

# Privacy van de mantelzorger

---

Zorgt de Algemene Verordening Gegevensbescherming voor meer of minder zorgen in de zorg?

|                     |                                          |
|---------------------|------------------------------------------|
| Auteur              | Danny Lucas                              |
| Studentnummer       | 2040638                                  |
| Stageorganisatie    | Stichting Steunpunt informele zorg Breda |
| Stagebegeleider     | Mw. U.K.M (Ursula) van Weert             |
| Opleiding           | HBO-Rechten                              |
| Onderwijsinstelling | Juridische Hogeschool Avans- Fontys      |
| Locatie             | Tilburg                                  |
| Stagedocent         | Dhr. mr. B.C.M. (Bart)Hooijdonk          |
| Datum               | Januari 2017                             |



# Privacy van de mantelzorger

---

De Algemene Verordening Gegevensbescherming zorgt voor minder zorgen in de zorg

|                     |                                          |
|---------------------|------------------------------------------|
| Auteur              | Danny Lucas                              |
| Studentnummer       | 2040638                                  |
| Stageorganisatie    | Stichting Steunpunt informele zorg Breda |
| Stagebegeleider     | Mw. U.K.M. (Ursula) van Weert            |
| Opleiding           | HBO-Rechten                              |
| Onderwijsinstelling | Juridische Hogeschool Avans- Fontys      |
| Locatie             | Tilburg                                  |
| Stagedocent         | Dhr. mr. B.C.M. (Bart)Hooijdonk          |
| Datum               | Januari 2017                             |



## **Voorwoord**

Graag wil ik in dit voorwoord degenen bedanken die mij geholpen hebben met het opzetten van dit onderzoeksrapport. Als eerste wil ik Ursula van Weert bedanken voor haar vertrouwen in mij. Zij heeft mij de kans gegeven om onderzoek te doen naar een onderwerp dat zeer belangrijk is voor haar organisatie. Daarnaast wil ik Bart Hooijdonk bedanken voor zijn begeleiding. Dit voorwoord zal niet zo uitgebreid zijn als mijn e-mails. Ook wil ik Karen van der Vorst bedanken voor haar assistentie bij het opstellen van de survey. Ten slotte wil ik alle medewerkers van StiB bedanken voor de tijd die zij vrij hebben gemaakt voor mijn onderzoek.

Danny Lucas

Breda, januari 2016

# Inhoudsopgave

|                                                                     |    |
|---------------------------------------------------------------------|----|
| Samenvatting                                                        | 8  |
| Lijst van afkortingen & verkortingen                                | 9  |
| Lijst van begrippen                                                 | 10 |
| Hoofdstuk 1 Onderzoeksopzet                                         | 11 |
| 1.1 Inleiding.....                                                  | 11 |
| 1.2 Probleembeschrijving .....                                      | 11 |
| 1.3 Centrale vraag.....                                             | 12 |
| 1.4 Doelstelling .....                                              | 12 |
| 1.5 Deelvragen.....                                                 | 12 |
| 1.6 Afbakening .....                                                | 13 |
| 1.7 Onderzoeksmethodiek & verantwoording .....                      | 13 |
| 1.8 Leeswijzer .....                                                | 14 |
| Hoofdstuk 2 De Algemene Verordening Gegevensbescherming             | 16 |
| 2.1 Toetsingskader rechtmatige gegevensverwerking .....             | 16 |
| 2.1.1 Beginselen inzake de verwerking van persoonsgegevens.....     | 16 |
| 2.1.2 De beginselen van proportionaliteit en subsidiariteit.....    | 18 |
| 2.1.3 De rechtmatigheidsgronden .....                               | 18 |
| 2.1.4 Voorwaarden voor toestemming.....                             | 20 |
| 2.1.5 Verwerking van bijzondere categorieën persoonsgegevens .....  | 21 |
| 2.1.6 Verwerking waarvoor identificatie niet is vereist .....       | 23 |
| 2.1.7 Verwerking voor andere doeleinden .....                       | 23 |
| 2.2 De rechten van de betrokkene .....                              | 23 |
| 2.2.1 Algemene regels .....                                         | 24 |
| 2.2.2 Het recht op informatie .....                                 | 25 |
| 2.2.2 Het recht op inzage .....                                     | 26 |
| 2.2.3 Recht op rectificatie.....                                    | 26 |
| 2.2.4 Recht op vergetelheid .....                                   | 26 |
| 2.2.5 Recht op beperking van verwerking .....                       | 27 |
| 2.2.6 Recht op overdraagbaarheid van gegevens .....                 | 27 |
| 2.2.7 Recht van bezwaar .....                                       | 28 |
| 2.2.8 Weigering en rechtsbescherming .....                          | 28 |
| 2.3 Plichten van de verwerkingsverantwoordelijke .....              | 28 |
| 2.3.1 Datalekken.....                                               | 28 |
| 2.3.2 Pseudonimiseren van gegevens .....                            | 29 |
| Hoofdstuk 3 - Privacy op de werkvloer                               | 31 |
| 3.1 Eerste ronde interviews .....                                   | 31 |
| 3.1.1 Doel van de interviews .....                                  | 31 |
| 3.1.2 Bevindingen uit het interview met mevrouw Van der Stoel ..... | 31 |
| 3.1.3 Bevindingen uit het interview met mevrouw Bakx.....           | 31 |
| 3.2 De survey.....                                                  | 32 |
| 3.2.1 Doel .....                                                    | 32 |
| 3.2.2 Bevindingen .....                                             | 32 |
| 3.3 Observaties.....                                                | 33 |
| 3.3.1 Doel .....                                                    | 33 |
| 3.3.2 Bevindingen .....                                             | 34 |

|              |                                                                                     |    |
|--------------|-------------------------------------------------------------------------------------|----|
| 3.4          | De tweede ronde interviews .....                                                    | 34 |
| 3.4.1        | Doel .....                                                                          | 34 |
| 3.4.2        | Bevindingen .....                                                                   | 35 |
| Hoofdstuk 4  | Het beleid van StiB en de Algemene Verordening Gegevensbescherming .....            | 36 |
| 4.1          | Inleiding.....                                                                      | 36 |
| 4.1.1        | Is StiB een hulpverleningsinstantie?.....                                           | 36 |
| 4.2          | Het toetsingskader voor rechtmatige gegevensverwerking.....                         | 37 |
| 4.2.1        | Beginnelen inzake het verwerken van persoonsgegevens .....                          | 37 |
| 4.2.2        | Rechtmatigheid van verwerking .....                                                 | 37 |
| 4.2.3        | Verwerking voor andere doeleinden .....                                             | 39 |
| 4.2.4        | Verwerken van bijzondere gegevens.....                                              | 40 |
| 4.3          | Het faciliteren van de rechten van de betrokkene .....                              | 40 |
| 4.3.1        | Algemene Regels.....                                                                | 40 |
| 4.3.2        | Het recht op informatie .....                                                       | 41 |
| 4.3.3        | Het recht op inzage .....                                                           | 41 |
| 4.3.4        | Het recht op rectificatie.....                                                      | 41 |
| 4.3.5        | Het recht op vergetelheid .....                                                     | 41 |
| 4.3.6        | Het recht op beperking van de bewerking .....                                       | 41 |
| 4.3.7        | Het recht op overdraagbaarheid van gegevens .....                                   | 42 |
| 4.3.8        | Het recht van bezwaar .....                                                         | 42 |
| 4.3.9        | Beperking van de rechten .....                                                      | 42 |
| 4.3.10       | Rechtsbescherming .....                                                             | 42 |
| 4.4          | Overige artikelen .....                                                             | 42 |
| 4.4.1        | Toegang tot informatie .....                                                        | 42 |
| 4.4.2        | Het inzetten van vrijwilligers .....                                                | 42 |
| 4.4.3        | Plichten van de verwerkingsverantwoordelijke .....                                  | 43 |
| Hoofdstuk 5  | Toetsing van de praktijk .....                                                      | 44 |
| 5.1          | Toepassing van het protocol in de praktijk.....                                     | 44 |
| 5.1.1        | Algemene indruk .....                                                               | 44 |
| 5.1.2        | De rechten van de betrokkene .....                                                  | 44 |
| 5.2          | Overige onderwerpen.....                                                            | 44 |
| 5.2.1        | BSN-nummers.....                                                                    | 44 |
| 5.2.2        | Bankrekeningnummer .....                                                            | 44 |
| 5.2.3        | Verwerking gegevens bij de mantelzorgwaardering .....                               | 45 |
| Hoofdstuk 6  | Conclusies en aanbevelingen .....                                                   | 46 |
| 6.1          | Conclusies .....                                                                    | 46 |
| 6.1.1        | Toetsing van het beleid aan de AVG .....                                            | 46 |
| 6.1.2        | Toepassing van het beleid in de praktijk.....                                       | 48 |
| 6.1.3        | Het privacyprotocol en de werknemers .....                                          | 48 |
| 6.1.4        | Het privacyprotocol en Zorg voor elkaar Breda .....                                 | 49 |
| 6.2          | Aanbevelingen .....                                                                 | 49 |
| 6.2.1        | Aanbevelingen ter bevordering van het beleid.....                                   | 49 |
| 6.2.2        | Aanbevelingen ter bevordering van de toepassing van het beleid .....                | 50 |
| 6.2.3        | Aanbevelingen ter bevordering van de werknemers .....                               | 50 |
| 6.2.4        | Aanbeveling ter bevordering van de samenwerking binnen Zorg voor elkaar Breda ..... | 51 |
| Bronnenlijst |                                                                                     | 52 |

## Samenvatting

---

De Stichting Steunpunt informele zorg Breda maakt onderdeel uit van Zorg voor elkaar Breda. De stichting is gericht op het ondersteunen van de informele verzorgers (de mantelzorgers) in Breda. Door middel van het geven van workshops, het beschikbaar stellen van vrijwilligers en op andere manieren bieden van ondersteuning zorgt de organisatie ervoor dat de mantelzorgers in Breda er niet alleen voor staan.

Sinds begin 2016 verwerkt de stichting persoonsgegevens conform het "Privacyprotocol Wijknetwerken Breda". Dit protocol gaat vooral over het harmoniseren van de wijze waarop de organisaties binnen Zorg voor elkaar Breda omgaan met privacygegevens. Al hoewel de stichting vol goede moed begon met het implementeren van het protocol, kwamen de medewerkers er al snel achter dat het protocol lastig te implementeren was in de praktijk.

Het protocol is zeer juridisch geschreven en de stichting heeft geen jurist in dienst. Dit brengt enige gevolgen met zich mee. Van de medewerkers wordt verwacht dat zij in staat zijn om zelf een beleid te vormen en de wettelijke regels toe te passen. Zonder juridische kennis in huis te hebben is dit makkelijker gezegd dan gedaan. Het protocol wordt gezien als "droog" en "saai", waardoor de medewerkers al snel zijn afgehaakt. Nieuwe medewerkers worden amper tot niet geattendeerd op de aanwezigheid van het protocol, waardoor ook deze nieuwe medewerkers de privacywetgeving niet (kunnen) toepassen.

De hierboven beschreven ontwikkeling is alles behalve gewenst. Met de komst van de Algemene Verordening Gegevensbescherming dreigt een groot probleem te ontstaan. De verordening scherpert niet alleen de privacyregels aan, maar geeft de nationale privacyautoriteiten de bevoegdheid om sancties op te leggen, indien een organisatie zich niet houdt aan de privacywetgeving. De stichting wil voorkomen dat zij tegen het einde van de overgangsperiode erachter komt dat de medewerkers niet in staat zijn om de wetgeving correct toe te passen. Het is dan ook de bedoeling dat wordt gezocht naar een oplossing voor dit probleem, waarbij meteen rekening wordt gehouden met de komst van de verordening. In het onderzoek is dus gekeken naar de wijzingen in de nieuwe wetgeving en is gezocht naar een manier om het protocol verteerbaar te maken voor de niet-jurist.

Uit het onderzoek blijkt dat het protocol geüpdate moet worden zodat het voldoet aan de nieuwe regelgeving. Daarbij maakt het protocol een aanname die in het geval van StiB niet gemaakt had moeten worden. Het protocol is opgesteld met het idee dat iedere organisatie binnen Zorg voor elkaar Breda een professionele zorginstelling is. Het protocol maakt dan ook veelvuldig gebruik van de regels die alleen toepasbaar zijn voor dit soort instellingen. StiB kan echter niet met zekerheid als zorginstelling worden gedefinieerd. Dit zorgt ervoor dat het protocol een verdere uitwerking nodig heeft, waarin staat vermeld welke regels van toepassing zijn voor de niet-zorginstellingen binnen Zorg voor elkaar Breda.

De stichting wordt dan ook aanbevolen om het protocol op de schop te nemen. Zowel op juridisch niveau als tekstueel niveau dient het een en ander veranderd te worden. Zo moet de stichting voortaan altijd toestemming vragen voordat ze begint met het verwerken van persoonsgegevens. Het protocol zal met minder juridische termen moeten worden herschreven. Daarbij hebben de medewerkers de voorkeur aan schema's of checklists in plaats van artikelen en toelichtingen. Ook zal het de stichting goeddoen om een inwerkmap te maken, waarin de privacyregels staan uitgelegd voor de nieuwe (en oude) medewerkers.

## Lijst van afkortingen & verkortingen

---

|                                |                                                                                                                                                                                                                                                                     |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AP                             | Autoriteit Persoonsgegevens                                                                                                                                                                                                                                         |
| AVG                            | De Algemene Verordening Gegevensbescherming                                                                                                                                                                                                                         |
| EVRM                           | Europees Verdrag voor de Rechten van de Mens en de fundamentele vrijheden                                                                                                                                                                                           |
| NAW-gegevens<br>(de) Richtlijn | Naam, adres en woongegevens<br>Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens |
| StiB                           | Stichting Steunpunt informele zorg Breda                                                                                                                                                                                                                            |
| Wbp                            | Wet bescherming persoonsgegevens                                                                                                                                                                                                                                    |
| Wbsn                           | Wet algemene bepalingen Burgerservicenummer                                                                                                                                                                                                                         |
| Wgbz                           | Wet gebruik burgerservicenummer in de zorg                                                                                                                                                                                                                          |

## Lijst van begrippen

---

De AVG maakt gebruik van een aantal begrippen.<sup>1</sup> Om ervoor te zorgen dat dit rapport duidelijk is voor de lezer die de AVG niet binnen bereik heeft, worden eerst de belangrijkste begrippen kort gedefinieerd. De begrippen die gedurende dit rapport worden gebruikt zijn:

- 1) “persoonsgegevens”: dit begrip omvat alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Als identificeerbaar wordt beschouwd een natuurlijke persoon die direct kan worden geïdentificeerd aan de hand van bepaalde persoonsgegevens;
- 2) “verwerking”: een bewerking van of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés;
- 3) “betrokkene<sup>2</sup>”: de persoon wiens persoonsgegevens worden verwerkt;
- 4) “verwerkingsverantwoordelijke”: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt;
- 5) “(een) derde”: een natuurlijke persoon of rechtspersoon, niet zijnde de betrokkene of de verwerkingsverantwoordelijke.

De hieronder staande begrippen zijn niet afkomstig uit de AVG, maar worden wel veelvuldig gebruikt in de komende hoofdstukken.

- 6) “(de) vrijwilliger”: een natuurlijke persoon die namens StiB werk verricht zonder recht te hebben op een bezoldiging. StiB heeft zowel vrijwilligers die op het kantoor werken als vrijwilligers die hulpvragers of mantelzorgers ondersteunen. Alleen de vrijwilligers op het kantoor verwerken gegevens;
- 7) “(de) mantelzorger: een natuurlijke persoon die voor een derde (vaak de hulpvrager) zorgt, zonder hiervoor een bezoldiging te ontvangen;
- 8) “(de) hulpvrager”: een natuurlijke persoon die de hulp van StiB inroept, niet zijnde een mantelzorger;
- 9) “(de) cliënt”: hiermee kan worden bedoeld een hulpvrager of een mantelzorger;
- 10) “(het) privacyprotocol”: wordt ook aangehaald als “het protocol” of “het beleid”. Het “Privacyprotocol Wijknetwerken Breda” bevat de geldende regels omtrent het verwerken van persoonsgegevens en de verplichtingen die voor de organisaties van Zorg voor elkaar Breda voortvloeien uit de Wet bescherming persoonsgegevens;

---

<sup>1</sup> Artikel 4 van de Algemene Verordening Gegevensbescherming.

<sup>2</sup> Het begrip “betrokkene” wordt niet met zoveel woorden in de Algemene Verordening Gegevensbescherming gedefinieerd. Het begrip staat wel opgenomen in de definitie van “persoonsgegevens”. Hieruit is op te maken wat er wordt bedoeld met het begrip “betrokkene”. Daarbij gebruiken zowel de Richtlijn 95/46/EG (artikel 2, onder a) als de Wet bescherming persoonsgegevens (artikel 1, onder f) dit begrip op dezelfde wijze.

# Hoofdstuk 1      Onderzoeksopzet

---

In dit hoofdstuk wordt het onderzoek ingeleid. Kort zal besproken worden wat voor organisatie Stichting Steunpunt informele zorg Breda (verder: StIB) is en wat zij doet. Vervolgens wordt beschreven welk juridisch probleem momenteel bij de organisatie heerst. Aan de hand van deze probleembeschrijving wordt een centrale vraag geformuleerd. Hierbij komt ook het doel van dit onderzoek aan bod. In de daaropvolgende paragrafen worden de methoden en technieken die gebruikt zijn om tot een beantwoording van de centrale vraag te komen uiteengezet en verantwoord. Ten slotte bevat het hoofdstuk een leeswijzer.

## 1.1 Inleiding

StIB is een van de vele organisaties die deel uitmaken van Zorg voor elkaar Breda. Zorg voor elkaar Breda onderhoudt een netwerk van verscheidene maatschappelijke organisaties gevestigd in Breda. De inwoners van Breda kunnen voor hulpvragen betreffende de zorg, ondersteuning bij de zorg of het inschakelen van zorg via Zorg voor elkaar Breda in contact worden gebracht met deze maatschappelijke organisaties.

StIB biedt advies, hulp en ondersteuning aan iedereen in Breda die langdurig zorgt voor een ander. De stichting beheert een netwerk van mantelzorgers, hulpvragers en vrijwilligers. Zij organiseert voor deze groepen workshops en begeleidt daar waar nodig. Daar waar de omgeving niet van dienst kan zijn, ondersteunen de vrijwilligers van StIB bij zorg thuis.<sup>3</sup> Daarbij functioneert StIB ook als kenniscentrum voor de mantelzorg. Zo kan iedereen die vragen heeft rondom het geheugen, dementie of niet-aangeboren hersenletsel (NAH) terecht in de Geheugenwinkel. Momenteel is het netwerk opgebouwd uit meer dan 3000 hulpvragers en 400 vrijwilligers.

## 1.2 Probleembeschrijving

Vanzelfsprekend hebben de medewerkers van StIB te maken met de regels omtrent het privacyrecht. StIB verwerkt dagelijks persoonsgegevens van haar cliënten. Zo worden de lichamelijke en/of geestelijke beperkingen van een hulpvrager geregistreerd, zodat de juiste vrijwilliger gekoppeld kan worden aan deze cliënt. Het spreekt voor zich dat met dit soort gegevens op de juiste wijze moet worden omgegaan.

Om die reden heeft Zorg voor elkaar Breda een privacyprotocol op laten stellen.<sup>4</sup> In het protocol worden de regels geldend op grond van de Wet bescherming persoonsgegevens uiteengezet en besproken. Het protocol gaat voornamelijk over de relatie tussen de cliënt en de organisatie. Daarbij is een document genaamd "privacyspelregels" opgesteld. In de spelregels staan enkele casussen opgenomen. Deze casussen worden uitgewerkt aan de hand van het privacyprotocol, zodat medewerkers kunnen lezen wat de gedachtegang is die zij moeten volgen bij het oplossen van vraagstukken tijdens hun werkzaamheden. De spelregels maken formeel gezien geen deel uit van het beleid van StIB.

Er heerst echter onduidelijkheid onder de medewerkers betreffende het huidige beleid. Sommige medewerkers hebben moeite met het maken van een vertaalslag van de regels naar de toepassing in de praktijk. Anderen zijn niet op de hoogte van het beleid en weten niet waar ze moeten beginnen. Het beleid is daarbij zeer juridisch opgesteld en heeft naar mening van sommige medewerkers weinig tot geen praktische waarde. Daarbij speelt ook dat StIB geen eigen jurist in dienst heeft. Het is momenteel voor de medewerkers niet mogelijk om uitleg te krijgen over het protocol.

---

<sup>3</sup> 'Over StIB' *Stichting Steunpunt informele zorg Breda*, stib-breda.nl.

<sup>4</sup> Zie Bijlage 1.

Dit baart StiB zorgen. De stichting ziet in dat de privacyregelgeving steeds belangrijker wordt en wil dat het privacyprotocol gaat leven in de organisatie. StiB wenst dan ook dat het geheel omtrent het privacyprotocol wordt gestructureerd en wordt verduidelijkt. Iedere medewerker dient op de hoogte te zijn van het beleid en moet weten *hoe* en *wanneer* een regel moet worden toegepast. Het toepassen van de privacyregelgeving moet efficiënt kunnen gebeuren.

Hierbij speelt ook nog dat de Algemene Verordening Gegevensbescherming (verder: AVG) is gepubliceerd. Deze Europese verordening zal de huidige nationale wetgeving vervangen. De kans bestaat dat het huidige beleid straks achterhaald is. Met de invoering van de verordening is er een overgangperiode gestart.<sup>5</sup> Organisaties hebben tot 25 mei 2018 de tijd om hun beleid aan te passen aan de nieuwe regelgeving. Vóór deze datum dient het beleid van StiB in orde te zijn. Tijdens het doorspitten van het huidige beleid dient dus rekening te worden gehouden met de mogelijke wijzigingen of (nieuwe) rechten en plichten die de AVG met zich meebrengt.

De stichting wenst een duidelijke en gemakkelijk te lezen vertaling van het protocol, waarbij rekening wordt gehouden met de komst van de AVG. Het is essentieel voor StiB om te weten aan welke regels zij zich moet houden tijdens het werken met cliënten, zodat zij zonder problemen haar diensten kan verlenen. StiB hoopt dat door middel van het opstellen van nieuwe producten die het protocol verduidelijken de privacyregels worden gewaarborgd.

### 1.3 Centrale vraag

Welke aanbevelingen zijn af te leiden uit een toetsing van het huidige privacybeleid, en de praktische toepassing daarvan, aangaande de omgang met cliënten van Stichting Steunpunt informele zorg Breda aan de Algemene Verordening Gegevensbescherming?

### 1.4 Doelstelling

Op 1 februari 2017 wordt een adviesrapport opgeleverd aan de bestuurder van de Stichting Steunpunt informele zorg Breda, waarin de aanpassingen en toevoegingen voortvloeiend uit de Algemene Verordening Gegevensbescherming zijn uitgewerkt, zodat nieuwe producten en beleidsregels kunnen worden ontworpen ten behoeve van de werknemers, zodat StiB ten opzichte van haar cliënten kan voldoen aan de rechten en plichten voortkomend uit de geldende privacywetgeving.

### 1.5 Deelvragen

De onderstaande deelvragen zijn opgesteld, zodat de centrale vraag gericht kan worden beantwoord.

1. Welke relevante rechten en plichten vloeien voort uit de Algemene Verordening Gegevensbescherming?
  - Subvraag 1: Welke rechten hebben c.q. krijgen de cliënten?
  - Subvraag 2: Welke plichten hebben de medewerkers van StiB tegenover de cliënten?
2. Hoe gaat StiB om met het verwerken van de persoonsgegevens van haar cliënten?
  - Subvraag 1: Welke persoonsgegevens van de cliënten worden verwerkt?
  - Subvraag 2: Op welke wijze verwerkt StiB de gegevens?
  - Subvraag 3: Op welke wijze informeert StiB de cliënt over het verwerken van persoonsgegevens?
3. Hoe gaat StiB intern om met het beleid?
4. In welke opzichten komt het beleid van StiB overeen met de Algemene Verordening Gegevensbescherming?

---

<sup>5</sup> Artikel 99, eerste lid, van de Algemene Verordening Gegevensbescherming. De verordening is op 25 mei 2016 in werking getreden en zal op 25 mei 2018 van toepassing zijn.

Subvraag 1: Welke procedures, voortvloeiend uit de Algemene Verordening Persoonsgegevens met betrekking tot de plichten die StiB heeft tegenover haar cliënten, zijn momenteel niet of onjuist geregeld?

## 1.6 Afbakening

Dit onderzoek beperkt zich voornamelijk tot de privacywetgeving omtrent de betrokkene (de cliënt) en de verwerkingsverantwoordelijke (StiB). Interne aangelegenheden, zoals het verwerken van en de omgang met persoonsgegevens van personeelsleden, worden niet besproken.

## 1.7 Onderzoeksmethodiek & verantwoording

Hieronder staat weergegeven welke onderzoeksstrategieën, bronnen en methoden zijn toegepast c.q. gebruikt tijdens het onderzoek. De verantwoording is tevens per deelvraag opgenomen.

### *Welke relevante rechten en plichten vloeien voort uit de Algemene Verordening Gegevensbescherming?*

De eerste deelvraag vormt het juridisch kader. Aan de hand van een onderzoek van het recht wordt gekeken welke relevante rechten en plichten de AVG in het leven roept. Hierbij is rekening gehouden met de inhoud van het privacyprotocol, zodat overbodige artikelen achterwege worden gelaten. Bij dit onderzoek is gebruikgemaakt van verschillende rechtsbronnen.

Zowel de AVG als de Wet bescherming persoonsgegevens (verder: Wbp), inclusief de daarbij behorende toelichtingen en kamerstukken, zijn veelvuldig geraadpleegd. Het spreekt voor zich dat het doornemen van de officiële publicaties uit het Publicatieblad van de Europese Unie en de Staatscourant hiervoor de meest betrouwbare bronnen zijn. Het toepassen van een inhoudsanalyse is hiervoor de meest geschikte optie. Er is gekozen om ook de Wbp en de bijbehorende memorie van toelichting te raadplegen, omdat de AVG niet alle onderdelen van de huidige regelgeving wijzigt. De toelichting behorende bij de Wbp bevat dan ook waardevolle informatie betreffende het doel van een artikel, de wijze van interpretatie en de wijze waarop het moet worden toegepast.

Daarnaast is aansluiting gezocht bij de literatuur over de AVG. De artikelen die worden gebruikt zijn grotendeels afkomstig uit bekende en vertrouwde tijdschriften zoals het Nederlandse Juristenblad en het Nederlands Tijdschrift voor Europees Recht. De overige artikelen zijn benaderd door middel van vertrouwde juridische databanken, zoals Kluwer Navigator en Legal Intelligence. Hierdoor wordt de kwaliteit van de artikelen gewaarborgd.

Ten slotte is er telefonisch een gesloten interview gehouden met de Autoriteit Persoonsgegevens. In dit interview zijn vragen gesteld om een aantal onduidelijkheden op te helderen.

### *Hoe gaat StiB om met het verwerken van de persoonsgegevens van haar cliënten?*

De opdrachtgever hanteert een beleid dat conform de Wbp is opgesteld. Aan de hand van dit beleid worden persoonsgegevens van de cliënten verwerkt. Om na te kunnen gaan of de huidige manier van werken aangepast dient te worden, zal bekeken moeten worden hoe StiB persoonsgegevens verwerkt en of dit conform het beleid gebeurt.

Door middel van een enkelvoudige casestudy wordt onderzocht welke persoonsgegevens worden verwerkt, op welke wijze dit gebeurt en hoe StiB haar cliënten informeert. De voornaamste onderzoeksmethoden zijn het observeren van medewerkers en het afnemen van (semigestructureerde) interviews. Tijdens het observeren wordt gekeken hoe een

medewerker de privacyregels toepast in het werkveld. Daarbij wordt ook gekeken of het verwerken conform het beleid gebeurt.

Er is rekening gehouden met de mogelijkheid dat een werknemer zich anders gaat gedragen tijdens de observatie. Hiervoor is een aanpak bedacht. Het observeren zal sporadisch gebeuren. De stichting werkt voornamelijk met flexwerkplekken. Medewerkers worden gemotiveerd om zoveel mogelijk gebruik te maken van deze flexwerkplekken. Door dagelijks van werkplek te wisselen, en dus steeds op een andere afdeling werkzaam te zijn, wordt voorkomen dat medewerkers zich bekeken voelen. Enkel de aanwezigheid van de onderzoeker betekent namelijk niet dat er wordt geobserveerd. De werknemers die zijn geïnterviewd, zijn gekozen aan de hand van de observaties. De vragen zijn gevormd aan de hand van deze observaties. De medewerker krijgt hierdoor de ruimte om het een en ander toe te lichten.

#### *Hoe gaat StiB intern om met het beleid?*

Bij de beantwoording van deze vraag wordt nogmaals gebruikgemaakt van het observeren van medewerkers en het houden van interviews. Anders dan bij de vorige deelvraag wordt bij deze deelvraag bekeken hoe werknemers onderling omgaan met het beleid. Om een globale indruk te krijgen is er eerst een survey uitgezet onder de werknemers. Het doel van deze survey is het onderzoeken of het beleid überhaupt wel leeft in de organisatie.

De medewerkers worden door middel van deze anonieme survey benaderd voor input. Er is gekozen voor een survey, omdat met een survey op een efficiënte wijze alle medewerkers benaderd kunnen worden. Deze wijze van onderzoeken is daarbij ook de meest geschikte optie, omdat de meeste medewerkers parttime werken en niet altijd op het kantoor aanwezig zijn. De survey is anoniem, zodat medewerkers vrijelijk kritiek kunnen uiten. Daarbij wordt de vragenlijst digitaal aangeleverd en kan worden geprint. Op deze manier blijft de identiteit van medewerker die de vragenlijst heeft ingevuld geheim. Met deze survey wordt tevens gekeken of de medewerkers, die menen bekend te zijn met het beleid, ook daadwerkelijk op de hoogte zijn van het beleid en de inhoud daarvan beheersen.

In de probleembeschrijving is al aangegeven, dat niet iedereen bekend is met het beleid. Het is vanzelfsprekend dat men niet conform het beleid kan handelen als men onbekend is met het beleid. Om dit te ontrafelen is ook meegekeken bij het inwerken van nieuwe medewerkers, zodat kan worden bekeken of het beleid tijdens het inwerkingstraject voldoende wordt besproken.

#### *In welke opzichten komt het beleid van StiB overeen met de Algemene Verordening Gegevensbescherming?*

Bij de laatste deelvraag wordt het huidige beleid getoetst aan de AVG. Aan de hand van de vorige deelvragen is onderzocht wat er volgens de AVG in het beleid moet staan en hoe StiB momenteel omgaat met het verwerken van gegevens. Door middel van deze toetsing wordt bekeken op welke gebieden StiB haar beleid moet aanpassen en wat nog geregeld moet worden.

De AVG en het beleid van StiB zijn de voornaamste bronnen bij de beantwoording van deze deelvraag. Verder worden artikelen en de bijbehorende toelichtingen bestudeerd om de correcte wijze van interpretatie te achterhalen.

## **1.8 Leeswijzer**

In het tweede hoofdstuk wordt de AVG bekeken. De relevante artikelen uit de AVG worden in dit hoofdstuk uitgelegd. Het derde hoofdstuk worden de survey, de observaties en de interviews die met de medewerkers zijn gehouden besproken. In dit hoofdstuk wordt onderzocht wat de medewerkers graag veranderd zien aan het beleid. In het vierde hoofdstuk is de AVG naast het protocol gelegd en is gekeken in hoeverre het protocol

inhoudelijk aangepast moet worden. In het vijfde hoofdstuk wordt kort besproken hoe StiB momenteel het protocol toepast. Het laatste hoofdstuk bestaat uit de conclusies en de aanbevelingen.

## Hoofdstuk 2 De Algemene Verordening Gegevensbescherming

---

In dit hoofdstuk wordt het juridische kader uiteengezet. Alleen de artikelen die voor dit onderzoek van belang zijn worden besproken. StiB heeft geen juristen in dienst. Om die reden wordt er per artikel een uitgebreide toelichting gegeven, zodat in de toekomst ook de niet-juristen aan de hand van de uitleg de artikelen kunnen toepassen.

### 2.1 Toetsingskader rechtmatige gegevensverwerking

De bescherming van persoonsgegevens is een grondrecht. Door iemands persoonsgegevens te verwerken wordt er inbreuk gemaakt op dit grondrecht. Artikel 8 van het Handvest van de Grondrechten van de Europese Unie stelt dat het verwerken van persoonsgegevens enkel in bepaalde gevallen mag en eerlijk moet gebeuren. Persoonsgegevens mogen alleen worden verwerkt, indien de doeleinden hiervoor zijn vastgelegd. Daarbij geldt dat verwerking enkel mag gebeuren met toestemming van de betrokkene of wanneer sprake is van een gerechtvaardigde grondslag. De wet voorziet in de grondslagen voor de rechtmatige verwerking van persoonsgegevens.

In hoofdstuk II van de AVG wordt het toetsingskader voor de rechtmatige verwerking van persoonsgegevens uiteengezet. De artikelen in dit hoofdstuk beogen de eerlijke verwerking van gegevens en voorzien in de gerechtvaardigde grondslagen waarop verwerking gebaseerd kan worden.

#### 2.1.1 Beginselen inzake de verwerking van persoonsgegevens

Artikel 5, eerste lid, van de AVG legt de beginselen voor het rechtmatig verwerken van persoonsgegevens neer. Het artikel bevat een aantal waarborgen waaraan een verwerkingsverantwoordelijke moet voldoen, alvorens hij overgaat tot het verwerken van persoonsgegevens. De verwerkingsverantwoordelijke dient zich te houden aan de volgende beginselen:

- 1) *de wijze van verwerking van de persoonsgegevens dient ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant te gebeuren;*

Het eerste beginsel legt de verwerkingsverantwoordelijke de plicht op om ervoor te zorgen, dat hij de gegevens rechtmatig, behoorlijk en transparant verwerkt. Met het "rechtmatig verwerken van persoonsgegevens" wordt bedoeld op het verkrijgen van toestemming of de aanwezigheid van een gerechtvaardigde grondslag. Met de "behoorlijke" en "transparante" verwerking van persoonsgegevens wordt bedoeld op het vermijden van heimelijkheid bij het verwerken van alle aspecten van persoonsgegevens.<sup>6</sup> Het moet voor de betrokkene duidelijk zijn welke gegevens van hem worden verwerkt en waarvoor dit gebeurt.<sup>7</sup>

- 2) *de persoonsgegevens mogen enkel worden verzameld indien hier welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden voor zijn en mogen niet voor andere doeleinden worden verwerkt dan wat is aangegeven;*

Iedere verwerkingsverantwoordelijke dient aan te geven waarvoor hij gegevens verzamelt; dit wordt ook wel doelbinding genoemd. Een onderneming zou als doel kunnen hebben: het verzamelen van persoonsgegevens voor het aanbieden van reclames of voor het uitvoeren van een overeenkomst. Wat precies de doeleinden zijn, hangt af van de organisatie.

---

<sup>6</sup> Jong, de, *RegelMaat* 2015, p. 9.

<sup>7</sup> Overweging 39 en 60 van de toelichting behorende bij de Algemene Verordening Gegevensbescherming.

Volgens de Artikel 29-Werkgroep moeten organisaties rekening houden met de wijze waarop zij hun doeleinden formuleren.<sup>8</sup> De doeleinden mogen niet te algemeen zijn opgesteld, maar ook niet overbodig gedetailleerd. Er moet een balans zijn. Bij het zoeken naar deze balans moet men de grootte van de organisatie in het achterhoofd houden. De bakker op de hoek mag zijn doelen algemener houden dan een multinational zoals Philips. Zo zou “ICT-gerelateerde doeleinden” of “ter uitvoering van een overeenkomst” voor Philips te breed zijn. Voor de bakker, die de gegevens alleen verwerkt om 's ochtends brood te kunnen bezorgen, kan dit al voldoende zijn.

De Artikel 29-Werkgroep raadt aan om gebruik te maken van een “*layered-notice approach*”. Dit houdt in dat de betrokkene in het algemeen wordt geïnformeerd (bijvoorbeeld: de gegevens worden verwerkt ter uitvoering van een overeenkomst), maar dat hij wel de mogelijkheid krijgt om specifiekere informatie op te zoeken c.q. te vragen (bijvoorbeeld: wat wordt er precies bedoeld met “de overeenkomst?” en “waarom zijn deze gegevens noodzakelijk?”).

Het verwerken van persoonsgegevens mag alleen als de doeleinden *gerechtvaardigd* zijn. De verwerkingsverantwoordelijke mag dus geen persoonsgegevens verwerken die niet nodig zijn voor de verwerking. De verwerkingsverantwoordelijke mag tevens geen persoonsgegevens verwerken voor doeleinden anders dan is medegedeeld.

- 3) *toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt;*

De verwerkingsverantwoordelijke dient ervoor te zorgen dat hij niet meer persoonsgegevens verwerkt dan wat noodzakelijk is voor het verwezenlijken van het doeleinde. Zo zal een bakker niet de geboortedatum van een willekeurige klant die langskomt in de bakkerij mogen verwerken in haar administratie. Daarbij geldt ook dat de gegevens alleen verwerkt mogen worden, indien er redelijkerwijs geen andere manier is om aan de doelstelling te voldoen.

- 4) *juist zijn en zo nodig worden geactualiseerd;*

Dit kort maar krachtige beginsel spreekt voor zich. Verwerkingsverantwoordelijken zijn verplicht om ervoor te zorgen dat de gegevens die worden verwerkt up-to-date zijn. De verwerkingsverantwoordelijke moet alle redelijke maatregelen nemen om aan deze verplichting te voldoen.<sup>9</sup>

- 5) *worden bewaard in een vorm die het mogelijk maakt de betrokkene niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is;*

Dit beginsel gaat over de “vorm” waarin persoonsgegevens bewaard worden. Hierbij kan gedacht worden aan een profiel in een administratiesysteem. Het moet mogelijk zijn om de betrokkene onidentificeerbaar te maken, wanneer de gegevens niet langer noodzakelijk zijn om het doeleinde te bereiken. Volgens de Autoriteit Persoonsgegevens (verder: AP) betekent dit dat de persoonsgegevens zoveel mogelijk worden geanonimiseerd en/of gepseudonimiseerd, indien de persoonsgegevens niet langer nodig zijn voor of de verwerkingsverantwoordelijke niet langer een belang heeft bij het doeleinde.<sup>10</sup>

- 6) *door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.*

<sup>8</sup> ‘Opinion 03/2013 on purpose limitation’, [ec.europa.eu/justice](http://ec.europa.eu/justice) 2 april 2013.

<sup>9</sup> Overweging 39 laat het begrip *redelijke maatregelen* open. Wat hieronder valt zal per organisatie verschillen. De ene organisatie zal meer mankracht hebben om periodiek de gegevens te actualiseren, terwijl de andere organisatie dit wellicht eens in de twee jaar kan doen.

<sup>10</sup> Zie Bijlage 2.

Dit laatste beginsel gaat over de beveiliging van een systeem waarin persoonsgegevens worden verwerkt. Persoonsgegevens kunnen zowel fysiek als digitaal worden opgeslagen. Afhankelijk van de wijze waarop de persoonsgegevens worden opgeslagen, zal een organisatie maatregelen moeten treffen die de veiligheid van de gegevens garanderen. Zo zou bij fysieke opslag gedacht kunnen worden aan de beveiliging van dossierkasten, zodat niet iedere persoon de kast kan openen. Bij de digitale opslag van gegevens gaat het om de (database)rechten van de gebruikers. Niet iedere gebruiker zou het recht mogen hebben om alle persoonsgegevens in te kijken, indien dit niet noodzakelijk is voor het uitvoeren van zijn werkzaamheden.

De beveiliging van systemen wordt nog verder uitgewerkt in de AVG.<sup>11</sup> Volgens dit artikel moet de organisatie maatregelen treffen waardoor het (vrijwel) onmogelijk wordt om bepaalde gegevens te verwerken die niet noodzakelijk zijn voor het te behalen doeleinde.<sup>12</sup> Door een formulier zo te ontwerpen dat deze gegevens niet kunnen worden genoteerd, wordt vermeden dat onnodige gegevens worden verwerkt.

### 2.1.2 De beginselen van proportionaliteit en subsidiariteit

Alvorens in te gaan op de rechtmatigheidsgronden dienen nog twee andere beginselen besproken te worden. Gesteld is dat geen inbreuk op een grondrecht mag worden gemaakt, tenzij dit noodzakelijk is en bij wet is voorzien. Met "bij wet voorzien" wordt bedoeld, dat een wet (of jurisprudentie, beleidsregel, enz.) aangeeft wanneer het toegestaan is om een inbreuk te maken.<sup>13</sup> De komst van de AVG verandert hieraan niets. De hierna te bespreken rechtmatigheidsgronden zijn de gronden waarop een inbreuk kan worden gebaseerd. Louter de aanwezigheid van een rechtmatigheidsgrond betekent echter nog niet dat er een inbreuk gemaakt mag worden op een grondrecht.

Volgens de vaste jurisprudentie moet men artikel 6 van de AVG in samenhang met artikel 8 van het Europees Verdrag voor de Rechten van de Mens (verder: EVRM) lezen.<sup>14</sup> Deze samenhang behelst dat men bij iedere verwerking van persoonsgegevens moet voldoen aan de beginselen van proportionaliteit en subsidiariteit. Deze beginselen vloeien voort uit het EVRM. Daarbij moet er een belangenafweging worden gemaakt, waarbij de belangen van de verwerkingsverantwoordelijke en die van de betrokkene tegen elkaar worden afgewogen. Het belang van de verwerkingsverantwoordelijke dient zwaarder te wegen dan die van de betrokkene. Is hier geen sprake van, dan is verwerking niet toegestaan.

Met het proportionaliteitsbeginsel wordt bedoeld dat niet meer gegevens mogen worden verwerkt dan nodig is om het doel te bereiken.<sup>15</sup> Het subsidiariteitsbeginsel houdt in dat eerst gekeken moet worden of een minder ingrijpend middel voor de hand ligt om een doel te kunnen bereiken. In het kader van de privacywetgeving betekent dit bijvoorbeeld dat de verwerkingsverantwoordelijke eerst moet kijken of het mogelijk is om toestemming te vragen. Wanneer toestemming niet mogelijk is of redelijkerwijs niet verkregen kan worden, mag de verwerkingsverantwoordelijke in bepaalde gevallen een beroep doen op een ingrijpend middel.

### 2.1.3 De rechtmatigheidsgronden

Het verwerken van persoonsgegevens is alleen rechtmatig, indien de verwerking wordt gebaseerd op een van de rechtmatigheidsgronden opgenomen in de AVG.<sup>16</sup> Deze lijst is limitatief. De verordening kent een zestal rechtmatigheidsgronden. De rechtmatigheidsgronden zijn:

<sup>11</sup> Artikel 25 van de Algemene Verordening Gegevensbescherming.

<sup>12</sup> Autoriteit Persoonsgegevens, 'Privacy by design', *autoriteitpersoonsgegevens.nl*.

<sup>13</sup> *Kamerstukken II 1997/98*, 25892, 3, p. 8.

<sup>14</sup> HR 9 september 2011, ECLI:NL:HR:2011:BQ8097, r.o. 4.5, 4.7 & 4.8.

<sup>15</sup> Kranenborg & Verhey 2010, p. 25.

<sup>16</sup> Artikel 6, eerste lid, van de Algemene Verordening Gegevensbescherming.

- a) de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;
- b) de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;
- c) de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;
- d) de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;
- e) de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen;
- f) de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of een derde. Hierbij geldt dat belangen, grondrechten of de fundamentele vrijheden van de betrokkene niet zwaarder mogen wegen dan die van de verwerkingsverantwoordelijke.

De twee beginselen besproken in de vorige paragraaf dienen bij het gebruik van iedere rechtmatigheidgrond te worden toegepast.

#### Verwerking op grond van toestemming

Indien men toestemming krijgt om persoonsgegevens te verwerken, dan is het in beginsel toegestaan om deze persoonsgegevens te verwerken. Verwerking op grond van toestemming kent wel een aantal inperkingen. De verwerkingsverantwoordelijke die persoonsgegevens verwerkt op grond van toestemming moet voldoen aan een groot aantal extra verplichtingen. Deze verplichtingen zorgen ervoor dat de betrokkene bekend is met het feit dat de verwerkingsverantwoordelijke zijn persoonsgegevens verwerkt en dat hij daar toestemming voor heeft gegeven. De AVG bevat een aparte regeling voor het geven van toestemming.<sup>17</sup>

#### Verwerking ter uitvoering van een overeenkomst

Deze "b-grond" geeft de verwerkingsverantwoordelijke de mogelijkheid om persoonsgegevens te verwerken, indien dit noodzakelijk is voor de uitvoering van een overeenkomst of om — op verzoek van de betrokkene — vóór de sluiting van een overeenkomst maatregelen te nemen (i.e. de precontractuele fase). Het moet hier wel gaan om een overeenkomst die *niet* ziet op het verwerken van persoonsgegevens.<sup>18</sup>

#### Verwerking om te voldoen aan een wettelijke verplichting

De wet kan een bepaalde instantie bevelen persoonsgegevens te verwerken. De betrokkene hoeft alleen de persoonsgegevens te verstrekken aan een instantie die noodzakelijk zijn voor deze instantie om aan de wet te voldoen. Hierbij kan gedacht worden aan het verstrekken van gezondheidsgegevens aan een zorgverzekeraar.

#### Verwerking om de vitale belangen van een natuurlijk persoon te beschermen

Verwerking is toegestaan, indien dit noodzakelijk is voor de vitale belangen van de betrokkene of een andere persoon. Volgens de uitleg in de memorie van toelichting dient deze grond "eng" te worden geïnterpreteerd.<sup>19</sup> Gegevens mogen alleen op deze wijze worden verwerkt, indien sprake is van leven of dood. Deze rechtsgrond lijkt daarom vrij beperkt. Dit geldt zeker, nu niet iedereen weet wanneer sprake is van zaak van een leven of dood. Iemand die bewusteloos is, kan geen toestemming geven. Het is echter niet zo dat een bewusteloos persoon in een levensbedreigende situatie verkeert. Dit is voor een leek niet altijd even makkelijk om vast te stellen. Gelukkig ziet de wetgever (zowel de Nederlandse als de Europese) dit ook in:

<sup>17</sup> Zie paragraaf 2.1.4.

<sup>18</sup> Kamerstukken II 1997/98, 25892, 3, p. 81.

<sup>19</sup> Kamerstukken II 1997/98, 25892, 3, p. 83.

*“Ook indien de noodzaak om op te treden zo dringend is dat in redelijkheid van de verantwoordelijke niet kan worden gevraagd toestemming van de betrokkene(n) te vragen, kan een gegevensverwerking op grond van dit voorschrift geoorloofd zijn.”<sup>20</sup>*

Verwerking ter vervulling van een taak van algemeen belang of uitoefening openbaar gezag  
Deze grond is van toepassing, indien verwerking noodzakelijk is voor de vervulling van een taak van een bestuursorgaan. Deze grondslag is enkel van toepassing in het publieksrecht

#### Verwerking in het belang van de verwerkingsverantwoordelijke

De "f-grond" kan enkel worden gebruikt, indien sprake is van een gerechtvaardigd belang van de verwerkingsverantwoordelijke. Dit belang dient zwaarder te wegen dan de fundamentele vrijheden, de grondrechten en belangen van de betrokkene. Een organisatie die een zwarte lijst bijhoudt, mag alleen personen op deze lijst noteren als het belang van de organisatie zwaarder weegt dan die van de betrokkene. Een betrokkene die is veroordeeld voor diefstal tijdens zijn werk zal niet langer welkom zijn bij deze organisatie. Het belang van de organisatie om niet langer met de betrokkene in aanraking te komen zal in dit voorbeeld zwaarder wegen dan het recht op privacy van de betrokkene.

#### 2.1.4 Voorwaarden voor toestemming

De verwerkingsverantwoordelijke dient aan te kunnen tonen dat de betrokkene toestemming heeft gegeven voor de verwerking van persoonsgegevens.<sup>21</sup> Wat opvalt is dat de verwerkingsverantwoordelijke de last krijgt om te bewijzen dat toestemming is verleend. Toestemming kan alleen worden verleend als een duidelijke actieve handeling hiertoe heeft geleid.<sup>22</sup> De aangehaalde overweging wijst er uitdrukkelijk op dat “stilzwijgen, het gebruik van reeds aangevinkte vakjes of inactiviteit” niet als toestemming mogen worden aangemerkt. Voorbeelden die worden gegeven voor “actieve handelingen” zijn het aanvinken van een vakje, het selecteren van technische instellingen voor diensten van de informatiemaatschappij en een verklaring of andere handelingen waaruit instemming blijkt.

De toestemming dient vrijelijk, specifiek, geïnformeerd en ondubbelzinnig te zijn gegeven. De ondubbelzinnigheid van de te geven toestemming houdt in dat uit de gegeven toestemming moet blijken dat de betrokkene precies weet waarom en waarvoor hij toestemming geeft.<sup>23</sup> De criteria vrijelijk, specifiek en geïnformeerd komen met andere woorden terug in het artikel.

Ten overvloede wordt eerst opgemerkt dat het te bespreken lid enkel spreekt over het verlenen van "schriftelijke toestemming voor meerdere aangelegenheden." Echter, de toelichting rept met geen woord over (enkel) deze schriftelijke toestemming.<sup>24</sup> Sterker nog, de toelichting praat juist over andere vormen van het verlenen van toestemming. Ook in de literatuur lijkt men ervan uit te gaan dat ook andere vormen van toestemming vrijelijk, specifiek en geïnformeerd moeten worden gegeven.<sup>25</sup> Hiervan zal dan ook worden uitgegaan.

De begrippen vrijelijk, specifiek en geïnformeerd zijn in art 7, lid 2 van de AVG als volgt verwoord:

***“...wordt het verzoek om toestemming in een begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal zodanig gepresenteerd dat een duidelijk onderscheid kan worden gemaakt met de andere aangelegenheden.”<sup>26</sup>***

<sup>20</sup> Kamerstukken II 1997/98, 25892, 3, p. 84.

<sup>21</sup> Artikel 7, eerste lid, van de Algemene Verordening Gegevensbescherming.

<sup>22</sup> Overweging 32 van de toelichting behorende bij de Algemene Verordening Gegevensbescherming.

<sup>23</sup> Artikel 6, eerste lid en sub a, van de Algemene Verordening Gegevensbescherming ziet op deze ondubbelzinnigheid.

<sup>24</sup> Overweging 32 van de toelichting behorende bij de Algemene Verordening Gegevensbescherming.

<sup>25</sup> Vries, de, & Goudsmit, *NJB* 2016, p. 1553.

<sup>26</sup> Artikel 7, tweede lid, van de Algemene Verordening Gegevensbescherming.

Voor de gemiddelde burger zijn de vele privacyreglementen en gebruikersvoorwaarden waar ze dagelijks mee te maken kunnen krijgen te ingewikkeld qua inhoud en manier van schrijven.<sup>27</sup> Veel personen lezen de tekst vluchtig door of slaan deze over en gaan akkoord met de gebruikersvoorwaarden. Vaak betekent dit dat toestemming wordt gegeven voor het verwerken van allerlei persoonlijke gegevens (bv: surfgedrag op het internet) die de betrokkene wellicht liever niet vrij zou geven.

Door striktere eisen te stellen aan de inlichtingsplicht hoopt de wetgever dat de burgers eerder de gebruikersreglementen doornemen voordat ze hiermee akkoord gaan.<sup>28</sup> De wetgever hoopt dat door het verplichten van een actieve handeling wordt voorkomen dat men gebruik blijft maken van reeds aangevinkte vakjes of andere voorgeselecteerde instellingen.

Per doeleinde dient de betrokkene aan te kunnen geven of zijn gegevens daarvoor mogen worden verwerkt. Indien deze mogelijkheid niet bestaat, wordt de toestemming als niet bindend gezien.

De betrokkene kan op ieder moment zijn toestemming intrekken.<sup>29</sup> De verwerkingsverantwoordelijke dient dit aan de betrokkene kenbaar te maken alvorens hij begint met het verwerken van de gegevens van de betrokkene. Het intrekken van de toestemming kan op eenzelfde wijze gebeuren als het geven van de toestemming. Het intrekken heeft als gevolg dat de verwerkingsverantwoordelijke direct dient te staken met het verwerken van persoonsgegevens. Het intrekken tast de rechtmatigheid van het verwerken van persoonsgegevens vóór de intrekking niet aan.

Als laatste voorwaarde geldt dat de betrokkene de keuze moet hebben over het wel of niet laten verwerken van bepaalde persoonsgegevens die *niet* noodzakelijk zijn voor het uitvoeren van een overeenkomst. Zo zou StiB van een cliënt kunnen verlangen dat hij aangeeft wat zijn religieuze overtuiging is.<sup>30</sup> Men kan zich afvragen of deze gegevens wel noodzakelijk zijn voor het uitvoeren van een overeenkomst. Indien de opvatting is dat dit niet noodzakelijk is, dan moet de betrokkene de optie hebben om het verwerken van deze gegevens te weigeren, zonder dat dit als gevolg heeft dat de overeenkomst niet zal/kan worden uitgevoerd. Indien deze mogelijkheid niet aanwezig is, kan worden geoordeeld dat de toestemming niet vrijelijk is gegeven.<sup>31</sup>

#### 2.1.5 Verwerking van bijzondere categorieën persoonsgegevens

Artikel 9 van de AVG gaat over de verwerking van bijzondere categorieën persoonsgegevens. De (relevante) bijzondere categorieën persoonsgegevens zijn gegevens waaruit het ras of de etnische afkomst, de politieke opvattingen, de seksuele geaardheid, de religieuze of levensbeschouwelijke overtuigingen, gezondheidsgegevens van de betrokkene blijken. Het is in beginsel verboden om deze gegevens te verwerken. Dit mag alleen als een van de rechtmatigheidsgronden opgenomen in artikel 9 van toepassing is. Om verwarring met de rechtmatigheidsgronden uit 2.1.3 te voorkomen, worden deze rechtmatigheidsgronden voor het gemak aangehaald als “uitzonderingen”, omdat het uitzonderingen zijn op het op verbod.

Anders dan bij het verwerken van reguliere persoonsgegevens is het niet toegestaan om, in het geval een ander dan de betrokkene zelf de gegevens prijsgeeft, deze bijzondere

<sup>27</sup> Moerel & Prins 2016, p. 21 & 91.

<sup>28</sup> De auteur van de hiervoor genoemde literatuur betoogt dat dit tevergeefs zal zijn en pleit voor een andere werkwijze.

<sup>29</sup> Artikel 7, derde lid, van de Algemene Verordening Gegevensbescherming.

<sup>30</sup> Bijzondere categorieën van persoonsgegevens komen in de volgende paragraaf aan bod.

<sup>31</sup> Overweging 42 van de toelichting behorende bij de Algemene Verordening Gegevensbescherming.

gegevens te verwerken en vervolgens de derde hierover in te lichten.<sup>32</sup> De gegevens mogen niet worden verwerkt, tenzij sprake is van een hierna te bespreken uitzondering.

#### Verwerking op grond van toestemming

De verwerkingsverantwoordelijke mag na het verkrijgen van toestemming voor het verwerken van bijzondere persoonsgegevens deze gegevens verwerken.<sup>33</sup> Hier is wel één kanttekening bij te maken. In het lid staat vermeld dat bepaalde gegevens niet verwerkt mogen worden, in het geval het Unierecht of het lidstatelijke recht dit verbiedt. Deze toevoeging stond al in de Richtlijn, maar was niet opgenomen in de Wet bescherming persoonsgegevens.<sup>34</sup> De reden waarom deze toevoeging niet is opgenomen, is in de documenten van de parlementaire behandeling van het wetsvoorstel niet aan de orde gekomen.

#### Verwerking is noodzakelijk voor arbeids-, sociaalzekerheids- of socialebeschermingsrecht

Indien bij Unierecht, lidstatelijk recht of collectieve arbeidsovereenkomst hiervoor toestemming is gegeven, mag een verwerkingsverantwoordelijke voor de uitvoering van verplichtingen of de uitoefening van rechten met betrekking tot arbeids-, sociaalzekerheids- of socialebeschermingsrecht persoonsgegevens verwerken.

#### Verwerking is noodzakelijk voor de vitale belangen van een natuurlijk persoon

Verwerking van bijzondere categorieën persoonsgegevens is mogelijk, indien dit voor het vitale belang van de betrokkene of een ander natuurlijk persoon gebeurt.<sup>35</sup> In paragraaf 2.1.2 is besproken wat bedoeld wordt met een *vitaal belang*.

#### Verwerking door bepaalde organisaties zonder winstoogmerk in het kader van gerechtvaardigde activiteiten

Instanties/organisaties zoals kerken, politieke partijen of vakbonden mogen persoonsgegevens over zijn/haar (voormalige) leden verwerken. Het is niet toegestaan om persoonsgegevens die op deze grond zijn verwerkt buiten de organisatie te brengen.

#### Verwerking van persoonsgegevens die openbaar zijn gemaakt

Gegevens die door de betrokkene openbaar zijn gemaakt, mogen zonder toestemming verwerkt worden. Het gaat hier wel om gegevens die vrijwillig door de betrokkene openbaar zijn gemaakt met het doel deze persoonsgegevens te openbaren. Een persoon die in een rolstoel zit, openbaart een gezondheidsgegeven. Het is echter niet de bedoeling van deze persoon om deze gegevens te openbaren. Een persoon wiens telefoonnummer in het telefoonboek staat opgenomen, heeft hier echter wel voor gekozen. Hij heeft zijn telefoonnummer openbaar gemaakt. Ook de registratie van een rechtspersoon in het Handelsregister wordt gezien als openbaarmaking, ook al is deze openbaarmaking bij wet verplicht.<sup>36</sup>

#### Verwerking is noodzakelijk om redenen van zwaarwegend algemeen belang

Met “zwaarwegend algemeen belang” wordt bedoeld op:

1. *afwijken van het verbod op gebieden als volksgezondheid, de sociale bescherming, wetenschappelijk onderzoek en overheidsstatistieken;*
2. *verwerking door overheidsinstanties op grond van het constitutionele recht of;*
3. *bij volkenrecht vastgestelde doelstellingen ten behoeve van officieel erkende religieuze verenigingen;*

<sup>32</sup> Zie Bijlage 2.

<sup>33</sup> Artikel 9, tweede lid en onder a, van de Algemene Verordening Gegevensbescherming.

<sup>34</sup> Artikel 8, tweede lid en onder a, van de Richtlijn 95/46/EG; Artikel 23, eerste lid en onder a, van de Wet bescherming persoonsgegevens.

<sup>35</sup> Artikel 9, tweede lid en onder c, van de Algemene Verordening Gegevensbescherming.

<sup>36</sup> *Kamerstukken II 1997/98, 25892, 3, p. 123 e.v.*

4. *het verwerken van gegevens betreffende de politieke overtuigingen van personen door politieke partijen.*<sup>37</sup>

#### 2.1.6 Verwerking waarvoor identificatie niet is vereist

De verwerkingsverantwoordelijke heeft niet de verplichting om de gegevens aan te vullen als identificatie niet (meer) nodig is voor het te behalen doeleind. Ter verduidelijk is in het interview met de AP nagevraagd wat precies werd bedoeld met “een doeleinde waarvoor identificatie niet langer is vereist”.<sup>38</sup> De AP heeft aangegeven dat dit artikel momenteel intern nog niet was uitgewerkt, waardoor het niet mogelijk was om een antwoord te geven op de vraag. Voorbeelden waren ook niet voorhanden.

De in paragraaf 2.2 te bespreken rechten van de betrokkene vervallen in beginsel wanneer de verwerkingsverantwoordelijke kan aantonen dat hij de betrokkene niet langer kan identificeren. Indien mogelijk stelt de verwerkingsverantwoordelijke de betrokkene hiervan op de hoogte. De rechten van de betrokkene herleven als de betrokkene door het verlenen van aanvullende informatie het (zelf) weer mogelijk maakt om hem te identificeren mits hij de aanvullende informatie verleent met de bedoeling om een beroep te doen op deze rechten.

#### 2.1.7 Verwerking voor andere doeleinden

In beginsel mogen persoonsgegevens enkel worden verwerkt voor de doeleinden waarvoor ze zijn verzameld. Toch is het mogelijk om van dit beginsel af te wijken.<sup>39</sup> Gegevens mogen voor andere doeleinden worden verwerkt, indien toestemming is verkregen om gegevens te verwerken voor een ander doeleinde dan waarvoor de gegevens oorspronkelijk zijn verzameld. Dit kan ongeacht of deze andere doeleinden verenigbaar zijn met de oorspronkelijke doeleinden.<sup>40</sup>

De verwerkingsverantwoordelijke mag *zonder* toestemming persoonsgegevens verwerken voor andere doeleinden, indien deze doeleinden verenigbaar zijn met de oorspronkelijke doeleinden. Doeleinden zijn verenigbaar wanneer een verband bestaat tussen de doeleinden van de oorspronkelijke en de verdere verwerking. Zo is het mogelijk dat de persoonsgegevens die zijn verzameld met als doel “het uitvoeren van een overeenkomst” worden gebruikt om nieuwsbrieven te versturen betreffende deze overeenkomst. Hoewel de persoonsgegevens niet zijn verzameld met als doel het verstrekken van nieuwsbrieven, kan men wegens het nauwe verband tussen de twee doeleinden de gegevens toch gebruiken voor dit andere doeleinde. Bij de beantwoording of de doeleinden verenigbaar zijn, moet de verwerkingsverantwoordelijke ook rekening houden met een aantal situaties:

- a) de verwerkingsverantwoordelijke dient rekening te houden met de verhouding tussen de betrokkene en de verwerkingsverantwoordelijke;
- b) een verenigbaar doeleinde zal minder snel worden aangenomen, indien sprake is van bijzondere gegevens;
- c) rekening moet worden gehouden met de gevolgen van de verdere verwerking voor de betrokkene;
- d) de betrokkene moet in ieder geval geïnformeerd worden over deze andere doeleinden en zijn rechten.

## 2.2 De rechten van de betrokkene

Hoofdstuk III van de AVG bespreekt de rechten van de betrokkene. Veel van deze rechten waren al vastgelegd in de Richtlijn en de daarop gebaseerde Wbp. Deze rechten blijven grotendeels hetzelfde, maar worden hier en daar verscherpt. Ter volledigheid worden zowel de al bestaande rechten als de nieuwe rechten hieronder besproken.

<sup>37</sup> Overweging 33 t/m 35 van de Richtlijn 95/46/EG geeft enkele handvatten voor een definitie. In de toelichting van de AVG is geen verduidelijking opgenomen.

<sup>38</sup> Zie Bijlage 2.

<sup>39</sup> Artikel 6, vierde lid, van de Algemene Verordening Gegevensbescherming.

<sup>40</sup> Tweede alinea van overweging 50 van de toelichting behorende bij de Algemene Verordening Gegevensbescherming.

### 2.2.1 Algemene regels

Artikel 12 van het derde hoofdstuk definieert een aantal regels die van toepassing zijn op (een aantal van) de daarop volgende artikelen. Om onnodige herhaling te voorkomen wordt volstaan met de volgende hoofdregel: de onderstaande regels zijn van toepassing op de rechten opgenomen in artikel 13 tot en met 22 en artikel 34 van de AVG. Indien sprake is van een afwijking zal dit worden aangegeven bij de bespreking van het desbetreffende artikel.

De verwerkingsverantwoordelijke neemt passende maatregelen om ervoor te zorgen dat de betrokkene de verzochte informatie op een beknopte, transparante, begrijpelijke en in een gemakkelijke vorm ontvangt. De informatie wordt in begrijpelijke en duidelijke taal schriftelijk dan wel elektronisch verstrekt. Hij dient ervoor te zorgen dat een betrokkene zonder hinder een beroep kan doen op zijn rechten. De betrokkene dient wel zijn identiteit eerst te bewijzen alvorens hij een beroep kan doen op een van zijn rechten.<sup>41</sup>

Deze identificatieplicht zal vele organisaties aan het denken zetten, nu de verificatie ook online dient te kunnen gebeuren. In een eerdere versie van de AVG stond in de toelichting vermeld wat hiermee bedoeld zou kunnen worden.<sup>42</sup> Overweging 52 luidde namelijk als volgt.

"De voor de verwerking verantwoordelijke dient, met name met betrekking tot onlinediensten en online-identificatiemiddelen, alle redelijke maatregelen te nemen om de identiteit te controleren van een betrokkene die om toegang verzoekt. (...) **De identiteit van de betrokkene dient ook digitaal te worden vastgesteld, bijvoorbeeld aan de hand van dezelfde persoonlijke beveiligingsgegevens, die door de betrokkene worden gebruikt voor het aanmelden op de door de verwerker van de gegevens aangeboden onlinedienst.** Een voor de verwerking verantwoordelijke dient persoonsgegevens niet uitsluitend te bewaren om op eventuele verzoeken te kunnen reageren."

Het is nog onzeker hoe de wetgever wil dat de verificatie online gebeurt. Een methode die gebruikt kan worden voor telefonische verificatie is niet terug te vinden.

Het tweede lid gaat over het faciliteren van de rechten die een betrokkene kan invoeren. Indien identificatie van een betrokkene niet langer is vereist voor het te behalen doeleinde, zoals besproken in paragraaf 2.1.5, mag een organisatie een verzoek weigeren, tenzij de betrokkene zich weer identificeerbaar maakt. Verder dient de verwerkingsverantwoordelijke binnen een maand antwoord te geven op het verzoek van de betrokkene.<sup>43</sup> De termijn kan eenmaal met twee maanden worden verlengd, indien het gaat om een complex verzoek.<sup>44</sup> Besluit de verwerkingsverantwoordelijke om geen gehoor te geven aan het verzoek, dan dient hij dit zo spoedig mogelijk aan de betrokkene mede te delen. De betrokkene dient tevens ingelicht te worden over de mogelijkheid om beroep aan te tekenen tegen het besluit van de verwerkingsverantwoordelijke bij de rechter of dat de betrokkene het recht heeft om een klacht in te dienen bij de toezichthoudende autoriteit.<sup>45</sup>

Het verstrekken van de informatie dient in beginsel kosteloos te gebeuren.<sup>46</sup> Een uitzondering bestaat in het geval dat de betrokkene misbruik maakt van een van zijn rechten. Van misbruik kan sprake zijn indien de verzoeken van de betrokkene kennelijk ongegrond of

<sup>41</sup> Overweging 64 van de Algemene Verordening Gegevensbescherming. De overweging spreekt enkel over het vaststellen van de identiteit van de betrokkene, indien om inzage wordt verzocht. Nu bij de overgebleven rechten er meer wordt verzocht dan alleen inzage in de gegevens, is het logisch dat identificatie ook dient te gebeuren alvorens een beroep gedaan kan worden op deze rechten.

<sup>42</sup> COM/2012/11 final.

<sup>43</sup> Artikel 11, derde lid, van de Algemene Verordening Gegevensbescherming.

<sup>44</sup> Artikel 12, derde lid, van de Algemene Verordening Gegevensbescherming.

<sup>45</sup> Artikel 12, vierde lid, van de Algemene Verordening Gegevensbescherming.

<sup>46</sup> Artikel 12, vijfde lid, eerste volzin, van de Algemene Verordening Gegevensbescherming.

buitensporig zijn, met name wanneer de verzoeken herhaaldelijk worden ingediend.<sup>47</sup> Indien de verwerkingsverantwoordelijke misbruik constateert, kan hij op twee manieren reageren:

- a) een redelijke vergoeding rekenen voor de gemaakte kosten;
- b) weigeren gevolg te geven aan het verzoek.

Bij het weigeren van het verzoek dient een deugdelijke motivering toegevoegd te worden.<sup>48</sup>

Mocht de verwerkingsverantwoordelijke twijfelen aan de identiteit van de verzoekende persoon, dan heeft hij het recht om aanvullende informatie ter identificatie te vragen aan de verzoeker.

### 2.2.2 Het recht op informatie

Verwerkingsverantwoordelijken kunnen op meerdere manieren informatie over een persoon verkrijgen. De betrokkene kan zelf de informatie aan de verwerkingsverantwoordelijke overdragen of een derde verstrekt de informatie. Niet anders dan in de Wbp heeft de verwerkingsverantwoordelijke de plicht om de betrokkene over de verwerking te informeren.<sup>49</sup> Dit beginsel geldt zowel voor het geval dat de betrokkene zelf de informatie prijsgeeft als wanneer een derde dit doet.<sup>50</sup> In het geval dat de betrokkene al over de informatie beschikt, hoeft de verwerkingsverantwoordelijke niet nogmaals de betrokkene te informeren.<sup>51</sup> Het kan ook zo zijn dat de betrokkene al deels geïnformeerd is. De verwerkingsverantwoordelijke dient dan enkel de resterende informatie mede te delen.

Verwerkingsverantwoordelijken dienen te waarborgen dat in beide gevallen in ieder geval de volgende algemene gegevens worden verstrekt:

- a) de identiteit en contactgegevens van de verwerkingsverantwoordelijke;
- b) indien van toepassing, de contactgegevens van de functionaris voor gegevensbescherming;
- c) de rechtsgrond en de verwerkingsdoeleinden;
- d) indien de verwerking geschiedt op grond van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of een derde, wat de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of de derde zijn;
- e) indien van toepassing, wie nog meer de gegevens zal ontvangen;
- f) in het geval dat een derde de gegevens heeft verstrekt, dient ook te worden medegedeeld welke categorieën van persoonsgegevens worden verwerkt.<sup>52</sup>

Om het transparantiebeginsel te waarborgen dient de verwerkingsverantwoordelijke, tenzij de betrokkene al over deze informatie beschikt, aan de betrokkene ook te verstrekken de hieronder staande aanvullende informatie:

- a) de periode (termijn) gedurende welke de persoonsgegevens zullen worden opgeslagen;
- b) de rechten die de betrokkene heeft ten opzichte van de verwerkingsverantwoordelijke (inzage, wissen, rectificatie, beperkingen en, indien van toepassing, bezwaar);
- c) het recht om toestemming in te trekken, zonder dat dit afbreuk doet aan de rechtmatigheid van de verwerking voor de intrekking;
- d) het klachtrecht;
- e) of het verwerken van de gegevens noodzakelijk is om te voldoen aan een overeenkomst of andere wettelijke plicht en of de betrokkene deze gegevens moet verstrekken en wat de gevolgen zijn in het geval de betrokkene niet wil dat zijn gegevens worden verwerkt;
- f) indien de gegevens van een derde zijn ontvangen, moet worden medegedeeld wie deze derde is.<sup>53</sup>

Mocht de verwerkingsverantwoordelijke voornemens zijn om de persoonsgegevens van een betrokkene voor een ander doeleinde te verwerken dan waarvoor ze waren verzameld, dan

<sup>47</sup> Artikel 12, vijfde lid, tweede volzin, van de Algemene Verordening Gegevensbescherming.

<sup>48</sup> Artikel 12, vijfde lid, laatste volzin, van de Algemene Verordening Gegevensbescherming.

<sup>49</sup> Artikel 13, eerste lid, van de Algemene Verordening Gegevensbescherming.

<sup>50</sup> Artikel 14 van de Algemene Verordening Gegevensbescherming.

<sup>51</sup> Artikel 13, vierde lid, van de Algemene Verordening Gegevensbescherming.

<sup>52</sup> Artikel 14, eerste lid en onder d, van de Algemene Verordening Gegevensbescherming.

<sup>53</sup> Artikel 13, tweede lid, van de Algemene Verordening Gegevensbescherming.

dient hij dit voor die verdere verwerking mede te delen aan de betrokkene.<sup>54</sup> Ten overvloede wordt opgemerkt dat StiB geen gebruik maakt van geautomatiseerde besluitvorming. Deze bepalingen worden dan ook overgeslagen.

Wel is er een verschil omtrent het moment waarop de informatie moet worden verstrekt. Bij verkrijging van informatie van de betrokkene dient de verstrekking bij de verkrijging van de informatie te geschieden.<sup>55</sup> Als de informatie door een derde is geleverd, dient de betrokkene binnen een maand te worden geïnformeerd over de verwerking. Ook moet worden aangegeven of, en zo ja, wanneer, de gegevens voor communicatie met de betrokkene zullen worden gebruikt. Mochten de gegevens worden verstrekt aan een ander, dan moet dit ook worden medegedeeld voordat de gegevens worden verstrekt.<sup>56</sup>

Voor de informatieplicht bij gegevens die zijn ontvangen van een derde geldt nog het volgende: mocht het informeren van de betrokkene onmogelijk zijn of onevenredig veel inspanning vergen, dan kan dit achterwege worden gelaten. Dit kan mits de verwerkingsverantwoordelijke passende maatregelen neemt om de rechten, vrijheden en belangen van de betrokkene te waarborgen. Dit kan door middel van het openbaar maken van de te verstrekken informatie.<sup>57</sup>

### 2.2.2 Het recht op inzage

De betrokkene heeft recht op inzage in de gegevens die de verwerkingsverantwoordelijke verwerkt. Dit geldt alleen voor de gegevens die betrekking hebben op zijn persoon.<sup>58</sup> De verwerkingsverantwoordelijke verstrekt een kosteloze kopie van de informatie. De verwerkingsverantwoordelijke mag een redelijke vergoeding verzoeken, indien de betrokkene meerdere kopieën verzoekt.<sup>59</sup>

### 2.2.3 Recht op rectificatie

Het recht op rectificatie houdt in dat de betrokkene het recht heeft om onjuiste persoonsgegevens te actualiseren.<sup>60</sup>

### 2.2.4 Recht op vergetelheid

Het recht op vergetelheid is de codificatie van een uitspraak van het Hof.<sup>61</sup> In deze zaak gaf het Hof antwoord op een aantal vragen gesteld door een Spaanse rechter. De vragen kwamen naar aanleiding van een geschil tussen een Spaanse onderdaan en de zoekmachine Google Inc. De Spanjaard wilde dat Google een aantal referenties naar oude krantenartikelen zou verwijderen, omdat de Spanjaard van mening was dat de gegevens niet langer relevant waren en dat deze hem in een slecht daglicht zetten. Hij stelde dat zijn grondrechten werden geschonden.<sup>62</sup>

Het Hof oordeelde in het voordeel van de Spanjaard.<sup>63</sup> Zoekmachines dien(d)en in bepaalde gevallen referenties naar artikelen te verwijderen. Hierbij was van belang dat een belangenafweging werd gemaakt tussen de fundamentele rechten van de betrokkene, de rechten van de zoekmachine en die van het publiek. Aan de ene zijde had het publiek het recht om geïnformeerd te worden over bepaalde zaken. Aan de andere zijde speelde het privéleven van de betrokkene en het recht op privacy een rol. Het hof oordeelde dat in

<sup>54</sup> Artikel 13, derde lid, juncto artikel 14, vierde lid, van de Algemene Verordening Gegevensbescherming.

<sup>55</sup> Artikel 14, eerste lid, van de Algemene Verordening Gegevensbescherming.

<sup>56</sup> Artikel 14, derde lid, van de Algemene Verordening Gegevensbescherming.

<sup>57</sup> Artikel 14, vijfde lid en onder b, van de Algemene Verordening Gegevensbescherming.

<sup>58</sup> Artikel 15, eerste lid, van de Algemene Verordening Gegevensbescherming.

<sup>59</sup> Zie overweging 61 en 62 van de toelichting behorende bij de Algemene Verordening Gegevensbescherming.

<sup>60</sup> Artikel 16 van de Algemene Verordening Gegevensbescherming.

<sup>61</sup> HvJ EU 13 mei 2014, ECLI:EU:C:2014:317.

<sup>62</sup> In casu waren artikel 7 en 8 van het Handvest van belang.

<sup>63</sup> Zie overweging 97 van de aangehaalde uitspraak.

beginsel het recht op privacy voor het recht van informatie (van zowel de zoekmachine als het publiek) en het economische belang van de zoekmachine gaat. Alleen in gevallen waar de belangen van het publiek zwaarder wegen, mag een zoekmachine het verzoek weigeren. Het Hof geeft als voorbeeld: de betrokkene die in het openbare leven een bepaalde rol speelt waarover het publiek moet worden geïnformeerd.<sup>64</sup>

Het recht op vergetelheid is in een algemenere vorm terug te vinden in de AVG. Het artikel is niet alleen van toepassing op zoekmachines, maar ook op iedere organisatie die gegevens verwerkt.<sup>65</sup> Betrokkenen kunnen een verzoek tot gegevenswissing indienen, indien:

- a) de persoonsgegevens niet langer nodig zijn om de doeleinden te verwezenlijken, of;
- b) de betrokkene toestemming heeft verleend overeenkomstig artikel 6, eerste lid onder a, en artikel 9, tweede lid en onder a, van de AVG en deze intrekt.

Mocht het zo zijn dat gegevens zijn gedeeld met andere organisaties, dan moeten deze organisaties worden ingelicht over het feit dat de gegevens verwijderd dienen te worden.

Een organisatie kan het verzoek weigeren, indien het recht op vrijheid van meningsuiting en informatie prevaleert. Zo zal een organisatie geen gegevens hoeven te verwijderen, waaruit is op te maken dat een betrokkene diefstal heeft gepleegd tijdens het uitvoeren van zijn vrijwilligerstaken. In dit geval zal het recht op informatie zwaarder wegen, omdat de organisatie anders niet kan voorkomen dat dezelfde persoon op een later tijdstip zich nogmaals probeert te registreren als een vrijwilliger.<sup>66</sup>

### 2.2.5 Recht op beperking van verwerking

De betrokkene kan het verwerken van gegevens door de verwerkingsverantwoordelijke beperken. Hiermee wordt bedoeld dat de betrokkene van de verwerkingsverantwoordelijke kan verlangen, dat zijn gegevens (bijvoorbeeld) niet worden aangepast of verwijderd.<sup>67</sup> Het recht kan worden ingeroepen, indien de betrokkene van mening is dat:

- 1) de gegevens onjuist zijn en moeten worden gecorrigeerd;
- 2) de gegevens onrechtmatig worden verwerkt en de betrokkene niet wil dat de gegevens worden verwijderd;
- 3) de betrokkene heeft de gegevens nodig voor de instelling, uitoefening of onderbouwing van een rechtsvordering en de verwerkingsverantwoordelijke heeft de persoonsgegevens niet meer nodig;
- 4) de gerechtvaardigde gronden van de verwerkingsverantwoordelijke minder zwaar wegen dan die van hemzelf en hij daar bezwaar tegen heeft gemaakt.

### 2.2.6 Recht op overdraagbaarheid van gegevens

Het recht van overdraagbaarheid houdt in dat een betrokkene het recht heeft om zijn gegeven in een gestructureerde, gangbare en machineleesbare vorm te verkrijgen en het recht heeft deze over te dragen.<sup>68</sup> Dit recht bestaat alleen als de betrokkene toestemming heeft gegeven voor de verwerking van zijn persoonsgegevens. Een betrokkene kan zijn persoonsgegevens opvragen, zodat deze overgedragen kunnen worden aan een andere verwerkingsverantwoordelijke. Dit recht is meer van belang voor gebruikers van social media websites, zoals Facebook.<sup>69</sup> Wel kan bedacht worden dat een cliënt zijn gegevens wil opvragen, om deze vervolgens over te dragen aan een andere organisatie die zich bezighoudt met de zorg.

<sup>64</sup> Zie overweging 99 van de aangehaalde uitspraak.

<sup>65</sup> Artikel 17, eerste lid, van de Algemene Verordening Gegevensbescherming.

<sup>66</sup> Artikel 17, derde lid en onder a, van de Algemene Verordening Gegevensbescherming.

<sup>67</sup> Artikel 18, eerste en tweede lid, van de Algemene Verordening Gegevensbescherming.

<sup>68</sup> Artikel 20, eerste lid, van de Algemene Verordening Gegevensbescherming.

<sup>69</sup> Sloot, van der, TvC 2012, p. 254.

### 2.2.7 Recht van bezwaar

Indien verwerking op grond van de e- of f-grond geschiedt, heeft de betrokkene het recht van bezwaar.<sup>70</sup> De betrokkene heeft dan het recht om bezwaar te maken tegen de verwerking van zijn persoonsgegevens. De verwerkingsverantwoordelijke dient een beslissing te nemen op het bezwaar. Indien de verwerkingsverantwoordelijke het bezwaar gegrond verklaart, staakt hij het verwerken van de gegevens.

### 2.2.8 Weigering en rechtsbescherming

De verwerkingsverantwoordelijke kan het verzoek van de betrokkene weigeren. Het besluit dient gemotiveerd aan te geven waarom de verwerkingsverantwoordelijke het verzoek weigert. Het besluit dient binnen één maand na ontvangst van het verzoek genomen te worden.<sup>71</sup>

De verwerkingsverantwoordelijke moet de betrokkene informeren over de mogelijkheid om een klacht in te dienen bij de Autoriteit Persoonsgegevens of om beroep in te stellen bij de rechtbank.<sup>72</sup>

De rechten van de betrokkene kunnen wel beperkt worden. Beperking is mogelijk in het geval sprake is van de bescherming van de rechten en vrijheden van anderen. In de memorie van toelichting wordt aangegeven, dat de verwerkingsverantwoordelijke van te voren een belangenafweging moet maken.<sup>73</sup> De Nederlandse wetgever dient eerst deze beperking te creëren door middel van een wettelijke bepaling. Zo moet aangegeven worden welke rechten worden beperkt en in *hoeveer* de rechten dan wel *wanneer* deze rechten beperkt mogen worden.<sup>74</sup>

## 2.3 Plichten van de verwerkingsverantwoordelijke

In paragraaf 2.2 zijn de rechten van de betrokkene besproken. De verwerkingsverantwoordelijke heeft de plicht om ervoor te zorgen dat de betrokkene een beroep kan doen op zijn rechten of dat deze worden gewaarborgd. De verwerkingsverantwoordelijke heeft nog een aantal andere plichten. Deze plichten gaan vooral over de verwerking van de gegevens in het algemeen. De meeste van deze plichten vallen buiten de scope van dit onderzoek. Deze plichten gaan vooral over zaken zoals de beveiliging van de gegevens of het wel of niet aanstellen van een functionaris voor gegevensbescherming. Deze plichten hebben geen directe invloed op de omgang met de cliënten.

Wel is ervoor gekozen om de plichten die een nauw verband hebben met de rechten van de betrokkene uit te werken. Dit zijn de meldplicht datalekken en het pseudonimiseren van persoonsgegevens. De eerste plicht gaat namelijk over het informeren van de betrokkene, indien een datalek is ontstaan. De plicht tot het pseudonimiseren van persoonsgegevens zal vooral van belang zijn, indien een betrokkene een beroep doet op zijn recht op inzage. Daarbij wordt van de verwerkingsverantwoordelijke verwacht dat er een beleid omtrent het pseudonimiseren van gegevens wordt opgesteld.<sup>75</sup>

### 2.3.1 Datalekken

Sinds 1 januari 2016 is de Wet meldplicht datalekken in werking getreden. Deze wet heeft artikel 34a toegevoegd aan de Wbp. Dit artikel is gebaseerd op (een oudere versie van) artikel 33 van de AVG. Een datalek is een inbreuk op de beveiliging van

<sup>70</sup> Zie paragraaf 2.1.3.

<sup>71</sup> Artikel 12, vierde lid, van de Algemene Verordening Gegevensbescherming.

<sup>72</sup> Artikel 77 juncto 79 van de Algemene Verordening Gegevensbescherming.

<sup>73</sup> *Kamerstukken II* 1997/98, 25892, 3, p. 176.

<sup>74</sup> Artikel 23, eerste lid, aanhef en sub i, van de Algemene Verordening Gegevensbescherming.

<sup>75</sup> Overweging 78 van de toelichting behorende bij de Algemene Verordening Gegevensbescherming.

persoonsgegevens.<sup>76</sup> Een datalek kan zowel virtueel als fysiek zijn. Er is sprake van een datalek op het moment dat er persoonsgegevens onbedoeld vrijkomen of niet kan worden uitgesloten dat deze onrechtmatig zijn verwerkt.<sup>77</sup>

Organisaties (die in Nederland zijn gevestigd) zijn op grond van de AVG verplicht om onverwijld en binnen 72 uur nadat de inbreuk is waargenomen melding te doen bij de AP over de inbreuk. De verwerkingsverantwoordelijke hoeft geen melding te doen, indien het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Indien de melding niet binnen 72 uur plaatsvindt, moet de organisatie een motivering voor de vertraging toevoegen. De melding dient de volgende gegevens te bevatten:

- 1) de aard van de inbreuk en (indien mogelijk) het aantal betrokkenen dat door de inbreuk wordt geraakt;
- 2) de naam en contactgegevens van de functionaris voor gegevensbescherming;
- 3) de waarschijnlijke gevolgen van de inbreuk;
- 4) de maatregelen die zijn voorgesteld c.q. genomen om de inbreuk aan te pakken en/of de nadelige gevolgen ervan te beperken.<sup>78</sup>

De verwerkingsverantwoordelijke documenteert alle inbreuken in verband met persoonsgegevens, met inbegrip van de soort inbreuk, de gevolgen van de inbreuk en de genomen maatregelen.<sup>79</sup>

Naast de melding bij de AP dient de organisatie ook de betrokkene(n) te informeren. De melding hoeft alleen in het geval de inbreuk een hoog risico inhoudt voor de rechten en vrijheden van de betrokkene te worden gedaan.<sup>80</sup> Dezelfde gegevens als bij de melding aan de AP dienen te worden vermeld.<sup>81</sup> In het geval dat de verwerkingsverantwoordelijke ervoor heeft gezorgd dat de gegevens onbegrijpelijk zijn voor derden (zie hierna paragraaf 2.3.2), dan hoeft deze melding niet te gebeuren. Ditzelfde geldt als de melding onevenredig veel inspanningen zou vergen of als de verwerkingsverantwoordelijke achteraf maatregelen heeft getroffen om de gegevens onbegrijpelijk te maken, zodat een toekomstige inbreuk geen groot risico voor de rechten en vrijheden van de betrokkene met zich meedraagt.<sup>82</sup>

Ten overvloede wordt opgemerkt dat de bepaling onder b in het derde lid van artikel 34 AVG tegenstrijdig lijkt ten opzichte van het doel van het gehele artikel. De aanhef van dit lid stelt dat maar aan één van de voorwaarden moet zijn voldaan. Dit zou inhouden dat, indien er een inbreuk is geconstateerd, dit niet gemeld hoeft te worden aan de betrokkene wanneer de verwerkingsverantwoordelijke ervoor heeft gezorgd dat het “waarschijnlijk” niet nogmaals kan gebeuren. De overige twee leden vereisen echter dat de gegevens van tevoren goed beveiligd zijn of dat de betrokkene op een alternatieve wijze wordt geïnformeerd.

### 2.3.2 Pseudonimiseren van gegevens

Een nieuw begrip en plicht voor de verwerkingsverantwoordelijke is het pseudonimiseren van persoonsgegevens. In een brief aan de voorzitter van de Eerste Kamer legt de minister van Veiligheid en Justitie uit wat wordt verstaan onder pseudonimiseren.<sup>83</sup> Kort samengevat houdt het pseudonimiseren het volgende in:

Het pseudonimiseren van gegevens houdt in dat bepaalde informatie, zoals de naam en achternaam van een persoon, wordt vervangen door een willekeurige letter of

<sup>76</sup> Artikel 34a, eerste lid, juncto artikel 13, eerste lid, van de Wet bescherming persoonsgegevens.

<sup>77</sup> 'Meldplicht Datalekken', *Autoriteit Persoonsgegevens*, [autoriteitpersoonsgegevens.nl](http://autoriteitpersoonsgegevens.nl).

<sup>78</sup> Artikel 33, derde lid, juncto artikel 4, twaalfde lid, van de Algemene Verordening Gegevensbescherming.

<sup>79</sup> Artikel 33, vijfde lid, van de Algemene Verordening Gegevensbescherming.

<sup>80</sup> Artikel 34, eerste lid, van de Algemene Verordening Gegevensbescherming.

<sup>81</sup> Artikel 34, tweede lid, van de Algemene Verordening Gegevensbescherming.

<sup>82</sup> Artikel 34, derde lid, van de Algemene Verordening Gegevensbescherming.

<sup>83</sup> *Kamerstukken I 2015/2016*, 33169, AF, p. 1.

lettercombinatie of getal. Deze combinatie wordt gezien als “sleutel”. Hiermee wordt bedoeld dat degene die weet wat de sleutel is, de gegevens kan lezen.

Wel bestaat de mogelijkheid dat gepseudonimiseerde gegevens tezamen met niet-gepseudonimiseerde gegevens een persoon identificeerbaar maken. Om die reden zijn gepseudonimiseerde gegevens nog wel persoonsgegevens in de zin van de verordening.<sup>84</sup> Alleen als deze gegevens geheel onherleidbaar worden gemaakt, zal de verordening niet langer van toepassing zijn. Dit laatste is het anonimiseren van gegevens.

---

<sup>84</sup> Overweging 26 van de toelichting behorende bij de Algemene Verordening Gegevensbescherming.

## Hoofdstuk 3 - Privacy op de werkvloer

---

In dit hoofdstuk worden de gegevens besproken die zijn verzameld door middel van het onderzoek naar de praktijk. In paragraaf 3.1 worden de eerste twee interviews besproken. Paragraaf 3.2 gaat in op de survey. Paragraaf 3.3 bespreekt de gedane observaties. Ten slotte wordt in paragraaf 3.4 de tweede ronde interviews besproken. Een verslag van de interviews is te vinden in de bijlage.<sup>85</sup>

### 3.1 Eerste ronde interviews

Op 20 augustus 2016 zijn twee interviews gehouden om informatie te verzamelen over de algemene gang van zaken binnen de organisatie met betrekking tot privacy. De geïnterviewde medewerkers zijn mevrouw Bakx en mevrouw Van der Stoel. Mevrouw Bakx is werkzaam op het secretariaat. Zij werkt daar voornamelijk met het gegevensverwerkingsysteem “CVRS”. Mevrouw Van der Stoel is werkzaam als coördinator mantelzorgondersteuning. Daarbij vervult mevrouw Van der Stoel ook de (onofficiële) rol van functionaris gegevensbescherming en is bekend met het privacybeleid van StiB.

#### 3.1.1 Doel van de interviews

Met mevrouw Van der Stoel is een open interview gehouden. Het doel van dit interview was het schetsen van een algemeen beeld over de wijze waarop StiB naar de belevenis van mevrouw Van der Stoel omging met het beleid. De focus ligt op handelingswijzen die wellicht in strijd zijn met de regelgeving

Mevrouw Bakx heeft twee vragen beantwoord. Deze vragen gaan over de beveiliging van het systeem (wie kan wat inzien) en welke persoonsgegevens StiB verwerkt.

#### 3.1.2 Bevindingen uit het interview met mevrouw Van der Stoel

De organisaties binnen Zorg voor elkaar Breda delen bijzondere persoonsgegevens met andere organisaties binnen en buiten Zorg voor elkaar Breda. Dit gebeurt wanneer de organisatie van mening is dat een andere organisatie de cliënt kan helpen. Het gevolg hiervan is dat een (voor de betrokkene) onbekende organisatie beschikt over gevoelige gegevens van de betrokkene.

Dit is volgens mevrouw Van der Stoel niet anders bij StiB. De gegevens worden direct verwerkt door de medewerkers van StiB. Men staat op dat moment niet stil bij het privacyprotocol. Mevrouw Van der Stoel ziet graag dat andere medewerkers hierbij stil staan, zodat ze een weloverwogen besluit kunnen nemen alvorens de persoonsgegevens te verwerken.

#### 3.1.3 Bevindingen uit het interview met mevrouw Bakx

StiB verwerkt primair NAW-gegevens en in bepaalde gevallen bijzondere persoonsgegevens betreffende de gezondheid van de cliënt. De bijzondere gegevens hebben vooral betrekking op de beperkingen of aandoeningen waar een hulpvrager mee kampt.

Wel wordt opgemerkt dat het momenteel ook mogelijk is om een bankrekeningnummer en een BSN-nummer te verwerken. Het bankrekeningnummer wordt alleen bij vrijwilligers die een onkostenvergoeding krijgen ingevuld, maar het veld staat bij iedere cliënt open. Naar het BSN-nummer wordt wel gevraagd.

Op dit moment kunnen alle medewerkers de persoonsgegevens van iedere cliënt inzien. Mevrouw Bakx geeft aan dat bij het ontwerp van het nieuwe systeem wel is verzocht om de mogelijkheid om gebruikers bepaalde rechten toe te wijzen. Dit is echter nog niet geïmplementeerd.

---

<sup>85</sup> Zie Bijlage 3.

## 3.2 De survey

### 3.2.1 Doel

De medewerkers werken sinds begin 2016 met het huidige beleid. Uit het interview met mevrouw Van der Stoel is gebleken dat niet iedere medewerker werkt volgens het beleid. Om erachter te komen hoe bekend de werknemers zijn met het beleid en of ze deze correct toepassen, is in samenwerking met de afdeling Communicatie een survey opgesteld voor de medewerkers. De medewerkers hebben tweeënhalve week de tijd gekregen om de survey anoniem in te vullen. Uiteindelijk hebben twaalf van de ongeveer twintig medewerkers gereageerd. Twee van de twaalf medewerkers hebben aangegeven niet met cliënten te werken, waardoor zij de survey verder niet in konden vullen. Er zijn aparte vragen opgesteld voor zowel degenen die bekend zijn met het beleid als degenen die dat niet zijn.<sup>86</sup>

De vragen die zijn gesteld aan degenen die bekend zijn met het beleid gaan voornamelijk over de kennis van de medewerker over het beleid. Hierbij wordt nagegaan of de medewerker het beleid correct kan toepassen. De vragen die zijn gesteld aan de werknemers die onbekend zijn met het beleid gaan voornamelijk over de reden waarom de medewerkers onbekend zijn met het beleid.

Het uiteindelijke doel is om deze gegevens te bestuderen en om het volgende te achterhalen:

1. zijn de medewerkers in staat om het beleid correct toe te passen;
2. zien de medewerkers onduidelijkheden in het beleid;
3. wat is volgens de medewerkers juist wel duidelijk;
4. wat kan StiB volgens de medewerkers doen om het beleid te laten "leven" in de organisatie.

### 3.2.2 Bevindingen

In deze paragraaf wordt een onderscheid gemaakt tussen de medewerkers die bekend waren met het beleid en degenen die dat niet waren.

#### *Bekend met het beleid*

---

Zes van de tien respondenten hebben aangegeven bekend te zijn met het huidige privacybeleid van Zorg voor elkaar Breda. Vijf van de zes respondenten waren van mening dat het privacyprotocol begrijpelijk was en dat de "checklist informatie delen zonder toestemming cliënt" simpel toe te passen was. Een van deze vijf respondenten gaf wel aan dat het inkorten en duidelijker maken van bepaalde passages uit het de checklist wenselijk was.

De zesde respondent gaf aan dat het privacyprotocol eruit zag als een "boekwerk". Hierdoor was de respondent eerder geneigd om een privacy gerelateerde vraag te stellen aan een collega dan zelf het protocol door te nemen en toe te passen.

De respondenten hebben aangegeven vaak gebruik te maken van elkaars kennis. Wanneer ze iets niet weten, dan zoeken ze een collega op om de casus te bespreken. Wel wordt er aangegeven dat ze graag zien dat het beleid wat vaker met het gehele team wordt besproken. Hierdoor kunnen de respondenten andere werknemers op de hoogte stellen van de casus of kunnen zij gezamenlijk de casus bespreken.

Uit de survey is gebleken dat niet iedere respondent in staat was de inhoudelijke vragen correct te beantwoorden. Zo waren de respondenten niet in staat om aan te geven welke twee doeleinden in het beleid staan opgenomen. De meeste respondenten gaven wel correct

---

<sup>86</sup> Zie Bijlage 4.

aan dat persoonsgegevens worden verwerkt ter bevordering van het verlenen van hulp. Het tweede doeleinde werd echter door geen enkele respondent opgenoemd.

De respondenten gaven ieder het gewenste antwoord op de vraag hoe ze te werk gaan bij het verwerken van persoonsgegevens. De respondenten voldoen aan de informatieplicht zoals opgenomen in artikel 8 van het privacyprotocol.

Bij de daarop volgende vragen varieerden de antwoorden aanzienlijk. Maar één van de respondenten gaf aan dat in de situatie waarbij een derde persoonsgegevens van een (mogelijke) cliënt verstrekt, de herkomst moet worden genoteerd.<sup>87</sup> Alleen deze respondent was tevens in staat om artikel 8 van het privacyprotocol toe te passen, al hoewel dit artikel niet expliciet wordt aangegeven in artikel 5 van het privacyprotocol.

Ook bij de vraag betreffende het delen van gegevens gaf maar één respondent aan gebruik te maken van de checklist "informatie delen zonder toestemming cliënt". De meeste respondenten gaven aan altijd bij een collega na te vragen of iets wel of niet gedeeld mag worden. Twee van de respondenten maakten een onderscheid tussen de cliënten die wel of juist geen toestemming hadden gegeven voor het delen van gegevens.<sup>88</sup> De titel van de checklist zou mogelijk ook voor onduidelijkheden zorgen. Uit de titel kan worden afgeleid dat de checklist alleen bespreekt wat men dient te doen als ze informatie willen delen zonder toestemming van de cliënt, terwijl de checklist de situatie waarbij wel toestemming wordt gegeven ook bespreekt. De gestelde vraag was zo geformuleerd dat het wel of niet gegeven van toestemming open was gelaten.

Een van de respondenten vindt verder dat het beleid te vaak praat over "hulpverleners". De respondent is van mening dat de medewerkers van StiB geen hulpverleners zijn.

### *Onbekend met het beleid*

---

De overige vier respondenten geven aan niet bekend te zijn met het privacyprotocol. Volgens de respondenten was de oorzaak hiervoor de gebrekkige inlichting over het bestaan van het privacyprotocol.

De vragen betreffende de leesbaarheid, bruikbaarheid en mogelijke verbeteringen van het privacyprotocol zijn door geen van de respondenten verder ingevuld. Volgens de respondenten was het beleid te uitgebreid om op het moment van het invullen van de survey door te nemen. Deze opmerking zal bij de beoordeling van het beleid worden meegenomen. Hieruit zou kunnen blijken dat het protocol niet gemakkelijk te raadplegen is.

## 3.3 Observaties

### 3.3.1 Doel

De gegevens verzameld door middel van de survey bleken onvoldoende te zijn om een duidelijk beeld te schetsen van de praktijksituatie bij StiB. Om die reden is besloten om een aantal medewerkers te observeren en om naar aanleiding hiervan interviews af te nemen.

De onderzoeker heeft besloten om op de achtergrond te blijven tijdens de observaties. Er is dus geen sprake geweest van een meeloopdag. De belangrijkste reden hiervoor betreft de vertrouwensrelatie tussen de cliënt en de coördinator. De cliënten bespreken vaak persoonlijke gebeurtenissen met de coördinatoren. Het zou zowel de cliënt als de coördinator geen goed doen als daar een derde bij plaats zou nemen. Ook zou de duidelijke aanwezigheid van de onderzoeker averechts kunnen werken. Het is de bedoeling dat wordt

---

<sup>87</sup> Conform artikel 5 van het privacyprotocol.

<sup>88</sup> Hierbij dient opgemerkt te worden dat niet expliciet is gevraagd of men een onderscheid kon maken tussen de twee groepen. Wel kan van een medewerker die meent bekend te zijn met het beleid worden verwacht dat hij zelf dit onderscheid maakt.

onderzocht hoe men het privacyprotocol toepast in de praktijk zonder dat iemand hierop aan het letten is.

De observaties hebben twee dagen in beslag genomen. Het observeren voor een langere tijd zou inefficiënt zijn en weinig toegevoegde waarde hebben. De coördinatoren hebben maar een beperkt aantal taken waar de onderzoeker bij aanwezig kan zijn en waar privacy een rol speelt.

Opgemerkt wordt dat geen observatie heeft plaatsgevonden bij het secretariaat. De reden hiervoor is dat twee van de medewerkers van het secretariaat ook werkzaam zijn op de afdeling mantelzorgwaardering.

### 3.3.2 Bevindingen

Tijdens de observaties is vooral gelet op de informatieplicht van de medewerker en de momenten waarop (nieuwe) persoonsgegevens worden verwerkt. Op 18 november 2016 is geobserveerd bij de afdeling Mantelzorgwaardering. Het interview met mevrouw Buijnsters is op diezelfde dag afgenomen. Op zowel 25 november 2016 als 1 december 2016 zijn de overige medewerkers geobserveerd. De interviews met de coördinatoren en de projectleidster van de mantelzorgwaardering zijn afgenomen op 6 december 2016.

#### De mantelzorgwaardering

Tijdens de observatie is gebleken dat de afdeling Mantelzorgwaardering persoonsgegevens verwerkt van zowel de mantelzorger die een waardering aanvraagt als van de persoon die door de mantelzorger wordt verzorgd. Aan de mantelzorger\* werd gevraagd of zijn gegevens mochten worden genoteerd. Voor het verwerken van de persoonsgegevens van de verzorgde/hulpvrager werd geen uitdrukkelijke toestemming gevraagd.

\*Ervan uitgaande dat de mantelzorger degene is die belde.

#### De coördinatoren

Op 1 december 2016 werd door een van de coördinatoren een nieuwe medewerker ingewerkt. Tijdens het inwerktraject werd niet stilgestaan bij het onderwerp privacy. Ook de overige coördinatoren bespraken het privacyprotocol niet. Voor de coördinatoren waren geen hulpmiddelen beschikbaar die gedurende de werkzaamheden geraadpleegd konden worden, indien een privacy gerelateerde vraag werd gesteld.

Een van de coördinator gaf aan dat pas sinds kort de overeenkomsten ondertekend moeten worden.<sup>89</sup> Ook gaven de coördinatoren aan niet stil te staan bij het protocol tijdens de gesprekken met cliënten.

## 3.4 De tweede ronde interviews

De vragen die voor het interview zijn opgesteld gaan vooral over de leesbaarheid en duidelijkheid van het protocol en de wijze waarop de medewerkers in aanraking komen met het protocol.

### 3.4.1 Doel

Uit de observaties schijnt dat de afdeling Mantelzorgwaardering bijzondere persoonsgegevens verwerkt zonder hiervoor toestemming te vragen. Door middel van een interview wordt geprobeerd om te achterhalen of dit werkelijk zo is. Bij de coördinatoren staat het inwerkproces van de medewerkers centraal. De onderzoeker probeert te achterhalen of het inwerkproces wellicht een oorzaak is voor de geringe kennis over het privacyprotocol

---

<sup>89</sup> StiB heeft tijdens het onderzoek het een en ander veranderd aan haar overeenkomsten. Dit is gedaan naar aanleiding van dit onderzoek.

onder de medewerkers. Daarnaast zijn enkele vragen gesteld over de inhoud van het privacyprotocol.

### 3.4.2 Bevindingen

De mantelzorgwaardering verwerkt zowel reguliere als bijzondere persoonsgegevens van zowel de mantelzorger als de hulpvrager. Er wordt geen rekening gehouden met de situatie dat de beller zonder toestemming van de derde partij gegevens ter verwerking prijsgeeft. De gegevens worden niet alleen gebruikt voor het verstrekken van de mantelzorgwaardering. De persoonsgegevens worden verwerkt in het CVRS-systeem. De coördinatoren gebruiken deze persoonsgegevens om contact te leggen met de mantelzorger. Dit wordt alleen gedaan als de mantelzorger aangeeft hier behoefte aan te hebben. Er wordt van te voren echter geen uitdrukkelijke toestemming gevraagd.

Het is volgens de afdeling Mantelzorgwaardering niet noodzakelijk om de persoonsgegevens van de hulpvrager te verwerken. Dit wordt vooral gedaan ter controle en om misbruik te voorkomen. Als uiteindelijk blijkt dat de huidige manier van werken niet is toegestaan, dan zal er wel een nieuwe manier bedacht moeten worden.

De medewerkers geven aan dat ze tijdens het inwerktraject niet zijn voorgelicht over het privacyprotocol. Daarnaast zijn ze van mening dat het protocol oninteressant overkomt, waardoor geen initiatief is genomen om het protocol zelf door te nemen. Het protocol komt stoffig en saai over. Dit komt voornamelijk door de hoeveelheid tekst in het protocol. De medewerkers zien liever een schema dat of flowchart die op een korte en begrijpelijke manier aangeeft wat iedere medewerkers moet weten.

Ten slotte waren geen van de geïnterviewden in staat om aan te geven wat volgens het privacyprotocol de twee verwerkingsdoeleinden van StiB waren.

## Hoofdstuk 4 Het beleid van StiB en de Algemene Verordening Gegevensbescherming

---

In dit hoofdstuk wordt het huidige beleid van StiB getoetst aan de AVG. Het beleid wordt in het geheel getoetst.

### 4.1 Inleiding

Tijdens de toetsing van het beleid is gebleken dat de schrijfster van het protocol alle organisaties binnen Zorg voor elkaar Breda als hulpverleningsinstantie heeft gedefinieerd. Het is het niet mogelijk geweest om te achterhalen waarom hiervoor is gekozen. Alvorens het beleid te toetsen wordt eerst gekeken of deze definitie van toepassing is op StiB.

#### 4.1.1 Is StiB een hulpverleningsinstantie?

Het protocol geeft niet aan wat wordt verstaan onder "hulpverleningsinstanties" of "hulpverleners". De definities van deze begrippen zijn echter wel van belang, omdat deze instanties c.q. personen op grond van de wet een aantal rechten en plichten krijgen. Zo mag een hulpverleningsinstantie bijzondere gegevens verwerken ter bevordering van de zorg zonder hiervoor toestemming te hebben gekregen.<sup>90</sup> De term hulpverlener komt alleen voor in de Jeugdwet.<sup>91</sup> In die context is een hulpverlener een natuurlijke persoon die beroepsmatig jeugdhulp verleent. Kort weergegeven wordt onder jeugdhulp verstaan:

- 1) *ondersteuning van en hulp en zorg, niet zijnde preventie, aan jeugdigen en hun ouders <> opvoedingsproblemen van de ouders of adoptiegerelateerde problemen;*
- 2) *het bevorderen van de deelname aan het maatschappelijk verkeer en van het zelfstandig functioneren van jeugdigen met een <> beperking, en*
- 3) *het ondersteunen bij of het overnemen van activiteiten op het gebied van de persoonlijke verzorging.*

Kijkende naar de maatschappelijke dienst die StiB verricht en door eenzelfde definitie van hulpverlener toe te passen, kan niet direct gezegd worden dat zij als hulpverleningsorganisatie aangemerkt kan worden. StiB ondersteunt primair degene die informele zorg biedt. Deze ondersteuning kan niet worden gezien als zorg, aangezien de mantelzorger zelf niets mankeert noch wordt de mantelzorger "verzorgt". Daarbij wordt de ondersteuning niet *beroepsmatig* verleend. Toch zou men kunnen stellen dat StiB een hulpverleningsinstantie is, omdat zij vrijwilligers plaatst bij hulpvragers en op die manier ondersteuning c.q. hulp biedt. Ook hier kan gesteld worden dat de vrijwilligers de cliënten niet verzorgen noch dit beroepsmatig doen. Het verzorgen van de hulpvragers namens StiB is contractueel uitgesloten.

Vervolgens is gekeken of de Wbp wellicht een aansluitingspunt biedt voor het begrip "hulpverlener". Artikel 21, eerste lid en sub a, van de Wbp is van toepassing in de gevallen dat een hulpverlener bijzondere gegevens verwerkt voor zover dit met het oog op de goede *behandeling of verzorging* van de betrokkene gebeurt. Alhoewel dit geen concrete definitie is, kan niet gezegd worden dat StiB zonder twijfel een beroep kan doen op dit artikel. De cliënten van StiB worden namelijk niet door haar medewerkers verzorgd noch is er sprake van een behandeling.

Met het bovenstaande in acht genomen wordt tijdens de toetsing van het beleid aan de AVG ervan uitgegaan dat StiB *geen* hulpverleningsinstantie is. Dit betekent echter niet dat StiB niet alsnog als hulpverleningsinstantie kan worden aangemerkt. Momenteel is er geen concreet aanknopingspunt dat hiertoe de mogelijkheid geeft. Indien StiB op een later moment wel als hulpverleningsinstantie aangemerkt kan worden, dan heeft dit geen nadelige gevolgen voor de manier waarop StiB persoonsgegevens op dat moment zou verwerken. De

---

<sup>90</sup> Artikel 21, eerste lid en sub a, van de Wet bescherming persoonsgegevens.

<sup>91</sup> Artikel 1.1 van de Jeugdwet.

regels voor normale organisaties zijn namelijk strenger dan de regels voor een hulpverleningsorganisatie.

## 4.2 Het toetsingskader voor rechtmatige gegevensverwerking

In paragraaf 2.1 zijn de beginselen voor het rechtmatig verwerken van persoonsgegevens uiteengezet en is uitgelegd wat de bijbehorende artikelen inhouden.

### 4.2.1 Beginselen inzake het verwerken van persoonsgegevens

#### Rechtmatige, behoorlijke en transparante verwerking

Volgens het eerste beginsel inzake het verwerken van persoonsgegevens dient verwerking transparant te gebeuren. Uit de artikelen 2 tot en met 8 van het privacyprotocol is op te maken dat dit beginsel wordt gewaarborgd. De medewerkers van StiB zijn belast met de taak om de cliënten te informeren over het verwerken van persoonsgegevens.

#### Doelomschrijving

In artikel 2 van het privacyprotocol worden de doelen van de gegevensverwerking omschreven. Het protocol geeft aan dat gegevens worden verwerkt voor “het realiseren van laagdrempelige samenwerking ten behoeve van personen die het niet alleen redden” en dat gegevens kunnen worden gedeeld om dit doel te verwezenlijken.

Volgens het beginsel betreffende de doelbinding dienen de doeleinden uitdrukkelijk omschreven te zijn.<sup>92</sup> In de besproken opinie van de Artikel 29-Werkgroep is aangegeven wat wordt volstaan onder “uitdrukkelijk omschreven”. De omschrijving van het doel dient niet te algemeen te zijn, maar ook niet te gedetailleerd. De huidige doelomschrijving voldoet in grote lijnen aan deze regel. De cliënt kan uit de omschrijving opmaken waarvoor zijn gegevens worden gebruikt.<sup>93</sup>

De Artikel 29-Werkgroep raadt organisaties tevens aan om een gedetailleerde omschrijving beschikbaar te stellen. De betrokkene kan dan zelf deze informatie raadplegen. Het huidige beleid biedt hiervoor nog niet de mogelijkheid. De algemene formulering van het eerste doeleinde laat wat te wensen over. StiB helpt niet alleen hulpvragers of mantelzorgers die het “niet alleen redden”. Sommige hulpvragers hebben behoefte aan gezelschap om eenzaamheid tegen te gaan. Anderen (lees: mantelzorgers) verlangen naar een paar vrije uren voor henzelf of schrijven zich in voor cursussen en workshops. De huidige formulering van het doeleinde gaat niet over deze doelgroepen.

Daarbij spreekt de tweede doelomschrijving over “hulpverleners”. Nu StiB niet onder deze noemer valt, is ook deze doelomschrijving onnauwkeurig geformuleerd.

#### Toereikend & het bewaren van gegevens

Het privacyprotocol spreekt niet over welke gegevens worden bewaard en de reden waarom deze gegevens nodig zijn. Het protocol vermeldt in artikel 11 wel dat niet meer gegevens mogen worden verwerkt dan noodzakelijk. In artikel 18 van het protocol wordt aangegeven waar rekening mee gehouden moet worden bij het vaststellen van een bewaartermijn. Een mogelijke bewaartermijn is niet opgenomen.

#### Passende technische of organisatorische maatregelen

Dit onderdeel wordt summier in het beleid besproken.<sup>94</sup>

### 4.2.2 Rechtmatigheid van verwerking

In artikel 6 van het privacyprotocol worden de mogelijke rechtmatigheidsgronden voor verwerking besproken. Op bladzijde 9 van het privacyprotocol wordt dit artikel verder toegelicht. Artikel 6 begint met de mogelijkheid om persoonsgegevens te verwerken op

<sup>92</sup> Artikel 5, eerste lid en onder b, van de Algemene Verordening Gegevensbescherming.

<sup>93</sup> Zie paragraaf 2.1.1.

<sup>94</sup> Artikel 7 en 11 van het privacyprotocol.

grond van een rechtmatigheidgrond anders dan het verkrijgen van toestemming.<sup>95</sup> In de toelichting hierop staat het volgende opgenomen:

*“Een misverstand in dit verband: het feit dat de cliënt de hulp vrijwillig accepteert, wil niet zeggen dat eerst ‘toestemming’ gevraagd moet worden om een dossier aan te leggen. Om gegevens over personen in overeenstemming met de privacywetgeving, rechtmatig, te verwerken kan toestemming één van de rechtmatige grondslagen zijn.*

*...*

*Het is zelfs af te raden om het verwerken van gegevens alleen van toestemming afhankelijk te stellen, omdat de toestemming te allen tijde kan worden ingetrokken en de verwerking van persoonsgegevens terstond moet stoppen. Dit zou voor de praktijk niet werkbaar zijn.”*

De onderzoeker is van mening dat artikel 6 van het protocol nog niet conform de AVG is opgemaakt. In de komende paragrafen wordt deze stelling beargumenteerd.

### De verwerkingsgrond en het subsidiariteitsbeginsel

Het privacyprotocol legt de nadruk op het verwerken van gegevens op grond van een noodzakelijkheidgrond. Verwerking op grond van toestemming komt pas aan bod nadat blijkt dat verwerking op grond van deze noodzakelijkheidgrond(en) niet mogelijk is. In paragraaf 2.1.2 is uitgelegd onder welke omstandigheden een inbreuk gemaakt mag worden op de grondrechten van een ander. In de aangehaalde paragraaf zijn de beginselen van proportionaliteit en subsidiariteit besproken.

Het lijkt alsof het de bedoeling is dat de rechtmatigheidgrond “toestemming” pas gebruikt zal worden nadat er gekeken is of verwerking niet op een van de noodzakelijkheidgronden gebaseerd kan worden.<sup>96</sup> Conform het subsidiariteitsbeginsel zou de correcte wijze van werken zijn: eerst nagaan of toestemming verkregen kan worden, pas daarna kan gekeken worden of verwerking kan plaatsvinden op grond van een noodzakelijkheidgrond. Deze afwijkende manier van werken wordt verder niet in het protocol beargumenteerd. In de komende alinea’s wordt gekeken of de noodzakelijkheidgronden voor StiB een grond zouden zijn voor het verwerken van persoonsgegevens, indien geen toestemming is verkregen.

Het protocol beschrijft een situatie waarin de cliënt de geboden hulp accepteert. Door het gebruik van het woord “accepteren” wordt aangenomen dat een overeenkomst tot stand is gekomen. Uitgesloten wordt dan ook dat het hier nog gaat om de precontractuele fase; er is immers al een overeenkomst. Tevens is er geen sprake van een vitaal belang. Zoals in paragraaf 2.1.3 is uitgelegd, is in het algemeen pas sprake van een vitaal belang in een situatie waarbij het gaat om leven of dood. Ook heeft StiB geen wettelijke verplichting tot het aanleggen van een dossier of het verwerken van persoonsgegevens, waardoor ook deze noodzakelijkheidgrond onbruikbaar is. De gronden die overblijven zijn het verwerken van persoonsgegevens voor de uitvoering van een overeenkomst of in het belang van de instelling.

### Verwerking voor de uitvoering van een overeenkomst

Verwerking van persoonsgegevens voor de uitvoering van een overeenkomst is in beginsel toegestaan. Bij StiB wordt bij het aangaan van de overeenkomst altijd gevraagd of persoonsgegevens verwerkt mogen worden.

Het kan zijn dat een betrokkene na het sluiten van de overeenkomst aangeeft zijn toestemming in te willen trekken. Op dat moment moet het verwerken van persoonsgegevens worden gestaakt. Ook het protocol geeft dit aan.<sup>97</sup> Het is niet toegestaan

<sup>95</sup> Voor het gemak worden de rechtmatigheidgronden anders dan het verkrijgen van toestemming verder aangehaald als: “noodzakelijkheidgronden”.

<sup>96</sup> Dit is vooral te lezen in artikel 1 van de toelichting behorende bij het privacyprotocol.

<sup>97</sup> Het protocol verwijst naar artikel 5 van de Wet bescherming persoonsgegevens.

dat persoonsgegevens alsnog voor de uitvoering van een overeenkomst verder worden verwerkt. Ter onderbouwing wordt verwezen naar de memorie van toelichting van de Wbp:

*“Het is denkbaar dat de betrokkene zijn toestemming verleent om in het kader van de uitvoering van de overeenkomst of in een precontractuele fase gegevens van hem te verwerken. De gegevensverwerking steunt dan op artikel 8, onder a, indien althans de toestemming rechtsgeldig is verleend. De betrokkene heeft dan te allen tijde het recht zijn toestemming in te trekken, ten gevolge waarvan de rechtsgrondslag aan de gegevensverwerking komt te ontvallen. Het is dan de verantwoordelijke niet toegestaan alsnog op grond van artikel 8, onder b, tot verwerking over te gaan. Dit stuit op de norm van artikel 6: de verwerking geldt dan als onbehoorlijk en onzorgvuldig ten opzichte van de betrokkene.”<sup>98</sup>*

#### Verwerking in het belang van de instelling

Evenals bij de verwerking op grond van toestemming dient een verwerkingsverantwoordelijke die de verwerking baseert op een noodzakelijkheidgrond zijn belangen tegen die van de betrokkene af te wegen.<sup>99</sup> Het belang van de verwerkingsverantwoordelijke dient zo zwaar te wegen, dat het de verwerking van persoonsgegevens zonder toestemming rechtvaardigt.

Artikel 6d van het protocol stelt dat het verwerken van persoonsgegevens toegestaan is, indien dit in het belang van de instelling is en het belang van de instelling zwaarder weegt dan het belang van de betrokkene. Het protocol stelt dat het intrekken van toestemming een onwerkbaar situatie in de praktijk zou creëren. Nu het protocol niets anders aangeeft, wordt “het onwerkbaar zijn in de praktijk” als het belang van de organisatie geïnterpreteerd.

De memorie van toelichting vermeldt dat in bepaalde gevallen “om redenen van reguliere bedrijfsactiviteiten” gegevens verwerkt mogen worden.<sup>100</sup> Het voorbeeld dat wordt aangehaald is de schadeverzekeraar. De schadeverzekeraar heeft de persoonsgegevens van een derde nodig (de tegenpartij of getuigen) om zijn bedrijfsactiviteiten te verrichten. Als de derde hem de mogelijkheid om persoonsgegevens te verwerken ontzegt, dan kan de schadeverzekeraar zijn beroep niet verrichten. Dit ligt anders bij StiB. Een cliënt maakt zelf de keuze om partij te worden bij de overeenkomst. Er is geen sprake van een derde partij wiens persoonsgegevens nodig zijn voor het uitvoeren van bedrijfsactiviteiten.

#### Onjuiste interpretatie van de wet

De stelling dat het intrekken van toestemming onwerkbaar zou zijn is geen zwaarwegend belang. Het is spijtig dat de bedrijfsactiviteiten van de organisatie hier stranden, maar het belang van de organisatie weegt minder zwaar dan het recht op privacy van de betrokkene.

#### 4.2.3 Verwerking voor andere doeleinden

Voorop wordt nogmaals gesteld dat de tweede doelomschrijving niet nauwkeurig genoeg (of juist te nauwkeurig) is geformuleerd. StiB valt niet onder één van de genoemde instanties. Om deze reden heeft StiB geen doeleinde waarin staat vermeld dat persoonsgegevens worden verwerkt met als doel het delen van deze gegevens met derden. Door de afwezigheid van dit doeleinde wordt het delen van informatie met derden dan ook gezien als “het verwerken van persoonsgegevens voor andere doeleinden”.

Artikel 6, vierde lid, van de AVG geeft aan waar onder meer rekening mee gehouden moet worden, indien de verwerkingsverantwoordelijke voornemens is gegevens te verwerken voor een ander doel dan waarvoor de gegevens oorspronkelijk zijn verzameld. Het protocol geeft

<sup>98</sup> Kamerstukken II 1997/98, 25892, 3, p. 81 e.v.

<sup>99</sup> Zie paragraaf 2.1.2.

<sup>100</sup> Kamerstukken II 1997/98, 25892, 3, p. 86.

alleen aan wanneer persoonsgegevens gedeeld mogen worden zonder toestemming. Over het verwerken van persoonsgegevens voor andere (verenigbare) doeleinden wordt niet gesproken. Het weglaten van deze informatie is niet direct in strijd met de AVG. Wel kan gesteld worden dat het achterwege laten van deze informatie tot tijdrovende situaties kan leiden. Zo bestaat de kans dat de organisatie aan alle cliënten toestemming gaat vragen, zonder dat dit nodig is.

Een verwerkingsverantwoordelijke kan juist ook besluiten om persoonsgegevens voor een ander doeleind te verwerken. Het protocol geeft niet aan wanneer dit wel of niet mag. Dit kan leiden tot de ongelukkige situatie, waarbij de verwerkingsverantwoordelijke persoonsgegevens verwerkt voor een doeleind dat niet verenigbaar is met het huidige doeleind. Hierdoor zou de verwerkingsverantwoordelijke in strijd handelen met de AVG. Nogmaals, het weglaten van deze informatie is niet in strijd met de AVG. Het is echter ter volledigheid wel aan te raden om dit op te nemen in het protocol.

#### 4.2.4 Verwerken van bijzondere gegevens

Het protocol beschrijft drie rechtmatigheidgronden voor het verwerken van gevoelige gegevens. Het verwerken van persoonsgegevens op grond van toestemming staat niet opgenomen. Twee van de genoemde rechtmatigheidgronden gaan specifiek over scholen en reclasseringsinstellingen. Deze rechtmatigheidgronden worden verder niet besproken. Het protocol baseert verwerking van bijzondere persoonsgegevens op artikel 21, eerste lid en sub a, van de Wbp. Deze rechtmatigheidgrond staat niet langer opgenomen in de AVG.<sup>101</sup>

Ter volledigheid wordt kort ingegaan op artikel 21 Wbp. Verwerking van bijzondere persoonsgegevens is toegestaan voor zover dit gebeurt met het oog op een goede behandeling of verzorging van de betrokkene. In paragraaf 4.1.1 is aangegeven dat StiB waarschijnlijk geen beroep kan doen op dit artikel, nu StiB geen zorg biedt. De afwezigheid van deze rechtmatigheidgrond in de AVG vormt echter wel een probleem als men van mening is dat StiB een hulpverleningsinstantie is en dus *wel* een beroep kan doen op dit artikel.

Momenteel verwerken medewerkers van StiB bepaalde gegevens waarvan zij menen dat deze van belang zijn voor (bijvoorbeeld) het plaatsen van de juiste vrijwilliger bij de juiste persoon. Hiervoor wordt niet altijd toestemming gevraagd. Als deze handeling wordt gezien als het verzorgen van de betrokkene, dan biedt artikel 9 van de AVG straks niet meer de mogelijkheid om de persoonsgegevens zonder toestemming te blijven verwerken.

Deze vraag is dan ook aan de AP voorgelegd. De onderzoeker is van mening dat een soortgelijke bepaling wel van belang is. In het geval van StiB kunnen bepaalde gevoelige gegevens het selecteren van een vrijwilliger beïnvloeden. De AP heeft aangegeven dat hier nog geen antwoord op gegeven kan worden. Indien in de toekomst blijkt dat de praktijk een soortgelijke bepaling nodig acht, dan zal deze vraag nogmaals gesteld moeten worden. Tot dat moment zal een medewerker een wel overwogen beslissing moeten maken op de vraag of het van belang is dat de privacywetgeving in een bepaald geval wordt geschonden.

### 4.3 Het faciliteren van de rechten van de betrokkene

#### 4.3.1 Algemene Regels

In het beleid worden de algemene regels niet volledig besproken. In plaats daarvan worden bepaalde regels herhaald daar waar ze van toepassing zijn.<sup>102</sup> Het beleid mist een aantal van de algemene regels die op grond van de AVG wel opgenomen moeten worden. Het moet voor de betrokkene duidelijk zijn *dat* hij bepaalde rechten heeft en *hoe* hij op deze rechten een beroep kan doen.<sup>103</sup> Het beleid geeft dit laatste niet aan. Nergens staat opgenomen

<sup>101</sup> Artikel 9 van de Algemene Verordening Gegevensbescherming.

<sup>102</sup> Zie bijvoorbeeld artikel 13, eerste lid en onder b, en het tweede lid en onder c, van het privacyprotocol.

<sup>103</sup> Het nader te bespreken recht op informatie waarborgt dit recht.

welke stappen een betrokkene moet doorlopen alvorens een beroep te kunnen doen op een van zijn rechten. Daarbij vermeldt het beleid niets over de wijze waarop de verwerkingsverantwoordelijke de informatie moet verstrekken.

#### 4.3.2 Het recht op informatie

Het huidige beleid geeft aan dat de volgende informatie gedeeld moet worden bij het eerste contact met de cliënt:

- *de wijze waarop persoonsgegevens worden verwerkt;*
- *de doeleinden van de verwerking;*
- *wie de verwerkingsverantwoordelijke is;*
- *de rechten waarop hij een beroep kan doen;*
- *indien sprake is van verkrijging van gegevens van een derde, wie de derde is.*<sup>104</sup>

In de toelichting is ook opgenomen dat de medewerkers vermelden:

- *wie de persoonsgegevens in kan zien;*
- *met welke instanties de persoonsgegevens worden gedeeld;*
- *dat de cliënt mag aangeven dat hij niet wil dat de persoonsgegevens met andere instanties worden gedeeld.*<sup>105</sup>

De AVG verandert het bovenstaande niet. De informatieplicht wordt wel uitgebreid. De verwerkingsverantwoordelijke moet op grond van de AVG ook vermelden:

- *de bewaartermijn van de gegevens;*
- *dat hij het recht heeft om zijn toestemming in te trekken, indien verwerking op toestemming is gebaseerd;*
- *of de gevraagde gegevens noodzakelijk zijn voor het sluiten van een overeenkomst c.q. een wettelijke of contractuele verplichting is, en of de betrokkene verplicht is om de gegevens te verstrekken en wat de gevolgen zijn als hij dit niet doet.*<sup>106</sup>

Ook in het geval de gegevens afkomstig zijn van een derde dient de betrokkene geïnformeerd te worden over deze punten. Indien de gegevens afkomstig zijn van een derde, dient de betrokkene binnen een maand geïnformeerd te worden na het verkrijgen van de persoonsgegevens.

#### 4.2.3 Het recht op inzage

In artikel 13 van het privacyprotocol wordt het recht op inzage besproken. Het protocol bespreekt de bedoeling van het recht op inzage en geeft aan welke gegevens wel en/of niet overhandigd dienen te worden. Het beleid geeft niet aan op welke wijze de opgevraagde gegevens moeten worden verstrekt. Artikel 15, derde lid en tweede volzin, van de AVG spreekt hier echter wel over.

#### 4.3.4 Het recht op rectificatie

Artikel 13, tweede lid en sub a, van het protocol geeft aan dat een betrokkene het recht heeft om zijn gegevens te corrigeren. Het protocol voldoet dan ook aan artikel 16 van de AVG.

#### 4.3.5 Het recht op vergetelheid

Het recht op vergetelheid is pas in de AVG geïntroduceerd. Het privacyprotocol heeft dan ook nog geen uitgewerkte regeling betreffende dit recht. Wel wordt in artikel 13, tweede lid en sub a, van het protocol gesproken op over het recht van verwijdering.

#### 4.3.6 Het recht op beperking van de bewerking

Dit recht wordt niet besproken in het protocol.

<sup>104</sup> Artikel 8 van het privacyprotocol.

<sup>105</sup> Bladzijde 9 van de toelichting behorende bij het privacyprotocol.

<sup>106</sup> Zie paragraaf 2.2.2.

#### 4.3.7 Het recht op overdraagbaarheid van gegevens

Dit recht wordt niet besproken in het protocol.

#### 4.3.8 Het recht van bezwaar

Het beleid bevat een summiere uitleg betreffende het recht van bezwaar. Hieruit is niet duidelijk op te maken wie een beroep kan doen op het recht van bezwaar. Zowel de AVG als de Wbp geven aan welke betrokkene bezwaar c.q. verzet kan indienen.<sup>107</sup> Alleen de betrokkene wiens gegevens worden verwerkt op grond van artikel 6, eerste lid en onder e of f, van de AVG of ten behoeve van direct marketing kunnen bezwaar indienen.

#### 4.3.9 Beperking van de rechten

In paragraaf 2.2.8 is besproken wanneer een verwerkingsverantwoordelijke een recht mag beperken. Er moet sprake zijn van een belang aan de kant van de verwerkingsverantwoordelijke die zwaarder weegt dan die van de betrokkene. Artikel 15 van het privacyprotocol geeft aan dat de betrokkene geen beroep kan doen op zijn rechten of de plichten van de verwerkingsverantwoordelijke, indien de betrokkene een acuut gevaar vormt voor de verwerkingsverantwoordelijke. Het is aan te nemen dat, indien de betrokkene een acuut gevaar vormt voor een medewerker, het belang van de medewerker zwaarder weegt dan die van de betrokkene. De AVG wijzigt het bovenstaande niet.<sup>108</sup> Het enige dat toegevoegd kan worden, is dat de Nederlandse wetgever moet bepalen wat de reikwijdte is van de beperking.

#### 4.3.10 Rechtsbescherming

Artikel 17 van het protocol bespreekt de rechtsbescherming van de cliënten, indien zij van mening zijn dat de verwerkingsverantwoordelijke het privacyprotocol niet naleeft. Het protocol bespreekt de mogelijkheid tot het indienen van een verzoekschrift bij de rechtbank of het indienen van een klacht bij de Autoriteit Persoonsgegevens.

### 4.4 Overige artikelen

Het privacyprotocol bevat enkele artikelen die niet in de vorige paragrafen geplaatst konden worden.

#### 4.4.1 Toegang tot informatie

Het protocol stelt dat alleen de hulpverlener toegang heeft tot de gegevens van de cliënt en dat vrijwilligers alleen mogen beschikken over “buitenkant informatie”. StiB maakt gebruik van vrijwilligers die ondersteuning bieden op locatie en vrijwilligers die de rol of taak van consulent, medewerker klanttevredenheid of vrijwillige palliatieve terminale zorg op zich nemen. Deze vrijwilligers dienen de persoonsgegevens van vrijwilligers in te zien, zodat ze weten waarmee ze te maken hebben en waar ze zich op moeten voorbereiden. Ook vrijwilligers die ondersteuning bieden aan bepaalde cliënten dienen in uitzonderlijke gevallen te weten wat er aan een cliënt mankeert.

Het protocol laat de mogelijkheid om dit door middel van een overeenkomst te regelen buiten beschouwing. Van tevoren kan aan de betrokkene worden gevraagd of bepaalde gegevens met een vrijwilliger gedeeld mogen worden. De cliënt heeft vervolgens de optie om hiermee akkoord te gaan of niet.

#### 4.4.2 Het inzetten van vrijwilligers

Artikel 16 van het privacyprotocol en artikel 8 van de toelichting bespreekt de mogelijkheid tot het inzetten van vrijwilligers. Het protocol verwijst naar artikel 21, eerste lid en sub a, van de Wbp en geeft aan dat vrijwilligers op grond dat artikel geen bijzondere gegevens

<sup>107</sup> Artikel 21 van de Algemene Verordening Gegevensbescherming; Artikel 40 van de Wet bescherming Persoonsgegevens.

<sup>108</sup> Artikel 23, eerste lid, aanhef en onder i, van de Algemene Verordening Gegevensbescherming.

betreffende de gezondheid van een cliënt in mogen zien. Het verwerken van bijzondere persoonsgegevens door hulpverleners staat niet langer opgenomen in de AVG.

Ter volledigheid wordt het volgende opgemerkt. Het protocol stelt dat artikel 21 van de Wbp alleen de hulpverleners de bevoegdheid geeft om medische gegevens van de cliënt te verwerken. Hierdoor zou het amper mogelijk zijn om vrijwilligers in te zetten, omdat niet meer dan de “buitenkant informatie” aan de vrijwilliger mag worden verstrekt. Artikel 23, eerste lid en sub a, van de Wbp geeft echter de mogelijkheid voor niet-hulpverleners om bijzondere persoonsgegevens te verwerken, indien hier toestemming voor wordt gevraagd. Ook het Burgerlijk Wetboek geeft deze mogelijkheid in het geval sprake is van een geneeskundige behandelingsovereenkomst. Artikel 7:457, eerste lid, BW geeft specifiek aan dat anderen het dossier van een cliënt mogen inzien, als de cliënt hier uitdrukkelijk toestemming voor heeft gegeven. Het gaat in dat geval wel om *hulpverleners* die een dossier bijhouden.

#### 4.4.3 Plichten van de verwerkingsverantwoordelijke

De laatste volzin van de laatste alinea van artikel 3 van de toelichting bespreekt de plicht tot het melden van gegevensverwerking aan de Autoriteit Persoonsgegevens. Met de komst van de AVG is deze plicht komen te vervallen. De plicht tot het melden van datalekken staat niet opgenomen in het beleid.

## Hoofdstuk 5 Toetsing van de praktijk

---

In dit hoofdstuk wordt naar de toepassing van het beleid in de praktijk gekeken.

### 5.1 Toepassing van het protocol in de praktijk

Tijdens het praktijkonderzoek is gekeken in hoeverre de medewerkers bekend zijn met het protocol en of zij het protocol correct toepassen.

#### 5.1.1 Algemene indruk

De toepassing van het privacyprotocol in de praktijk laat nog veel te wensen over. Al hoewel het privacyprotocol wel aanwezig is, gebruiken de medewerkers het amper.

Zo wordt pas sinds kort de cliënt gevraagd om een overeenkomst te ondertekenen. Een informatieve brief of iets dergelijks over het gebruik van persoonsgegevens ontbreekt en de coördinatoren houden zich niet bezig met de informatieplicht. Uit de interviews en de survey blijkt tevens dat deze kennis niet paraat staat bij de medewerkers. Zo kunnen degenen die aangeven bekend te zijn met de inhoud van het privacyprotocol de vragen die in de survey zijn gesteld niet correct beantwoorden.

#### 5.1.2 De rechten van de betrokkene

In paragraaf 4.3.1 is gekeken naar de rechten waar volgens het protocol een betrokkene een beroep op zou kunnen doen. StiB heeft momenteel nog niets geregeld omtrent deze rechten.

### 5.2 Overige onderwerpen

Tijdens het praktijkgericht onderzoek zijn een aantal zaken geconstateerd betreffende de omgang met de persoonsgegevens van cliënten. Deze onderwerpen staan niet opgenomen in het huidige beleid. Om ervoor te zorgen dat deze onderwerpen conform de AVG worden benaderd is verder onderzoek gedaan. De bevindingen worden in deze paragraaf besproken.

#### 5.2.1 BSN-nummers

Tijdens het interview met mevrouw Bakx is gebleken, dat StiB de BSN-nummers van haar cliënten vraagt. Op grond van het huidige artikel 24, eerste lid, van de WBP en artikel 87 van de AVG mogen BSN-nummers alleen worden verwerkt, indien de doeleinden daarvoor bij wet zijn bepaald. In Nederland wordt dit bepaald in Wbsn en de Wgbz.

In de Wbsn krijgen overheidsorganen de bevoegdheid om BSN-nummers te verwerken.<sup>109</sup> Krachtens artikel 4 van de Wgbz mogen zorgaanbieders BSN-nummers verwerken. In artikel 1, onder c, van de Wgbz wordt verwezen naar de Wet kwaliteit, klachten en geschillen zorg voor de definitie van zorgaanbieder. In artikel 1, eerste lid, van de hiervoor genoemde wet staat dat met zorgaanbieders wordt bedoeld: een instelling dan wel solistische werkende zorgverlener. In ditzelfde artikel wordt tevens gedefinieerd dat een zorgverlener een natuurlijke persoon is die beroepsmatig zorg verleent. StiB verleent geen beroepsmatige zorg. Zij biedt vooral ondersteuning aan mantelzorgers en hulpvragers. Hieruit is te concluderen dat StiB in ieder geval niet valt onder de noemer "zorgaanbieder".

StiB valt niet onder de Wbsn noch de Wgbz.

#### 5.2.2 Bankrekeningnummer

In het interview met mevrouw Bakx is tevens geconstateerd dat bij iedere cliënt de mogelijkheid bestaat om een bankrekeningnummer in te vullen. Mevrouw Bakx heeft aangegeven dat dit enkel wordt ingevuld bij een vrijwilliger die een onkostenvergoeding ontvangt.

---

<sup>109</sup> Artikel 10 van de Wet algemene bepalingen burgerservicenummer.

Conform artikel 25 van de AVG dient een verwerkingssysteem zo te zijn ingedeeld, dat het niet mogelijk is om gegevens te verwerken die niet noodzakelijk zijn voor het te behalen doel. Dat deze gegevens bij iedere aangemaakte cliënt ingevuld kan worden, dient op grond van dit artikel vermeden te worden.

### 5.2.3 Verwerking gegevens bij de mantelzorgwaardering

Tijdens de observatie en het interview met mevrouw Buijnsters is gebleken dat de medewerkers van de mantelzorgwaardering bijzondere gegevens van een derde noteren, zonder dat de derde hiervan op de hoogte is. Het gaat hier voornamelijk om de bijzondere persoonsgegevens van de persoon die wordt verzorgd door een mantelzorger. Met de komst van de AVG vervalt de grond waarop het protocol momenteel het verwerken van bijzondere persoonsgegevens baseert.<sup>110</sup> Dit betekent dat de mantelzorgwaardering niet langer zonder toestemming deze bijzondere persoonsgegevens mag verwerken.

---

<sup>110</sup> Zie paragraaf 4.2.4.

## Hoofdstuk 6 Conclusies en aanbevelingen

In dit onderzoek staat de volgende vraag centraal:

*“Welke aanbevelingen zijn af te leiden uit een toetsing van het huidige privacy beleid, en de praktische toepassing daarvan, aangaande de omgang met cliënten van Stichting Steunpunt informele zorg Breda aan de Algemene Verordening Gegevensbescherming?”*

Aan de hand van enkele conclusies wordt antwoord gegeven op deze vraag. Om de conclusies overzichtelijk te houden wordt de centrale vraag in drie delen behandeld. Het eerste deel bespreekt hetgeen geconcludeerd uit de toetsing van het beleid aan de AVG. Het tweede deel bespreekt de wijze waarop medewerkers het beleid toepassen in de praktijk. Bij het laatste deel staat de relatie tussen de medewerkers en de AVG c.q. het privacyprotocol centraal. Er is ook een vierde conclusie die wordt besproken. Deze conclusie (en de bijbehorende aanbeveling) heeft geen direct verband met de centrale vraag. Het is echter wel van belang dat deze conclusie wordt besproken.

### 6.1 Conclusies

#### 6.1.1 Toetsing van het beleid aan de AVG

Uit de toetsing van het privacyprotocol aan de AVG is geconcludeerd dat het beleid nog niet voldoet aan de regels voortvloeiend uit de verordening. Hiervoor zijn meerdere oorzaken.

Als eerste is van belang om aan te geven dat StiB geen hulpverleningsinstantie is. In het huidige beleid wordt hier constant over gesproken. De medewerkers van StiB verzorgen de cliënten niet. Zij ondersteunen de cliënten op andere wijzen. Dit is van belang, omdat de privacyregels met betrekking tot hulpverleningsinstanties anders zijn dan de regels voor instanties die geen zorg verlenen. Het huidige beleid is dan ook niet toepasbaar in de meeste gevallen. Met dit in het achterhoofd is het protocol naast de AVG gelegd.

Ten eerste wordt geconcludeerd dat de opgenomen doeleinden het een en ander te wensen overlaat. Hiervoor zijn twee argumenten. Het eerste doeleind stelt dat “alleen de persoonsgegevens van personen die het niet alleen redden” worden verwerkt. StiB verwerkt ook persoonsgegevens van anderen. Zo verwerkt StiB persoonsgegevens van mantelzorgers die deelnemen aan workshops. Het tweede argument legt een nadruk op de formulering van de doeleinden. Het eerste doeleind omvat zowel hulpverleningsinstanties als instanties die een maatschappelijke dienst verrichten. Het tweede doeleind, dat gaat over het delen van persoonsgegevens onderling, spreekt echter niet over de organisaties die een maatschappelijke dienst verrichten. Dit heeft als gevolg dat aan StiB geen toestemming wordt gegeven tot het delen van persoonsgegevens met andere organisaties. Hierbij is ook niet duidelijk of het delen wordt beperkt tot de organisaties binnen Zorg voor elkaar Breda.

Vervolgens wordt geconcludeerd dat het beleid niet concreet aangeeft welke persoonsgegevens worden verwerkt en waarom juist deze persoonsgegevens worden verwerkt. Dit is wel iets dat kenbaar gemaakt moet worden aan de betrokkene. Ook de uitleg/regeling betreffende het verwerken voor andere doeleinden is grotendeels achterwege gelaten.

Uit de toetsing is verder te concluderen dat het beleid op een onjuiste wijze de regels omtrent de rechtmatigheid van het verwerken van persoonsgegevens toepast. Dit geldt voor zowel een hulpverleningsinstantie als een niet-geïndiceerde instantie. Primair wordt aangegeven dat gegevens altijd mogen worden verwerkt, indien dit noodzakelijk is voor het uitvoeren van een overeenkomst of in het belang van het bedrijf. Secundair wordt gesteld dat het vragen van toestemming pas gedaan hoeft te worden, indien het verwerken op een andere grond niet mogelijk is.

Indien men een inbreuk gaat maken op een grondrecht van een ander, dient conform het subsidiariteitsbeginsel gehandeld te worden. Het subsidiariteitsbeginsel houdt in dat degene die een inbreuk gaat maken op een grondrecht eerst de minst ingrijpende manier moet toepassen. Pas nadat blijkt dat deze manier ontoereikend of onbruikbaar is, mag men een zwaardere manier toepassen. Het vragen van toestemming is de minst ingrijpende manier, aangezien men toestemming vraagt om een inbreuk te maken op een grondrecht van de betrokkene. De overige gronden (de noodzakelijkheidsgronden) zijn zwaarder, omdat zonder dat de toestemming van de betrokkene gegevens worden verwerkt. Op grond van het subsidiariteitsbeginsel is deze volgorde dus onjuist.

Hierbij speelt ook dat de noodzakelijkheidsgronden opgenomen in het beleid niet door StiB toegepast kunnen worden. Volgens het beleid zijn deze noodzakelijkheidsgronden leidend, omdat het onwerkbaar zou zijn voor een organisatie als een betrokkene zijn toestemming voor het verwerken van zijn gegevens intrekt.

De noodzakelijkheidsgrond die strekt tot het verwerken van persoonsgegevens ter uitvoering van overeenkomst is niet bruikbaar, omdat bij het aangaan van StiB altijd toestemming moet vragen. Men kan, zoals het beleid ook aangeeft, niet gedwongen worden tot het accepteren van vrijwillige hulp c.q. ondersteuning. De memorie van toelichting behorende bij de Wbp geeft aan dat verwerking in het geval toestemming is gegeven geschiedt op grond van deze toestemming. Het is niet toegestaan om dan alsnog op grond van een noodzakelijkheidsgrond gegevens te verwerken.

De noodzakelijkheidsgrond met betrekking tot het verwerken in het vitale belang van de betrokkene is tevens ontoereikend. Het vitale belang houdt in dat gegevens worden verwerkt in een situatie van leven of dood, waarbij niet gewacht kan worden op toestemming van een betrokkene. Dit soort situaties komen eigenlijk niet voor. Daarbij is StiB niet degene die de gegevens moet verwerken in het geval sprake zou zijn van een vitaal belang.

StiB heeft ook geen wettelijke verplichting voor het verwerken van gegevens, waardoor de noodzakelijkheidsgrond die betrekking heeft tot deze situatie ook niet bruikbaar is.

De laatste noodzakelijkheidsgrond die het privacyprotocol behandelt, is het verwerken van persoonsgegevens in het belang van organisatie. De achterliggende belangenafweging die in het beleid wordt gebruikt, is onjuist. Volgens het beleid is het belang van de organisatie: het kunnen verrichten van haar werkzaamheden. Het niet langer kunnen verwerken van persoonsgegevens, indien de betrokkene zijn toestemming intrekt, zou reden zijn om toch de gegevens te verwerken van de betrokkene. De memorie van toelichting behorende bij de Wbp geeft aan dat verwerking in het belang van de werkzaamheden van de organisatie niet van toepassing is op organisaties zoals StiB. De memorie spreekt over organisaties wiens werkzaamheden niet voltooid kunnen worden als een (derde) partij geen toestemming geeft tot het werken van persoonsgegevens. Het voorbeeld dat wordt aangehaald is een schadeverzekeraar.

Op grond van het bovenstaande is geconcludeerd dat verwerking bij StiB enkel mogelijk is op grond van toestemming. Ditzelfde geldt voor het verwerken van bijzondere gegevens. In het geval van de bijzondere persoonsgegevens verzaakt het beleid te melden dat verwerking van bijzondere gegevens ook dient te geschieden op grond van toestemming.

Hierbij komt nog kijken dat het beleid stelt dat bijzondere persoonsgegevens ook verwerkt mogen worden, indien dit gebeurt met het oog een goede behandeling of verzorging. De wetgever geeft in de memorie van toelichting aan dat het hier gaat om medische behandelingen en verzorging. Dit is (nogmaals) niet wat StiB doet.

Vervolgens wordt geconcludeerd dat het beleid nog niet alle rechten van de betrokkene bespreekt noch een regeling c.q. procedure hiervoor heeft opgesteld. Een gedeeltelijke

verklaring hiervoor is dat op het moment van schrijven (van het beleid) deze rechten nog niet bestonden. Deze verklaring geldt echter niet voor de overige rechten.

Ook zijn de regelingen omtrent het melden van een datalek en pseudonimiseren van gegevens niet opgenomen. Het melden van een datalek was bij de oplevering van het privacyprotocol al een bestaande verplichting, waardoor deze plicht al in het beleid had moeten staan.

Ten slotte wordt geconcludeerd dat het beleid een onjuiste uitleg geeft over het gebruik van vrijwilligers. Het beleid stelt dat vrijwilligers niet intensief gebruikt kunnen worden, omdat zij alleen de “buitenkant-informatie” mogen inzien. Dit kan echter bij overeenkomst worden geregeld. Ditzelfde geldt ook voor hulpverleningsinstanties, aangezien de wet hiervoor de mogelijkheid biedt.

#### 6.1.2 Toepassing van het beleid in de praktijk

Uit het onderzoek van de praktijk is te concluderen dat StiB het privacyprotocol momenteel nog niet overal toepast.

Uit de interviews en de survey is naar voren gekomen dat de meeste medewerkers aangeven “wel iets” van het beleid toe te passen in de praktijk. Zij doen dit echter ieder op hun eigen manier. Dit heeft als gevolg dat in de meeste gevallen StiB niet voldoet aan haar informatieplicht.

Tevens wordt uit de interviews en de observaties geconcludeerd dat StiB momenteel nog geen procedures heeft de rechten van de betrokkene waarborgen. Hierdoor voldoet StiB niet aan haar verplichting om de rechten van de betrokkene te faciliteren.

Uit de observaties is geconcludeerd dat de Mantelzorgwaardering het beleid onjuist c.q. niet toepast. De afdeling verwerkt persoonsgegevens van de aanvrager (en in bepaalde gevallen de persoonsgegevens van de persoon die wordt verzorgd) zonder dat hiervoor toestemming is gevraagd.

StiB verwerkt ook BSN- en bankrekeningnummers van cliënten en vrijwilligers. Dit is niet toegestaan op grond van de Wbsn en de Wbp c.q. AVG.

#### 6.1.3 Het privacyprotocol en de werknemers

##### **Medewerkers bekend**

De medewerkers die van mening zijn dat ze bekend zijn met het beleid blijken minder te weten van de inhoud dan dat zij zelf verwachten. De medewerkers geven in de survey aan dat het protocol goed leesbaar en makkelijk is toe te passen, maar zijn meestal niet in staat om de correcte antwoorden te geven op de inhoudelijke vragen in de survey. Wel geven een aantal van de medewerkers aan dat de organisatie meer aandacht moet besteden aan het privacyprotocol.

##### **Medewerkers onbekend**

Uit de afgenomen interviews blijkt dat de medewerkers zich amper tot niet bezighouden met het privacyprotocol. Daarbij geven deze medewerkers aan gedesinteresseerd te zijn in het onderwerp. De desinteresse wordt voornamelijk veroorzaakt door de wijze waarop het protocol is opgesteld. Medewerkers geven aan dat ze geen tijd hebben of willen nemen om het beleid door te lezen, omdat het te juridisch en langdradig overkomt. De voorkeur gaat uit naar een uitleg die ter zake en makkelijk verteerbaar is.

Tijdens het observeren van deze medewerkers is gebleken dat deze desinteresse ook de nieuwe medewerkers benadeeld. De nieuwe medewerkers worden tijdens de inwerkperiode amper tot niet op het privacyprotocol gewezen. Hierdoor wordt de nieuwe medewerker onvoldoende geïnformeerd over het beleid. Het gevolg hiervan is dat steeds meer medewerkers in de organisatie onbekend zijn met het beleid.

Ook StiB als organisatie moet volgens de medewerkers meer doen om het protocol levendig te maken. Hierbij moet niet alleen gekeken worden naar de begrijpbaarheid van het protocol. De huidige manier waarop de privacyregelgeving wordt besproken is onvoldoende en bereikt weinig medewerkers. De inhoud van een presentatie blijft niet al te lang hangen.

Uit hetgeen besproken in paragraaf 6.1.2 en 6.1.3 is te concluderen dat StiB als organisatie niet genoeg tijd besteed aan het inlichten en trainen van haar medewerkers op het gebied van privacy.

#### 6.1.4 Het privacyprotocol en Zorg voor elkaar Breda

Het privacyprotocol is opgesteld voor Zorg voor elkaar Breda. In de hiervoor besproken conclusies is aangegeven dat het beleid niet geheel van toepassing is op StiB, omdat StiB geen geïndiceerde hulpverleningsorganisatie is. De huidige doelomschrijving strekt niet tot het delen van informatie tussen de hulpverleningsorganisaties binnen Zorg voor elkaar Breda en StiB. Hierdoor is het niet mogelijk voor bijvoorbeeld GGZ Breburg om gezondheidsgegevens te delen met StiB. In de praktijk wordt dit echter wel gedaan. Hulpverleningsorganisaties delen gevoelige informatie met StiB, terwijl strikt gezien hiervoor geen toestemming wordt gevraagd. De huidige formulering is dus niet alleen onwerkbaar voor StiB, maar ook voor Zorg voor elkaar Breda.

De samenwerking binnen Zorg voor elkaar Breda is praktisch gezien goed geregeld, maar juridisch gezien laat het privacyprotocol ook op dit niveau het een en ander te wensen over.

## 6.2 Aanbevelingen

### 6.2.1 Aanbevelingen ter bevordering van het beleid

Het huidige beleid is niet toegespitst op een organisatie zoals StiB, maar op een hulpverleningsorganisatie. Hierdoor zijn een groot aantal aanbevelingen gericht op het verbeteren van het protocol op deze punten. Om herhaling te voorkomen wordt in het algemeen gesteld, dat StiB over moet stappen op een beleid waarbij niet uit wordt gegaan van een hulpverleningsinstantie.

Ten eerste is aan te bevelen om verwerking van persoonsgegevens niet langer te baseren op een van de noodzakelijkheidsgronden die momenteel staan opgenomen in het privacyprotocol. StiB zal het verwerken van persoonsgegevens moeten baseren op toestemming. Dit heeft wel het gevolg dat StiB voortaan bij het eerste contact toestemming zal moeten vragen voor het verwerken van persoonsgegevens. Dit geldt ook in de situaties waarbij geen overeenkomst wordt getekend, maar waarbij StiB wel de persoonsgegevens van een cliënt verwerkt. Ditzelfde geldt voor het verwerken van bijzondere persoonsgegevens. StiB zal het verwerken van gezondheidsgegevens moeten baseren op grond van toestemming.

Vervolgens is aan te bevelen om de formulering van de doeleinden aan te passen. Deze dienen vooral duidelijk en omvattend. Met dit laatste wordt bedoeld dat alle redenen waarom StiB persoonsgegevens verwerkt in de doeleinden worden opgenomen. Hierbij kan gebruik worden gemaakt van de “layered-notice approach” zoals beschreven in dit onderzoek.

Het beleid dient ook aan te geven wanneer sprake is van verwerking voor andere doeleinden en wanneer dit mag. Tevens dient het beleid een regeling te treffen omtrent het wel of niet pseudonimiseren van persoonsgegevens.

StiB dient daarbij een procedure op te stellen voor de cliënt die een beroep wil doen op zijn rechten. Hierbij moet rekening gehouden worden met de bevestiging van de identificatie en welke persoonsgegevens aan de cliënt geopenbaard mogen worden. Het huidige privacyprotocol voorziet al in dit laatste.

Ten slotte dient het beleid aan te geven hoe de organisatie handelt indien een datalek wordt geconstateerd. In dit beleid moet in ieder geval komen te staan de wijze waarop StiB handelt op het moment dat een datalek wordt geconstateerd en hoe het lek wordt gedicht. Zo zou het eerste deel van het beleid kunnen bestaan uit de volgende onderwerpen: hoe bepaal je de “grootte” van het lek, wanneer meldt StiB een datalek, welke medewerker is hiervoor verantwoordelijk en wat komt er in de melding te staan. Hierbij wordt gewezen op het feit dat niet ieder lek gemeld hoeft te worden. Dit hangt af van de impact van het datalek. Het vervolg van het beleid dient te gaan over de manier waarop het lek zal worden gedicht. Hiervoor gelden geen wettelijke regels.

### 6.2.2 Aanbevelingen ter bevordering van de toepassing van het beleid

Het is aan te raden om een folder of een flyer te ontwerpen waarop de privacy gerelateerde gegevens van de organisatie staan opgenomen. Op deze hand-out staan minimaal ook de globale doeleinden van de organisatie uitgewerkt. Daaronder kan een verwijzing geplaatst worden naar de website van StiB. Op de website worden de doeleinden verder gespecificeerd. De rechten van de betrokkene en de verplichtingen van de organisatie kunnen op de achterkant worden opgesomd.

De afdeling Mantelzorgwaardering dient over te stappen van de telefonische inschrijving van aanvragen naar een inschrijvingsformulier voor aanvragen. Dit formulier kan zowel op papier als digitaal geleverd worden. Van belang is dat het formulier is ondertekend door de aanvrager en (indien van toepassing) degene wiens persoonsgegevens ook worden verwerkt. In het geval sprake is van een persoon die niet langer zelf een formulier kan ondertekenen, kan (zoals in het privacyprotocol aangezien) gewerkt worden met een door de aanvrager te verstrekken machtiging.

De overeenkomsten die StiB sluit met cliënten bevatten nog geen clausules met betrekking tot de privacy van de cliënt. Deze dienen opgenomen te worden. Een optie is om in de overeenkomst te verwijzen naar de folder die hierboven wordt aangeraden. Hierdoor voldoet StiB meteen aan haar informatieplicht. Daarbij is het aan te raden om iedere cliënt de overeenkomst te laten ondertekenen.

Om te voldoen aan de regels met betrekking tot gegevensbescherming door ontwerp en standaardinstellingen zal StiB haar verwerkingssysteem zo moeten aanpassen, dat het niet langer mogelijk is om het bankrekeningnummer van cliënten te verwerken. Deze optie mag wel blijven bestaan voor vrijwilligers, aangezien vrijwilligers een onkostenvergoeding ontvangen.

Ten slotte dient StiB te stoppen met het verwerken van BSN-nummers. Ook mag het verwerkingssysteem niet langer over een invulveld beschikken waarin een BSN-nummer kan worden genoteerd.

### 6.2.3 Aanbevelingen ter bevordering van de werknemers

Voor de medewerkers is het van belang dat het privacyprotocol gaat leven in de organisatie. Het is aan te bevelen dat StiB een hand-out voor haar medewerker maakt met daarop (een aantal) stappenplannen die de medewerker moet volgen. Deze stappenplannen kunnen worden opgesteld aan de hand van het privacyprotocol. Wel dienen de hierboven staande aanbevelingen eerst te worden verwerkt in het protocol.

Bij het inwerken van nieuwe medewerkers dient StiB meer aandacht te besteden aan het beleid. De medewerker moet eigenlijk op de eerste dag al meteen in aanraking komen met het protocol. Om te zorgen dat dit gebeurt, kan StiB overwegen om een “inwerkmap” te maken. In deze map wordt aangegeven wat op de eerste werkdag minimaal besproken dient te worden. Privacy is natuurlijk het eerste en belangrijkste punt.

Het is tevens aan te bevelen om maandelijks een moment in te plannen, waarbij de medewerkers met elkaar (on)beantwoorde privacy vragen of casussen bespreken. Op deze

manier worden medewerkers maandelijks eraan herinnerd dat het privacyprotocol een actueel onderwerp is en blijft. Doordat medewerkers aan elkaar uitleg geven, wordt tevens de kennis over het onderwerp vergroot.

#### 6.2.4 Aanbeveling ter bevordering van de samenwerking binnen Zorg voor elkaar Breda

Het is aan te raden om te onderzoeken of het mogelijk is om de doelomschrijving op het niveau van Zorg voor elkaar Breda aan te passen. Mogelijk zal dan ook onderzocht moeten worden hoe en of het verlenen van toestemming op het niveau van Zorg voor elkaar Breda geregeld kan worden.

Zo zou gekeken kunnen worden of het wellicht mogelijk is om vanuit Zorg voor elkaar Breda een overeenkomst of toestemmingformulier op te stellen, waarmee cliënten toestemming kunnen geven voor het onderling delen van persoonsgegevens binnen Zorg voor elkaar Breda. Hiermee zal het mogelijk zijn voor een organisatie zoals GGZ Breburg om de benodigde persoonsgegevens met StiB te delen, indien zij van mening is dat (de mantelzorger van) een cliënt ondersteuning nodig heeft. De precieze formulering, de uitsluitingen of uitzonderingen enzovoorts, zal in dit onderzoek aan bod moeten komen.

Van belang is dus dat in ieder geval gekeken wordt of de samenwerking binnen Zorg voor elkaar Breda ook juridisch soepel kan verlopen. Het privacyprotocol dient, indien Zorg voor elkaar Breda één algemeen privacy beleid wil blijven voeren, een aantal nuances en daar waar nodig afwijkende regels te bespreken.

## Bronnenlijst

---

### Artikelen

#### **Jong, de, RegelMaat 2015, p. 9.**

J.P. de Jong, 'De Algemene verordening gegevensbescherming: de rechtsopvolger van de Wbp', *Regelmaat* 2015 (30) 1, p. 6-18.

#### **Sloot, van der, TvC 2012, p. 254.**

Mr. drs. B. van der Sloot, 'De nieuwe consumentenrechten in de Algemene verordening gegevensbescherming: vergeten worden, dataportabiliteit en profilering', *Tijdschrift voor Consumentenrecht en handelspraktijken* 2012-6, p. 254-256.

#### **Vries, de, & Goudsmit, NJB 2016, p. 1553.**

Mr. dr. H. de Vries & mr. M. Goudsmit, 'Voorsorteren op de Algemene Verordening Gegevensbescherming', *Nederlands Juristenblad* 2016, afl. 22, p. 1553.

### Literatuur

#### **Kranenborg & Verhey 2010, p. 25.**

H.R. Kranenborg & L.F.M. Verhey, *Wet bescherming persoonsgegevens in Europees perspectief*, Deventer: Kluwer 2011.

#### **Moerel & Prins 2016, p. 21 & 91.**

E.M.L. Moerel & J.E.J. Prins, 'Privacy voor de homo digitalis', in: *Homo digitalis. Preadviezen* (Handelingen Nederlandse Juristen-Vereniging, deel 2016-I), Deventer: Wolters Kluwer 2016/1, p. 21 & 91 (online publiek).

### Parlementaire stukken

#### **Kamerstukken I 2015/2016, 33169, AF.**

Brief van de minister van Veiligheid en Justitie: *EU-voorstel: Richtlijn bescherming persoonsgegevens bij gebruik door politieke en justitiële autoriteiten (COM(2012)10) en EU-voorstel Verordening algemeen kader bescherming persoonsgegevens (COM(2012)11)*

#### **Kamerstukken II 1997/98, 25 892, nr. 3.**

Memorie van toelichting: *Wet bescherming persoonsgegevens*

### Elektronische bronnen

#### **Website Autoriteit Persoonsgegevens**

<autoriteitpersoonsgegevens.nl>

#### **Website Stichting Steunpunt informele zorg Breda**

<stib-breda.nl>

### Rapporten

#### **Opinie 03/2013 van de Artikel 29-Werkgroep**

Artikel 29-Werkgroep, *Opinion 03/2013 on purpose limitation*, Brussel: Artikel 29-Werkgroep 2013.

### Stukken van de Europese Unie

COM/2012/11 final.