzondere persoonsgegevens
De verwerking van persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging is verboden behoudens de uitzonderingen in artikel 17 t/m 22 Wbp en de meer algemene uitzondering in artikel 23 Wbp.[52] Het verbod geldt voor zowel direct, als indirect gevoelige persoonsgegevens. Indirecte gegevens hebben geen rechtstreekse betrekking op een gevoelig kenmerk, maar dit kan daar wel rechtstreeks uit worden afgeleid.[53] Een voorbeeld hiervan is het adressenbestand van alle leden van een kerkgenootschap. Dit is niet direct een persoonsgegeven betreffende iemands godsdienst, maar indirect blijkt dit wel uit het lid zijn van een bepaalde kerk. Hierbij is nog van belang dat het algemene regime zoals hierboven toegelicht, ook van toepassing is op deze bijzondere persoonsgegevens. De voorwaarden gelden dus cumulatief.

In het kader van dit onderzoek zal enkel extra aandacht worden besteed aan de uitzondering uit artikel 21 Wbp. Dit artikel gaat over de gegevens betreffende de gezondheid als bijzondere persoonsgegevens. Onder deze categorie vallen niet alleen gegevens in het kader van medisch onderzoek of de medische behandeling, maar alle gegevens die gaan over de geestelijke of lichamelijke gezondheid van een persoon.

In beginsel mogen gegevens betreffende de gezondheid niet worden verwerkt op grond van artikel 21[54]. Dit artikel geeft echter een aantal uitzonderingen op grond waarvan gegevens betreffende de gezondheid wel mogen worden verwerkt.

De GGD valt onder categorie a uit artikel 21 Wbp. Het gaat immers om een instelling voor gezondheidszorg of maatschappelijke dienstverlening. Voor hen geldt dus een uitzondering op het verbod uit artikel 16 Wbp. De bijzondere persoonsgegevens mogen alleen worden verwerkt voor zover dat met het oog op een goede behandeling of verzorging, dan wel het beheer van de instelling of beroepspraktijk noodzakelijk is. Volgens de Memorie van Toelichting is van beheer sprake als het gaat om het

[48] Artikel 14 lid 2 Wet bescherming persoonsgegevens.
[49] Artikel 33 en 34 Wet bescherming persoonsgegevens.
[50] H. Kranenborg 2011, p. 120.
[51] Artikel 33 lid 2 en 34 lid 3 Wet bescherming persoonsgegevens.
[52] Artikel 16 Wet bescherming persoonsgegevens.
[53] Autoriteitpersoonsgegevens.nl (zoek op *indirect direct persoonsgegeven).*
[54] Artikel 21 Wet bescherming persoonsgegevens.

waarborgen van de kwaliteit van de verleende zorg, maar ook wanneer sprake is van intercollegiale toetsing door hulpverleners onderling.[55]

Lid 2 van artikel 21 Wbp geeft als eis dat de persoonsgegevens door bovengenoemde instellingen alleen mogen worden verwerkt door personen die uit hoofde van hun beroep of krachtens overeenkomst tot geheimhouding zijn verplicht.

Het feit dat bijvoorbeeld een gemeente zou kunnen worden aangemerkt als een organisatie die maatschappelijke dienstverlening biedt, betekent nog niet dat zorgprofessionals daarom zonder toestemming van de cliënt verplicht zouden zijn om gezondheidsgegevens te verstrekken aan de gemeente. Ook al heb je een grondslag op basis waarvan je persoonsgegevens vastlegt, betekent dat niet dat er ook een plicht bestaat om deze gegevens te verstrekken aan de gemeente.[56]

Het verbod op het verwerken van andere bijzondere persoonsgegevens uit artikel 16 geldt op grond van het derde lid niet wanneer 'dit noodzakelijk is in aanvulling op de verwerking van persoonsgegevens betreffende iemands gezondheid als bedoeld in het eerste lid, onder a, met het oog op een goede behandeling of verzorging van de betrokkene'.[57] In sommige gevallen kan het bijvoorbeeld van belang zijn om het ras, de godsdienst of de seksuele voorkeur van een persoon te betrekken bij de geneeskundige behandeling.

In geval van genetische gegevens blijven deze gegevens op grond van het vierde lid beperkt tot de betrokkene zelf die deze heeft verstrekt, behoudens de uitzonderingen in sub a en b.[58]

De algemene uitzonderingen uit artikel 23 Wbp bestaan onder andere uit de uitdrukkelijke toestemming van de betrokkene en als de betrokkene zelf de gegevens duidelijk openbaar heeft gemaakt. Aan de toestemming bij verwerking van gevoelige gegevens worden strengere eisen gesteld dan aan de toestemming die is vereist bij normale persoonsgegevens. De betrokkene moet in dit geval expliciet zijn wil omtrent de verwerking van de bijzondere gegevens hebben geuit.[59]

2.2.7 Meldplicht datalekken

Het sinds 1 januari 2016 nieuwe artikel 34a Wbp bevat de meldplicht datalekken. Dit artikel speelt in op de veranderingen die gaan optreden als de Europese Verordening in 2017 in werking zal treden. Om te kijken of sprake is van een meldingsplichtige datalek moet een bedrijf zich de volgende vragen stellen:[60]

1. Is er sprake op een inbreuk op de veiligheidsmaatregelen? Zo ja,
2. Zijn er persoonsgegevens verloren gegaan? Als dit niet het geval is, kan redelijkerwijs worden uitgesloten dat persoonsgegevens onrechtmatig zijn verwerkt?

Tussenconclusie: sprake van een datalek.

3. Heeft de inbreuk tot gevolg gehad dat de verwerkte persoonsgegevens zijn blootgesteld aan een aanmerkelijke kans op nadelige gevolgen voor de persoonsgegevens die door hem worden verwerkt?

[55] Kamerstukken II 1997-1998, 25 892, nr. 3, p. 110.
[56] S. Nouwt *NJB* 2014/2158, p. 4.
[57] Artikel 21 lid 3 Wet bescherming persoonsgegevens.
[58] Artikel 21 lid 4 Wet bescherming persoonsgegevens.
[59] CBP 7 augustus 2006, z2006-00454.
[60] Kamerstukken II 2012-2013, 33 662, nr. 3. p. 7.

De nadelige gevolgen zullen zich met name voordoen in de vorm van verlies of onrechtmatige verwerking. Er moet naar feitelijke omstandigheden worden vastgesteld of er kans is dat persoonsgegevens zijn blootgesteld aan deze nadelige gevolgen. Ook of er sprake is van een aanmerkelijke kans hangt af van de omstandigheden van het geval. De noodzaak om melding te doen hangt samen met de aard van de persoonsgegevens. Van een instelling als de GGD wordt een bepaalde professionaliteit verwacht in de omgang met de gegevens. Een datalek zal als het gaat om persoonsgegevens van klanten al snel leiden tot een aanmerkelijke inbreuk op de persoonlijke levenssfeer. Het gaat immers vaak om gegevens betreffende de gezondheid. Dit vergt een extra zorgvuldige aanpak ten opzichte van bijvoorbeeld een sportclub waar een adressenbestand wordt bijgehouden van de leden.

Een datalek moet worden gemeld bij de Autoriteit Persoonsgegevens (hierna: AP), voorheen het College bescherming persoonsgegevens (hierna: Cbp). Het niet tijdig doen van een melding kan leiden tot een bestuurlijke boete opgelegd door de AP.

2.2.8 De Functionaris gegevensbescherming

Een organisatie heeft op grond van de Wbp de mogelijkheid een Functionaris voor de gegevensbescherming (hierna: functionaris) aan te stellen.[61] Deze functionaris moet door de organisatie worden gemeld bij de AP. Een verantwoordelijke is wettelijk verplicht om melding te maken aan de AP van geheel of gedeeltelijke geautomatiseerde verwerking van persoonsgegevens.[62] Door het aanstellen van een functionaris mag de melding in plaats van aan de AP aan deze persoon worden gedaan.

2.2.9 Verhouding Wbp en bijzondere wetgeving

In het sociale domein zijn mensen vaak gebonden aan de geheimhoudingsplicht zoals door de Ambtenarenwet, de Wet BIG of de WGBO. Op grond van artikel 9 lid 4 Wbp moet bij verdere verwerking van persoonsgegevens rekening worden gehouden met een daaraan in de weg staande geheimhoudingsplicht. Er moet in zo'n geval dus naast een grondslag voor de verwerking van persoonsgegevens als bedoeld in artikel 8 Wbp, ook een grond zijn voor de doorbreking van de geheimhoudingsplicht.[63] Dit beroepsgeheim verhindert dus dat inlichtingen worden verstrekt aan derden, tenzij een grond uit de bijzondere wetten van toepassing is. Bijvoorbeeld toestemming of conflict van plichten.

[61] Artikel 62 Wet bescherming persoonsgegevens.
[62] Artikel 27 Wet bescherming persoonsgegevens.
[63] S. Nouwt NJB 2014/2158, p. 2.

Hoofdstuk 3. De Algemene Verordening Gegevensbescherming

De Algemene Verordening Gegevensbescherming (AVG) is op 27 april 2016 vastgesteld en zal per 25 mei 2018 van toepassing zijn.[64] De AVG komt in de plaats van de op dit moment geldende richtlijn en de daarop gebaseerde Wbp. Omdat de verordening geldend recht is, voldoet een organisatie ook aan huidige wet- en regelgeving op het moment dat er voldaan wordt aan de vereisten uit de verordening.

De EU heeft gekozen voor een verordening in plaats van een richtlijn, omdat de richtlijn niet heeft kunnen zorgen voor harmonisatie van de wetgeving tussen de verschillende lidstaten van de Europese Unie. Het verschil in beschermingsniveau van persoonsgegevens tussen de verschillende lidstaten kan zorgen voor belemmering van het vrij verkeer van gegevens binnen de Unie.[65] Hiervan kan sprake zijn op het moment dat in land X het beschermingsniveau hoger ligt dan in land Y. Hierna volgen de belangrijkste veranderingen die de AVG met zich meebrengt ten opzichte van de Wbp nader toelichten. Hierbij wordt meer specifiek aandacht besteed aan de wijzigingen die voor de GGD van belang zijn.

De eerste wijziging die aandacht verdient is het territoriale bereik dat de AVG heeft.[66] De AVG is niet alleen van toepassing op de organisaties die binnen de EU zijn gevestigd. Ook op organisaties buiten de EU die diensten en producten aanbieden binnen de EU of het gedrag van personen binnen de EU monitoren is de AVG van toepassing.

Enkele begrippen die in artikel 3 van de AVG worden toegelicht, zijn nieuw of enigszins gewijzigd ten opzichte van de Wbp. Zo is de bewerker de verwerker geworden, de verantwoordelijke de verwerkingsverantwoordelijke en kent de AVG de ondubbelzinnige en expliciete toestemming. De bewijslast van deze toestemming ligt bij de organisatie.[67] De GGD moet kunnen aantonen dat een duidelijke, actieve handeling heeft geleid tot deze toestemming. Uit deze toestemming moet blijken dat de betrokkene weet voor welke verwerking hij toestemming heeft gegeven.[68] De betrokkene moet daarom per doeleind aan kunnen geven of zijn gegevens daarvoor verwerkt mogen worden. Daarnaast moet de betrokkene op de hoogte worden gesteld van de mogelijkheid deze toestemming weer in te trekken op het moment dat de toestemming verleend wordt.[69]

Beginselen

Ook wat betreft beginselen zijn er verschillende wijzigingen ten opzichte van de Wbp. Zo is het transparantiebeginsel als beginsel opgenomen in de AVG. Ook is accountability een belangrijk begrip in de AVG. Dit heeft mede tot gevolg dat de verantwoordelijke nu de plicht heeft om verantwoording af te leggen.[70] Op grond van de AVG is de GGD verplicht om documentatie te hebben waarin zij uitgebreid alle aspecten van verwerking beschrijft.[71] Hier moet onder andere het doel, de wettelijke grondslag en bewaartermijn zijn opgenomen. Daarnaast wordt de betrokkene op de hoogte gesteld van het recht op inzage, het recht vergeten te worden, het recht op rectificatie, het recht om eerder verleende toestemming in te trekken en het recht om een klacht in te dienen bij de toezichthoudende autoriteit. Als de verwerkingsverantwoordelijke de persoonsgegevens verder wil verwerken voor een ander doel dan waarvoor ze zijn verzameld, wordt aan de

[64] Autoriteitpersoonsgegevens.nl (zoek op: Europese privacywetgeving).
[65] J.P. de Jong 2016.
[66] Artikel 3 Algemene Verordening Gegevensbescherming.
[67] J.P. de Jong 2015, p. 10.
[68] Overweging 38 Algemene Verordening Gegevensbescherming.
[69] Artikel 7 lid 3 Algemene Verordening Gegevensbescherming.
[70] C. Arts 2016.
[71] Artikel 13 Algemene verordening Gegevensbescherming.

betrokkene informatie over dit andere doel verstrekt alvorens de persoonsgegevens verder worden verwerkt.

De GGD verwerkt op grote schaal bijzondere categorieën persoonsgegevens, namelijk gegevens betreffende de gezondheid. Daarom is het op grond van de AVG verplicht een gegevensbeschermingseffectbeoordeling, ook wel een PIA genoemd, uit te voeren. Bij een PIA worden de privacyaspecten aan een door de organisatie aangeboden dienst of product onderzocht. Op die manier krijgt de organisatie inzicht in de risico's met betrekking tot de privacy. De PIA kan ervoor zorgen dat voorafgaand overleg met of voorafgaande toestemming van de toezichthouder moet volgen. Hier kan in zo´n geval ook een taak voor de functionaris zijn weggelegd.[72]

3.1 Functionaris gegevensbescherming

Waar het voorheen voor organisaties een keuze was om een functionaris voor de gegevensbescherming (hierna: functionaris) aan te stellen,[73] is dit voor de GGD op grond van de AVG een verplichting geworden.[74] Deze plicht bestaat voor de GGD op grond van artikel 37 lid 1 sub a en sub c, omdat de GGD een overheidsorgaan is en deze organisatie belast is met grootschalige verwerking van bijzondere categorieën van persoonsgegevens. De functionaris moet toegang hebben tot persoonsgegevens en verwerkingsactiviteiten en is op grond van de AVG tot geheimhouding verplicht.[75] De functionaris moet worden aangewezen op grond van zijn professionele kwaliteiten en meer in het bijzonder zijn deskundigheid op het gebied van de wetgeving en de praktijk inzake gegevensbescherming.[76] De functionaris moet door de organisatie naar behoren en tijdig worden betrokken bij alle aangelegenheden die verband houden met de verwerking van persoonsgegevens. Bovendien brengt hij rechtstreeks verslag uit aan de hoogste leidinggevende van de verwerkingsverantwoordelijke of de verwerker.[77]

De functionaris moet tenminste de volgende taken vervullen:[78]

- informeren en adviseren aan de verwerkingsverantwoordelijke/verwerker en de werknemers die verwerken over hun verplichtingen ogv wet- en regelgeving;
- toezien op naleving van deze verordening en van het beleid dat wordt gevoerd. Daar hoort bij het wijzen op verantwoordelijkheden en bewustmaking en opleiding van het bij de verwerking betrokken personeel;
- desgevraagd advies verstrekken met betrekking tot de gegevenbeschermingseffect-beoordeling en toezien op de uitvoering daarvan;
- met de toezichthoudende autoriteit samenwerken;
- optreden als contactpunt voor de toezichthoudende autoriteit.

De functionaris moet deze taken onafhankelijk uit kunnen voeren. Dit betekent dat hij bij de uitvoering van deze taken geen instructies mag krijgen.[79] De functionaris mag niet worden ontslagen of gestraft voor de uitvoering van zijn taken. Er is dus een zekere mate van ontslagbescherming voor deze persoon.

[72] J.P. de Jong 2015, p. 12.
[73] Artikel 62 Wet bescherming persoonsgegevens.
[74] Artikel 37 Algemene Verordening Gegevensbescherming.
[75] Artikel 38 lid 2 Algemene Verordening Gegevensbescherming.
[76] Artikel 37 lid 5 Algemene Verordening Gegevensbescherming.
[77] Artikel 38 lid 3 Algemene Verordening Gegevensbescherming.
[78] Artikel 39 Algemene Verordening Gegevensbescherming.
[79] Artikel 38 lid 3 Algemene Verordening Gegevensbescherming.

Er wordt door de variatie in onderwerpen en de grote verantwoordelijkheid van de functionaris een groot beroep gedaan op zijn deskundigheid.[80]

3.2 Privacy by design en by default

Nieuw in de AVG is dat er een plicht ontstaat om bij nieuwe verwerkingen van persoonsgegevens al in het ontwerpproces rekening te houden met de bescherming van deze gegevens. Systemen moeten zo worden ingericht dat de privacy wordt gewaarborgd. De organisatie moet achteraf ook aan kunnen tonen dit gedaan te hebben. Er worden daarom zo min mogelijk gegevens verwerkt en met name gedeeld. Voorbeelden hiervan zijn het zo inrichten van het systeem dat het pseudonimiseren van gegevens wordt gefaciliteerd en het afschermen van bepaalde gegevens voor bepaalde personen.

3.3 Gegevenbeschermingseffectbeoordeling.

In sommige gevallen is op grond van artikel 35 van de AVG een Gegevensbeschermings-effectbeoordeling (hierna: PIA) verplicht voor organisaties. Bij de PIA wordt vooraf een inschatting gemaakt over de gevolgen die bepaalde verwerking heeft voor de privacy van de betrokkenen. Lid 3 van dit artikel geeft aan wanneer een PIA verplicht is voor een organisatie. Voor de GGD is grond b van toepassing.[81] De organisatie verwerkt namelijk op grote schaal bijzondere persoonsgegevens. De AVG bepaalt niet uitvoerig wat moet worden opgenomen in de PIA. Wel geeft lid 7 onderwerpen die in elk geval aan de orde moeten komen in de PIA:

- Een systematische beschrijving van de beoogde verwerkingen en verwerkingsdoeleinden;
- Een beoordeling van de noodzaak en evenredigheid van de verwerkingen met betrekking tot de doeleinden;
- Een beoordeling van de in lid 1 bedoelde risico's voor de rechten en vrijheden van de betrokkenen en;
- De beoogde maatregelen om de risico's aan te pakken, waaronder waarborgen, veiligheidsmaatregelen en mechanismen om de bescherming van persoonsgegevens te garanderen en om aan te tonen dat aan deze verordening is voldaan, met inachtneming van de rechten en gerechtvaardigde belangen van de betrokkenen en andere personen in kwestie.

Als uit de beoordeling blijkt dat er sprake is van een hoog risico, moet de toezichthouder worden geraadpleegd op grond van artikel 36.[82]

3.4 Meldplicht datalekken

In de AVG wijzigt een aantal dingen ten opzichte van de onlangs ingevoerde wet meldplicht datalekken zoals die is opgenomen in de Wbp. In artikel 33 wordt gesproken over "melding van een inbreuk in verband met persoonsgegevens".[83] In lid 5 staat een belangrijk verschil ten opzichte van de Wbp.[84] Waar bij de Wbp alleen een administratie moest worden gemaakt van meldingsplichtige inbreuken, moet dit in de AVG van alle inbreuken. Het gaat hierbij dus om elke situatie waarbij iemand, zonder daartoe bevoegdheid te hebben, toegang krijgt tot gegevens. Er is dan namelijk al sprake van een inbreuk volgens de beleidsregels van de AP.[85] Omdat er in de AVG geen nadere regels

[80] P.L. Coté 2014.
[81] Artikel 35 lid 3 onder b Algemene Verordening Gegevensbescherming.
[82] Artikel 36 Algemene Verordening Gegevensbescherming.
[83] Artikel 33 Algemene Verordening Gegevensbescherming.
[84] Artikel 33 lid 5 Algemene Verordening Gegevensbescherming.
[85] Beleidsregels meldplicht datalekken in de Wet bescherming persoonsgegevens.

zijn opgesteld over wanneer sprake is van een datalek, wordt hiervoor aansluiting gevonden bij het beleid zoals dat is opgesteld voor de Wbp.

3.5 Recht om vergeten te worden

Artikel 17 kent het recht op vergetelheid dat is geïntroduceerd in jurisprudentie en nu is gecodificeerd en gespecificeerd in de AVG.[86] De betrokkene heeft het recht op wissing van hem betreffende persoonsgegevens te verkrijgen in de volgende gevallen:[87]

- de persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor zij zijn verzameld of anderszins verwerkt;
- de betrokkene trekt zijn toestemming in;
- de betrokkene maakt bezwaar tegen verwerking overeenkomstig artikel 21 lid 2;
- de persoonsgegevens zijn onrechtmatig verwerkt;
- op grond van wettelijke plicht moeten de gegevens worden verwijderd;
- de persoonsgegevens zijn verzameld in verband met een aanbod van diensten van de informatiemaatschappij als in artikel 8 lid 1.

Als de verwerkingsverantwoordelijke de persoonsgegevens openbaar heeft gemaakt en op grond van bovenstaande verplicht is te wissen, moet hij maatregelen nemen om verwerkingsverantwoordelijken die de persoonsgegevens verwerken op de hoogte te stellen van het verzoek tot wissing.

3.6 Pseudonimisering en profilering

Van pseudonimisering is sprake indien de persoonsgegevens zodanig worden verwerkt dat ze niet meer te koppelen zijn aan een identificeerbaar persoon zonder dat er aanvullende gegevens worden gebruikt. Bij aanvullende gegevens kan men denken aan het vervangen van de persoonsgegevens door een letter of een getal. Deze zogenaamde sleutel is dan nodig om de aanvullende gegevens die leiden tot identificeerbaarheid van het individu te achterhalen. Deze aanvullende gegevens moeten dan wel apart bewaard worden en er moeten maatregelen worden getroffen, zodat de persoonsgegevens niet aan een identificeerbaar persoon gekoppeld kunnen worden.[88]

De toepassing van pseudonimisering kan zorgen voor minder risico's voor de betrokkene. Daarmee kan het de verplichtingen voor de verwerkingsverantwoordelijke vergemakkelijken.

Het verschil tussen geanonimiseerde gegevens en gepseudonimiseerde gegevens is dat bij die eerste de identificatie geheel niet meer mogelijk is, terwijl dat bij pseudonimisering wel mogelijk is. Op geanonimiseerde gegevens is de privacywetgeving niet van toepassing. Pseudonimisering kan worden gezien als een techniek om beveiliging van persoonsgegevens te verbeteren. Volgens de AVG is pseudonimisering expliciet niet bedoeld om andere beveiligingsmaatregelen uit de AVG te omzeilen.[89]

Van profilering is sprake indien er een geautomatiseerde verwerking plaatsvindt waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijk persoon worden geëvalueerd.[90] Op basis van het profiel worden dan maatregelen toegepast en voorspellingen gedaan die een effect hebben op dat individu.[91] Het doel is dan om bijvoorbeeld economische situatie, gezondheid, persoonlijke voorkeuren en

[86] HvJ EU 13 mei 2014 (*Google Spanje/ AEPD en Costeja*).
[87] Artikel 17 Algemene Verordening Gegevensbescherming.
[88] Minister Veiligheid en Justitie *NJB* 2016/16, p. 1163.
[89] Overweging 28 Algemene Verordening Gegevensbescherming, p. 5.
[90] Artikel 20 Algemene Verordening Gegevensbescherming.
[91] J. Gerritsen 2015/6.

interesses te analyseren of te voorspellen.[92] Op grond van de AVG heeft iedere natuurlijke persoon het recht om niet onderworpen te worden aan een maatregel die is gebaseerd op profilering doormiddel van uitsluitend geautomatiseerde verwerking.[93] Dit verbod geldt niet indien sprake is van de uitzonderingen uit dit artikel. De belangrijkste hiervan is de uitdrukkelijke toestemming van betrokkene.

3.7 Boetebevoegdheid

Een belangrijke reden voor veel organisaties om de bescherming van persoonsgegevens meer aandacht te geven is de verandering in de boetebevoegdheid van de AP. Artikel 83 geeft de mogelijkheid voor het opleggen van een administratieve geldboete. Deze boete kan oplopen tot 10 miljoen euro. Daarnaast moeten lidstaten sancties opstellen die van toepassing zijn op inbreuken op de verordening.[94]

[92] Artikel 4 lid 4 Algemene Verordening Gegevensbescherming.
[93] Overweging 58 Algemene Verordening Gegevensbescherming, p. 30.
[94] Artikel 84 Algemene Verordening Gegevensbescherming.

Hoofdstuk 4. Het beleid en de werkwijze binnen de GGD

4.1 Het beleid

De GGD werkt met veel verschillende persoonsgegevens. De vraag vanuit de organisatie was in beginsel om het huidige beleid omtrent verwerking van persoonsgegevens te toetsen aan huidige en in de toekomst in te voeren wet- en regelgeving. Binnen het overkoepelende systeem Decos, waar interne documenten in worden verwerkt en door middel van gesprekken ben ik daarom op zoek gegaan naar het beleid dat wordt gevoerd met betrekking tot de verwerking van persoonsgegevens.

Bij mijn eerste vraag naar het huidige privacybeleid van de GGD werd ik doorverwezen naar het intranet. Op deze interne website van de GGD is specifieke aandacht besteed aan informatieveiligheid.[95] Hierin stelt de GGD zorgvuldig om te gaan met informatie. *"Dat doen we door de bedrijfsvoering op die onderdelen veilig te stellen die met informatievoorziening te maken hebben en wettelijke verplichtingen na te komen".* Dit gaat de GGD doen door stap voor stap de informatieveiligheid op het vereiste niveau te krijgen. In het stukje op intranet worden medewerkers verzocht om verantwoord gedrag te vertonen. Op het intranet is daarnaast een lijst met do's en don'ts opgenomen (zie bijlage II).[96] Hierin zijn tips opgenomen om informatie zo goed mogelijk te beschermen. Voor informatieveiligheid is echter meer nodig dan de bescherming van verwerkte persoonsgegevens. Wat op het intranet niet duidelijk wordt, is op welke manier de persoonsgegevens verwerkt dienen te worden. Dat er bijvoorbeeld een toets moet worden gedaan op proportionaliteit en subsidiariteit voordat persoonsgegevens worden verwerkt.

4.1.1 Beleid in het verleden

Het beleid 2009-2013 informatiebeveiliging richtte zich op de beveiliging van persoonsgegevens. Uit navraag bij de medewerkers die op dit moment bezig zijn beleid omtrent informatieveiligheid op te stellen, blijkt dat dit niet het huidige beleid binnen de GGD is.

Dan is er nog de Privacyrichtlijn GGD Hart voor Brabant 2013.[97] Deze richtlijn dateert uit 2013. Waar de richtlijn in het begin algemeen van aard is, richt zij zich uiteindelijk in het bijzonder op de Jeugdgezondheidszorg (JGZ), waar het systeem Kidos wordt gebruikt. Deze richtlijn is niet geheel conform huidige en in de toekomst in te voeren wet- en regelgeving. Deze richtlijn blijft voor dit onderzoek verder buiten beschouwing, aangezien zij niet het gehele onderzoek omvat. Wel kan de GGD deze richtlijn doormiddel van dit onderzoek later eenvoudig aanpassen.

4.1.2 Huidig beleid

Op het intranet wordt op dit moment aandacht besteed aan de meldplicht datalekken. Er zijn intern afspraken gemaakt over hoe medewerkers moeten handelen op het moment dat zij een datalek constateren. Zij melden dit bij de servicedesk en de servicedesk communiceert dit met de functionaris. De functionaris maakt dan een afweging over het al dan niet melden van het datalek aan de AP en aan de betrokkene.

Er is een beleidsplan onderdeel informatieveligheid 2015-2017 (hierna: beleidsplan). Volgens het beleidsplan is het doel in deze periode een informatieveiligheidsbeleid op te stellen en in 2017 het basisniveau informatieveiligheid bereikt te hebben (zie bijlage I).[98]

Daarnaast is er het document "Prestatie indicatoren bij onderdeel beleidsplan informatieveiligheid 2016". Hieruit blijkt dat ernaar wordt gestreefd om in 2016 een aantal

[95] Informatieveiligheid intranet GGD.
[96] Bijlage II, do's en don'ts.
[97] Privacyrichtlijn 2013.
[98] Bijlage I, Beleidsplan 2015-2017.

punten aan te pakken (zie bijlage III).[99] Op dit moment inventariseert de GGD daarom welke persoonsgegevens worden verwerkt binnen de organisatie. Daarnaast werkt de organisatie aan het sluiten van bewerkersovereenkomsten met de verschillende bewerkers waarmee wordt samengewerkt. De meeste verwerkers hebben deze overeenkomst inmiddels ondertekend. Er wordt nog gewerkt aan de verwerkers die dat tot op heden niet hebben gedaan. Bovendien besteed de GGD op dit moment aandacht aan het juist inrichten van systemen waarin persoonsgegevens worden verwerkt door het inventariseren van autorisatie en authenticatie binnen de systemen. Er wordt gestuurd naar verantwoorde functiescheiding waar dit nodig is.

Middels intranet wordt gewerkt aan de kennis en het bewustzijn van medewerkers wat betreft informatieveiligheid.

Op basis van een vergelijking tussen het beleidsplan en de praktijk is duidelijk dat een groot aantal aspecten van het beleidsplan al daadwerkelijk worden uitgevoerd.

Conclusie:
Binnen de GGD is beleid geweest over de beveiliging van persoonsgegevens. Dit beleid was het informatiebeveiligingsbeleid en het was van toepassing tot 2013. Het sloeg, zoals de naam al aangeeft, enkel op de beveiliging van persoonsgegevens.

Daarnaast is er een richtlijn waarvan de naam suggereert dat het een GGD-brede richtlijn is. Nader onderzoek wijst echter uit dat deze richtlijn voornamelijk wordt gebruikt door JGZ medewerkers. Ook deze richtlijn dateert uit 2013.

Aan de hand van een meer recent document[100] (Bijlage I) luidt de conclusie dat er op dit moment geen beleid is dat GGD-breed geldt, als het gaat om de verwerking van persoonsgegevens. Er wordt hard gewerkt om dit beleid tot stand te brengen.

Voor enkele van de te behalen doelen is de voortgang al duidelijk. Zo wordt er op dit moment een inventarisatie gemaakt van de verwerking van persoonsgegevens en wordt er gewerkt aan het bewustzijn van de medewerkers. Van groot belang voor het op te stellen beleid is dat er niet enkel beleid komt omtrent de beveiliging van de persoonsgegevens, maar omtrent het gehele proces dat behoort tot verwerking van persoonsgegevens.

Uit het stuk op intranet blijkt hoe medewerkers om moeten gaan met de bescherming van persoonsgegevens om dit verantwoord te doen. Er blijkt echter niet op welke wijze er verantwoord persoonsgegevens kunnen worden verwerkt. Over de meldplicht datalekken staat op het intranet een stuk. Hierin staat hoe werknemers moeten handelen als een datalek geconstateerd wordt. Dit stuk is summier. Er moet concreter uitgewerkt worden wanneer sprake is van een datalek en wanneer dit gemeld moet worden. Ook moet er meer aandacht worden besteed aan de andere aspecten die de verwerking van persoonsgegevens omvat. Op dit moment wordt er enkel gewezen op de bescherming van persoonsgegevens.

[99] Bijlage III, Prestatie indicatoren.
[100] Bijlage I, Beleidsplan 2015-2017.

Hoofdstuk 5. Werkwijze GGD

Bij de GGD komt dagelijks een grote stroom van persoonsgegevens binnen. Doormiddel van verschillende kanalen en systemen verwerkt de GGD deze gegevens. Om de werkwijze van de GGD te toetsen aan de Wbp is er voor gekozen het onderwerp af te bakenen. Omdat de stroom van persoonsgegevens zo omvangrijk is, is er in overleg met de organisatie voor gekozen een beperkt aantal systemen waarmee binnen de GGD gegevens worden verwerkt te analyseren. De systemen die binnen dit onderzoek vallen, zijn Kidos, Orion Globe, Orion Forensisch, HP Zone, Topdesk KCC en Tubis.

Voor dit onderzoek zijn verschillende gesprekken gevoerd met de functioneel beheerders van bovengenoemde systemen. Zij hebben in beeld hoe de systemen werken en hoe binnen deze systemen wordt omgegaan met de verschillende aspecten van verwerking van persoonsgegevens. De functioneel beheerders die zelf niet dagelijks met de systemen werken hebben mij voor nadere informatie doorverwezen naar collega´s die dat wel doen. Doormiddel van deze gesprekken is duidelijk geworden wat de huidige werkwijze is binnen de GGD bij de verwerking van persoonsgegevens.

Hierna volgt een korte omschrijving van ieder systeem. Daarna volgt een schematische weergave van de bevindingen zoals die naar voren zijn gekomen uit dit onderzoek.

Kidos
Kidos is het systeem waarmee gewerkt wordt door de Jeugdgezondheidszorg (hierna: JGZ). In dit systeem worden op verschillende wijzen persoonsgegevens verwerkt. Gemeenten transporteren GBA-gegevens van kinderen naar dit systeem, maar ook de persoonsgegevens van de ouders worden verwerkt. Daarnaast importeren medewerkers van het Klantcontactcentrum van de GGD persoonsgegevens in dit systeem. Ook de medewerkers van JGZ verwerken gegevens in het systeem. Hierbij valt te denken aan verpleegkundigen, jeugdartsen en secretarieel medewerkers.

Orion Globe
Dit is het systeem dat wordt gebruikt door het team Reizigerszorg. In dit systeem wordt bijvoorbeeld verwerkt welke reizen klanten maken en welke vaccinaties zij daarvoor hebben gehad.

Orion Forensisch
Dit systeem wordt gebruikt door het team Forensische geneeskunde. Op deze afdeling wordt onder andere arrestantenzorg verleend. Arrestantenzorg wordt bijvoorbeeld verleend wanneer een persoon wordt gearresteerd en medische hulp nodig heeft in de cel. De politie schakelt op dat moment de GGD in om deze zorg te verlenen. Artsen werken hier in 24- uurs diensten, zodat er altijd een arts beschikbaar is. Verschillende artsen werken daarom vaak met eenzelfde persoon en hebben dus ook de gegevens van deze personen nodig. Daarnaast doet dit team lijkschouwingen en verwerkt hij de gegevens daarover.

HP Zone
Dit systeem wordt gebruikt op de afdeling Infectieziektebestrijding en SOA van de GGD. In dit systeem worden gegevens verwerkt naar aanleiding van telefoongesprekken met klanten waarin vragen worden gesteld. Er wordt een melding in dit systeem aangemaakt na een telefoongesprek. Voor sommige infectieziekten geldt een meldplicht. Van personen die zo'n ziekte melden worden dan ook gegevens vermeld. In dat geval worden de naam, geboortedatum het bsn-nummer en de infectieziekte gemeld. Daarnaast komen er meldingen binnen van kinderdagverblijven en scholen, bijvoorbeeld over geconstateerde huiduitslag. Als van deze situatie sprake is, worden enkel de gegevens van de melder verwerkt en niet die van de personen met de aandoening. Ook labuitslagen

die binnenkomen via de zorgmail, vanuit ziekenhuizen of huisartslaboratoria worden verwerkt in het systeem.

Topdesk KlantContactCentrum (KCC)
Topdesk KCC is het systeem dat op het Klantcontactcentrum wordt gebruikt. Met dit systeem worden vragen van klanten verwerkt. In de eerste plaats kunnen er e-mailberichten binnen komen met een hulpvraag van de klant. Medewerkers van het Klantcontactcentrum sturen deze e-mailberichten door naar de juiste afdeling. De berichten worden op dat moment verwerkt in het systeem. Daarnaast zitten er medewerkers op het Klantcontactcentrum die klanten telefonisch te woord staan. Zij plannen afspraken in voor klanten in de verschillende afspraaksystemen. Deze systemen zijn vervolgens weer gekoppeld aan de afdeling waarvoor zij bestemd zijn. Zo kan een medewerker van het Klantcontactcentrum dus bijvoorbeeld in het systeem Orion Globe en Kidos om afspraken in te plannen.

Tubis
Tubis is een landelijke database van de GGD voor tuberculose (TBC). Tubis wordt volgend jaar vervangen door een ander systeem. In principe zie je als medewerker van de GGD HvB alleen de gegevens van de klanten die staan geregistreerd binnen de GGD HvB. Het systeem bestaat uit 2 delen. Je hebt enerzijds het dossier waarin de gegevens van de klanten staan. Anderzijds worden er de röntgenfoto's van klanten geregistreerd. Deze twee verschillende dossiers worden door het systeem aan elkaar gekoppeld.

5.1 Schematische weergave

In het schema in bijlage IV staat vermeld welke persoonsgegevens worden verwerkt binnen elk systeem.[101] Deze gegevens zijn uit voormelde gesprekken naar voren gekomen tijdens het onderzoek. De gevoerde gesprekken waren gericht op onderzoek naar de vraag welke persoonsgegevens zijn verwerkt. Per systeem is daarnaast onderzocht of er volgens de medewerkers een doel is geformuleerd om de persoonsgegevens te verwerken en op welke wettelijke grondslag de verwerking is gebaseerd. Daarnaast is onderzocht hoe de autorisatie, het delen van persoonsgegevens, de bewaartermijnen, de manier van vernietigen en het inzagerecht is geregeld. Ten slotte is onderzocht of men op de werkvloer op de hoogte is van de meldplicht datalekken en de beoogde handelswijze bij datalekken.

Dit onderzoek richt zich uitsluitend op de verwerking van persoonsgegevens van klanten binnen de 6 voormelde systemen. Uit het onderzoek blijkt (zie bijlage IV) dat binnen de onderzochte systemen van de GGD de volgende persoonsgegevens van klanten worden verwerkt:

- naam, adres en woonplaats (hierna: NAW);
- contactgegevens (e-mailadressen en telefoonnummers);
- gegevens betreffende de gezondheid, medische gegevens, patiëntendossiers;
- BSN nummer;
- geboortedatum;
- nationaliteit;
- geslacht;
- verzekeringsgegevens.

5.2 Werkwijze in de praktijk

Alvorens de huidige werkwijze, die blijkt uit onderzoek binnen de 6 systemen, te toetsen aan de Wbp en vervolgens de belangrijkste wijzigingen die de AVG meebrengt te toetsen volgen hierna de bevindingen uit het praktijkonderzoek.

[101] Bijlage IV, Schematische weergave van de gevoerde gesprekken.

Tijdens het onderzoek dat voornamelijk heeft bestaan uit het voeren van gesprekken met medewerkers (zie bijlage V) bleek dat de informatieveiligheid vooral op niveau van het management als een belangrijk punt wordt gezien.[102] Dit blijkt ook uit het beleid dat op dit moment wordt opgesteld. Het management wijst er bij de medewerkers op dat deuren gesloten moeten blijven voor mensen die geen sleutel hebben. Zo vraagt hij aan medewerkers om zelf je gasten bij de receptie op te halen. Daarnaast moet het scherm van de computer worden vergrendeld bij het verlaten van je werkplek. Bovendien moet er “clean-desk” worden gewerkt. Dit betekent dat de medewerker er bij het verlaten van de werkplek voor moet zorgen dat er geen vertrouwelijke informatie achterblijft.

De mensen die dagelijks met de systemen en de persoonsgegevens werken, hebben de informatieveiligheid niet altijd even hoog op de agenda staan. Zij richten zich in de eerste plaats op de primaire taak, het verlenen van zorg. Daarbij heeft niet iedereen altijd in de gaten hoe kwetsbaar het systeem wordt als daarbij de informatieveiligheid uit het oog wordt verloren. Zo stonden tijdens dit onderzoek gedurende tenminste 2 dagen de beveiligde deuren op de locatie Tilburg geopend. Dit betekent dat iedereen, ook een onbevoegde, naar binnen kon lopen in de ruimtes waar gewerkt wordt met persoonsgegevens. Daarnaast viel het op dat tijdens de lunchpauze verschillende computers niet vergrendeld waren. Hierdoor is geen autorisatie nodig om in systemen te komen waarin persoonsgegevens zijn verwerkt. Deze combinatie zorgt voor een situatie waarin de bescherming van persoonsgegevens niet kan worden gewaarborgd.

Waar het voor de personen die bezig zijn met het opstellen van het beleid goed duidelijk is wanneer er sprake is van een datalek en hoe er in een dergelijke situatie moet worden gehandeld, blijkt uit de gevoerde gesprekken dat dit onder de medewerkers vaak niet het geval te zijn.

Binnen de verschillende systemen is voor de medewerkers over het algemeen duidelijk met welke persoonsgegevens gewerkt wordt. Ook is duidelijk wanneer sprake is van verwerking van de gegevens. Men is zich er binnen de organisatie over het algemeen van bewust dat al snel sprake is van verwerking.

Het formuleren van een doel en het vaststellen van een wettelijke grondslag op basis waarvan de persoonsgegevens worden verwerkt is niet in ieder systeem concreet geregeld. Hetzelfde geldt voor de bewaartermijnen en de afspraken omtrent vernietiging na verloop van deze termijnen.

Intern delen GGD-medewerkers veel persoonsgegevens. Zowel binnen teams als tussen sommige teams onderling. Alle medewerkers hebben een geheimhoudingsverklaring moeten tekenen op het moment van in dienst treden bij de GGD (zie bijlage VI).[103]

5.3 Toetsing aan de Wbp

De Wbp is van toepassing op de GGD, omdat de organisatie persoonsgegevens verwerkt. Er worden zowel handmatig als geautomatiseerd gegevens verwerkt die een identificeerbare natuurlijke persoon betreffen.

Om te kunnen achterhalen of de huidige manier waarop persoonsgegevens worden verwerkt door de GGD conform de Wbp is, volgt hierna een stapsgewijze toetsing van de werkwijze aan de Wbp.

Aangezien er op dit moment geen geldend beleid is binnen de GGD voor de verwerking van persoonsgegevens, zal dit onderzoek zich hierna enkel richten op de toetsing van de huidige werkwijze aan wet- en regelgeving.

[102] Bijlage V , Uitgewerkt gevoerde gesprekken met medewerkers.
[103] Bijlage VI, Geheimhoudingsverklaring.

Ten eerste dient bij de toetsing te worden opgemerkt dat de WGBO op de verwerking van een aantal persoonsgegevens van toepassing is. In bepaalde gevallen is sprake van een geneeskundige behandelingsovereenkomst. Zo worden op de afdelingen Tuberculose, Jeugdgezondheidszorg en Infectieziekten, mensen behandeld voor aandoeningen door artsen. In dat geval geldt de extra plicht dat er een wettelijke grondslag moet zijn om de wettelijke geheimhoudingsplicht te doorbreken.[104] Deze plicht geldt naast de eisen uit de Wbp. Dit betekent dat het enkel aanwezig zijn van een grondslag om de geheimhoudingsplicht te doorbreken niet voldoende is. Er moet namelijk bovendien worden voldaan aan de eisen uit de Wbp. Het zijn dus cumulatieve voorwaarden waar aan moet worden voldaan alvorens de gegevens die onder de WGBO vallen bijvoorbeeld te delen.

Ook voor andere geheimhoudingsplichten uit bijzondere wetten die van toepassing zijn op de GGD geldt dat het cumulatieve voorwaarden betreffen.

Hierna volgt een stapsgewijze toetsing van de huidige werkwijze aan de Wbp.

5.3.1 Doelbinding

Voor de verwerking van persoonsgegevens moet een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doeleinde zijn. De GGD heeft een register verwerking persoons-gegevens (zie bijlage VII).[105] Voor de systemen Kidos, Orion Globe, Tubis, HP Zone en Orion Forensisch zijn hierin uitdrukkelijk de doeleinden van verwerking geformuleerd. Binnen Topdesk KCC is geen uitdrukkelijk omschreven doel vastgesteld. Het vaststellen van dit doel is van belang om later de rechtmatigheid van de verwerking te kunnen aantonen. Een doel dat voor Topdesk KCC kan worden geformuleerd, is bijvoorbeeld “het verzamelen en verwerken van gegevens om dit naar de juiste afdeling binnen de GGD te kunnen zenden”.

5.3.2 Grond

De verwerking van veel gegevens binnen de systemen gebeurt op grond van een wettelijke plicht.[106]

De eerste wettelijke plicht die hierbij aandacht verdient is die uit de Wet publieke gezondheid (hierna: Wpg). Op grond van deze wet is het voor de afdeling JGZ namelijk verplicht om een digitaal dossier bij te houden.[107] Het zogenaamde “kinddossier”. Hierbij zijn alle privacy eisen uit zowel de WGBO als de Wbp van toepassing.[108]

Voor infectieziekten geldt op grond van de Wpg in bepaalde gevallen een meldingsplicht aan de GGD.[109] In die gevallen moet in elk geval de naam, het adres, de geboortedatum, het BSN nummer, de verblijfplaats van de betrokkene en de infectieziekte worden gemeld. tuberculose is een meldingsplichtige infectieziekte. De verwerking van de gegevens omtrent tuberculose in het systeem Tubis is dus ook gebaseerd op de wettelijke plicht.[110]

Omdat deze wettelijke plichten zijn gericht op de dossiervoering, kan de GGD zijn wettelijke verplichting redelijkerwijs niet nakomen zonder de verwerking van de persoonsgegevens.[111]

---

[104] Artikel 7:457 Burgerlijk Wetboek.
[105] Bijlage VII, Register verwerking persoonsgegevens.
[106] Artikel 8 onder c Wet bescherming persoonsgegevens.
[107] Artikel 5 Wet publieke gezondheid.
[108] Kamerstukken II 2007-2008 , 31 316, nr. 3, p. 32.
[109] Artikel 21 Wet publieke gezondheid.
[110] Artikel 1 onder f Wet publieke gezondheid.
[111] Artikel 8 onder c Wet bescherming persoonsgegevens.

Verder wordt er binnen de systemen Topdesk KCC en Orion Globe met name gewerkt met veronderstelde toestemming. Er wordt bij het Klantcontactcentrum bijvoorbeeld vanuit gegaan dat klanten er bij het delen van gegevens mee instemmen dat deze gegevens worden verwerkt door de GGD. Ook bij afdeling Reizigers waar het systeem Orion Globe wordt gebruikt wordt uitgegaan van toestemming voor de verwerking. Binnen de afdeling Infectieziekten wordt geen expliciete toestemming gevraagd voor de verwerking van persoonsgegevens. Waar een wettelijke plicht geldt voor de verwerking van gegevens omtrent meldingsplichtige infectieziekten, is dit niet het geval voor niet meldingsplichtige infectieziekten. Voor de verwerking van deze gegevens moet dus een andere grondslag zijn dan de wettelijke plicht.

De toestemming waarop de verwerking volgens de wet mag worden gebaseerd moet ondubbelzinnig zijn.[112] Bij de GGD mag dus geen enkele twijfel bestaan over de vraag of de betrokkene zijn toestemming heeft verleend. De manier waarop op dit moment de toestemming wordt verondersteld voldoet niet aan deze eis uit de wet. Er wordt over het algemeen niet geïnformeerd of klanten toestemming geven voor de verwerking. Binnen Kidos, waar de verwerking tevens kan worden gebaseerd op een wettelijke grondslag, wordt soms tijdens een consult de toestemming gevraagd voor de verwerking en het delen van persoonsgegevens.

Voor klanten is door de wijze waarop toestemming op dit moment wordt verondersteld, niet duidelijk waarvoor zij concreet toestemming zouden hebben verleend. Om aan deze wettelijke eis te voldoen, zou de GGD voorafgaand aan de verwerking van persoons-gegevens de toestemming moeten vragen aan klanten. Op die wijze kan er geen onduidelijkheid bestaan over de al dan niet verleende toestemming en de reikwijdte van deze toestemming. De toestemming kan worden gevraagd door een formulier in te laten vullen door klanten voorafgaand aan de verwerking. Hierop kan de klant aangeven of hij akkoord is met de verwerking van de persoonsgegevens en voor welke verwerking hij akkoord geeft. Voor het Klantcontactcentrum is het voorafgaand vragen van toestemming middels een formulier niet mogelijk. Zij hebben immers enkel contact met klanten via de mail of de telefoon. In dat geval kan de GGD telefonisch de toestemming vragen. Dit valt de eerste drie maanden nog te bewijzen door de opnames van de gesprekken terug te luisteren. Omdat het bewijs na die drie maanden verdwijnt moet er gezocht worden naar een andere oplossing. Zo kan de GGD een bevestiging verzenden aan de betrokkene over de al dan niet verleende toestemming. Bovendien kan de GGD verwijzen naar een privacybeleid dat dan op het internet moet worden gezet.

De grond medische noodzaak zal voor de GGD zelden van toepassing zijn.[113] Het komt niet vaak voor dat het een kwestie van leven of dood betreft. Dit zou vooral het geval kunnen zijn binnen de afdeling Forensische geneeskunde, omdat daar arrestantenzorg wordt verleend. Het kan zijn dat een arrestant in een situatie van leven of dood terechtkomt waarbij de GGD de gegevens moet verwerken. Daarnaast speelt de GGD een belangrijke rol in rampenbestrijding binnen gemeenten. In het geval van ernstige rampen kan deze grond van toepassing zijn.

De conclusie is dat de GGD op basis van artikel 8 onder c voor de verwerking van bepaalde persoonsgegevens een gerechtvaardigde grondslag heeft, namelijk de wettelijke plicht. De veronderstelde toestemming voor de overige persoonsgegevens voldoet niet aan de wettelijke eisen. De GGD zal dus actief de toestemming moeten vragen van klanten om de persoonsgegevens te verwerken of verder te verwerken. Als de organisatie dit niet doet, kan zij er niet vanuit gaan dat de klanten toestemming hebben

[112] Artikel 8 onder a Wet bescherming persoonsgegevens.
[113] Artikel 8 onder d Wet bescherming persoonsgegevens.

verleend. Bovendien is dan niet duidelijk voor welke verwerking de klanten toestemming hebben verleend.

Proportionaliteit en subsidiariteit
De verwerking van persoonsgegevens door de GGD moet ten alle tijden proportioneel en subsidiair zijn.[114] Dit betekent dat de verwerking niet onevenredig mag zijn ten opzichte van het te dienen doel. En het doel moet niet op een minder ingrijpende manier bereikt kunnen worden dan door deze verwerking. In de praktijk betekent dit voor de GGD dat er in bepaalde gevallen over moet worden gegaan tot bijvoorbeeld anonimiseren van persoonsgegevens. Dat is soms een minder ingrijpende manier om het zelfde doel te bereiken. Voor statistieken is het bijvoorbeeld niet nodig om de gegevens zodanig te bewaren dat ze herleidbaar zijn tot een identificeerbaar individu. Anonimiseren zorgt in dat geval voor een minder ingrijpende manier om een zelfde doel te bereiken.

5.3.3 Bewaartermijn
Binnen de GGD is veelal niets geregeld over de bewaartermijn en de wijze van vernietiging van persoonsgegevens. Uit onderzoek blijkt dat dit met name te maken heeft met de digitalisering van de systemen. Waar voor de papieren dossiers vaak afspraken zijn over de bewaartermijn en de wijze van vernietiging, is dit voor de digitale systemen niet geregeld. Een enkel systeem baseert de bewaartermijn op een wettelijke grondslag. Zo mogen medische gegevens 10 jaar worden bewaard op grond van de wet.[115] In het systeem HP Zone refereert de functioneel beheerder aan deze bewaartermijn. Ook daar wordt echter aangegeven dat dossiers enkel worden gesloten, maar nooit worden vernietigd. Binnen het systeem Kidos is een bewaartermijn. Onduidelijk is wat deze bewaartermijn is, maar ook binnen dit systeem worden geen gegevens verwijderd. Binnen Tubis wordt aangegeven dat er niet voldoende mankracht is om digitale dossier te verwijderen. Er is geen manier om dit op grote schaal te doen en voor het individueel verwijderen van dossiers is geen tijd.

Conclusie: Op dit moment voldoet de GGD niet aan de Wbp op het punt van de bewaartermijnen. In de digitale systemen worden persoonsgegevens op dit moment nooit verwijderd. Om aan de Wbp te voldoen moet de GGD per systeem en per categorie persoonsgegevens nagaan of er nog voldoende grond is om bepaalde gegevens te bewaren. De wet kent geen algemene bewaartermijn. Er moet beleid komen omtrent de bewaartermijnen en de vernietiging van de persoonsgegevens. Het gaat daarbij om een afweging die de organisatie zelf moet maken. Deze bewaartermijnen zullen per systeem verschillen, omdat er steeds met verschillende gegevens en op basis van verschillende doeleinden wordt verwerkt.

5.3.4 Beveiliging van persoonsgegevens
De GGD is als verantwoordelijke verplicht om passende maatregelen te treffen ter beveiliging van persoonsgegevens.[116] Binnen de systemen wordt altijd gewerkt met autorisatie. In het ene systeem is de autorisatie concreter geregeld dan in andere. Zo wordt binnen zowel Orion Globe als Kidos door de functioneel beheerder aangegeven dat deze autorisatie strikter zou kunnen. Op dit moment kunnen daar mensen bij persoonsgegevens waar zij in beginsel geen toegang tot hoeven te hebben. Er moeten meer lagen aangebracht worden in de autorisatie. Zo hoeven de secretarieel medewerkers niet de zelfde autorisatie te hebben als de artsen die in de medische dossiers van betrokkenen moeten kunnen.

Binnen het KCC wordt soms gewerkt op het account van collega's. Dit is op dit moment enkel nog het geval bij het onderdeel reizigerszorg. De autorisatie wordt hier dus als het

[114] HRECLI:NL:HR:2011:BQ8097.
[115] Artikel 7:454 lid 3 Burgerlijk Wetboek.
[116] Artikel 13 Wet bescherming persoonsgegevens.

ware doorgegeven. Voor een betere beveiliging van persoonsgegevens is het van belang dat iedere persoon een eigen account heeft met de juiste autorisatie in de systemen.

De GGD werkt samen met verschillende verwerkers. Zo wordt voor het systeem Tubis gewerkt met de externe verwerker Rosenboom (Alca/ACHA) en voor het systeem HP Zone met Infact. Omdat de GGD ook voor de beveiliging van deze persoonsgegevens verantwoordelijk is, moet de organisatie afspraken maken met de verwerkers. Dit kan middels een bewerkersovereenkomst. Met de meeste verwerkers binnen alle systemen waarmee gewerkt wordt binnen de GGD is op dit moment al een bewerkersovereenkomst afgesloten. Een aantal verwerkers heeft deze overeenkomst echter nog niet willen tekenen. Voor dit onderzoek van belang is in dat kader de bewerkersovereenkomst met Infact die op dit moment nog ontbreekt door het uitblijven van ondertekenen door de bewerker.

5.3.5 Informatie

Een van de rechten die de betrokkene op grond van de Wbp heeft is het recht op informatie.[117] Dit recht bestaat uit het recht op kennisneming van de betrokkene en de plicht om informatie te verstrekken van de verantwoordelijke.[118]

Bij de systemen Kidos, Tubis, Orion Forensisch en Topdesk KCC is het mogelijk voor de betrokkene om een formulier in te vullen. Met dit formulier kan hij aangeven op welke manier hij de verwerkte persoonsgegevens wil inzien. Dit kan door het dossier bij de organisatie zelf in te zien, maar ook door een uitdraai van het dossier mee te krijgen. In het systeem Orion Globe is op dit moment niets geregeld omtrent het recht op informatie van de betrokkene. Dit punt staat bij de medewerkers op dit moment wel op de agenda. Het gaat op deze afdeling meestal om vaccinatieboekjes van klanten. Het plan op deze afdeling is om ervoor te zorgen dat klanten straks zelf in kunnen loggen om het vaccinatieboekje te downloaden. Binnen het systeem HP Zone is het nog nooit voorgekomen dat een klant gebruik heeft gemaakt van het recht op informatie. Als een klant daar een beroep op doet, wordt dit geregeld. Er is echter niets afgesproken over de manier waarop dit moet gebeuren.

Om aan de Wbp te voldoen moet binnen ieder systeem het recht op informatie gewaarborgd zijn. Op dit moment wordt dit recht ten alle tijden gewaarborgd, omdat de klant altijd toegang krijgt tot de gegevens. Waar het echter voor de systemen Kidos, Tubis, Orion Forensisch en Topdesk KCC via vaste kanalen wordt gewaarborgd, is dit bij de systemen Orion Globe en HP Zone nog niet het geval. Deze twee laatste systemen moeten zorgen voor een manier waarop zij structureel gaan voldoen aan de plicht om op zijn verzoek informatie te verstrekken aan de betrokkene.

5.3.6 Verwerking van bijzondere persoonsgegevens

Binnen de GGD vindt op grote schaal verwerking van bijzondere persoonsgegevens plaats. Hierbij worden vooral gegevens betreffende de gezondheid verwerkt. Daarnaast verwerkt de GGD soms ook gegevens betreffende iemands seksuele leven.

Op grond van de Wbp is het in beginsel verboden om bijzondere persoonsgegevens te verwerken. Er moet een uitzondering van toepassing zijn om dit te mogen doen. Op de GGD is een uitzondering van toepassing, omdat de organisatie valt onder artikel 21 Wbp.[119]

Op grond van de Wbp mogen persoonsgegevens door de GGD enkel worden verwerkt door personen die uit hoofde van hun ambt, beroep, wettelijke plicht of krachtens

[117] Artikel 33 tot en met 35 Wet bescherming persoonsgegevens.
[118] Artikel 33 en 34 Wet bescherming persoonsgegevens.
[119] Artikel 21 lid 1 onder a Wet bescherming persoonsgegevens.

overeenkomst tot geheimhouding zijn verplicht.[120] Er zijn medewerkers binnen de GGD die op grond van hun ambt een geheimhoudingsplicht hebben. Dit zijn bijvoorbeeld artsen en verpleegkundigen.[121] [122] Daarnaast zijn er medewerkers die op grond van de wettelijke plicht een geheimhoudingsplicht hebben op grond van de ambtenarenwet.[123] Naast deze wettelijke geheimhoudingsplichten hebben alle medewerkers van de GGD een geheimhoudingsverklaring moeten tekenen bij indiensttreding. Dat betekent dat alle medewerkers ten minste contractueel gebonden zijn aan de geheimhouding, maar de meeste ook wettelijk op grond van bovenstaande wettelijke bepalingen.

Soms kan het voor de GGD noodzakelijk zijn om andere bijzondere persoonsgegevens te verwerken. Hierbij valt bijvoorbeeld te denken aan het verwerken van iemands seksuele leven als er een behandeling nodig is tegen een SOA. Dit is op grond van de Wbp ook toegestaan, omdat het verwerken van deze gegevens noodzakelijk is met het oog op een goede behandeling van de betrokkene.[124] Zonder deze gegevens kan de GGD de betrokkene niet voorzien van de juiste zorg.

Conclusie: Op grond van de Wbp is het de GGD toegestaan om bijzondere persoonsgegevens te verwerken. Omdat de GGD valt onder een uitzondering uit de wet is het verbod op de organisatie niet van toepassing.

Wat betreft de verwerking van persoonsgegevens voldoen de systemen binnen de GGD aan de Wbp. Er hoeft op dit gebied dus niets te veranderen om te voldoen aan huidige wet- en regelgeving. De verwerking van bijzondere persoonsgegevens binnen de GGD is rechtmatig.

5.3.7 Meldplicht datalekken

Uit een gesprek met de functionaris gegevensbescherming van de organisatie blijkt dat hij duidelijk in beeld heeft wanneer sprake is van een datalek. Ook heeft hij een schema om na te gaan of de plicht bestaat om een melding te doen aan de AP op het moment dat sprake is van een datalek. De functionaris is van mening dat er zo transparant mogelijk moet worden gewerkt, met name richting de klant. Op het moment dat er sprake is van een datalek zal de GGD dat dus altijd communiceren met de betrokkene. Op dit punt voldoet de GGD dus aan de Wbp.

Het is echter wel de vraag of een datalek altijd wordt geconstateerd. Uit navraag onder medewerkers blijkt dat zij veelal niet weten wanneer sprake is van een datalek. Het is voor hen bovendien niet duidelijk waar zij een datalek moeten melden. Het bewustzijn op dit gebied moet beter worden. Omdat veel verschillende werknemers met persoonsgegevens werken, moeten zij op de hoogte zijn van de wetgeving om te kunnen zorgen dat deze wordt nageleefd. Als men niet weet wanneer sprake is van een datalek, zal dit niet tijdig worden geconstateerd en kan het juiste proces niet in werking worden gesteld. Dit probleem kan worden opgelost door het geven van uitleg, bijvoorbeeld in een presentatie, waarin stapsgewijs wordt uitgelegd wanneer er sprake is van een datalek. Om te zorgen dat de afweging over het al dan niet meldingsplichtig zijn van een datalek goed gebeurt, moet dit over worden gelaten aan de functionaris. Het moet voor de medewerkers duidelijk zijn dat zij ieder mogelijk lek melden. De functionaris kan dan nagaan of er stappen moeten worden ondernomen richting de AP en de betrokkene.

5.3.8 Functionaris gegevensbescherming

Een organisatie die gegevens verwerkt moet dit op grond van de Wbp melden aan de AP,

[120] Artikel 21 lid 2 Wet bescherming persoonsgegevens.
[121] Artikel 7:457 Burgerlijk wetboek.
[122] Artikel 88 Wet op de Beroepen in de Individuele Gezondheidszorg.
[123] Artikel 125 a Ambtenarenwet.
[124] Artikel 21 lid 3 Wet bescherming persoonsgegevens.

wanneer er sprake is van geheel of gedeeltelijk geautomatiseerde verwerking.[125] Een organisatie kan er echter voor kiezen om een functionaris gegevensbescherming (hierna: functionaris) aan te stellen.[126] Als er een functionaris is aangesteld, moet voormelde melding worden gedaan aan de functionaris.[127] In deze melding moet tenminste het volgende worden opgenomen dat voor de GGD van belang is:

- de naam en het adres van de verantwoordelijke;
- het doel of de doeleinden van de verwerking;
- een beschrijving van de categorieën van betrokkenen en van de gegevens of categorieën van gegevens die daarop betrekking hebben;
- de ontvangers of categorieën van ontvangers aan wie de gegevens kunnen worden verstrekt;

De functionaris die is aangesteld binnen de GGD is René van Kessel, ook directiesecretaris. De taak van de functionaris is op dit moment, op het gebied van informatieveiligheid, tamelijk passief. Hij wordt vooral betrokken bij situaties als er iets mis is. Als er bijvoorbeeld een datalek geconstateerd is, wordt dit doorgegeven aan de functionaris. De functionaris is op dit moment niet actief bezig met informatieveiligheid en taken die hier mee te maken hebben.

De functie van de functionaris voldoet aan de eisen van de Wbp.[128] Hij is een natuurlijk persoon. Bovendien ontvangt hij bij de uitoefening van zijn taken geen aanwijzingen van de organisatie.

De functionaris moet toezien op de verwerking van persoonsgegevens overeenkomstig de wet. Op dit moment wordt de functionaris enkel betrokken in het proces van de verwerking van persoonsgegevens als er iets mis is, bijvoorbeeld wanneer sprake is van een datalek. Dit is niet voldoende om te voldoen aan de Wbp. De functionaris moet de meldingen omtrent de gegevensverwerking ontvangen en hier toezicht op houden. Om aan de Wbp te voldoen moet de GGD de functie van de functionaris wijzigen. De functionaris moet een actieve rol krijgen in het proces van de verwerking van persoonsgegevens.

5.4 Conclusie

Om aan de Wbp te voldoen moet de GGD nog een aantal acties ondernemen. Waar al een compleet beeld is ontstaan van de verschillende persoonsgegevens die per systeem worden verwerkt, ontbreekt het duidelijk omschreven doel voor de verwerking binnen de afdeling KCC. Er moet een doel worden geformuleerd op grond waarvan de GGD de persoonsgegevens verwerkt binnen dit systeem.

Daarnaast is het verstandig om de verleende toestemming van de betrokkene te concretiseren in de gevallen dat de verwerking niet op een andere grondslag zoals de wettelijke plicht kan worden gebaseerd. Het advies is om het beleid in die zin op te stelen dat er per consult met cliënten, uitdrukkelijk de toestemming wordt gevraagd voor de verwerking van persoonsgegevens. Nu wordt uitgegaan van verleende toestemming. Als hierover later discussie ontstaat met de betrokkene, sta je als organisatie niet erg sterk. Op het moment dat er niet is nagegaan of de betrokkene toestemming heeft verleend, is het achteraf namelijk moeilijk te bewijzen dat deze toestemming bestond. Bovendien is het voor zowel de cliënten als de organisatie op dit moment niet duidelijk waarvoor de cliënt dan stilzwijgend toestemming zouden hebben verleend.

[125] Artikel 27 lid 1 Wet bescherming persoonsgegevens.
[126] Artikel 62 Wet bescherming persoonsgegevens.
[127] Artikel 27 lid 3 Wet bescherming persoonsgegevens.
[128] Artikel 62 tot en met 64 Wet bescherming persoonsgegevens.

De organisatie moet in het beleid bewaartermijnen van persoonsgegevens opnemen. Op dit moment is er een persoon bezig met het inventariseren van alles wat er op dit gebied geregeld is. Deze persoon heeft kennis van zowel de Wbp als van de Archiefwet. De verwachting is daarom dat de GGD binnen afzienbare tijd werkt in overeenstemming met huidige, maar ook in de toekomst in te voeren wet- en regelgeving.

De autorisatie moet binnen sommige systemen worden geconcretiseerd. Dit is vooral het geval binnen de systemen Orion Forensisch en Kidos. Binnen het KCC wordt gewerkt op elkaars autorisatie. Dit kan niet worden aangemerkt als passende maatregel ter beveiliging van persoonsgegevens. De GGD moet dus zorgen voor voldoende accounts voor medewerkers op het KCC. Als er voldoende accounts met de juiste autorisatie zijn, hoeven medewerkers niet langer in te loggen op een ander account dan dat van zichzelf.

Alleen binnen de systemen Orion Globe en HP Zone moet een verandering worden doorgevoerd om op een systematische manier te voldoen aan het recht op inzage voor betrokkene. Het recht wordt op dit moment wel overeenkomstig huidige wet- en regelgeving gewaarborgd. Als een betrokkene immers zijn recht op inzage uit wil gebruiken, wordt hier zowel binnen Orion Globe als HP Zone geregeld. Verder is dit binnen de overige geanalyseerde systemen systematisch en overeenkomstig huidige wet- en regelgeving geregeld. De verandering die binnen deze systemen kan worden doorgevoerd is het bieden van een gestandaardiseerde mogelijkheid om de verwerkte persoonsgegevens in te zien. Voor HP Zone ontbreekt deze mogelijkheid op dit moment en binnen Orion Globe is deze procedure nog niet uitgewerkt.

Wat betreft verwerking van bijzondere persoonsgegevens voldoet de GGD aan huidige wet- en regelgeving. De GGD is bevoegd deze gegevens te verwerken op grond van de wet.

Wat betreft de meldplicht datalekken moet een breder bewustzijn ontstaan onder de medewerkers. Zij zijn de personen die een datalek veelal moeten herkennen en daarop actie moeten kunnen ondernemen. Om het bewustzijn te verbeteren kan een presentatie worden gegeven over de meldplicht datalekken. Vervolgens kunnen de medewerkers een stappenplan krijgen aan de hand waarvan zij na kunnen gaan of er sprake is van een datalek. Om te voorkomen dat er een verkeerde afweging wordt gemaakt over het al dan niet meldingsplichtig zijn van een datalek moeten medewerkers alle datalekken melden bij de functionaris. Vervolgens kan de functionaris beslissen of er sprake is van een meldingsplicht. De processen omtrent datalekken zijn goed op orde. Op dit punt voldoet de GGD dus aan de huidige wetgeving.

5.5 Toetsing aan de Algemene Verordening Gegevensbescherming (AVG)

Om aan de AVG te voldoen moet de GGD nog een aantal stappen zetten. Hierna volgen de veranderingen die door de organisatie moeten worden gerealiseerd voordat de werkwijze voldoet aan de eisen die vanaf mei 2018 gelden op grond van de verordening. Een aantal wijzigingen uit de AVG werkt breder dan enkel binnen de geanalyseerde systemen. Deze wijzigingen zullen dan ook in het GGD brede beleid moeten worden verwerkt. Hierbij is van groot belang dat de boetebevoegdheid van de AP verandert. De boetes die door de AP kunnen worden opgelegd zijn enorm. Het is daarom van het grootste belang om aan de eisen uit de verordening te voldoen.

5.5.1 Toestemming

Op grond van de AVG kan de verwerking van persoonsgegevens op grond van toestemming nog steeds plaatsvinden. In dit opzicht verandert er dus niets ten opzichte van de Wbp. Wat wel verandert is dat het op grond van de AVG moet gaan om ondubbelzinnige of expliciete toestemming. De bewijslast van deze al dan niet gegeven toestemming komt bij de GGD te liggen. Een duidelijke, actieve handeling van de betrokkene moet leiden tot de toestemming. De veronderstelde toestemming waar op dit

moment mee wordt gewerkt binnen de systemen HP Zone, Orion Globe en Topdesk KCC voldoet dus niet aan de AVG.

Bij het geven van toestemming moet het voor de betrokkene duidelijk zijn voor welke verwerking toestemming wordt gegeven. Ook moet op het moment van het verkrijgen van de toestemming worden vermeld dat deze toestemming op een later moment weer kan worden ingetrokken.

Om aan de AVG te voldoen zal de organisatie ervoor moeten zorgen dat er, bijvoorbeeld middels standaardformulieren, toestemming gevraagd wordt aan cliënten alvorens de persoonsgegevens worden verwerkt. Hierbij moet de betrokkene per doeleinde aan kunnen geven of zijn gegevens daarvoor mogen worden verwerkt. Wanneer persoonsgegevens worden verwerkt naar aanleiding van gevoerde telefoongesprekken en binnenkomende email is het standaardformulier geen optie. In het geval van telefoon-gesprekken moet mondeling de toestemming worden gevraagd. Na afloop van het telefoongesprek moet de GGD een bevestiging van deze toestemming verzenden naar de Betrokkene. Telefoongesprekken met klanten worden opgenomen en gedurende 3 maanden bewaard. De eerste drie maanden kan de verleende toestemming door de GGD worden bewezen op basis van die opnames. Vervolgens kan de GGD middels de verzonden bevestiging van de toestemming bewijzen dat de betrokkene akkoord is gegaan met de verwerking van persoonsgegevens. In geval van emailberichten die worden verwerkt door de GGD, moet de klant alvorens de mail kan worden verzonden beslissen over de toestemming voor de verwerking van persoonsgegevens. De klant moet hier ten alle tijden een keuzevrijheid in hebben.

5.5.2 Accountability

De plicht die ontstaat op grond van de AVG wat betreft documentatie is belangrijk voor de organisatie. Op dit moment vindt een inventarisatie plaats van de persoonsgegevens die worden verwerkt binnen de GGD. Binnen de geanalyseerde systemen bestaat echter al een compleet beeld van de verwerkte persoonsgegevens. Enkel in beeld hebben welke persoonsgegevens worden verwerkt binnen de organisatie is echter niet voldoende op grond van de AVG.

Waar het bij de Wbp voldoende was een doel te formuleren op basis waarvan de persoonsgegevens worden verwerkt, is het op grond van de AVG verplicht dit vast te leggen.[129] Alle aspecten van de verwerking moeten worden beschreven. Het doel, de wettelijke grondslag en de bewaartermijn moeten vastliggen in documentatie. Dit betekent voor alle systemen dat de wettelijke grondslag gedocumenteerd moet worden en dat er een bewaartermijn vastgesteld moet worden. Enkel voor Topdesk KCC moet nog een uitdrukkelijk omschreven doel worden gedocumenteerd, dit is immers voor de andere systemen al gedaan.

Daarnaast moet de betrokkene actief worden geïnformeerd over zijn rechten (zie hiervoor hoofdstuk 3). In de praktijk zouden deze rechten kunnen worden opgenomen in een standaardformulier op het moment dat de toestemming van de cliënt wordt gevraagd. In de gevallen waarin het standaardformulier niet kan worden gebruikt wordt verwezen naar een formulier dat op internet beschikbaar wordt gesteld. Dit zal een zelfde formulier zijn als het standaardformulier zoals dit tijdens een consult wordt voorgelegd aan de klant.

5.5.3 Gegevensbeschermingseffectbeoordeling

Binnen de GGD wordt veel gewerkt met bijzondere persoonsgegevens. Om aan de eisen uit de AVG te voldoen, moet de organisatie een PIA (gegevenbeschermings-effectbeoordeling) uitvoeren.[130] De organisatie moet op die manier inzicht krijgen in de

[129] Artikel 13 Algemene Verordening Gegevensbescherming.
[130] Artikel 35 lid 3 sub b Algemene Verordening Gegevensbescherming.

risico's met betrekking tot privacy. Ik beveel de GGD aan om de PIA uit te laten voeren door een jurist die gespecialiseerd is in de AVG. Deze jurist moet dit doen in samenwerking met een IT specialist die de organisatie goed kent. Op die manier wordt de PIA zowel juridisch als technisch op juiste wijze uitgevoerd. De PIA moet GGD breed worden uitgevoerd en niet enkel binnen de zes onderzochte systemen.

5.5.4 Privacy by Design & Privacy by Default.

Op grond van de AVG bestaat de verplichting om al tijdens het ontwerpproces van systemen rekening te houden met bescherming van persoonsgegevens. Dit moet de GGD achteraf ook kunnen aantonen. De GGD moet onderzoeken welke technische en organisatorische maatregelen de bescherming van persoonsgegevens moeten waarborgen. Dit kan doormiddel van pseudonimisering, het zo min mogelijk verwerken van persoonsgegevens, het strikt regelen van autorisatie en het opstellen van een privacybeleid.

Veel systemen binnen de GGD zijn al ontworpen, of worden niet door de organisatie zelf ontworpen. Om aan deze begrippen te voldoen, moet de GGD de systemen waarin de persoonsgegevens worden verwerkt optimaal beveiligen. Dit moet door middel van autorisatie, maar ook door virusscanners en andere technische maatregelen. Zoals reeds eerder besproken moet de autorisatie binnen de systemen Kidos en Orion Forensisch strikter worden geregeld om de systemen goed te beveiligen.

Om aan de Privacy by Design en Privacy by Default te voldoen moet de GGD inventariseren of er al wordt voldaan aan deze begrippen en of dit voldoet aan de AVG. Een PIA (zie voor verdere uitleg paragraaf 5.7.3) kan bijdragen aan de inventarisatie hiervan. Voor het systeem Tubis komt op de korte termijn een vervangend systeem. Voor dit systeem moet de GGD dus aan kunnen tonen dat bij het ontwerp van het systeem rekening is gehouden met de bescherming van persoonsgegevens.

5.5.5 Functionaris gegevensbescherming

Op grond van de Wbp was het aanstellen van een functionaris een keuze. Op grond van de AVG is de GGD dit verplicht.[131] Deze verplichting kan in het geval van de GGD worden gebaseerd op twee grondslagen. Ten eerste is de GGD een overheidsorgaan, waardoor op grond van de Wbp een verplichting bestaat een functionaris aan te stellen.[132] Daarnaast verwerkt de GGD op grote schaal een bijzondere categorie persoonsgegevens. Daarom bestaat dezelfde verplichting op grond van sub c van de AVG.[133]

Ook wat betreft de rol van de functionaris verandert een en ander op het moment dat aan de AVG moet worden voldaan.

De functionaris moet zijn aangewezen op grond van, in het bijzonder, zijn deskundigheid op het gebied van de wetgeving en de praktijk inzake gegevensbescherming. De rol van de functionaris wordt meer actief dan verplicht was op grond van de Wbp. De functionaris moet door de organisatie worden betrokken bij alle aangelegenheden die verband houden met de verwerking van persoonsgegevens. Bovendien moet de functionaris toegang hebben tot de persoonsgegevens en verwerkingsactiviteiten. Tenslotte moet de functionaris rechtstreeks verslag uitbrengen aan de hoogste leidinggevende.[134]

De functionaris krijgt bovendien een aantal specifieke taken (zie hiervoor paragraaf 3.1).

[131] Artikel 37 Algemene Verordening Gegevensbescherming.
[132] Artikel 37 lid 1 sub a Algemene Verordening Gegevensbescherming.
[133] Artikel 37 lid 1 sub c Algemene Verordening Gegevensbescherming.
[134] Artikel 38 lid 3 Algemene Verordening Gegevensbescherming.

Om aan de AVG te voldoen zal binnen de GGD de rol van de functionaris moeten worden uitgebreid. Er moet toegang komen tot de persoonsgegevens en de verwerkings-activiteiten voor de functionaris. Bovendien moet de functionaris werken aan zijn kennis op het gebied van wet- en regelgeving en de praktijk inzake gegevensbescherming. De huidige functionaris is zeer goed bekend met de organisatie. Op dat gebied hoeft dus niets te veranderen.

5.5.6 Meldplicht datalekken

De GGD moet op grond van de AVG een administratie bij gaan houden van alle inbreuken in verband met persoonsgegevens die plaatsvinden. Op grond van de Wbp is enkel verplicht om meldingsplichtige inbreuken in de administratie op te nemen. Vanaf 25 mei 2018 moet de GGD een administratie bijhouden van alle inbreuken in verband met persoonsgegevens. [135] Van elke situatie waarbij iemand toegang krijgt tot persoonsgegevens waarvoor hij niet bevoegd is, moet dan dus melding worden gemaakt. Kijkend naar de werkwijze binnen de GGD kan dat flinke gevolgen hebben. Op het moment dat een persoon is ingelogd in een systeem met persoonsgegevens en weg gaat van de computer zonder het scherm te vergrendelen, kan iemand toegang krijgen tot persoonsgegevens waarvoor hij niet bevoegd is. Het open laten staan van deuren kan zorgen voor toegang van personen die niet bevoegd zijn. Als zij hierdoor in contact kunnen komen met persoonsgegevens, is dit een datalek en moet het dus worden gedocumenteerd. Hierbij hoeft niet vast te staan dat zij daadwerkelijk in contact zijn gekomen met de persoonsgegevens. Het feit dat de GGD op dat moment niet redelijkerwijs uit kan sluiten dat persoonsgegevens onrechtmatig zijn verwerkt betekent dat er sprake is van een datalek.[136] Wanneer en datalek gemeld moet worden bij de AP en betrokkene blijkt uit lid 1.[137] Hierbij kan worden verwezen naar hetgeen op grond van de Wbp geldt over meldingsplichtige datalekken.[138]

5.5.7 Pseudonimisering

De AVG geeft de mogelijkheid tot pseudonimisering.[139] Dit zorgt niet voor een verplichting voor de GGD. Wel kan het een mogelijkheid zijn om de beveiliging van persoonsgegevens te versterken.[140] De risico's van de verwerking voor de betrokkene worden verminderd. De persoonsgegevens zijn door middel van pseudonimisering niet langer direct te koppelen aan de betrokkene. Om de persoonsgegevens te koppelen aan de betrokkene is immers een sleutel nodig die niet toegankelijk is voor iedereen. Bijvoorbeeld binnen het systeem HP Zone zou deze mogelijkheid kunnen worden gebruikt. Door de infectieziekten los te koppelen van het individu worden deze gegevens nog beter beschermd. Middels de sleutel kunnen de gegevens door de personen die dit nodig hebben alsnog aan elkaar worden gekoppeld.

5.5.8 Conclusie

Om aan de AVG te voldoen moet de GGD nog een aantal belangrijke stappen zetten. Ten eerste moet er een manier komen om expliciete toestemming te vragen aan de betrokkene voor de verwerking van de persoonsgegevens als de verwerking niet gebaseerd wordt op bijvoorbeeld de wettelijke plicht. Er moet daarnaast aan de informatieplicht worden voldaan. Middels een standaard document kan aan beide verplichtingen worden voldaan door de GGD. Dit document wordt fysiek aan klanten aangeboden indien mogelijk. Tijdens telefoongesprekken wordt de toestemming mondeling gevraagd en wordt verwezen naar de website waar het formulier wordt

[135] Artikel 33 lid 5 Algemene Verordening Gegevensbescherming.
[136] Beleidsregels meldplicht datalekken in de Wet bescherming persoonsgegevens.
[137] Artikel 33 lid 1 Algemene Verordening Gegevensbescherming.
[138] Artikel 34a Wet bescherming persoonsgegevens.
[139] Artikel 4 lid 5 Algemene Verordening Gegevensbescherming.
[140] Artikel 25 en overweging 28 Algemene Verordening Gegevensbescherming.

opgenomen. Klanten kunnen het formulier dan digitaal invullen. Op een email volgt een automatische reactie met een verwijzing naar de website met daarop het standaardformulier. Bepaalde gegevens worden op grond van een wettelijke grondslag verwerkt. Dit wordt op het standaardformulier vermeld.

Er moet een meer uitgebreide administratie worden bijgehouden op het gebied van persoonsgegevens. Zo zal een doel, de wettelijke grondslag en de bewaartermijn moeten worden vastgesteld. Daarnaast moet de organisatie een PIA uitvoeren. Bovendien moet de GGD bij de verwerking van nieuwe persoonsgegevens al in het ontwerpproces rekening houden met de bescherming van deze gegevens. Dit moet achteraf ook aangetoond kunnen worden.

De functionaris gegevensbescherming moet een andere, meer actieve rol krijgen. Om de huidige functionaris te laten voldoen aan de eisen van de AVG moet er worden geïnvesteerd in kennis op het gebied van wet- en regelgeving en de praktijk inzake gegevensbescherming. De kennis van de functionaris over de organisatie is optimaal. Dit in combinatie met de extra kennis over wet- en regelgeving en praktijk inzake gegevensbescherming gaat deze functionaris geschikt maken. Bovendien moet de functionaris een aantal taken extra uit gaan voeren.

Het pseudonimiseren van gegevens is een aspect dat voortvloeit uit de AVG. Dit brengt geen verplichting voor de GGD met zich mee. Het is echter wel een mogelijkheid om bepaalde persoonsgegevens beter te beveiligen. Het risico voor de betrokkene wordt immers verkleind, omdat de persoonsgegevens niet langer direct te koppelen zijn aan de betrokkene.

Hoofdstuk 6. Conclusies en aanbevelingen

Tijdens dit onderzoek heeft de vraag ‘Welke aanbevelingen kunnen worden gedaan aan de GGD Hart voor Brabant om het privacy-beleid en de werkwijze omtrent de verwerking van persoonsgegevens in overeenstemming te krijgen met de huidige en in de toekomst in te voeren wet- en regelgeving?’ centraal gestaan. Uit het onderzoek blijkt dat het beleid op dit moment wordt opgesteld. Ook blijkt dat de werkwijze nog niet geheel conform huidige en in de toekomst in te voeren wet- en regelgeving is.

Hierna volgt een aantal bevindingen uit het onderzoek en de aanbevelingen die kunnen worden gedaan om de werkwijze en het beleid conform huidige en in de toekomst in te voeren wet- en regelgeving te krijgen.

6.1 Toetsing van het beleid aan de Wet bescherming persoonsgegevens

6.1.1 Beleid

Conclusie

Aan de hand van het beleidsplan 2015-2017 luidt de conclusie dat er op dit moment geen beleid binnen de gehele organisatie van de GGD geldt over de verwerking van persoonsgegevens. Een van de doelen die is gesteld in dit beleidsplan is het opstellen van beleid. Voor enkele van de andere te behalen doelen uit het beleidsplan is de voortgang al duidelijk. Zo wordt er op dit moment een inventarisatie gemaakt van de verwerking van persoonsgegevens. Er wordt geïnventariseerd welke persoonsgegevens in welke systemen worden verwerkt en hoe deze gegevens worden beveiligd. Bovendien wordt er gewerkt aan het bewustzijn van de medewerkers ten aanzien van de verwerking en bescherming van persoonsgegevens.

Via het intranet worden medewerkers geïnformeerd over hoe zij persoonsgegevens moeten beschermen. Met betrekking tot de overige aspecten van verwerking is in dat stuk geen uitleg opgenomen. Wat betreft de meldplicht datalekken staat op intranet hoe werknemers moeten handelen als een datalek geconstateerd wordt. Dit stuk is summier

Aanbevelingen

1) Stel beleid op dat het gehele proces met betrekking de tot verwerking van persoonsgegevens bevat. Ik beveel aan om tenminste alle aspecten van verwerking die in het onderzoek naar voren zijn gekomen in het beleid op te nemen. Zo moet er bijvoorbeeld terug komen wat het vastgestelde doel is en wat de bewaartermijnen zijn van de verwerkte persoonsgegevens.
2) Neem in het beleid op dat de GGD elke verwerking van persoonsgegevens moet toetsen aan de proportionaliteit en subsidiariteit. Zorg ervoor dat er altijd voor het minst zware middel wordt gekozen om het doel te bereiken.
3) Informeer de medewerkers over het beleid door het op te nemen op het intranet.
4) Neem ook de meldplicht datalekken op in het beleid en plaats een stappenplan hieromtrent op het intranet. Medewerkers kunnen dan eenvoudig vaststellen of er sprake is van een datalek.
5) Bundel alles wat er nu al is binnen de organisatie over de verwerking van persoonsgegevens in een document, door het bijvoorbeeld op te nemen in het beleid. De medewerker weet dan waar hij moet zoeken bij vragen over de verwerking van persoonsgegevens.

6.2 Toetsing van de werkwijze aan de Wet bescherming persoonsgegevens

6.2.1 Doelbinding

Conclusie

Binnen alle systemen, behalve voor het systeem Topdesk dat door het team KCC wordt gebruikt, is duidelijk en uitdrukkelijk een doel omschreven voor de verwerking van persoonsgegevens. De meeste systemen voldoen op dit punt dus aan de Wbp.

Aanbevelingen

6) Omschrijf voor het systeem Topdesk KCC een doel voor de verwerking. Een voorbeeld van een duidelijk en uitdrukkelijk omschreven doel voor dit systeem is: ‘het verzamelen en verwerken van gegevens om dit naar de juiste afdeling binnen de GGD te versturen, zodat de beste hulp aan klanten kan worden gegeven’.

6.2.2 Grondslag

Conclusie

De verwerking van persoonsgegevens door de JGZ-medewerkers in het systeem Kidos is gebaseerd op de grondslag ‘wettelijke plicht’. Dit geldt ook voor de meldingsplichtige infectieziekten in het systeem HP Zone en de verwerking van persoonsgegevens in het systeem Tubis.

In de systemen Topdesk KCC en Orion Globe worden persoonsgegevens verwerkt op basis van veronderstelde toestemming. Ook voor de persoonsgegevens die in HP Zone worden verwerkt en die geen betrekking hebben op meldingsplichtige infectieziekten worden verwerkt op basis van veronderstelde toestemming. Bij de organisatie mag echter geen twijfel bestaan over de verleende toestemming. Hiervan is op dit moment geen sprake. Het is niet duidelijk of klanten toestemming hebben verleend, en als zij al toestemming hebben verleend waar zij toestemming voor hebben verleend. Op dit punt handelt de GGD dus niet overeenkomstig de Wbp.

De verwerking van persoonsgegevens moet bovendien ten alle tijden proportioneel en subsidiair zijn. Het geformuleerde doel mag niet op een minder ingrijpende manier bereikt kunnen worden dan door deze verwerking.

Aanbevelingen

7) Stel voor elke verwerking van persoonsgegevens vast wat de wettelijke grondslag is. Indien de wettelijke grondslag de wettelijke plicht is, hoeft er niets te worden gewijzigd om aan de huidige wet- en regelgeving te voldoen.
8) Vraag klanten om toestemming voor de verwerking van persoonsgegevens als de wettelijke grondslag voor verwerking toestemming is. Doe dit middels een standaardformulier dat tijdens een consult aan de klant wordt voorgelegd. Voor gegevens die worden verwerkt naar aanleiding van telefoongesprekken wordt tijdens dit gesprek de toestemming van de betrokkene gevraagd. Vervolgens wordt een bevestiging van deze al dan niet verleende toestemming verzonden aan de betrokkene. Alvorens klanten een mail kunnen versturen naar de GGD moeten zij een keuze maken over het al dan niet verlenen van toestemming voor de verwerking van persoonsgegevens. Ook deze al dan niet verleende toestemming wordt middels een mail bevestigd aan de betrokkene.
9) Ga na of de GGD voldoet aan de eis van proportionaliteit en subsidiariteit bij de verwerking. Ga dus na of het doel op een minder ingrijpende wijze bereikt kan worden dan door de verwerking die plaatsvindt. Deze toetsing moet plaatsvinden door de opstellers van het beleid. Soms kan dan de keuze gemaakt worden om gegevens te anonimiseren of pseudonimiseren. Als gegevens bijvoorbeeld voor

langere tijd bewaard moeten worden, voor statistieken of wetenschappelijk onderzoek, is dit een goed alternatief.

6.2.3 Bewaartermijn

Conclusie

Persoonsgegevens die digitaal worden verwerkt worden op dit moment niet verwijderd door de GGD. Binnen HP Zone en Kidos is men ervan op de hoogte dat er een bewaartermijn geldt. Wat deze bewaartermijn is, is onduidelijk. Bovendien worden de gegevens na afloop van deze termijn niet verwijderd, maar hooguit gearchiveerd. Op dit punt voldoet de GGD niet aan de Wbp.

Aanbevelingen

10) Stel per systeem en per categorie persoonsgegevens vast wat een redelijke termijn is om de gegevens te bewaren. Er moet worden beredeneerd tot wanneer de persoonsgegevens nodig zijn om het vastgestelde doel te bereiken.
11) Stel voor medische gegevens de bewaartermijn bijvoorbeeld op 10 jaar, overeenkomstig de WGBO.
12) Stel voor Kidos een bewaartermijn van bijvoorbeeld 18 jaar. Dit is een redelijke termijn, omdat de GGD gegevens van een kind bewaart tot het kind meerderjarig is. Daarom moeten deze gegevens gedurende langere tijd worden verwerkt.
13) Stel voor de persoonsgegevensgegevens binnen Topdesk KCC een korte bewaartermijn vast van hoogstens een jaar. Deze gegevens komen immers later in de daarvoor bestemde systemen. Het doel, namelijk het doorsturen van de informatie naar de juiste afdelingen, is al binnen afzienbare tijd bereikt.
14) Pas de systemen zo aan dat er een gestandaardiseerde manier komt om gegevens te verwijderen. Binnen ieder systeem moet een manier komen om meerdere dossiers tegelijk te verwijderen, zodat het medewerkers niet veel tijd kost om aan deze plicht te voldoen.

6.2.4 Beveiliging van persoonsgegevens

Conclusie

Binnen alle systemen wordt gewerkt met een autorisatie doormiddel van het invoeren van en gebruikersnaam en wachtwoord. Binnen de systemen Kidos en Orion Forensisch wordt aangegeven dat deze autorisatie strikter geregeld zou kunnen worden. Zo kunnen op de afdeling Forensische geneeskunde de secretarieel medewerkers bij het volledige medische dossier terwijl dit niet nodig is. Binnen Kidos wordt ook aangegeven dat de autorisatie strikter moet worden geregeld.

In het systeem Topdesk KCC onderdeel reizigers wordt gewerkt op de autorisatie van collega's. Om goede beveiliging van persoonsgegevens te waarborgen moet dit veranderen. Een medewerker moet enkel op eigen gegevens in kunnen loggen.

Er moet een bewerkersovereenkomst worden afgesloten met de externe bewerkers van persoonsgegevens binnen de GGD. Voor het systeem Tubis is deze overeenkomst al getekend, voor HP Zone is dit nog niet het geval. Bij de overige systemen wordt niet gewerkt met een externe bewerker en is dit dus niet van toepassing.

Aanbeveling

15) Pas in het systeem Kidos en Orion Forensisch de autorisatie aan zodat deze strikter is. Dit kan worden verwezenlijkt door een scheiding aan te brengen in de autorisatie, zoals bijvoorbeeld in het systeem Orion Globe. Per laag wordt dan autorisatie gegeven indien dit nodig is voor de werkzaamheden van de medewerker.

16) Maak voor Topdesk KCC extra accounts aan voor het onderdeel reizigers. Zo kunnen medewerkers ten alle tijden inloggen op een eigen account en gebruiken zij enkel die systemen waarvoor zij autorisatie hebben gekregen.
17) Zorg dat er een bewerkersovereenkomst wordt getekend met de bewerker voor het systeem HP Zone. Doe dit door in gesprek te gaan met de wederpartij. Beweeg de wederpartij ertoe de overeenkomst alsnog te ondertekenen.

6.2.5 Het recht op informatie

Conclusie

De GGD voldoet op dit moment aan de Wbp als het gaat om het waarborgen van het recht van informatie van de betrokkene.

Binnen de meeste systemen is er een standaardprocedure voor het waarborgen van dit recht. Bij het systeem HP Zone is hiervoor geen standaardprocedure, maar daar is het nog niet voorgekomen dat een betrokkene een beroep heeft gedaan op zijn recht op informatie. Bij het systeem Orion Globe is tot op heden ook geen vaste procedure voor het waarborgen van dit recht.

Aanbeveling

Ondanks het feit dat de GGD voldoet aan de Wbp adviseer ik in dit opzicht:

18) Stel voor zowel het systeem Orion Globe, als voor het systeem HP Zone een standaardprocedure op via welke weg het recht op informatie wordt gewaarborgd. Op die manier is het voor de GGD makkelijker om aan dit recht van de betrokkene tegemoet te komen. Binnen het team Reizigerszorg, waar Orion Globe gebruikt wordt, zal dit worden gerealiseerd door de betrokkene een mogelijkheid te geven om online in te loggen en het vaccinatieboekje te downloaden. Dit is naar mijn idee een goede manier om dit aan te pakken. Voor HP Zone kan een aanvraagformulier worden opgesteld. Doormiddel van dit formulier kan de betrokkene zijn dossier opvragen.

6.2.6 De verwerking van bijzondere persoonsgegevens

Conclusie

De GGD is bevoegd om bijzondere persoonsgegevens te verwerken, omdat de GGD een instelling is voor de gezondheidszorg. Bovendien hebben alle medewerkers een geheimhoudingsverklaring moeten tekenen bij het in dienst treden. De meeste medewerkers hebben daarnaast een geheimhoudingsplicht uit hoofde van hun beroep of ambt.

De systemen van de GGD voldoen aan de eisen om bijzondere persoonsgegevens te mogen verwerken.

Aanbeveling

Er zijn geen aanbevelingen op dit punt.

6.2.7 De meldplicht datalekken

Conclusie

De functionaris is goed op de hoogte van de procedure rondom datalekken. Hij weet hoe hij moet toetsen of een datalek gemeld moet worden en waar dit gemeld moet worden.

De medewerkers van de GGD zijn echter niet goed op de hoogte. Zij weten ten eerste meestal niet wanneer er sprake is van een datalek. Daarnaast kennen zij de procedure niet die zij moeten volgen als er een datalek wordt geconstateerd. Er worden op dit moment datalekken geconstateerd door het management. Het is echter van groot belang dat de medewerkers zich hier ook bewust van worden.

Aanbeveling

19) Informeer medewerkers over de procedure rondom datalekken. Het bewustzijn van de medewerkers moet groter worden. Dit kan door het geven van een presentatie over datalekken. Deze presentatie kan vervolgens op het intranet geraadpleegd worden. Als medewerkers na willen gaan wanneer er sprake is van een datalek en hoe er daarna gehandeld moet worden, dan is deze informatie voor hen vrij toegankelijk.
20) Informeer medewerkers dat zij een datalek ten alle tijden moeten melden bij de functionaris. De functionaris moet daarna de afweging maken of de GGD het datalek moet melden. Op die manier is er in de eerste plaats een compleet overzicht van geconstateerde datalekken. Daarnaast kan de functionaris de afweging over het melden altijd doen. De besluiten over de meldingen zullen dan steeds op een zelfde wijze tot stand komen.
21) Hou een administratie bij van alle meldingsplichtige datalekken.

6.2.8 De Functionaris gegevensbescherming

Conclusie

Het functioneren van de functionaris binnen de GGD voldoet op dit moment niet aan de Wbp. De rol van de functionaris is op dit moment te passief. De GGD betrekt hem nu pas bij de verwerking van persoonsgegevens op het moment dat er iets mis is. Hij ontvangt bovendien geen meldingen over de verwerking van persoonsgegevens.

Aanbeveling

22) Geef een meer actieve invulling aan de rol van de functionaris. Hij moet de meldingen omtrent de verwerking van persoonsgegevens ontvangen en hier toezicht op houden. Hierbij is in elk geval van belang dat de functionaris de ontwikkeling, implementatie en uitvoering van het privacybeleid binnen de GGD monitort. Daarnaast moet de functionaris beslissen over het melden van datalekken.

6.3 Toetsing van de werkwijze aan de Algemene Verordening Gegevensbescherming

Aanbevelingen die hierna volgen moeten voor 25 mei 2018 worden ingevoerd om aan de in de toekomst in te voeren regelgeving te voldoen.

6.3.1 Toestemming

Conclusie

De eisen die de AVG stelt aan de toestemming van de betrokkene voor de verwerking zijn strenger dan bij de Wbp. De bewijslast van de al dan niet verleende toestemming komt bij de GGD te liggen. Een duidelijke en actieve handeling van de betrokkene moet leiden tot de toestemming. Het is dus niet langer toegestaan om persoonsgegevens te verwerken op grond van de veronderstelde toestemming van de klant.

Aanbeveling

23) Voor de aanbevelingen over de toestemming op grond van de AVG zoek ik deels aansluiting bij de aanbevelingen die eerder zijn gedaan over de toestemming op grond van de Wbp in aanbeveling 2 van de vorige paragraaf. Vanaf 25 mei 2018 moet de GGD er echter voor zorgen dat de toestemming door een actieve handeling wordt verleend. De veronderstelde toestemming voldoet dan niet langer.
24) Zorg ervoor dat persoonsgegevens pas worden verwerkt nadat de toestemming middels het formulier, of mondelinge toestemming die is bevestigd, kenbaar is gemaakt. Wijs er bij klanten dan ook op dat zij over deze toestemming moeten

beslissen alvorens over kan worden gegaan tot de verwerking van persoonsgegevens.

6.3.2 Accountability

Conclusie

Op grond van de AVG is het voor de organisatie verplicht om alle aspecten van de verwerking vast te leggen. Binnen de onderzochte systemen is een aantal aspecten al vastgelegd. De wettelijke grondslag en de bewaartermijn zijn op dit moment echter niet gedocumenteerd.

Ook bestaat er de verplichting om de betrokkene actief in te lichten over zijn rechten als het gaat om de verwerking van persoonsgegevens. Dat gebeurt op dit moment niet.

Aanbeveling

25) Documenteer alle aspecten van de verwerking van persoonsgegevens. De wettelijke grondslag van de verwerking blijkt uit dit onderzoek. De bewaartermijnen worden opgesteld door de archivaris die werkzaam is binnen de GGD. Als de GGD aan deze documentatieplicht voldoet kunnen alle benodigde gegevens ten alle tijden worden getoond op verzoek van de betrokkene of de AP.
26) Neem in het eerder genoemde standaardformulier voor het verkrijgen van toestemming de onderdelen van de informatieplicht op. Informeer de betrokkene hierin over de rechten die zij hebben op grond van de AVG. Hierin moet tenminste worden opgenomen; het recht om vergeten te worden, het recht op inzage, het recht op rectificatie, het recht om eerder verleende toestemming in te trekken en het recht om een klacht in te dienen bij de toezichthoudende autoriteit.

6.3.3 Gegevensbeschermingseffectenbeoordeling

Conclusie

De GGD is op grond van de AVG verplicht om een gegevensbeschermingseffecten-beoordeling (PIA) te doen, omdat er op grote schaal bijzondere persoonsgegevens worden verwerkt.

Aanbeveling

27) Laat een PIA uitvoeren door een jurist die gespecialiseerd is in de AVG. Deze jurist moet dit doen in samenwerking met een IT-specialist van de GGD. Op die manier wordt de PIA zowel juridisch als technisch op juiste wijze uitgevoerd. De PIA moet GGD breed worden uitgevoerd en niet enkel binnen de zes in dit onderzoek bekeken systemen.

6.3.4 Privacy by design en by default:

Conclusie

Bij het ontwerpen van systemen moet de GGD al rekening houden met de bescherming van persoonsgegevens. Voor het systeem Tubis komt op de korte termijn een vervangend systeem. Voor de systemen die al ontworpen zijn of die extern worden ontworpen moet de GGD organisatorische en technische maatregelen treffen om de bescherming van de persoonsgegevens te waarborgen.

Aanbeveling

28) Inventariseer, bijvoorbeeld doormiddel van een PIA, of er al wordt voldaan aan de begrippen Privacy by design en by default en of dit voldoet aan de AVG.
29) Zorg voor een optimale beveiliging van de persoonsgegevens. Dit moet mede doormiddel van het regelen van strikte autorisatie en goede virusscanners. Bovendien draagt het minimaliseren van de verwerking, het pseudonimiseren van

gegevens en andere technische en organisatorische maatregelen bij aan de optimale beveiliging van de persoonsgegevens.

30) Stel vast hoe er bij het ontwerpen van het nieuwe systeem voor de afdeling Tuberculose rekening is gehouden met de bescherming van persoonsgegevens. Als dit niet is gedaan, zorg er dan voor dat dit alsnog gebeurt voordat het systeem in gebruik wordt genomen.

6.3.5 Functionaris gegevensbescherming

Conclusie

De GGD is op grond van de AVG verplicht een functionaris te hebben. De directiesecretaris vervult op dit moment de functie van de functionaris binnen de organisatie. De functionaris moet zijn aangewezen op grond van, in het bijzonder, zijn deskundigheid op het gebied van de wetgeving en de praktijk inzake gegevensbescherming. Er is een aantal taken die de functionaris op grond van de AVG moet gaan vervullen (zie hiervoor paragraaf 3.1). De rol van de functionaris binnen de organisatie zoals die op dit moment wordt vervult is niet overeenkomstig de AVG.

Aanbeveling

31) Pas de rol van de functionaris binnen de GGD aan. Om aan de AVG te voldoen moet de rol worden uitgebreid. De functionaris moet toegang verkrijgen tot de persoonsgegevens en de verwerkingsactiviteiten.
32) De functionaris moet werken aan zijn kennis op het gebied van wet- en regelgeving en de praktijk inzake gegevensbescherming. Laat de functionaris een cursus volgen waardoor zijn kennis op het gebied van wet- en regelgeving wordt geactualiseerd. De huidige functionaris is zeer goed bekend met de organisatie. Op dat gebied hoeft dus niets te veranderen.

6.3.6 De meldplicht datalekken

Conclusie

Op grond van de AVG moet de GGD van alle datalekken een documentatie bijhouden. Dit is een verandering ten opzichte van de regeling uit de Wbp, omdat op grond daarvan alleen meldingsplichtige datalekken gedocumenteerd moesten worden.

Aanbeveling

33) Hier zoek ik aansluiting bij aanbeveling 19. Informeer de medewerkers.
34) Hou een administratie bij van alle geconstateerde datalekken.

6.3.7 Pseudonimisering

Conclusie

Van pseudonimisering is sprake wanneer persoonsgegevens worden losgekoppeld van de identificeerbare natuurlijke persoon. Er wordt een sleutel gemaakt, waardoor deze gegevens later nog gekoppeld kunnen worden aan de persoon.

Aanbeveling

35) Om te voldoen aan de AVG hoeft de GGD op dit punt geen actie te ondernemen. Pseudonimisering kan worden gezien als een extra maatregel ter beveiliging van persoonsgegevens en kan op die manier dus worden gebruikt door de GGD.

Literatuurlijst

Beleidsregels meldplicht datalekken in de Wet bescherming persoonsgegevens. Autoriteit persoonsgegevens.

C. Arts 2016
C. Arts 2016, 'Het accountability principe onder de Algemene Verordening Gegevensbescherming', *consideratie* augustus 2016.

P.L. Coté 2014
P.L. Coté 2014, 'De functionaris voor gegevensbescherming: een schaap met vijf poten', *Duthler Associates* 2014.

J. Gerritsen 2015
J. Gerritsen, 'Waar gaat het heen met de avg'*, Informatie* augustus 2015.

J.P. de Jong 2015
J.P. de Jong, 'De algemene verordening gegevensbescherming. De rechtsopvolger van de Wbp', *RegelMaat* 2015(30).

J.P. de Jong 2016
J.P. de Jong, 'De algemene verordening gegevensbescherming', *Ars Aequi* oktober 2016.

H. Kranenborg 2011.
H. Kranenborg*, Wet bescherming persoonsgegevens in Europees perspectief,* Deventer: Wolters Kluwer.

H.R. Kranenborg 2013, p. 310.
H.R. Kranenborg, 'nieuwe regels voor de bescherming van persoonsgegevens: van belang voor iedereen', *SEW Tijdschrift voor Europees en economisch recht* 2013, afl. 7, p. 310.

H.H. de Vries 2001, p. 22.
H.H. de Vries en D.J. Rutgers, *Actualiteiten sociaal recht, Wet bescherming persoonsgegevens,* Deventer: Wolters Kluwer.

H. de Vries 2016
H.de Vries & M. Goudsmit, 'Voorsorteren op de Algemene Verordening Gegevensbescherming', *NJB* 2016/1077, p. 7.

J. Leegemaate *NJB* 2011/2097.
J. Leegemaate, 'Beperken van het medisch beroepsgeheim?', *NJB* 2011/2097.

L. Janssen 2012, p. 12.
L. Janssen, *Staats- en bestuursrecht bronnenboek,* Den Haag: Boom juridische uitgevers.

L.Janssen 2015.
L.Janssen, *Gezondheidsrecht begrepen. Praktische inleiding in het gezondheidsrecht voor (para)medici en verpleegkundigen,* Den Haag: Boom Lemma uitgevers 2015.

Minister van Veiligheid en Justitie *NJB 2016/16*
Minister van Veiligheid en Justitie, 'Pseudonimisering en de verordening gegevensbescherming', *NJB* 2016/16.

Richtsnoeren beveiliging 2013.
Autoriteit persoonsgegevens.

S. Nouwt *NJB 2014/2158.*
S. Nouwt, ‘Gemeentezorg en privacyzorgen’, *NJB* 2014/2158, p.4