

# Merford versus de AVG

Een praktijkgericht juridisch onderzoek naar de privacyverklaringen en de huidige werkwijze gelet op de nieuwe privacywetgeving



|                                |                                                        |
|--------------------------------|--------------------------------------------------------|
| <b>Naam student:</b>           | Shalini Gadjdjo                                        |
| <b>Studentnummer:</b>          | 2089559                                                |
| <b>Onderwijsinstelling:</b>    | Juridische Hogeschool Avans-Fontys te 's-Hertogenbosch |
| <b>Opleiding:</b>              | HBO-Rechten                                            |
| <b>Periode:</b>                | april 2018 – oktober 2018                              |
| <b>Eerste afstudeerdocent:</b> | mevr. mr. M.R.M. Brugman                               |
| <b>Tweede afstudeerdocent:</b> | mevr. mr. E.M. Strooper-Lammerts                       |
| <b>Afstudeerorganisatie:</b>   | Merford                                                |
| <b>Afstudeermentor:</b>        | mevr. drs. A.J. Vertooren                              |

Gorinchem, 12 oktober 2018

# Merford versus de AVG

Een praktijkgericht juridisch onderzoek naar de privacyverklaringen en de huidige werkwijze gelet op de nieuwe privacywetgeving

|                                |                                                        |
|--------------------------------|--------------------------------------------------------|
| <b>Naam student:</b>           | Shalini Gadjdjo                                        |
| <b>Studentnummer:</b>          | 2089559                                                |
| <b>Onderwijsinstelling:</b>    | Juridische Hogeschool Avans-Fontys te 's-Hertogenbosch |
| <b>Opleiding:</b>              | HBO-Rechten                                            |
| <b>Periode:</b>                | april 2018 – oktober 2018                              |
| <b>Eerste afstudeerdocent:</b> | mevr. mr. M.R.M. Brugman                               |
| <b>Tweede afstudeerdocent:</b> | mevr. mr. E.M. Strooper-Lammerts                       |
| <b>Afstudeerorganisatie:</b>   | Merford                                                |
| <b>Afstudeermentor:</b>        | mevr. drs. A.J. Vertooren                              |
| <b>Plaats en datum:</b>        | Gorinchem, 12 oktober 2018                             |

## Voorwoord

Voor de afronding van mijn opleiding HBO-Rechten, heb ik de mogelijkheid gekregen om mijn afstudeerstage te lopen bij Merford te Gorinchem. Gedurende mijn stageperiode heb ik onderzoek verricht naar de nieuwe privacywetgeving, die per 25 mei 2018 flink is veranderd. De vraag die centraal staat binnen dit onderzoek luidt als volgt:

*“Welke aanbevelingen kunnen, gelet op de relevante bepalingen uit de AVG, aan Merford worden gegeven ten aanzien van de privacyverklaringen en de huidige werkwijze met betrekking tot de verwerking van de persoonsgegevens van haar klanten en leveranciers?”*

Ik wil mijn afstudeermentor mevrouw Vertooren bedanken voor de begeleiding en alle hulp tijdens mijn afstudeerperiode. Verder wil ik mijn afstudeerdocent mevrouw Brugman bedanken voor haar begeleiding, hulp en feedback gedurende mijn afstudeerperiode. Mevrouw Strooper-Lammerts wil ik ook graag bedanken voor de feedback. Verder wil ik alle geïnterviewde medewerkers van Merford bedanken voor hun tijd, openheid en eerlijkheid. Ten slotte wil ik de collega's binnen Merford bedanken voor de leuke, gezellige en leerzame tijd. Mijn stageperiode bij Merford was een hele mooie en positieve ervaring.

*“At least in Europe, we consider the right to privacy a fundamental right and it is a very serious matter.” – Jose Manuel Barroso<sup>1</sup>*

Ik wens u veel leesplezier toe!

Shalini Gadjdjoe

Gorinchem, 12 oktober 2018

---

<sup>1</sup> [www.azquotes.com](http://www.azquotes.com) (zoek op Jose Manuel Barroso privacy).

# Inhoudsopgave

|                                                                           |           |
|---------------------------------------------------------------------------|-----------|
| <b>Samenvatting.....</b>                                                  | <b>11</b> |
| <b>Lijst van afkortingen .....</b>                                        | <b>11</b> |
| <b>Begrippenlijst .....</b>                                               | <b>11</b> |
| <b>Hoofdstuk 1 Inleiding .....</b>                                        | <b>11</b> |
| 1.1 De organisatie.....                                                   | 11        |
| 1.2 Probleemomschrijving.....                                             | 11        |
| 1.3 Centrale vraag .....                                                  | 12        |
| 1.4 Deelvragen .....                                                      | 13        |
| 1.5 Doelstelling .....                                                    | 13        |
| 1.6 Verantwoording bronnen en methoden .....                              | 13        |
| 1.7 Leeswijzer.....                                                       | 15        |
| <b>Hoofdstuk 2 Belangrijkste bepalingen uit de AVG voor Merford .....</b> | <b>16</b> |
| 2.1 Wat houdt de AVG in? .....                                            | 16        |
| 2.1.1 Totstandkoming.....                                                 | 16        |
| 2.1.2 Vaststelling.....                                                   | 17        |
| 2.1.3 Doelstelling.....                                                   | 17        |
| 2.1.4 Inwerkingtreding .....                                              | 17        |
| 2.1.5 Toepassingsgebied .....                                             | 17        |
| 2.2 De belangrijkste bepalingen uit de AVG voor Merford .....             | 18        |
| 2.2.1 Definities .....                                                    | 18        |
| 2.2.2 Verwerkingsbeginselen.....                                          | 18        |
| 2.2.3 Rechtmatigheid verwerking .....                                     | 20        |
| 2.2.4 Rechten van de betrokkene.....                                      | 21        |
| 2.2.5 Verplichtingen verwerkingsverantwoordelijke .....                   | 23        |
| 2.2.6 Onafhankelijke toezichthoudende autoriteiten .....                  | 28        |
| 2.2.7 Europees Comité voor gegevensbescherming .....                      | 28        |
| 2.2.8 Sancties .....                                                      | 28        |
| 2.3 Tussenconclusie .....                                                 | 29        |
| <b>Hoofdstuk 3 Privacyverklaringen van Merford versus de AVG.....</b>     | <b>30</b> |
| 3.1 Privacyverklaring Merford Holding B.V. ....                           | 30        |
| 3.1.1 Gebruik van persoonsgegevens .....                                  | 30        |
| 3.1.2 Reclame .....                                                       | 30        |
| 3.1.3 Contactformulier en nieuwsbrief .....                               | 30        |
| 3.1.4 Locatiegegevens .....                                               | 31        |
| 3.1.5 Publicatie en verstrekking aan derden .....                         | 31        |
| 3.1.6 Cookies .....                                                       | 31        |
| 3.1.7 Google Analytics en Hotjar .....                                    | 32        |
| 3.1.8 Beveiliging .....                                                   | 33        |
| 3.1.9 Bewaartermijnen.....                                                | 33        |
| 3.1.10 Websites van derden .....                                          | 33        |
| 3.1.11 Wijzigingen in deze privacyverklaring .....                        | 33        |
| 3.1.12 Inzage en wijzigen van uw gegevens.....                            | 33        |
| 3.1.13 Autoriteit Persoonsgegevens.....                                   | 34        |
| 3.2 Privacyverklaring Akoestiekwinkel .....                               | 34        |
| 3.2.1 Gebruik van persoonsgegevens .....                                  | 34        |
| 3.2.2 Registreren.....                                                    | 34        |

|                                                    |    |
|----------------------------------------------------|----|
| 3.2.3 Afhandelen bestelling .....                  | 34 |
| 3.2.4 Reviews .....                                | 35 |
| 3.2.5 Deelname aan winacties .....                 | 35 |
| 3.2.6 Reclame .....                                | 35 |
| 3.2.7 Contactformulier en nieuwsbrief .....        | 35 |
| 3.2.8 Locatiegegevens .....                        | 36 |
| 3.2.9 Publicatie .....                             | 36 |
| 3.2.10 Verstrekking aan derden .....               | 36 |
| 3.2.11 Cookies .....                               | 36 |
| 3.2.12 Google Analytics .....                      | 36 |
| 3.2.13 Beveiliging .....                           | 37 |
| 3.2.14 Bewaartermijnen .....                       | 37 |
| 3.2.15 Verwijdering van gegevens .....             | 37 |
| 3.2.16 Websites van derden .....                   | 37 |
| 3.2.17 Wijzigingen in deze privacyverklaring ..... | 37 |
| 3.2.18 Inzage en wijzigen van uw gegevens .....    | 37 |
| 3.2.19 Autoriteit Persoonsgegevens .....           | 37 |
| 3.3 Tussenconclusie .....                          | 38 |

## **Hoofdstuk 4 Huidige werkwijze Merford versus de AVG .....39**

|                                                      |    |
|------------------------------------------------------|----|
| 4.1 Verzameling en verwerking persoonsgegevens ..... | 39 |
| 4.2 Bewaartermijnen .....                            | 40 |
| 4.3 Realisatie rechten van betrokkene .....          | 40 |
| 4.4 Beveiliging .....                                | 41 |
| 4.5 Privacy by design and privacy by default .....   | 41 |
| 4.6 Datalekken .....                                 | 42 |
| 4.7 Functionaris gegevensbescherming .....           | 42 |
| 4.8 Doorgifte persoonsgegevens .....                 | 42 |
| 4.9 Samenwerking met partijen buiten de EU .....     | 43 |
| 4.10 Tussenconclusie .....                           | 43 |

## **Hoofdstuk 5 Wijzigingen om AVG-proof te worden .....44**

|                                                     |    |
|-----------------------------------------------------|----|
| 5.1 Privacyverklaring Merford Holding B.V. ....     | 44 |
| 5.1.1 Inleiding privacyverklaring .....             | 44 |
| 5.1.2 Reclame .....                                 | 44 |
| 5.1.3 Contactformulier en nieuwsbrief .....         | 44 |
| 5.1.4 Locatiegegevens .....                         | 44 |
| 5.1.5 Verstrekking aan derden .....                 | 45 |
| 5.1.6 Cookies .....                                 | 45 |
| 5.1.7 Google Analytics en Hotjar .....              | 45 |
| 5.1.8 Bewaartermijnen .....                         | 45 |
| 5.1.9 Inzage en wijzigen van persoonsgegevens ..... | 45 |
| 5.2 Privacyverklaring Akoestiekwinkel .....         | 45 |
| 5.2.1 Inleiding privacyverklaring .....             | 46 |
| 5.2.2 Registratie .....                             | 46 |
| 5.2.3 Afhandelen bestelling .....                   | 46 |
| 5.2.4 Deelname aan winacties .....                  | 46 |
| 5.2.5 Reclame .....                                 | 46 |
| 5.2.6 Contactformulier en nieuwsbrief .....         | 46 |
| 5.2.7 Locatiegegevens .....                         | 46 |
| 5.2.8 Publicatie .....                              | 47 |
| 5.2.9 Verstrekking aan derden .....                 | 47 |
| 5.2.10 Cookies .....                                | 47 |
| 5.2.11 Google Analytics .....                       | 47 |
| 5.2.12 Bewaartermijnen .....                        | 47 |

|                                                         |           |
|---------------------------------------------------------|-----------|
| 5.2.13 Verwijdering van gegevens.....                   | 47        |
| 5.3 Werkwijze .....                                     | 47        |
| 5.3.1 Verzameling en verwerking persoonsgegevens.....   | 47        |
| 5.3.2 Bewaartermijnen.....                              | 48        |
| 5.3.3 Realisatie rechten van betrokkenen.....           | 48        |
| 5.3.4 Beveiliging .....                                 | 48        |
| 5.3.5 Privacy by design and privacy by default .....    | 48        |
| 5.3.6 Datalekken .....                                  | 49        |
| 5.3.7 Functionaris gegevensbescherming .....            | 49        |
| 5.3.8 Doorgifte persoonsgegevens.....                   | 49        |
| 5.3.9 Bewustwording creëren .....                       | 49        |
| 5.4 Overig .....                                        | 49        |
| 5.4.1 Gegevensbeschermingsbeleid.....                   | 49        |
| 5.4.2 Verwerkingsregister .....                         | 50        |
| 5.4.3 Data Privacy Impact Assessment .....              | 50        |
| 5.5 Tussenconclusie .....                               | 50        |
| <b>Hoofdstuk 6 Conclusies en aanbevelingen .....</b>    | <b>51</b> |
| 6.1 Privacyverklaring Merford Holding B.V. ....         | 51        |
| 6.1.1 Conclusies.....                                   | 51        |
| 6.1.2 Aanbevelingen.....                                | 51        |
| 6.2 Privacyverklaring Akoestiekwinkel.....              | 52        |
| 6.2.1 Conclusies.....                                   | 52        |
| 6.2.2 Aanbevelingen.....                                | 53        |
| 6.3 Huidige werkwijze .....                             | 54        |
| 6.3.1 Conclusies.....                                   | 54        |
| 6.3.2 Aanbevelingen.....                                | 55        |
| <b>Bronnenlijst .....</b>                               | <b>56</b> |
| <b>Bijlagen</b>                                         |           |
| <b>Bijlage 1 Privacyverklaring Merford Holding B.V.</b> |           |
| <b>Bijlage 2 Privacyverklaring Akoestiekwinkel</b>      |           |
| <b>Bijlage 3 Verwerkersovereenkomst Google</b>          |           |
| <b>Bijlage 4 Verwerkersovereenkomst Hotjar</b>          |           |
| <b>Bijlage 5 Verwerkersovereenkomst Kiyoh</b>           |           |
| <b>Bijlage 6 Verwerkersovereenkomst MailCampaigns</b>   |           |
| <b>Bijlage 7 Interview 1</b>                            |           |
| <b>Bijlage 8 Interview 2</b>                            |           |
| <b>Bijlage 9 Interview 3</b>                            |           |
| <b>Bijlage 10 Interview 4</b>                           |           |
| <b>Bijlage 11 Interview 5</b>                           |           |

## Samenvatting

Merford is een familiebedrijf waar innovatieve en technisch hoogwaardige producten worden geproduceerd. Gedacht kan worden aan ergonomische cabines voor kranen, vaar- en voertuigen, geluidstudio's en speciale deuren. Merford heeft te maken met het verwerken van persoonsgegevens. Tot 25 mei 2018 had elke lidstaat in de EU een eigen privacywetgeving. Vanaf 25 mei 2018 is in de hele EU dezelfde privacywetgeving van toepassing, namelijk de AVG. De AVG is ook van toepassing voor Merford. Er is namelijk sprake van een geautomatiseerde verwerking door Merford. Verder is Merford gevestigd in Nederland en verwerkt zij een deel van de persoonsgegevens binnen de organisatie zelf. De AVG heeft aanmerkelijk meer impact op organisaties dan gedacht. Ook Merford is zich bewust van de implicaties. Indien de AVG niet of niet juist wordt toegepast, kunnen er boeten worden opgelegd tot twintig miljoen euro of tot vier procent van de totale wereldwijde jaaromzet, indien dit cijfer hoger is dan twintig miljoen euro. Merford wil graag weten welke processen moeten worden herzien om volledig te voldoen aan de AVG. Dit rapport betreft een onderzoek naar de privacyverklaringen en de huidige werkwijze met betrekking tot de verwerking van persoonsgegevens van de klanten en leveranciers van Merford, gelet op de relevante bepalingen uit de AVG.

Merford heeft twee privacyverklaringen, namelijk een algemene privacyverklaring en een privacyverklaring voor de webwinkel. De webwinkel verwerkt namelijk meer privacygevoelige persoonsgegevens. Beide verklaringen zijn op de website van Merford te vinden en zijn uitgebreid geanalyseerd. Zowel de algemene privacyverklaring als de privacyverklaring van de webwinkel blijken nog niet AVG-proof te zijn. Uit het onderzoek blijkt dat de inleiding van de privacyverklaring van Merford niet voldoet aan de AVG. Ook de paragrafen contactformulier en nieuwsbrief, Google Analytics, Hotjar en inzage en wijzigen van uw gegevens voldoen niet aan de AVG. De paragraaf AP voldoet wel aan de AVG. Voor de overige paragrafen geldt dat deze niet in strijd zijn met de AVG, maar als onduidelijk kunnen worden ervaren door de betrokkene. Het wordt aanbevolen dat Merford de paragrafen die in strijd zijn met de AVG aanpast, zodat deze AVG-proof zijn. Verder is het gewenst om de paragrafen die een toelichting vereisen, indien mogelijk, nader toe lichten. Uit het onderzoek naar de privacyverklaring van de webwinkel blijkt dat de inleiding ook niet voldoet aan de AVG. Verder voldoen de paragrafen contactformulier en nieuwsbrief en Google Analytics niet aan de AVG. De paragrafen reviews, AP en inzage en wijzigen van uw gegevens voldoen volledig aan de AVG. De overige paragrafen zijn niet in strijd met de AVG, maar kunnen als onduidelijk worden ervaren door de minimale toelichting. Het verdient te aanbeveling dat Merford de paragrafen in de privacyverklaring van de webwinkel, die in strijd zijn met de AVG, zo snel mogelijk aanpast. Verder is het gewenst om de paragrafen die toelichting vereisen, nader toe te lichten.

Om achter de huidige werkwijze van Merford te komen zijn voor dit onderzoek vijf medewerkers geïnterviewd die verschillende functies bekleden. De huidige werkwijze is vervolgens getoetst aan de AVG. Uit het onderzoek blijkt dat de verzameling en verwerking van de persoonsgegevens, de beveiliging, het gegevensbeschermingsbeleid en het verwerkingsregister nog niet conform de AVG zijn. Ook blijkt dat de bewaartermijnen, realisatie rechten van betrokkenen en uitwisseling persoonsgegevens niet volledig AVG-proof zijn. Verder blijkt uit het onderzoek dat de privacy by design and privacy by default en de samenwerking met partijen buiten de EU volledig voldoen aan de AVG. Ten slotte blijkt uit het onderzoek dat een FG en DPIA niet verplicht zijn voor Merford. Het is aan te bevelen dat Merford de procedure van verzameling en verwerking van de persoonsgegevens aanpast. Ook is het aan te bevelen dat Merford procedures opstelt voor de verwijdering van de persoonsgegevens, de bewaartermijnen en om de beveiliging te testen te beoordelen en te evalueren. Verder verdient het de aanbeveling dat Merford een blokkade op het systeem zet voor de gegevensuitwisseling. Ten slotte wordt aanbevolen om een verwerkingsregister bij te houden en om een gegevensbeschermingsbeleid op te stellen, zodat er niet in strijd wordt gehandeld met de AVG.

## Lijst van afkortingen

|              |                                                            |
|--------------|------------------------------------------------------------|
| AP           | Autoriteit Persoonsgegevens                                |
| AVG          | Algemene Verordening Gegevensbescherming                   |
| DPIA         | Data Privacy Impact Assessment                             |
| EC           | Europees Comité voor gegevensbescherming                   |
| EU           | Europese Unie                                              |
| FG           | Functionaris voor gegevensbescherming                      |
| Handvest     | Handvest van de grondrechten van de Europese Unie          |
| HvJ EU       | Hof van Justitie van de Europese Unie                      |
| Jo.          | Juncto                                                     |
| KvK          | Kamer van Koophandel                                       |
| MAM          | Merford Acoustic Materials                                 |
| MSD          | Merford Special Doors                                      |
| MvT          | Memorie van Toelichting                                    |
| NAW-gegevens | Naam, adres en woonplaats                                  |
| NJB          | Nederlands Juristenblad                                    |
| P&I          | Privacy & Informatie                                       |
| PbEG         | Publicatieblad van de Europese Gemeenschappen              |
| PbEU         | Publicatieblad van de Europese Unie                        |
| Richtlijn    | Europese richtlijn bescherming persoonsgegevens (85/46/EG) |
| UAVG         | Uitvoeringswet Algemene verordening gegevensbescherming    |
| VWEU         | Verdrag betreffende de werking van de Europese Unie        |
| Wbp          | Wet bescherming persoonsgegevens                           |

## Begrippenlijst

### Bestand

Elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn. De persoonsgegevens moeten via criteria, zoals naam of andere kenmerken van personen, te vinden of te selecteren zijn.<sup>2</sup> Hierbij maakt het niet uit of het geheel gecentraliseerd is of gedecentraliseerd is, dan wel op functionele of geografische gronden is verspreid.<sup>3</sup>

### Betrokkene

De betrokkene is degene van wie persoonsgegevens worden verwerkt.<sup>4</sup>

### Inbreuk in verband met persoonsgegevens

Een inbreuk op de beveiliging van de persoonsgegevens. Een inbreuk doet zich voor indien er sprake is van een vernietiging, een verlies, een wijziging, een verstrekking of een toegang tot persoonsgegevens. Een inbreuk kan per ongeluk geschieden (zoals bij een brand) of op onrechtmatige wijze (zoals misbruik van andermans computer).<sup>5</sup>

### Persoonsgegevens

Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd aan de hand van een identicator zoals een naam, identificatienummer, locatiegegevens, een online identicator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.<sup>6</sup>

### Pseudonimisering

Het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt. Deze aanvullende gegevens moeten apart worden bewaard en er moeten technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld.<sup>7</sup>

### Toestemming

Voor de toestemming van de betrokkene om de gegevens te verwerken, geldt dat deze vrijwillig moet worden gegeven. De toestemming moet gericht zijn op een specifieke verwerking. Ten slotte moet de toestemming berusten op informatie en moet deze ondubbelzinnig zijn. De betrokkene moet in duidelijke en eenvoudige taal zijn geïnformeerd over het wat en hoe.<sup>8</sup>

### Vestiging

Iedere duurzame, reële en daadwerkelijke activiteit in een lidstaat, zelfs indien deze activiteit slechts gering is.<sup>9</sup>

---

<sup>2</sup> Engelfriet, Chew-Meij & Kager 2018, p. 25.

<sup>3</sup> Artikel 4 lid 6 AVG.

<sup>4</sup> Versmissen, Terstegge & Krijgsman 2017, p. 19.

<sup>5</sup> Engelfriet, Chew-Meij & Kager 2018, p. 30.

<sup>6</sup> Artikel 4 lid 1 AVG.

<sup>7</sup> Artikel 4 lid 5 AVG.

<sup>8</sup> Engelfriet, Chew-Meij & Kager 2018, p. 28-29.

<sup>9</sup> HvJ EU 1 oktober 2016, C-230/14 (*Weltimmo*).

**Verwerking**

Eén of meerdere bewerkingen met betrekking tot (een geheel van) persoonsgegevens. Hierbij is het niet van belang of de bewerking geautomatiseerd of handmatig wordt verricht. Onder verwerking moet onder andere worden verstaan het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, verspreiden, combineren, afschermen, wissen of vernietigen van persoonsgegevens.<sup>10</sup>

**Verwerker**

De verwerker is degene die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.<sup>11</sup>

**Verwerkingsverantwoordelijke**

Een natuurlijke persoon, rechtspersoon, overheidsinstantie, een dienst of een ander orgaan die, alleen of samen met anderen, het doel van en de middelen voor de verwerking van de persoonsgegevens vaststelt.<sup>12</sup>

---

<sup>10</sup> Artikel 4 lid 2 AVG.

<sup>11</sup> Artikel 4 lid 8 AVG.

<sup>12</sup> Artikel 4 lid 7 AVG.

## Hoofdstuk 1 Inleiding

In dit inleidende hoofdstuk wordt eerst een omschrijving gegeven van de organisatie. Vervolgens wordt in de probleemomschrijving de aanleiding van het onderzoek beschreven. Aan de hand van de probleemomschrijving zijn de vraagstelling, met deelvragen, en doelstelling geformuleerd. Hierna worden per deelvraag de bronnen en methoden verantwoord. Ten slotte volgt de leeswijzer van dit onderzoek.

### 1.1 De organisatie

Merford is een krachtig familiebedrijf in het midden van Nederland, waar innovatieve en technisch hoogwaardige producten worden geproduceerd. Gedacht kan worden aan ergonomische cabines voor kranen, vaar- en voertuigen, geluidsstudio's en speciale deuren. Ieder mens heeft recht op een gezonde, veilige en comfortabele woon- werk- en leefomgeving. Dat lijkt vanzelfsprekend, maar Merford ziet elke dag weer hoeveel er verbeterd kan worden aan de omgeving. Hierbij kan gedacht worden aan het lawaai van fabrieksmachines, de houding van een kraanmachinist, of de swingende beat uit de discotheek. Merford biedt voor elke specifieke situatie de juiste oplossing. De organisatie van ruim 180 medewerkers wordt aangestuurd door een inspirerende en jonge directie met een heldere visie voor de toekomst. De organisatie bestaat uit vijf business units met zelfstandige aansturing, waarbij de verantwoordelijkheid zo laag mogelijk in de organisatie ligt.<sup>13</sup>

### 1.2 Probleemomschrijving

Merford is door de jaren heen uitgegroeid tot een bedrijf met een diversiteit aan producten en diensten, onderverdeeld in vijf business units. De business units bestaan uit: Merford Noise Control, Merford Special Doors (hierna: MSD), Merford Cabins, Merford Acoustic Materials (hierna: MAM) en Merford Plaatbewerking. De klant staat centraal bij Merford. De medewerkers werken dan ook altijd samen met de klanten om zo tot de beste resultaten te komen. Samen bouwen ze een waardevolle en langdurige relatie op, waarin eerlijkheid, openheid en creativiteit centraal staan en waar de kwaliteit van de geleverde producten voorop staat.<sup>14</sup> Merford heeft ook te maken met het verwerken van persoonsgegevens. Hierbij moet gedacht worden aan het verwerken van persoonsgegevens van medewerkers, sollicitanten, klanten en leveranciers. Verder worden er nieuwsbrieven verstuurd naar de belangstellenden. Ook hiervoor zijn persoonlijke gegevens nodig, evenals bij het plaatsen van een bestelling in de webwinkel van MAM. Verder heeft Merford twee privacyverklaringen die openbaar staan. Deze zijn te vinden op de website van Merford<sup>15</sup> en op de webwinkel van MAM<sup>16</sup>. Deze verklaringen voldoen aan de Wet bescherming persoonsgegevens (hierna: Wbp) en zijn van belang voor de toetsing aan de vernieuwde privacywetgeving.

Tot 25 mei 2018 had elke lidstaat in de Europese Unie (hierna: EU) een eigen privacywetgeving. Deze nationale wetten waren gebaseerd op de Europese richtlijn bescherming persoonsgegevens (85/46/EG)<sup>17</sup> (hierna: richtlijn) uit 1995. Deze richtlijn was in de Wbp geïmplementeerd.<sup>18</sup>

Tussen 1995 en nu is de samenleving gedigitaliseerd, waardoor er een enorme stijging is in het dataverkeer. Ook de technologie ontwikkelt zich steeds sneller. Het gevolg hiervan is een toename in het verzamelen en delen van gegevens, een toename in de risico's van cybercrime en een toename in de vraag van de burger wat er met zijn of haar persoonsgegevens wordt gedaan. De wetgeving was toe aan vernieuwing en zo is de Algemene Verordening Gegevensbescherming (hierna: AVG) voorgesteld door de Europese

---

<sup>13</sup> [www.merford.com](http://www.merford.com) (zoek op over Merford, organisatie).

<sup>14</sup> [www.merford.com](http://www.merford.com) (zoek op over Merford, organisatie).

<sup>15</sup> [www.merford.com](http://www.merford.com).

<sup>16</sup> [www.akoestiekwinkel.nl](http://www.akoestiekwinkel.nl).

<sup>17</sup> Richtlijn 65/46/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 (PbEG 1995, L 281/31).

<sup>18</sup> [www.autoriteitpersoonsgegevens.nl](http://www.autoriteitpersoonsgegevens.nl) (zoek op algemene informatie AVG).

Commissie.<sup>19</sup> Vanaf 25 mei 2018 is in de hele EU dezelfde privacywetgeving van toepassing, namelijk de AVG<sup>20</sup>. De AVG vervangt de richtlijn en de Wbp.<sup>21</sup>

De Europese richtlijn bescherming persoonsgegevens van 1995 is, zoals de naam al zegt, een richtlijn en de AVG is een verordening. Tussen een richtlijn en een verordening zit een verschil. Een richtlijn is een aanwijzing voor een te volgen gedrag.<sup>22</sup> De richtlijn is een rechtshandeling die een bepaald doel vastlegt dat de EU-landen moeten bereiken, maar de landen mogen zelf de wetgeving vaststellen om dat doel te bereiken. Een richtlijn is dus geen dwingend voorschrift. Een verordening is daarentegen een uitgevaardigde bindende regeling.<sup>23</sup> De verordening is een bindende rechtshandeling die in de hele EU van toepassing is.<sup>24</sup> De AVG is na de inwerkingtreding in de hele EU van toepassing.

De privacywetgeving is een actueel onderwerp en de invoering van de AVG heeft aanmerkelijk meer impact op organisaties dan gedacht. Ook Merford is zich bewust van de implicaties. Aangezien Merford gebruik maakt van persoonlijke gegevens, is het van belang dat deze gewaarborgd worden. Eenieder heeft namelijk recht op eerbiediging van zijn persoonlijke levenssfeer.<sup>25</sup> Dit grondrecht is verankerd in de Nederlandse grondwet. Grondrechten zijn rechten die burgers de vrijheid geven om zonder bemoeienis van de overheid te leven.<sup>26</sup>

Indien de AVG, niet of niet juist wordt toegepast, kunnen er boeten worden opgelegd tot twintig miljoen euro of tot vier procent van de totale wereldwijde jaaromzet, indien dit cijfer hoger is dan twintig miljoen euro.<sup>27</sup> Geen enkele organisatie wil zo een grote boete riskeren, dit geldt ook voor Merford. Merford wil graag weten welke processen moeten worden herzien om volledig aan de AVG te voldoen. Aangezien er een beperkte tijd beschikbaar was voor dit onderzoek, wordt in dit onderzoek de nadruk gelegd op de verwerking van persoonsgegevens van klanten en leveranciers en op de privacyverklaringen van Merford. Hierbij worden alleen de relevante bepalingen uit de AVG voor Merford behandeld. Voor het onderzoek naar de verwerking van persoonsgegevens van klanten en leveranciers en de privacyverklaringen, wordt een onderzoek naar het recht en een onderzoek naar de praktijk verricht. Naar aanleiding hiervan is het voor Merford duidelijk wat, indien nodig, veranderd moet worden met betrekking tot de verwerking van persoonsgegevens van klanten en leveranciers en de privacyverklaringen. Tevens wordt een flyer opgesteld voor Merford.

### 1.3 Centrale vraag

Uit de probleemomschrijving is de volgende centrale vraag naar voren gekomen:

*Welke aanbevelingen kunnen, gelet op de relevante bepalingen uit de AVG, aan Merford worden gegeven ten aanzien van de privacyverklaringen en de huidige werkwijze met betrekking tot de verwerking van de persoonsgegevens van haar klanten en leveranciers?*

---

<sup>19</sup> [www.europadecentraal.nl](http://www.europadecentraal.nl) (zoek op *de nieuwe privacywet: de Algemene Verordening Gegevensbescherming*).

<sup>20</sup> Verordening (EU) 2016/679 van het Europees Parlement en Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PbEU 2016, L 119/1).

<sup>21</sup> [www.autoriteitpersoonsgegevens.nl](http://www.autoriteitpersoonsgegevens.nl) (zoek op *algemene informatie AVG*).

<sup>22</sup> [www.vandale.nl](http://www.vandale.nl) (zoek op *richtlijn*).

<sup>23</sup> [www.vandale.nl](http://www.vandale.nl) (zoek op *verordening*).

<sup>24</sup> [www.europa.eu](http://www.europa.eu) (zoek op *verordeningen, richtlijnen en andere rechtshandelingen*).

<sup>25</sup> Artikel 10 Grondwet.

<sup>26</sup> [www.rijksoverheid.nl](http://www.rijksoverheid.nl) (zoek op *Grondwet en Statuut*).

<sup>27</sup> Artikel 83 AVG.

## 1.4 Deelvragen

Om de centrale vraag goed te beantwoorden, worden eerst de onderstaande deelvragen beantwoord:

1. Wat houdt de AVG in en wat zijn de belangrijkste bepalingen uit de AVG voor Merford?
2. Voldoen de huidige privacyverklaringen van Merford aan de AVG?
3. Voldoet de huidige werkwijze van Merford, met betrekking tot de verwerking van persoonsgegevens van haar klanten en leveranciers, aan de AVG?
4. Welke wijzigingen moet Merford doorvoeren om AVG-proof te zijn?

## 1.5 Doelstelling

Naar aanleiding van de voorgaande paragrafen geschetste situatie is de volgende doelstelling opgesteld:

*Het doel van dit onderzoek is om uiterlijk vrijdag 12 oktober 2018 een onderzoeksrapport te overhandigen aan mevrouw A. Vertooren, algemeen directeur van Merford, waarin conclusies worden getrokken en aanbevelingen worden gegeven over de privacyverklaringen en de verwerking van persoonsgegevens van klanten en leveranciers binnen Merford. Naar aanleiding van dit onderzoek kan Merford, indien nodig, de privacyverklaringen, de werkwijze van de verwerking van de persoonsgegevens aanpassen en de auteur van dit onderzoek een flyer laten opstellen voor de medewerkers.*

## 1.6 Verantwoording bronnen en methoden

Hieronder wordt per deelvraag aangegeven welke onderzoeksstrategie en methoden er zijn gebruikt en welke bronnen zijn geraadpleegd. Tevens is per deelvraag verantwoord waarom gebruik is gemaakt van de betreffende strategie, methode en bronnen.

### *1. Wat houdt de AVG in en wat zijn de belangrijkste bepalingen uit de AVG voor Merford?*

Voor de beantwoording van deze deelvraag is eerst een onderzoek verricht naar de inhoud van de AVG. Hierbij is de totstandkoming, de vaststelling, de doelstelling, de inwerkingtreding en de reikwijdte onderzocht. Vervolgens is een onderzoek verricht naar de AVG zelf. Als onderzoeksstrategie is gebruik gemaakt van rechtsbronnen- en literatuuronderzoek. Voor een onderzoek naar het recht, in dit geval de AVG, is een rechtsbronnen- en literatuuronderzoek de meeste gebruikte strategie. De methode die hier is toegepast, is een inhoudsanalyse. Om informatie te verkrijgen over de AVG zijn diverse bestaande bronnen geanalyseerd. De bronnen die voor de beantwoording van deze deelvraag zijn gebruikt, zijn: rechtsbronnen, literatuur en documenten. Rechtsbronnen zijn betrouwbare bronnen, omdat deze normen bevatten die hun gezag ontleen aan de autoriteit die de normen heeft gesteld.<sup>28</sup> De rechtsbronnen die voor deze deelvraag zijn gebruikt, zijn: wetten, verdragen en jurisprudentie. Verder is gebruik gemaakt van literatuur in de vorm van boeken en tijdschriften. Het voordeel van wetenschappelijk literatuur is dat deze over het algemeen beschouwd kan worden als een betrouwbare en controleerbare bron van kennis.<sup>29</sup> De boeken en tijdschriften zijn geraadpleegd via de mediatheek van de Juridische Hogeschool en via de databanken die beschikbaar zijn gesteld door de Juridische Hogeschool zoals Legal Intelligence, Kluwer Navigator en Sdu OpMaat. Ook is er gebruik gemaakt van documenten voor de beantwoording van deze deelvraag, zoals de Memorie van Toelichting (hierna: MvT). Het gebruik van documenten heeft als voordeel dat ze eindeloos geraadpleegd kunnen worden. Verder spelen bij documenten geen reactieve effecten een rol. Hier kan sprake van zijn, wanneer bepaald gedrag wordt uitgelokt. Van uitgelokt gedrag is sprake als er vragen worden gesteld aan personen. Strategische of sociale wenselijke antwoorden kunnen dan een rol gaan spelen.<sup>30</sup>

---

<sup>28</sup> Schaaijk 2015, p. 98.

<sup>29</sup> Schaaijk 2015, p. 100.

<sup>30</sup> Schaaijk 2015, p. 100.

## *2. Voldoen de huidige privacyverklaringen van Merford aan de AVG?*

Voor de beantwoording van deze deelvraag is een onderzoek naar de praktijk verricht. Als onderzoeksstrategie is gebruik gemaakt van een casestudy. De onderzoeksmethode die voor deze deelvraag is toegepast, is een inhoudsanalyse. De documenten die geanalyseerd zijn, zijn de privacyverklaringen van Merford. Er is gekeken naar wat er met de tekstfragmenten wordt bedoeld, niet alleen wat deze letterlijk schrijft of zegt, maar ook wat geïnterpreteerd kan worden door de gebruikers.<sup>31</sup> Zoals hierboven is aangegeven, heeft Merford twee privacyverklaringen die openbaar staan. De bronnen die zijn geraadpleegd zijn documenten, literatuur en media. De documenten die zijn geraadpleegd, zijn de privacyverklaringen die Merford heeft. Dit gaat gepaard met media, omdat de privacyverklaringen ook te vinden zijn via het internet. De bevindingen uit de privacyverklaring zijn getoetst aan de AVG.

## *3. Voldoet de huidige werkwijze van Merford, met betrekking tot de verwerking van persoonsgegevens van haar klanten en leveranciers, aan de AVG?*

Voor de beantwoording van deze deelvraag is ook een onderzoek naar de praktijk verricht. Hier wordt als onderzoeksstrategie gebruik gemaakt van een veldonderzoek aangevuld met een casestudy. De onderzoeksmethode die voor deze deelvraag is gebruikt, is een interview. In totaal zijn vijf personen geïnterviewd. De eerste persoon die geïnterviewd is, heeft te maken met het invoeren van orders.<sup>32</sup> Ten tweede is een persoon geïnterviewd die applicatiebeheerder is en veel over de systemen van Merford weet.<sup>33</sup> Ten derde is iemand geïnterviewd die te maken heeft met projecten en klantenorders.<sup>34</sup> De vierde persoon die geïnterviewd is, houdt zich bezig met de webwinkel en de nieuwsbrieven.<sup>35</sup> Ten slotte is iemand geïnterviewd die te maken heeft met leveranciers.<sup>36</sup> Samen hebben zij kunnen aangeven wat de huidige werkwijze van Merford is met betrekking tot de verwerking van de persoonsgegevens. De vijf business units van Merford hebben wat betreft klanten en leveranciers te maken met gelijke processen, daarom is er bewust voor gekozen om niet één persoon per business unit te interviewen. De bronnen die voor deze deelvraag zijn geraadpleegd, zijn: documenten, literatuur en personen. De personen die zijn geraadpleegd, hebben informatie kunnen geven over situaties en processen. Voor het interview is gebruik gemaakt van individuele face-to-face gesprekken. De gesprekken zijn, met toestemming van de geïnterviewden, opgenomen. Tijdens de interviews zijn er ook geschreven notities gemaakt. Het opnemen van een interview heeft als grote voordeel dat het letterlijke gesprek binnen handbereik is en het teruggeluisterd kan worden. Het interview was half gestructureerd. Vooraf is op papier geschreven welke vragen er moeten beantwoord worden en welke onderwerpen aan bod moeten komen. De bevindingen over de huidige werkwijze van Merford zijn getoetst aan de AVG.

## *4. Welke wijzigingen moet Merford doorvoeren om AVG-proof te zijn?*

Voor de laatste deelvraag is ook een casestudy als onderzoeksstrategie gebruikt. De onderzoeksmethode die voor deze deelvraag is gebruikt, is een inhoudsanalyse. Het gevonden en verzamelde materiaal is met elkaar vergeleken, om te controleren of de privacyverklaringen en de huidige werkwijze voldoen aan de nieuwe privacywetgeving. Op basis hiervan worden conclusies getrokken en aanbevelingen gegeven. De bronnen die voor deze deelvraag zijn gebruikt, zijn literatuur en media. De media hebben zowel voor- als nadelen. Een voordeel van het gebruik van media is dat het een zeer snelle en goedkope manier is om gegevens te verzamelen. Andere voordelen zijn, de hoge actualiteit en informatiedichtheid. Het nadeel is dat de informatie niet of nauwelijks gecontroleerd wordt en een vluchtig karakter kan hebben.<sup>37</sup> Het is dan ook belangrijk dat de bronnen die via het

---

<sup>31</sup> Schaaijk 2015, p. 103.

<sup>32</sup> Bijlage 7 Interview 1.

<sup>33</sup> Bijlage 8 Interview 2.

<sup>34</sup> Bijlage 9 Interview 3.

<sup>35</sup> Bijlage 10 Interview 4.

<sup>36</sup> Bijlage 11 Interview 5.

<sup>37</sup> Schaaijk 2015, p. 101-102.

internet geraadpleegd worden, betrouwbare bronnen zijn. Daarom zijn er niet willekeurige websites gebruikt, maar zijn de websites onderzocht op betrouwbaarheid.

### 1.7 Leeswijzer

Dit onderzoeksrapport bestaat uit zes hoofdstukken. In het eerste hoofdstuk wordt het onderzoek ingeleid. Het tweede hoofdstuk van dit onderzoeksrapport geeft informatie weer over de geschiedenis van de AVG en de belangrijkste bepalingen uit de AVG voor Merford. In het derde hoofdstuk van dit onderzoeksrapport worden de huidige privacyverklaringen van Merford getoetst aan de AVG. Het vierde hoofdstuk van dit onderzoeksrapport beschrijft de toetsing van de huidige werkwijze van Merford met betrekking tot de verwerking van persoonsgegevens van haar klanten en leveranciers aan de AVG. In het vijfde hoofdstuk van dit rapport wordt besproken welke wijzigingen Merford moet doorvoeren om AVG-proof te worden. Ten slotte staan in het laatste hoofdstuk de conclusies en aanbevelingen op basis van de gedane bevindingen.

## Hoofdstuk 2 Belangrijkste bepalingen uit de AVG voor Merford

In dit hoofdstuk wordt eerst beschreven wat de AVG inhoudt. Hierbij wordt de geschiedenis van de AVG besproken. Hierna volgt een analyse met belangrijkste bepalingen uit de AVG voor Merford. Ten slotte volgt de conclusie van dit hoofdstuk.

### 2.1 Wat houdt de AVG in?

In deze paragraaf wordt eerst besproken op welke manier de AVG tot stand is gekomen. Hierna worden de vaststelling en de doelstelling van de AVG besproken. Vervolgens wordt de inwerkingtreding van de AVG besproken en ten slotte wordt het toepassingsgebied van de AVG besproken.

#### 2.1.1 Totstandkoming

Regelingen op het gebied van de bescherming van de persoonlijke levenssfeer in Europees verband bestaan al sinds de Tweede Wereldoorlog. Het Verdrag van Straatsburg<sup>38</sup> van 28 januari 1981 was destijds van belang om belemmering van het vrije verkeer van persoonsgegevens te voorkomen. Het verdrag leidde echter tot interpretatieverschillen. Ter harmonisatie verscheen in 1995 daarom de richtlijn. De nadere invulling van deze richtlijn werd aan de afzonderlijke lidstaten overgelaten. In de praktijk leidde dit alsnog tot grote interpretatieverschillen. Bovendien liep de invulling van de richtlijn niet parallel met de technologische ontwikkeling van het aanbod van diensten in de informatiemaatschappij. Om die reden besloot de Europese Commissie te komen met een verordening, die bindend is voor alle lidstaten.<sup>39</sup>

De rechtsgrondslag voor de AVG kent twee dimensies. Ten eerste is er een grondrechtelijke dimensie en ten tweede is er een wetgevingsdimensie. De grondrechtelijke dimensie ligt verankerd in het Handvest van de grondrechten van de Europese Unie<sup>40</sup> (hierna: Handvest). Het Handvest garandeert eenieder recht op bescherming van zijn persoonsgegevens.<sup>41</sup> Deze gegevens moeten eerlijk worden verwerkt, voor bepaalde doeleinden en met de toestemming van de betrokkene of met een andere gerechtvaardigde grondslag. Eenieder heeft recht op toegang over zijn verzamelde gegevens en recht op rectificatie daarvan.<sup>42</sup> Ten slotte staat in het Handvest over de bescherming van persoonsgegevens dat een onafhankelijke autoriteit toeziet op de naleving van de bovenstaande regels.<sup>43</sup> De tweede dimensie is de wetgevingsdimensie. De rechtsgrondslag voor deze verordening is vastgelegd in het Verdrag betreffende de werking van de Europese Unie (hierna: VWEU). Hierin wordt geregeld dat het Europees Parlement en de Raad volgens de gewone wetgevingsprocedure de voorschriften vaststellen over de bescherming van natuurlijke personen ten aanzien van de verwerking van de persoonsgegevens door de instellingen, organen en instanties van de EU. Evenals door de lidstaten die bij de activiteiten binnen het toepassingsgebied van het recht van de EU vallen, alsmede de voorschriften betreffende het vrije verkeer van gegevens.<sup>44</sup> De Europese Commissie heeft in 2012 gekozen voor de indiening van een ontwerpverordening in plaats van een ontwerp-richtlijn. De wetgever is de Europese Commissie gevolgd in deze keuze.<sup>45</sup> De doelstellingen en beginselen van de richtlijn blijven geldend, maar de richtlijn heeft niet kunnen voorkomen dat het recht van de lidstaten is gaan afbrokkelen, dat er rechtsonzekerheid is ontstaan en zorg bij het publiek over een tekortschietende bescherming van persoonsgegevens bij online activiteiten.<sup>46</sup>

<sup>38</sup> Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens.

<sup>39</sup> Holvast, *P&I* 2016, p. 98.

<sup>40</sup> Handvest van de grondrechten van de Europese Unie (*PbEG* 2000, C 364/1).

<sup>41</sup> Artikel 8 lid 1 Handvest.

<sup>42</sup> Artikel 8 lid 2 Handvest.

<sup>43</sup> Artikel 8 lid 3 Handvest.

<sup>44</sup> Artikel 16 lid 2 VWEU.

<sup>45</sup> Overwegingen 9-13 AVG.

<sup>46</sup> De Jong, *Ars Aequi* 2016/10, p. 770.

### 2.1.2 Vaststelling

In Brussel werd op 27 april 2016 de AVG vastgesteld. De AVG heeft de hiervoor geldende richtlijn vervangen. De verordening, samen met een richtlijn voor gegevensbescherming op het gebied van opsporing, de vervolging en de strafrechtstoepassing,<sup>47</sup> vormen de herziening van het gegevensbeschermingsrecht van de EU.

### 2.1.3 Doelstelling

Privacyregels zijn bedoeld om de persoonlijke levenssfeer van burgers te beschermen en om te bewaken dat beroepskrachten en instellingen zorgvuldig omgaan met de persoonsgegevens van burgers.<sup>48</sup>

De doelstelling van de AVG is een krachtig en coherent kader voor gegevensbescherming in de EU, dat wordt gesteund door strenge handhaving. Dit is van belang voor het vertrouwen dat nodig is om de digitale economie zich in de EU te laten ontwikkelen en om meer rechtszekerheid te bieden.<sup>49</sup> Om de doelstelling van de AVG te bereiken, zijn regels vastgesteld betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en zijn regels vastgesteld betreffende het vrije verkeer van persoonsgegevens.<sup>50</sup> Door het reguleren van de verwerking van persoonsgegevens ontstaat een markt voor persoonsgegevens. Dit sluit aan op het vrij verkeer van diensten, wat een grondrecht is binnen de EU.<sup>51</sup>

Hoewel het doel van de AVG een geharmoniseerd gegevensbeschermingsrecht is, biedt de AVG de lidstaten toch op een aantal punten ruimte om specifieke bepalingen op te nemen. In Nederland zijn deze bepalingen vastgelegd in de Uitvoeringswet Algemene verordening gegevensbescherming (hierna: UAVG).<sup>52</sup>

### 2.1.4 Inwerkingtreding

De AVG treedt in werking op de twintigste dag na die van de bekendmaking ervan in het Publicatieblad van de Europese Unie. De AVG is bekendgemaakt op 4 mei 2016 en is in werking getreden op 25 mei 2016.<sup>53</sup> Twee jaar na de inwerkingtreding is de AVG van toepassing.<sup>54</sup> Ondernemingen hebben hiermee twee jaar de tijd gehad om hun bedrijfsvoering in overeenstemming te brengen met de AVG.

### 2.1.5 Toepassingsgebied

Om te bepalen of de AVG van toepassing is, moet er gekeken worden naar het materieel en het territoriaal toepassingsgebied. Voor het materieel toepassingsgebied geldt dat de verordening van toepassing is op de geheel of gedeeltelijke geautomatiseerde verwerking, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.<sup>55</sup> Hier is al sprake van als een handeling via ICT-middelen of het internet wordt verricht.<sup>56</sup> Een in het geheel niet geautomatiseerde verwerking valt slechts onder de AVG, indien sprake is van een bestand met persoonsgegevens.<sup>57</sup> Op de hoofdregel zijn enkele uitzonderingen van toepassing.<sup>58</sup> Zo is de AVG niet van toepassing op de activiteiten die buiten de werkingssfeer van het Unierecht

---

<sup>47</sup> Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen en betreffende het vrije verkeer van die gegevens en tot intrekking van kaderbesluit 2008/977/JBZ van de Raad (*PbEU* 2016, L 119/89).

<sup>48</sup> Janssen 2018, p. 17.

<sup>49</sup> Overweging 7 AVG.

<sup>50</sup> Artikel 1 lid 1 AVG.

<sup>51</sup> Engelfriet, Chew-Meij & Kager 2018, p.13.

<sup>52</sup> Schermer, Hagenauw & Falot 2018, p. 19.

<sup>53</sup> Artikel 99 lid 1 AVG.

<sup>54</sup> Artikel 99 lid 2 AVG.

<sup>55</sup> Artikel 2 lid 1 AVG.

<sup>56</sup> Engelfriet, Chew-Meij & Kager 2018, p.15.

<sup>57</sup> Engelfriet, Chew-Meij & Kager 2018, p.13 jo. artikel 4 lid 6 AVG.

<sup>58</sup> Artikel 2 lid 2 AVG.

vallen.<sup>59</sup> Ook is de AVG niet van toepassing voor het verwerken van persoonsgegevens voor privégebruik.<sup>60</sup> Nog een belangrijke uitzondering is dat, de AVG niet van toepassing is op de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van strafrechtelijke sancties, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid.<sup>61</sup>

Het territoriaal toepassingsgebied van de AVG is breed. De AVG is van toepassing op de verwerking van persoonsgegevens door een verwerkingsverantwoordelijke of een verwerker in de EU, ongeacht of de verwerking in de EU plaatsvindt.<sup>62</sup> Verder is de AVG van toepassing op de verwerking van persoonsgegevens van betrokkenen die zich in de EU bevinden, maar de verwerkingsverantwoordelijke of verwerker is niet gevestigd in de EU. De verwerking dient dan verband te houden met het aanbieden van goederen of diensten aan de betrokkenen of de verwerking dient verband te houden met het monitoren van het gedrag van de betrokkenen die in de EU plaatsvindt.<sup>63</sup> Ten slotte is de AVG van toepassing op de verwerking van persoonsgegevens door een verwerkingsverantwoordelijke die niet in de EU is gevestigd, maar op een plaats waar krachtens het internationaal publiekrecht, het lidstatelijke recht van toepassing is.<sup>64</sup>

Het is nu de vraag of de AVG van toepassing is voor Merford. Voor de verwerking van persoonsgegevens maakt Merford gebruik van ICT-middelen. Er is dus sprake van een geautomatiseerde verwerking. De uitzonderingen zijn niet van toepassing voor Merford, wat betekent dat aan het materieel toepassingsgebied wordt voldaan. Merford is gevestigd in Nederland, verricht haar activiteiten in de organisatie zelf en verwerkt een deel van de persoonsgegevens ook binnen de organisatie. Dit betekent dat ook aan het territoriaal toepassingsgebied wordt voldaan. Er wordt zowel aan het materieel en territoriaal toepassingsgebied voldaan, dus is de AVG voor Merford van toepassing.

## 2.2 De belangrijkste bepalingen uit de AVG voor Merford

In de vorige paragraaf is vastgesteld dat de AVG van toepassing is voor Merford. De AVG is met 99 artikelen en 173 overwegingen veelomvattend. Niet alles uit de AVG is van belang voor Merford. In deze paragraaf worden de bepalingen uit de AVG besproken die belangrijk zijn voor Merford.

### 2.2.1 Definities

In artikel 4 AVG worden de definities genoemd die van toepassing zijn voor de AVG. De definities die van belang zijn voor Merford, zijn te vinden in de begrippenlijst. De begrippenlijst is in dit onderzoeksrapport voor de inleiding te vinden.

### 2.2.2 Verwerkingsbeginselen

In artikel 5 AVG staan zes basisbeginselen opgesomd waar elke verwerking van persoonsgegevens aan moet voldoen. Hieronder worden de beginselen weergegeven met een toelichting ernaast.

| Beginselen                                                             | Toelichting                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>1. Beginsel van rechtmatigheid, behoorlijkheid en transparantie</b> | Dit beginsel houdt in dat elke verwerking van persoonsgegevens rechtmatig, behoorlijk en transparant dient te zijn. De rechtmatigheid van de verwerking wordt nader toegelicht in paragraaf 2.2.3. De verwerking moet in overeenstemming zijn met de hiervoor geldende regels en dient op een nette, juiste manier plaats te vinden. <sup>65</sup> |

<sup>59</sup> Artikel 2 lid 2 sub a AVG.

<sup>60</sup> Artikel 2 lid 2 sub c AVG.

<sup>61</sup> Artikel 2 lid 2 sub d AVG.

<sup>62</sup> Artikel 3 lid 1 AVG.

<sup>63</sup> Artikel 3 lid 2 AVG.

<sup>64</sup> Artikel 3 lid 3 AVG.

<sup>65</sup> Van den Eijnden, Jansen, Van den Bosch & Van de Pas 2018, p. 19.

|                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>2. Beginsel van doelbinding en verenigbaarheid</b>   | Dit beginsel houdt in dat persoonsgegevens alleen verzameld mogen worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Verwerking mag dus alleen gebeuren voor specifieke en gerechtvaardigde doeleinden, die zijn vastgesteld voordat de verwerking begint of voor andere doelen die daarmee verenigbaar zijn. Het doel mag, logischerwijs, niet in strijd zijn met de wet en moet dus rechtmatig zijn. <sup>66</sup>                                                                                                                                                                                                                                                                                                                                                          |
| <b>3. Beginsel van dataminimalisatie</b>                | Dit beginsel houdt in dat dat persoonsgegevens toereikend dienen te zijn, ter zake dienen te zijn en beperkt worden tot wat noodzakelijk is voor de doelen waarvoor zij worden verwerkt. Er moet voor worden gezorgd dat niet meer persoonsgegevens worden verwerkt dan noodzakelijk is. Hieruit volgt dat de gegevens zo snel mogelijk moeten worden gewist of onherkenbaar worden gemaakt. Om dit te realiseren, dient de verwerkingsverantwoordelijke termijnen vast te stellen. Verder moet de vraag gesteld worden: 'Heb ik al deze gegevens nodig of kan het met minder?' <sup>67</sup> Hierbij geldt dat honderd procent juistheid vrijwel nooit te realiseren is. De verwerkingsverantwoordelijke moet daarom een afweging maken in hoe nauwkeurig en actueel de gegevens moeten zijn. <sup>68</sup> |
| <b>4. Beginsel van juistheid</b>                        | Dit beginsel eist dat de gegevens juist en actueel moeten zijn. De verwerkingsverantwoordelijke heeft hierbij een inspanningsplicht. Indien gewerkt wordt met onjuiste of achterhaalde gegevens, kan dit vervelende gevolgen hebben voor de betrokkene. De verwerkingsverantwoordelijke moet daarom alle redelijke maatregelen nemen om de onjuiste of achterhaalde gegevens onverwijld te wissen of te rectificeren. <sup>69</sup>                                                                                                                                                                                                                                                                                                                                                                          |
| <b>5. Beginsel van opslagbeperking</b>                  | Dit beginsel houdt in dat de persoonsgegevens niet langer mogen worden bewaard dan noodzakelijk is voor de verwerking. De AVG noemt geen termijnen, maar verlangt van de verwerkingsverantwoordelijke dat deze op basis van zijn verwerkingen concrete termijnen vaststelt. Langere opslag is toegestaan ten behoeve van archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden. <sup>70</sup>                                                                                                                                                                                                                                                                                                                                                              |
| <b>6. Beginsel van integriteit en vertrouwelijkheid</b> | Dit beginsel houdt in dat de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen moet nemen. De persoonsgegevens moeten op een zodanige manier worden verwerkt dat een passende beveiliging ervan is gewaarborgd. De maatregelen dienen ervoor te zorgen dat de persoonsgegevens beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking ervan en bescherming tegen onopzettelijk verlies, vernietiging of beschadiging. <sup>71</sup>                                                                                                                                                                                                                                                                                                                                   |

<sup>66</sup> Engelfriet, Chew-Meij & Kager 2018, p. 40.

<sup>67</sup> Van den Eijnden, Jansen, Van den Bosch & Van de Pas 2018, p. 20.

<sup>68</sup> Versmissen, Terstegge & Krijgsman 2017, p. 59.

<sup>69</sup> Engelfriet, Chew-Meij & Kager 2018, p. 41.

<sup>70</sup> Engelfriet, Chew-Meij & Kager 2018, p. 42.

<sup>71</sup> Van den Eijnden, Jansen, Van den Bosch & Van de Pas 2018, p. 21.

### 2.2.3 Rechtmatigheid verwerking

De voorgaande paragraaf geeft aan welke beginselen een rol spelen bij de verwerking van persoonsgegevens. De verwerking is echter alleen rechtmatig, indien aan een van de onderstaande voorwaarden is voldaan.<sup>72</sup>

#### Toestemming

De betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden.<sup>73</sup> De definitie van toestemming is te vinden in de begrippenlijst.

In artikel 7 AVG zijn de voorwaarden voor toestemming uitgewerkt. De verwerkingsverantwoordelijke moet kunnen aantonen dat de betrokkene toestemming heeft gegeven voor de verwerking van zijn persoonsgegevens.<sup>74</sup> Indien de betrokkene schriftelijke toestemming geeft, waarvan de verklaring ook op andere aangelegenheden betrekking heeft, moet het verzoek om toestemming in een begrijpelijke en gemakkelijk toegankelijk vorm worden gepresenteerd. Tevens moet een duidelijk onderscheid worden gemaakt met de andere aangelegenheden.<sup>75</sup> Verder heeft de betrokkene te allen tijde het recht om zijn toestemming in te trekken. De betrokkene moet voor het geven van toestemming hiervan in kennis worden gesteld.<sup>76</sup> Dit heeft geen terugwerkende kracht. De eerdere verrichte verwerkingen, met de toestemming, blijven rechtmatig.<sup>77</sup> Ten slotte moet de toestemming vrijwillig worden gegeven.<sup>78</sup>

Indien de toestemming niet op de juiste wijze wordt gegeven, kan de verwerking geheel of gedeeltelijk onrechtmatig worden.<sup>79</sup>

#### Noodzakelijk voor uitvoering van een overeenkomst

De verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene voor de sluiting van een overeenkomst maatregelen te nemen.<sup>80</sup>

#### Noodzakelijk om te voldoen aan een wet

De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust.<sup>81</sup>

#### Noodzakelijk om vitale belangen te beschermen

De verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen.<sup>82</sup> Een vitaal belang raakt het leven van die persoon, zoals het verwerken van medische gegevens bij een ongeval.<sup>83</sup>

#### Noodzakelijk in verband met openbaar belang of uitvoering openbaar gezag

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.<sup>84</sup> Onder algemeen belang valt onder andere gezondheidsdoelen zoals volksgezondheid en sociale bescherming.<sup>85</sup>

#### Noodzakelijk voor belangenafweging

De verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke, behalve wanneer de belangen of grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens dienen, zwaarder wegen dan de belangenafweging.<sup>86</sup>

---

<sup>72</sup> Artikel 6 AVG.

<sup>73</sup> Artikel 6 lid 1 sub a AVG.

<sup>74</sup> Artikel 7 lid 1 AVG.

<sup>75</sup> Artikel 7 lid 2 AVG.

<sup>76</sup> Artikel 7 lid 3 AVG.

<sup>77</sup> Engelfriet, Chew-Meij & Kager 2018, p. 52.

<sup>78</sup> Artikel 7 lid 4 AVG.

<sup>79</sup> Berkvens, Vinken, Wiegerinck, Wolters, Reijner & Van Gerwen, p. 87.

<sup>80</sup> Artikel 6 lid 1 sub b AVG.

<sup>81</sup> Artikel 6 lid 1 sub c AVG.

<sup>82</sup> Artikel 6 lid 1 sub d AVG.

<sup>83</sup> Engelfriet, Chew-Meij & Kager 2018, p. 44.

<sup>84</sup> Artikel 6 lid 1 sub e AVG.

<sup>85</sup> Overweging 45 AVG.

<sup>86</sup> Artikel 6 lid 1 sub f AVG.

De verwerking van persoonsgegevens ten behoeve van direct marketing, kan worden beschouwd als uitgevoerd met het oog op gerechtvaardigd belang.<sup>87</sup>

#### 2.2.4 Rechten van de betrokkene

Hieronder worden de rechten van de betrokkene besproken. Dit is van belang voor Merford, omdat Merford aan de rechten van de betrokkene gehoor moet geven. Indien Merford dit niet doet, handelt zij niet in overeenstemming met de AVG.

##### 2.2.4.1 Recht op informatie

De betrokkene kan verzoeken aan de verwerkingsverantwoordelijke om informatie te geven over de vraag of er persoonsgegevens van hem worden verwerkt. Indien dit het geval is kan de betrokkene verzoeken om informatie over de gegevensverwerking.<sup>88</sup> Bij de verkrijging van de persoonsgegevens verstrekt de verwerkingsverantwoordelijke al diverse informatie. Dit houdt onder andere in de identiteit en contactgegevens van de verwerkingsverantwoordelijke en de contactgegevens van de functionaris voor gegevensbescherming (hierna: FG), indien deze aanwezig is. Verder wordt aangegeven wat de verwerkingsdoeleinden zijn, de gerechtvaardigde belangen en de ontvangers van de persoonsgegevens.<sup>89</sup> Verder verstrekt de verwerkingsverantwoordelijke bij verkrijging aanvullende informatie om een behoorlijke en transparante verwerking te waarborgen. Hieronder wordt verstaan: de bewaartermijnen, de rechten van de betrokkenen, het recht om een klacht in te dienen bij de Autoriteit Persoonsgegevens (hierna: AP), hoe de verwerkingsverantwoordelijke aan de gegevens is gekomen en het eventuele bestaan van geautomatiseerde besluitvorming.<sup>90</sup>

##### 2.2.4.2 Recht op inzage

De betrokkene heeft het recht om van de verwerkingsverantwoordelijke inzage te verkrijgen van zijn persoonsgegevens en van de volgende informatie: de verwerkingsdoeleinden, de betrokken categorieën van persoonsgegevens, de ontvangers aan wie de persoonsgegevens zullen worden verstrekt, de bewaartermijnen, zijn rechten, alle informatie over de bron van de verwerker en het bestaan van een eventuele geautomatiseerde besluitvorming.<sup>91</sup> De verwerkingsverantwoordelijke verstrekt de betrokkene een kopie van de persoonsgegevens die worden verwerkt.<sup>92</sup> Het recht van inzage is bedoeld om de uitoefening van de rechten van rectificatie, gegevenswisseling en beperking mogelijk te maken.<sup>93</sup>

##### 2.2.4.3 Recht op rectificatie

De betrokkene heeft het recht om van de verwerkingsverantwoordelijke onverwijld rectificatie van hem betreffende onjuiste persoonsgegevens te verkrijgen.<sup>94</sup> De verwerkingsverantwoordelijke en verwerker dienen alle redelijke maatregelen te nemen om ervoor te zorgen dat de onjuiste persoonsgegevens worden gerectificeerd. Hierbij is het irrelevant of de onjuistheid berust op een fout van de verwerkingsverantwoordelijke of verwerker. Het aanpassen van iemands naam, omdat deze wijzigt na een huwelijk, valt ook onder het recht uit dit artikel.<sup>95</sup>

---

<sup>87</sup> Overweging 47 AVG.

<sup>88</sup> Van der Sloot 2018, p. 120.

<sup>89</sup> Artikel 13 lid 1 AVG.

<sup>90</sup> Artikel 13 lid 2 AVG.

<sup>91</sup> Artikel 15 lid 1 AVG.

<sup>92</sup> Artikel 15 lid 3 AVG.

<sup>93</sup> Engelfriet, Chew-Meij & Kager 2018, p. 85.

<sup>94</sup> Artikel 16 AVG.

<sup>95</sup> Engelfriet, Chew-Meij & Kager 2018, p. 90.

#### 2.2.4.4 Recht op gegevenswissing/vergetelheid

De betrokkene heeft het recht om te verzoeken dat (verouderde) gegevens worden verwijderd.<sup>96</sup> De verwerkingsverantwoordelijke moet de persoonsgegevens zonder onredelijke vertraging wissen. Dit is in beginsel een maand.<sup>97</sup> Het recht op vergetelheid kan worden ingeroepen als aan een van de volgende punten is voldaan:<sup>98</sup>

- De persoonsgegevens zijn niet langer nodig voor het doel waarvoor zij zijn verzameld of verwerkt.
- De betrokkene trekt de toestemming in en verder is er geen andere rechtsgrond voor de verwerking.
- De betrokkene maakt bezwaar tegen de verwerking.
- De persoonsgegevens zijn onrechtmatig verwerkt.
- De persoonsgegevens moeten worden gewist om te voldoen aan de wettelijke verplichting die op de verwerkingsverantwoordelijke rust.
- De persoonsgegevens zijn verzameld in verband met een aanbod van diensten van de informatiemaatschappij.

Het recht op vergetelheid is met name in het leven geroepen, zodat mensen op het internet niet altijd (ten onrechte) met hun verleden worden geconfronteerd.<sup>99</sup> Sinds het arrest Google Spain<sup>100</sup> van het Hof van Justitie van de EU was de uitoefening van het recht op vergetelheid tegenover de exploitanten van zoekmachinediensten al erkend.<sup>101</sup>

Wanneer de gegevens moeten worden vergeten, moeten de gegevens ook echt weg zijn. De verwerkingsverantwoordelijke moet kunnen aantonen dat de gegevens op een veilige manier zijn gewist en dat de gegevens bij de verwerker worden gewist. Sommige persoonsgegevens kunnen technisch niet, of slechts met veel moeite worden gewist. Voor back-ups geldt dat de organisatie hierbij een duidelijk, legitiem belang heeft bij het bewaren van de back-ups. De organisatie moet wel na herstel van een back-up direct de verzochte gegevens wissen.<sup>102</sup>

#### 2.2.4.5 Recht op beperking van de verwerking

Het recht op beperking van de verwerking houdt in dat de verwerking van de persoonsgegevens tijdelijk stil worden gezet. Het gaat hierbij om alle verwerkingsprocessen, behalve de opslag van de persoonsgegevens.<sup>103</sup> De beperking kan in vier situaties verlangd worden. De eerste situatie is wanneer de betrokkene de juistheid van de persoonsgegevens betwist. De tweede situatie is wanneer een verwerking rechtmatig is en de betrokkene zich verzet tegen het wissen van de persoonsgegevens en verzoekt om beperking van het gebruik ervan. De derde situatie is dat de betrokkene een rechtsvordering wil instellen, uitoefenen of onderbouwen en betreffende persoonsgegevens nodig heeft. De vierde situatie is wanneer er bezwaar is gemaakt en de betrokkene nog in afwachting is van antwoord.<sup>104</sup>

#### 2.2.4.6 Recht op overdraagbaarheid van gegevens/dataportabiliteit

De betrokkene heeft het recht om de persoonsgegevens die hij aan een verwerkingsverantwoordelijke heeft verstrekt, over te dragen aan een andere verwerkingsverantwoordelijke, zonder daarbij te worden gehinderd. Hierbij is het van belang dat er geen afbreuk wordt gedaan aan de rechten en vrijheden van anderen. Verder is het van belang dat de persoonsgegevens via de geautomatiseerde weg zijn verwerkt.

---

<sup>96</sup> Artikel 17 AVG.

<sup>97</sup> Artikel 12 lid 3 AVG.

<sup>98</sup> Artikel 17 lid 1 sub a t/m f AVG.

<sup>99</sup> Schermer, Hagenauw & Falot, p. 80.

<sup>100</sup> HvJ EU 13 mei 2014, C-131/12 (*Google Spain SL, Google Inc t. Agencia Española de Protección de Datos, Mario Costeja González*).

<sup>101</sup> De Jong, *Ars Aequi* 2016/10, p. 772.

<sup>102</sup> Engelfriet, Chew-Meij & Kager, p. 72-73.

<sup>103</sup> Van der Sloot 2018, p. 137.

<sup>104</sup> Artikel 18 lid 1 sub a t/m d AVG.

De betrokkene heeft het recht om deze gegevens in een gestructureerde, gangbare en machineleesbare vorm te verkrijgen.<sup>105</sup> Het doel van het recht op overdraagbaarheid van gegevens is de zeggenschap van de betrokkene over zijn gegevens te vergroten.<sup>106</sup>

#### 2.2.4.7 Recht van bezwaar

De betrokkene heeft te allen tijde het recht om met zijn specifieke situatie verband houdende redenen bezwaar te maken tegen de verwerking zijn persoonsgegevens. Dit geldt ook wanneer persoonsgegevens ten behoeve van direct marketing worden verwerkt. De verwerkingsverantwoordelijke staakt de verwerking van de persoonsgegevens, tenzij hij dwingende gerechtvaardigde gronden voor de verwerking aanvoert.<sup>107</sup>

#### 2.2.4.8 Recht om een klacht in te dienen

Iedere betrokkene heeft het recht om een klacht in te dienen bij een toezichthoudende autoriteit, indien de betrokkene van mening is dat de verwerking van zijn persoonsgegevens inbreuk maakt op de AVG. Dit kan in de lidstaat waar hij gewoonlijk verblijft, waar hij zijn werkplek heeft of waar de inbreuk is begaan.<sup>108</sup>

De betrokkene heeft ook het recht om een doeltreffende voorziening in rechte in te stellen tegen een verwerkingsverantwoordelijke of verwerker. Dit kan als de betrokkene van mening is dat zijn rechten uit de AVG zijn geschonden naar aanleiding van de verwerking van zijn persoonsgegevens die niet aan de AVG voldoet.<sup>109</sup> De betrokkene kan dus ook naar de rechter gaan. Op basis van het Nederlands recht zal de verordening gebaseerd zijn op grond van een onrechtmatige daad.<sup>110</sup>

#### 2.2.4.9 Recht op schadevergoeding

Eenieder die materiële of immateriële schade heeft geleden als gevolg van een inbreuk op de AVG, heeft het recht om van de verwerkingsverantwoordelijke of de verwerker schadevergoeding te ontvangen voor de geleden schade.<sup>111</sup>

De betrokkene mag een verzoek, om zijn recht te honoreren, op iedere manier doen. Dit kan door het persoonlijk langskomen, een brief te sturen of door middel van een elektronisch verzoek. De verwerkingsverantwoordelijke is in alle gevallen verplicht het verzoek te honoreren.<sup>112</sup>

### 2.2.5 Verplichtingen verwerkingsverantwoordelijke

Hierboven staan de rechten van de betrokkene opgesomd. De verwerkingsverantwoordelijke moet gehoor geven aan deze rechten, tenzij de verzoeken van de betrokkene ongegrond of buitensporig zijn. De uitvoering van de rechten van de betrokkenen mag niet bemoeilijkt worden door de verwerkingsverantwoordelijke.<sup>113</sup> Verder staan in de AVG diverse verplichtingen voor de verwerkingsverantwoordelijke opgesomd. In deze paragraaf zullen de belangrijkste verplichtingen voor Merford worden besproken.

#### 2.2.5.1 Transparantie, informatie en communicatie

De transparantie van gegevensverwerkingen is een belangrijk element in de privacywetgeving. De verwerkingsverantwoordelijke moet passende maatregelen nemen, zodat de betrokkene de informatie in verband met de gegevensverwerking in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in een duidelijke eenvoudige taal ontvangt.<sup>114</sup>

---

<sup>105</sup> Artikel 20 lid 1 AVG.

<sup>106</sup> Schermer, Hagenauw & Falot, p. 81.

<sup>107</sup> Artikel 21 AVG.

<sup>108</sup> Artikel 13 lid 2 sub d jo. artikel 77 AVG.

<sup>109</sup> Artikel 79 AVG.

<sup>110</sup> Engelfriet, Chew-Meij & Kager 2018, p. 274-275.

<sup>111</sup> Artikel 82 AVG.

<sup>112</sup> Engelfriet, Chew-Meij & Kager, p. 77.

<sup>113</sup> Schermer, Hagenauw & Falot, p. 73.

<sup>114</sup> Artikel 12 lid 1 AVG.

De verwerkingsverantwoordelijke verstrekt de betrokkene onverwijld, maar in ieder geval binnen een maand na de ontvangst van het verzoek, de opgevraagde informatie. Deze termijn kan verlengd worden met nog eens twee maanden. Indien hier gebruik van wordt gemaakt, dient de betrokkene binnen een maand na ontvangst van het verzoek in kennis te worden gesteld van de verlenging.<sup>115</sup> Indien de verwerkingsverantwoordelijke geen gehoor geeft aan het verzoek van de betrokkene, deelt hij dit onverwijld en uiterlijk binnen een maand met motivatie en de rechten van de betrokkene bij een afwijzing.<sup>116</sup> De AVG vereist dat de verwerkingsverantwoordelijke kosteloos de vereiste informatie verstrekt en kosteloos de betrokkene voorziet in hun rechten of informatie over datalekken verstrekt.<sup>117</sup>

#### 2.2.5.2 Kennisgevingsplicht

De verwerkingsverantwoordelijke stelt alle ontvangers aan wie persoonsgegevens zijn verstrekt, in kennis van elke rectificatie, gegevenswissing of beperking. Hiervan kan afgeweken worden indien dit onmogelijk blijkt of onevenredig veel inspanning vergt.<sup>118</sup> Doel van de kennisgeving is dat de ontvangers vervolgens de betreffende rectificatie, wissing of beperking ook doorvoert.<sup>119</sup>

#### 2.2.5.3 Gegevensbeschermingsbeleid

De verwerkingsverantwoordelijke treft passende technische en organisatorische maatregelen om te kunnen waarborgen en om aan te kunnen tonen dat de verwerking in overeenstemming met de AVG wordt uitgevoerd.<sup>120</sup>

Bovenstaande is gefocust op de maatregelen voorafgaand, tijdens en rondom de verwerking. De genomen maatregelen moeten passend zijn. Hiervoor moeten allerlei zaken in de afweging betrokken worden. Enerzijds het soort verwerking en anderzijds de risico's voor de betrokkene. De effectiviteit van de maatregelen moeten regelmatig beoordeeld worden en worden aangepast waar nodig is.<sup>121</sup> Van de verwerkingsverantwoordelijke wordt verwacht dat de genomen maatregelen worden uitgewerkt in een beleid, dat vervolgens in de praktijk ook daadwerkelijk wordt uitgevoerd.<sup>122</sup>

#### 2.2.5.4 Privacy by design and privacy by default<sup>123</sup>

Door het omvangrijke aantal systemen dat persoonsgegevens verwerkt, is het niet mogelijk voor toezichthouders om systematisch alle systemen te controleren op rechtmatigheid en om bij onrechtmatigheid tijdig sancties op te leggen. Om dit probleem te ondervangen is gekozen voor privacy by design and privacy by default.<sup>124</sup>

Privacy by design betekent gegevensbescherming door ontwerp. Dit houdt in dat de voor de verwerking van persoonsgegevens gebruikte mechanismen zo zijn ontworpen, dat zij zo veel mogelijk rekening houden met de privacy van de betrokkenen en de vereisten uit de AVG. Dit geldt voor zowel systemen als maatregelen.<sup>125</sup> Privacy by default betekent een gegevensbescherming door standaardinstellingen. Dit houdt in dat een dienst of product op een zodanige manier moet worden aangeboden, dat de inbreuk van de gebruiker zo veel mogelijk wordt beperkt.

De standaardinstellingen van een website moeten bijvoorbeeld zo zijn ingesteld dat de gebruiker alleen door middel van het geven van akkoord, verwerking van meer persoonsgegevens mogelijk maakt.<sup>126</sup>

<sup>115</sup> Artikel 12 lid 3 AVG.

<sup>116</sup> Artikel 12 lid 4 AVG.

<sup>117</sup> Engelfriet, Chew-Meij & Kager 2018, p. 72.

<sup>118</sup> Artikel 19 AVG.

<sup>119</sup> Engelfriet, Chew-Meij & Kager 2018, p. 98.

<sup>120</sup> Artikel 24 AVG.

<sup>121</sup> Versmissen, Terstegge & Krijgsman, p. 38-39.

<sup>122</sup> Engelfriet, Chew-Meij & Kager 2018, p. 117.

<sup>123</sup> Artikel 25 AVG.

<sup>124</sup> Berkvens, Vinken, Wiegerinck, Wolters, Reijner & Van Gerwen, p. 121.

<sup>125</sup> Engelfriet, Chew-Meij & Kager 2018, p. 119.

<sup>126</sup> Van den Eijnden, Jansen, Van den Bosch & Van de Pas 2018, p. 86-87.

#### 2.2.5.5 Verwerker en verwerkersovereenkomst

De verwerkingsverantwoordelijke heeft de mogelijkheid om de verwerking uit te laten besteden. De verwerking door een verwerker wordt geregeld in een overeenkomst of een andere rechtshandeling die de verwerker ten aanzien van de verwerkingsverantwoordelijke bindt. Het doel hiervan is dat de verwerker voldoende garanties biedt, zodat de verwerking aan de AVG voldoet en de bescherming van de rechten van de betrokkene is gewaarborgd.<sup>127</sup> Een verwerkersovereenkomst is het meest gebruikelijk. De verplichte onderwerpen voor een verwerkersovereenkomst staan opgesomd in artikel 28 lid 3 AVG. De verwerkingsverantwoordelijke blijft ook bij de uitbesteding verantwoordelijk voor de verwerking van de persoonsgegevens.<sup>128</sup> De verwerker en eenieder die onder het gezag van de verwerkingsverantwoordelijke of verwerker handelt en toegang heeft tot de persoonsgegevens, verwerkt deze gegevens uitsluitend in opdracht van de verwerkingsverantwoordelijke.<sup>129</sup>

#### 2.2.5.6 Documentatieplicht

Om de naleving van de AVG aan te kunnen tonen, dienen de verwerkingsverantwoordelijke en verwerker een register bij te houden van de verwerkingsactiviteiten die hebben plaatsgevonden.<sup>130</sup> Merford heeft de verplichting om een verwerkingsregister bij te houden, omdat de verwerking van de persoonsgegevens niet incidenteel is en dus niet onder de uitzonderingen valt.<sup>131</sup> De verwerkingsregister moet in een schriftelijke vorm worden opgesteld, een elektrische vorm valt hier ook onder.<sup>132</sup> De verwerkingsregister moet in ieder geval een aantal gegevens bevatten:<sup>133</sup>

- De naam en contactgegevens van de verwerkingsverantwoordelijke en de vertegenwoordiger. Evenals de naam en contactgegevens van de FG.
- De verwerkingsdoeleinden.
- Een beschrijving van de categorieën van de betrokkenen en van de categorieën persoonsgegevens.
- De categorieën van ontvangers van de persoonsgegevens.
- Indien van toepassing, doorgiften van persoonsgegevens aan derde landen.
- Indien mogelijk, de bewaartermijnen.
- Indien mogelijk, een algemene beschrijving van technische en organisatorische beveiligingsmaatregelen.

#### 2.2.5.7 Medewerking toezichthoudende autoriteit

Indien een toezichthouder verzoekt om medewerking, is de verwerkingsverantwoordelijke verplicht daaraan mee te werken.<sup>134</sup> Verder bepaalt artikel 5:20 Algemene wet bestuursrecht dat eenieder verplicht is aan een toezichthouder alle medewerking te verlenen binnen de door hem gestelde redelijke termijn.

#### 2.2.5.8 Beveiliging van verwerking

De beveiliging is een cruciaal vereiste binnen het privacyrecht. De AVG legt de verwerkingsverantwoordelijke allerlei regels op, op het gebied van de bescherming van persoonsgegevens. Dit heeft weinig of geen nut als de gegevens vervolgens slecht of niet beveiligd worden. De verwerkingsverantwoordelijke moet daarom passende technische en organisatorische maatregelen nemen om de beveiliging van de persoonsgegevens te waarborgen.<sup>135</sup>

---

<sup>127</sup> Artikel 28 AVG.

<sup>128</sup> Berkvens, Vinken, Wiegerinck, Wolters, Reijner & Van Gerwen, p. 61.

<sup>129</sup> Artikel 29 AVG.

<sup>130</sup> Overweging 82 AVG.

<sup>131</sup> Artikel 30 AVG.

<sup>132</sup> Artikel 30 lid 3 AVG.

<sup>133</sup> Artikel 30 lid 1 sub a t/m g AVG.

<sup>134</sup> Artikel 31 AVG.

<sup>135</sup> Artikel 32 lid 1 AVG.

De maatregelen dienen een passend niveau van beveiliging te waarborgen. Hierbij moet rekening worden gehouden met de stand van de techniek en de uitvoeringskosten afgezet tegen de risico's en de aard van de te beschermen persoonsgegevens.<sup>136</sup> De AVG noemt een viertal maatregelen die een organisatie ten minste moet nemen indien dit passend is:<sup>137</sup>

- De pseudonimisering en versleuteling van persoonsgegevens.
- Een kwalitatief goede inrichting van de diensten en systemen waarmee de verwerking plaatsvindt.<sup>138</sup>
- De mogelijkheid om bij een incident de beschikbaarheid en toegang tijdig te herstellen.
- Een procedure om de beveiliging van de verwerking te testen, te beoordelen en om te evalueren.

Een kernbegrip bij de beveiliging is risicovermijding. Het is voor een organisatie niet realistisch om iedere week het nieuwste softwarepakket aan te schaffen. Hoeveel er moet worden gedaan, verschilt per geval. Hoe gevoeliger de gegevens hoe zwaarder de veiligheidsmaatregelen moeten zijn.<sup>139</sup>

#### 2.2.5.9 Meldplicht datalekken

Indien een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, meldt de verwerkingsverantwoordelijke dit indien mogelijk uiterlijk binnen 72 uur nadat er kennis is genomen van de inbreuk, maar in ieder geval zonder onredelijke vertraging. De definitie van inbreuk in verband met persoonsgegevens is te vinden in de begrippenlijst. De melding vindt plaats bij de bevoegde toezichthoudende autoriteit, de AP, tenzij het onwaarschijnlijk is dat de inbreuk van persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen.<sup>140</sup> De melding is vormvrij,<sup>141</sup> maar bevat ten minste het volgende:<sup>142</sup>

- De aard van de inbreuk in verband met de persoonsgegevens.
- De naam en de contactgegevens van de FG of een ander contactpunt waar meer informatie kan worden verkregen (*ook van belang voor melding aan de betrokkene*).
- De waarschijnlijke gevolgen van de inbreuk (*ook van belang voor melding aan de betrokkene*).
- De maatregelen die de verwerkingsverantwoordelijke heeft voorgesteld of heeft genomen om de inbreuk in verband met de persoonsgegevens aan te pakken (*ook van belang voor melding aan de betrokkene*).

Alle inbreuken in verband met persoonsgegevens moeten gedocumenteerd worden.<sup>143</sup>

Als de inbreuk in verband met de persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, moet de verwerkingsverantwoordelijke de betrokkene de inbreuk onverwijld mededelen.<sup>144</sup> De informatie die de melding aan de betrokkene ten minste moet bevatten, is hierboven in cursief aangegeven.<sup>145</sup>

#### 2.2.5.10 Data Privacy Impact Assessment

Een Data Privacy Impact Assessment (hierna: DPIA) is in het Nederlands ook bekend als gegevensbeschermingseffectbeoordelingen. Wanneer een verwerking waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, voert de verwerkingsverantwoordelijke voor de verwerking een beoordeling uit van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens.<sup>146</sup>

<sup>136</sup> Overweging 83 AVG.

<sup>137</sup> Artikel 32 lid 1 sub a t/m d AVG.

<sup>138</sup> Engelfriet, Chew-Meij & Kager 2018, p. 139.

<sup>139</sup> Van der Sloot 2018, p. 102.

<sup>140</sup> Artikel 33 lid 1 AVG.

<sup>141</sup> Engelfriet, Chew-Meij & Kager 2018, p. 142.

<sup>142</sup> Artikel 33 lid 3 sub a t/m d AVG.

<sup>143</sup> Artikel 33 lid 5 AVG.

<sup>144</sup> Artikel 34 lid 1 AVG.

<sup>145</sup> Artikel 34 lid 2 AVG.

<sup>146</sup> Artikel 35 lid 1 AVG.

Een DPIA is vereist in de volgende gevallen:<sup>147</sup>

- Bij een systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen, die gebaseerd is op geautomatiseerde verwerking.
- Bij een grootschalige verwerking van bijzondere categorieën van persoonsgegevens.
- Bij stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten.

Een DPIA is dus niet voor alle organisaties verplicht, maar dit is vaak wel nuttig om als standaard te hanteren.<sup>148</sup>

Een DPIA is een drietrapsraket. Ten eerste moet de verwerkingsverantwoordelijke bij iedere verwerking een eerste beoordeling maken van de risico's die daarbij kunnen bestaan. Ten tweede moet, als uit de eerste stap volgt dat er waarschijnlijk een hoog risico kleeft aan de verwerking, een uitgebreide DPIA worden uitgevoerd.<sup>149</sup> Als uit de tweede stap blijkt dat het hoge risico niet kan worden beperkt met redelijke maatregelen, moet de toezichthouder voorafgaand de verwerking worden geraadpleegd.<sup>150</sup>

#### 2.2.5.11 Functionaris gegevensbescherming

Een FG staat in het Engels bekend als data protection officer, afgekort als DPO. Dit is een afkorting, die samen met FG vaak wordt gebruikt. Een FG is niet verplicht in elke organisatie. Een FG moet in ieder geval bij overheidsinstanties en overheidsorganen worden aangesteld. Dit geldt ook voor organisatie die hoofdzakelijk het uitvoeren van regelmatige en stelselmatige observatie op grote schaal van betrokkenen als hoofdactiviteit hebben. Verder is een FG verplicht voor organisaties die hoofdzakelijk zijn belast met grootschalige verwerking van bijzondere persoonsgegevens.<sup>151</sup> Een organisatie kan ook vrijwillig een FG benoemen.

De FG ziet onder andere toe op de naleving van de AVG, verstrekt desgevraagd advies, werkt samen met de toezichthoudende autoriteit en treedt op als contactpunt.<sup>152</sup> Er is geen vastomlijnd functieprofiel voor een FG. De FG moet wel kennis hebben van multidisciplinaire zaken zoals privacy, IT, informatiebeveiliging, compliance, governance en crisismanagement.<sup>153</sup> Een belangrijke voorwaarde is dat de FG onafhankelijk moet zijn.<sup>154</sup> De FG is verder verplicht tot geheimhouding van hetgeen hem op grond van een klacht of een verzoek van betrokkene bekend is geworden, tenzij de betrokkene met de bekendmaking toestemt.<sup>155</sup> Ten slotte is het van belang dat de FG voldoende betrouwbaar wordt geacht. Deze betrouwbaarheid uit zich bijvoorbeeld door alle bij de verwerkingen betrokken belangen op een onafhankelijke wijze tegen elkaar te kunnen afwegen.<sup>156</sup>

#### 2.2.5.12 Schadevergoeding en aansprakelijkheid

Zoals in paragraaf 2.2.4.9 is besproken, heeft eenieder recht op schadevergoeding, indien diegene materiële of immateriële schade heeft geleden als gevolg van een inbreuk op de AVG. De verwerkingsverantwoordelijke moet alle schade vergoeden die iemand kan lijden ten gevolge van een verwerking die inbreuk maakt op de AVG.<sup>157</sup> Elke verwerkingsverantwoordelijke die bij de verwerking is betrokken, is aansprakelijk voor de schade.<sup>158</sup> Een verwerkingsverantwoordelijke wordt vrijgesteld van de aansprakelijkheid, indien hij bewijst dat hij op geen enkele wijze verantwoordelijk is voor het schadeveroorzakende feit.<sup>159</sup> Hierbij kan gedacht worden aan situaties van overmacht.

<sup>147</sup> Artikel 35 lid 3 sub a t/m c AVG.

<sup>148</sup> Van der Sloot, p. 97.

<sup>149</sup> Engelfriet, Chew-Meij & Kager 2018, p. 149.

<sup>150</sup> Artikel 36 AVG.

<sup>151</sup> Artikel 37 AVG.

<sup>152</sup> Artikel 39 AVG.

<sup>153</sup> Van Schaik & Abassi, *Bedrijfsjuridische berichten* 2017/95, p. 324.

<sup>154</sup> Nouwt, *P&I* 2017/1, p. 6.

<sup>155</sup> Artikel 39 UAVG.

<sup>156</sup> Artikel 39 MvT UAVG.

<sup>157</sup> Overweging 146 AVG.

<sup>158</sup> Artikel 82 lid 2 AVG.

<sup>159</sup> Artikel 82 lid 3 AVG.

### 2.2.6 Onafhankelijke toezichthoudende autoriteiten

Iedere lidstaat is verplicht om een toezichthouder in te stellen. De toezichthouder controleert in alle onafhankelijkheid de naleving van de AVG en de bescherming van de grondrechten van de burger ten aanzien van de persoonsgegevens.<sup>160</sup> De toezichthoudende autoriteit is in Nederland de AP.<sup>161</sup>

De AP treedt volledig onafhankelijk op bij de uitvoering van de taken en de uitoefening van de bevoegdheden die in de AVG aan haar zijn toegewezen.<sup>162</sup> De AVG geeft de volgende punten om de onafhankelijkheid van de AP te waarborgen:

- Alle leden van elke toezichthoudende autoriteit blijven vrij van al dan niet rechtstreekse externe invloed, vragen of instructies.<sup>163</sup>
- Elke lidstaat zorgt ervoor dat elke toezichthoudende autoriteit beschikt over de personele, technische en financiële middelen en de bedrijfsruimten en infrastructuur die nodig zijn voor het effectief uitvoeren van haar taken en uitoefenen van haar bevoegdheden.<sup>164</sup>
- Elke lidstaat zorgt ervoor dat elke toezichthoudende autoriteit eigen en zelfgekozen personeelsleden heeft.<sup>165</sup>

De taken die aan de toezichthoudende autoriteiten zijn opgelegd, staan opgesomd in artikel 57 lid 1 sub a tot en met v AVG. Verder heeft iedere toezichthouder in beginsel drie bevoegdheden:

- Onderzoeksbevoegdheden conform artikel 58 lid 1 AVG, zoals een inlichtingenrecht.
- Bevoegdheden tot het nemen van corrigerende maatregelen conform artikel 58 lid 2 AVG, zoals het opleggen van sancties.
- Autorisatie- en adviesbevoegdheden conform artikel 58 lid 3 AVG.

### 2.2.7 Europees Comité voor gegevensbescherming

Het Europees Comité voor gegevensbescherming (hierna: EC) is ingesteld als onafhankelijk orgaan van de EU.<sup>166</sup> Het EC staat ook wel bekend als European Data Protection Board, afgekort als EDPB. Het EC vervangt sinds 25 mei 2018 het vorige netwerk van autoriteiten, namelijk de Artikel 29-Werkgroep. Het EC stelt beleidsregels op, geeft adviezen met een bindende werking en kan in sommige situaties bindende besluiten nemen over de handhaving van de AVG.<sup>167</sup> De taken van het EC staan uitgebreid omschreven in artikel 70 lid 1 sub a tot en met y AVG. Het EC treedt bij de uitvoering van zijn taken of de uitoefening van zijn bevoegdheden onafhankelijk op.<sup>168</sup>

### 2.2.8 Sancties

Ter afschrikking van de overtreding van de AVG, hebben de toezichthouders de bevoegdheid om administratieve geldboeten op te leggen aan de verwerkingsverantwoordelijken en de verwerkers. Deze bevoegdheid geldt naast de corrigerende bevoegdheden uit artikel 58 lid 2 AVG.<sup>169</sup> Voor de inbreuken die niet onder de categorie administratieve geldboeten vallen, is er de mogelijkheid voor de lidstaten om zelf regels op te stellen inzake andere sancties.<sup>170</sup> Dit is nader uitgewerkt in artikel 17 UAVG. Er zijn twee soorten boetecategorieën:

- Boeten tot tien miljoen euro of tot twee procent van de totale wereldwijde jaaromzet indien dit cijfer hoger is.<sup>171</sup>

<sup>160</sup> Engelfriet, Chew-Meij & Kager 2018, p. 209.

<sup>161</sup> Artikel 51 lid 1 AVG jo. artikel 6 UAVG.

<sup>162</sup> Artikel 52 lid 1 AVG.

<sup>163</sup> Artikel 52 lid 2 AVG.

<sup>164</sup> Artikel 52 lid 4 AVG.

<sup>165</sup> Artikel 52 lid 6 AVG.

<sup>166</sup> Artikel 68 AVG.

<sup>167</sup> Hijmans, *NJB* 2018/356, p. 473.

<sup>168</sup> Artikel 69 AVG.

<sup>169</sup> Engelfriet, Chew-Meij & Kager 2018, p. 281.

<sup>170</sup> Artikel 84 AVG.

<sup>171</sup> Artikel 83 lid 4 AVG.

Onder deze categorie boeten vallen de overtredingen die zien op de (verantwoordings)plichten die rusten op organisaties, zoals het verrichten van een DPIA of het melden van een datalek.<sup>172</sup>

- Boeten tot twintig miljoen euro of tot vier procent van de totale wereldwijde jaaromzet indien dit cijfer hoger is.<sup>173</sup>

Onder deze hoogste boetecategorie vallen onder andere de inbreuken op de basisbeginselen, de rechten van de betrokkene, de doorgiften van persoonsgegevens, verplichtingen die volgen uit nationale wetgeving en niet-naleving van een bevel van de toezichthouder.

Bij het opleggen van een boete dient de toezichthouder gemotiveerd aan te geven hoe men aan het betreffende bedrag komt.<sup>174</sup>

### 2.3 Tussenconclusie

In dit hoofdstuk is eerst kort besproken wat de AVG inhoudt. De AVG is kortgezegd een verordening die betrekking heeft op de bescherming van de persoonsgegevens die bindend is voor alle lidstaten. Vervolgens zijn in dit hoofdstuk de belangrijkste bepalingen uit de AVG voor Merford besproken. Hierbij is, voor zover dat mogelijk was, de chronologie van de AVG aangehouden. Diverse definities uit de AVG zijn van toepassing voor Merford. De definities die van toepassing zijn, staan in de begrippenlijst. In artikel 5 AVG staan zes basisbeginselen, waaraan elke verwerking van persoonsgegevens moet voldoen. Merford verwerkt persoonsgegevens en daarom is dit artikel van belang voor Merford. Een verwerking van persoonsgegevens moet ook rechtmatig zijn. De voorwaarden hiervoor zijn opgenomen in de AVG en van belang voor Merford. De betrokkene hebben diverse rechten. Voor Merford zijn deze rechten van belang, omdat Merford aan de rechten van de betrokkene gehoor moet geven. Als Merford hier geen gehoor aan geeft, handelt ze in strijd met de AVG. Merford heeft als verwerkingsverantwoordelijke natuurlijk ook verplichtingen, die zijn uitgewerkt in de AVG. In Nederland is de toezichthoudende autoriteit de AP. Verder is de EC het onafhankelijke orgaan van de EU. Bij het niet naleven van de AVG, kan de AP administratieve geldboeten opleggen aan de verwerkingsverantwoordelijke. De boeten kunnen oplopen tot twintig miljoen euro of tot vier procent van de totale wereldwijde omzet, indien dit bedrag hoger is. In de volgende hoofdstukken worden de huidige verklaringen en werkwijze van Merford getoetst aan de besproken bepalingen uit de AVG.

---

<sup>172</sup> Schermer, Hagenauw & Falot, p. 91.

<sup>173</sup> Artikel 83 lid 5 AVG.

<sup>174</sup> Engelfriet, Chew-Meij & Kager 2018, p. 282.

## Hoofdstuk 3 Privacyverklaringen van Merford versus de AVG

In dit hoofdstuk worden de huidige privacyverklaringen van Merford getoetst aan de AVG. Merford heeft twee privacyverklaringen, namelijk een algemene privacyverklaring en een privacyverklaring voor de webwinkel. Er zijn twee privacyverklaringen, omdat voor de webwinkel andere en meer gegevens verwerkt worden dan voor de website van Merford. Eerst wordt de algemene privacyverklaring van Merford besproken en vervolgens de privacyverklaring van de webwinkel. Ten slotte volgt de conclusie van dit hoofdstuk.

### 3.1 Privacyverklaring Merford Holding B.V.<sup>175</sup>

De algemene privacyverklaring van Merford is op hun website te vinden.<sup>176</sup> Deze privacyverklaring is voor het laatst aangepast op 22 mei 2018. In de privacyverklaring staat dat via de website van Merford privacygevoelige gegevens worden verwerkt. Merford acht een zorgvuldige omgang met persoonsgegevens van groot belang. Bij de verwerking houdt Merford zich aan de eisen die de AVG stelt. Dit wordt puntsgewijs nader toegelicht in de privacyverklaring. De punten uit privacyverklaring worden hieronder besproken, waarbij de AVG wordt toegepast.

#### 3.1.1 Gebruik van persoonsgegevens

Door Merford worden uitsluitend de persoonsgegevens bewaard en gebruikt, die door de betrokkene rechtstreeks worden opgegeven. De gegevens die gebruikt worden zijn naam, adres en woonplaats (hierna: NAW-gegevens), geslacht en e-mailadres. De gegevens worden gebruikt voor de in de privacyverklaring genoemde doelen, zoals het versturen van een nieuwsbrief.<sup>177</sup> Elke verwerking van persoonsgegevens moet voldoen aan de zes basisbeginselen conform artikel 5 AVG, deze beginselen zijn uitgewerkt in paragraaf 2.2.2. Indien is voldaan aan de basisbeginselen voor de verwerking van de persoonsgegevens en de toestemming op de juiste wijze is gegeven, is er sprake van een rechtmatige verwerking. De grondslag uit de AVG die wordt gebruikt voor het gebruik van persoonsgegevens, is toestemming. Toestemming is vastgelegd in artikel 6 lid 1 sub a AVG jo. artikel 7 AVG. Voor Merford is het belangrijk dat zij kan aantonen dat de betrokkene vrijwillig toestemming heeft gegeven voor het verwerken van de persoonsgegevens. Verder is het van belang dat Merford de betrokkene op de hoogte stelt dat hij het recht heeft om te allen tijde zijn toestemming in te trekken. Dit is niet terug te vinden in de privacyverklaring van Merford.

#### 3.1.2 Reclame

In de privacyverklaring staat dat de betrokkene, naast de informatie op de website, ook op de hoogte gebracht kan worden van nieuwe producten en diensten per e-mail of via sociale media.<sup>178</sup> Voor sociale media geldt dat de betrokkene zelf kan kiezen of hij Merford wil volgen. De betrokkene kan ook op de hoogte gehouden worden van nieuwe producten per e-mail. Of de betrokkene zich hiervoor moet aanmelden en waar dit kan, is niet duidelijk terug te vinden op de website noch in de privacyverklaring. Hierbij kan nog de vraag gesteld worden of reclame en nieuwsbrief onder elkaar vallen of los staan van elkaar. Indien de verwerkingsbeginselen van artikel 5 AVG in acht worden genomen en de toestemming voor het versturen van reclame per e-mail op de juiste wijze wordt gegeven, is er sprake van een rechtmatige verwerking van persoonsgegevens.

#### 3.1.3 Contactformulier en nieuwsbrief

Via de website wordt de mogelijkheid geboden om vragen te stellen middels een contactformulier. De gegevens die worden toegestuurd, worden bewaard zolang het naar de aard van het formulier of de inhoud van de e-mail nodig is voor een volledige beantwoording en afhandeling van de vraag.<sup>179</sup> Voor de verwerking van de persoonsgegevens van het

<sup>175</sup> Bijlage 1 Privacyverklaring Merford Holding B.V.

<sup>176</sup> [www.merford.com](http://www.merford.com).

<sup>177</sup> Bijlage 1 Privacyverklaring Merford Holding B.V. (Zie paragraaf *Gebruik van persoonsgegevens*).

<sup>178</sup> Bijlage 1 Privacyverklaring Merford Holding B.V. (Zie paragraaf *Reclame*).

<sup>179</sup> Bijlage 1 Privacyverklaring Merford Holding B.V. (Zie paragraaf *Contactformulier en nieuwsbrief*).

contactformulier geldt, dat er geen specifieke toestemming wordt gegeven. De rechtmatigheid van de verwerking zou gekwalificeerd kunnen worden als noodzakelijk voor de belangenafweging. Zonder de contactgegevens van de betrokkene kan Merford namelijk geen contact opnemen met de betrokkene die een vraag heeft. Het doel van de verwerking van de persoonsgegevens is de vraag van de betrokkene te behandelen. Aan het beginsel van dataminimalisatie wordt ook voldaan. De verplichte persoonsgegevens die door de betrokkene ingevuld moeten worden, zijn: de voornaam, de achternaam en het e-mailadres. Het opgeven van een telefoonnummer is optioneel. De persoonsgegevens worden bewaard voor de volledige beantwoording en de afhandeling van de vraag. Aan het beginsel van opslagbeperking wordt dus ook voldaan. De verwerking van de persoonsgegevens middels het contactformulier kan als rechtmatig gekwalificeerd worden.

Voor geïnteresseerden in de producten en/of diensten van Merford wordt een nieuwsbrief aangeboden. Iedere nieuwsbrief bevat een link voor afmelding. Het e-mailadres wordt automatisch toegevoegd aan de lijst van abonnees.<sup>180</sup> Inschrijven voor een nieuwsbrief kan via de website van Merford. De persoonsgegevens die hierbij verwerkt worden, zijn: naam, achternaam, bedrijfsnaam en e-mailadres. Voor het inschrijven van een nieuwsbrief moet de betrokkene bewuste acties ondernemen, zoals klikken op de link 'Blijf op de hoogte', het invullen van de persoonsgegevens en op de button versturen klikken. Door deze bewuste acties kan Merford aantonen dat een betrokkene vrijwillige toestemming heeft gegeven voor het verwerken van de persoonsgegevens. Het doel van de verwerking van de persoonsgegevens is om de betrokkene te informeren over de producten en/of diensten van Merford. Aan de overige verwerkingsbeginselen wordt ook voldaan. De vraag is echter of bij de afmelding het e-mailadres ook automatisch wordt verwijderd uit de lijst van abonnees.

#### 3.1.4 Locatiegegevens

Indien het nodig is voor de dienst, kunnen locatiegegevens door Merford verzameld worden. Hiervoor wordt op het moment zelf toestemming gevraagd. Deze gegevens kunnen worden opgeslagen en worden verwerkt door de aanbieder van de navigatie-/kaartensoftware. Merford heeft hier geen invloed op en door Merford wordt aangeraden om de relevante privacyverklaring(en) te lezen van betreffende aanbieder.<sup>181</sup> Indien de betrokkene vrijwillig toestemming geeft voor het verzamelen en het verwerken van de persoonsgegevens, is de verwerking rechtmatig. Het doel van het verzamelen van de locatiegegevens, is de dienst volledig te kunnen verrichten. Wat er met de gegevens gebeurt als ze niet meer nodig zijn en hoe lang de gegevens worden bewaard, wordt niet vermeld in de privacyverklaring. Verder is het onduidelijk hoe de locatiegegevens verzameld worden.

#### 3.1.5 Publicatie en verstrekking aan derden

De klantgegevens worden niet gepubliceerd.<sup>182</sup> Op de website zijn sociale media buttons opgenomen, waarmee de beheerder van deze diensten de persoonsgegevens van betrokkenen verzamelt.<sup>183</sup> In deze paragraaf ontbreekt een toelichting. Welke gegevens worden door derden verzameld, waarom mogen deze gegevens worden verzameld en geldt dit voor alle betrokkenen?

#### 3.1.6 Cookies

Op de website wordt gebruik gemaakt van cookies. De derden die zijn ingeschakeld door Merford plaatsen ook cookies. Bij een eerste bezoek aan de website wordt een mededeling getoond met de uitleg waarom cookies worden gebruikt door Merford. Verder gebruik van de website wordt opgevat als toestemming voor gebruik van cookies. Het staat vrij om cookies uit te schakelen middels de browser van de gebruiker. Met de derden die cookies plaatsen zijn afspraken gemaakt over het gebruik van de cookies en applicaties. Merford heeft geen

<sup>180</sup> Bijlage 1 Privacyverklaring Merford Holding B.V. (Zie paragraaf *Contactformulier en nieuwsbrief*).

<sup>181</sup> Bijlage 1 Privacyverklaring Merford Holding B.V. (Zie paragraaf *Locatiegegevens*).

<sup>182</sup> Bijlage 1 Privacyverklaring Merford Holding B.V. (Zie paragraaf *Publicatie*).

<sup>183</sup> Bijlage 1 Privacyverklaring Merford Holding B.V. (Zie paragraaf *Verstrekking aan derden*).

volledige controle over de aanbieder van deze applicaties. Hiervoor wordt verwezen naar de privacyverklaring(en) van betreffende partijen.<sup>184</sup> Zoals hiervoor al is besproken, moet de verwerking van de persoonsgegevens rechtmatig zijn. Om cookies te gebruiken, wordt via de website van Merford toestemming gevraagd. De betrokkene heeft de keuze om wel of geen toestemming te geven. Dit betekent dat de toestemming vrijwillig wordt gegeven. Waarom gebruik wordt gemaakt van cookies, is niet duidelijk terug te vinden in de privacyverklaring. Verder zijn er verschillende soorten cookies te onderscheiden.<sup>185</sup> In de privacyverklaring staat niet omschreven welke cookies Merford gebruikt. Verder is het belangrijk dat de toestemming ondubbelzinnig wordt verleend. Dit houdt in dat de handeling waarmee toestemming wordt gegeven, niet voor meerdere interpretaties vatbaar mag zijn.<sup>186</sup> In de privacyverklaring staat dat Merford het verdere gebruik van de website opvat als toestemming voor gebruik van cookies. Het is niet realistisch om bij iedere klik weer opnieuw toestemming te vragen voor gebruik van cookies op een website die ter informatie bedoeld is. Het is wel verstandig om te vermelden bij het geven van toestemming dat verder gebruik van de website wordt opgevat als toestemming voor het gebruik van cookies.

### 3.1.7 Google Analytics en Hotjar

Om bij te houden hoe bezoekers de website van Merford gebruiken, wordt Google Analytics gebruikt. Hiervoor is een verwerkersovereenkomst afgesloten op 26 maart 2018.<sup>187</sup> Google heeft geen toestemming verkregen om de Analytics informatie te gebruiken voor andere Google-diensten. IP-adressen worden geanonimiseerd, zodat deze niet persoonlijk herleid kunnen worden. Via de link in de privacyverklaring komt de betrokkene uit bij het privacybeleid van Google, die gericht is op de Analytics. Het beleid is bedoeld om de betrokkene inzicht te geven in de gegevens die verzameld worden, waarom deze verzameld worden, hoe de betrokkene de gegevens kan updaten, beheren, exporteren en verwijderen.<sup>188</sup> Google biedt ook een blokkademogelijkheid voor het volgen van het bezoek aan de website met Google Analytics, hierop kan de betrokkene gewezen worden, maar daar is in de privacyverklaring geen gebruik van gemaakt.<sup>189</sup>

Om de gebruikerservaring van de website te verbeteren, wordt gebruik gemaakt van Hotjar (een softwareprogramma). Ook hiermee is een verwerkersovereenkomst<sup>190</sup> afgesloten op 6 juni 2018.<sup>191</sup> In de verwerkersovereenkomst wordt rekening gehouden met de AVG. Het verwerken van de persoonsgegevens geschiedt voor marketingdoeleinden. Dit kan als rechtmatige verwerking van persoonsgegevens worden beschouwd, als het noodzakelijk is voor de belangenafweging op grond van artikel 6 lid 1 sub f AVG. Er dient echter een afweging plaats te vinden tussen het belang van de verwerkingsverantwoordelijke bij het verwerken van de persoonsgegevens en het recht van de betrokkene op privacy. Om erachter te komen welke gegevens er verzameld worden door Hotjar, moet de website van Hotjar geraadpleegd worden. Deze is te raadplegen via de link in de privacyverklaring. Verder staat vermeld hoe de betrokkene bezwaar kan maken tegen de gegevensverwerking door Hotjar.

---

<sup>184</sup> Bijlage 1 Privacyverklaring Merford Holding B.V. (Zie paragraaf Cookies).

<sup>185</sup> Berkvens, Vinken, Wiegerinck, Wolters, Reijner & Van Gerwen, p. 61.

<sup>186</sup> Engelfriet, Chew-Meij & Kager 2018, p. 29.

<sup>187</sup> Bijlage 3 Verwerkersovereenkomst Google.

<sup>188</sup> Bijlage 1 Privacyverklaring Merford Holding B.V. (Zie paragraaf Google Analytics).

<sup>189</sup> Engelfriet, Chew-Meij & Kager 2018, p. 50.

<sup>190</sup> Bijlage 4 Verwerkersovereenkomst Hotjar.

<sup>191</sup> Bijlage 1 Privacyverklaring Merford Holding B.V. (Zie paragraaf Hotjar).

### 3.1.8 Beveiliging

Door Merford worden beveiligingsmaatregelen genomen om misbruik van en ongeautoriseerde toegang tot persoonsgegevens te beperken. In het bijzonder worden de volgende maatregelen genomen:<sup>192</sup>

- De gegevens worden na ontvangst opgeslagen in een apart afgeschermd systeem.
- Fysieke maatregelen voor toegangsbescherming.
- Er wordt gebruik gemaakt van beveiligde verbindingen.

Conform artikel 32 AVG wordt van de verwerkingsverantwoordelijke verlangd dat zij passende, technische en organisatorische maatregelen neemt om de beveiliging van de persoonsgegevens te waarborgen. Verdere informatie over de beveiliging van Merford is te vinden in paragraaf 4.4.

### 3.1.9 Bewaartermijnen

De gegevens worden niet langer dan noodzakelijk voor het doel waarvoor ze zijn ontvangen bewaard.<sup>193</sup> Op grond van artikel 5 lid 1 sub e AVG, mogen de persoonsgegevens niet langer worden bewaard dan noodzakelijk is voor het doel. De AVG noemt geen specifieke bewaartermijnen. De persoonsgegevens die via een contactformulier worden ingevuld, worden binnen één jaar na het laatste contactmoment verwijderd. Indien cookies geplaatst worden, wordt de informatie maximaal vijftig maanden bewaard in Google Analytics. Hierbij is het de vraag of deze termijn noodzakelijk is. Indien deze termijn niet noodzakelijk is, wordt er niet voldaan aan het beginsel van opslagbeperking. Op grond van artikel 30 lid 1 sub f AVG moeten de bewaartermijnen vastgelegd worden in een verwerkingsregister, indien mogelijk.

### 3.1.10 Websites van derden

De privacyverklaring is niet van toepassing op websites van derden, die door middel van links met de website van Merford verbonden zijn. Merford kan niet garanderen dat deze derden op een betrouwbare of veilige manier met de persoonsgegevens omgaan. Het wordt aangeraden om de privacyverklaring van betreffende website te lezen, alvorens gebruik te maken van de website.<sup>194</sup> Conform de AVG is het niet verplicht om bovenstaande op te nemen in een privacyverklaring. Dit is echter wel verstandig.

### 3.1.11 Wijzigingen in deze privacyverklaring

Merford behoudt het recht om wijzigingen aan te brengen in deze privacyverklaring. Het verdient aanbeveling om deze privacyverklaring geregeld te raadplegen, zodat de betrokkene van de wijzigingen op de hoogte is.<sup>195</sup> Nergens in de AVG staat dat een privacyverklaring niet gewijzigd mag worden, zolang de privacyverklaring maar niet in strijd is met de AVG.

### 3.1.12 Inzage en wijzigen van uw gegevens

De betrokkene kan een verzoek sturen om zijn gegevens in te zien, te wijzigen of te verwijderen. Om misbruik te voorkomen, kan aan de betrokkene gevraagd worden om zich te identificeren. Indien de gegevens niet kloppen, kan er verzocht worden om de gegevens te wijzigen of te laten verwijderen.<sup>196</sup> Deze rechten voor de betrokkene zijn vastgelegd in de artikelen 15 tot en met 17 AVG, welke door Merford gehoorzaamd moeten worden. Het recht uit artikel 18 AVG, beperking van de verwerking, wordt niet genoemd in deze privacyverklaring.

---

<sup>192</sup> Bijlage 1 Privacyverklaring Merford Holding B.V. (Zie paragraaf *Beveiliging*).

<sup>193</sup> Bijlage 1 Privacyverklaring Merford Holding B.V. (Zie paragraaf *Bewaartermijnen*).

<sup>194</sup> Bijlage 1 Privacyverklaring Merford Holding B.V. (Zie paragraaf *Websites van derden*).

<sup>195</sup> Bijlage 1 Privacyverklaring Merford Holding B.V. (Zie paragraaf *Wijzigingen in deze privacyverklaring*).

<sup>196</sup> Bijlage 1 Privacyverklaring Merford Holding B.V. (Zie paragraaf *Inzage en wijzigen van uw gegevens*).

### 3.1.13 Autoriteit Persoonsgegevens

Merford helpt de betrokkene graag verder als hij klachten heeft over de verwerking van zijn persoonsgegevens. Op grond van de privacywetgeving heeft de betrokkene het recht om een klacht in te dienen bij de AP. De betrokkene kan hiervoor contact opnemen met de AP.<sup>197</sup> Dit recht voor de betrokkene is vastgelegd in artikel 13 lid 2 sub d AVG. Dit recht moet expliciet aan de betrokkene gemeld worden.<sup>198</sup> Hier wordt door Merford aan voldaan, door dit recht in de privacyverklaring te noemen.

## 3.2 Privacyverklaring Akoestiekwinkel <sup>199</sup>

Voor de webwinkel van de Akoestiekwinkel van Merford is een aparte privacyverklaring opgesteld.<sup>200</sup> Voor de webwinkel worden meer privacygevoelige gegevens verwerkt, zoals betalingsgegevens. Voor de webwinkel is er daarom een aparte privacyverklaring opgesteld. Ook deze privacyverklaring is voor het laatst aangepast op 22 mei 2018. In de privacyverklaring staat dat via de website van Merford privacygevoelige gegevens worden verwerkt. Merford acht een zorgvuldige omgang met persoonsgegevens van groot belang. Bij de verwerking houdt Merford zich aan de eisen die de AVG stelt. Dit wordt puntsgewijs nader toegelicht in de privacyverklaring. De punten uit privacyverklaring worden hieronder besproken, waarbij de AVG wordt toegepast.

### 3.2.1 Gebruik van persoonsgegevens

Door de webwinkel worden uitsluitend de gegevens bewaard en gebruikt die door de betrokkene rechtstreeks worden gegeven. De gegevens die gebruikt worden, zijn: NAW-gegevens, telefoonnummer, factuuradres, e-mailadres en betalingsgegevens. Deze gegevens worden gebruikt voor de in de privacyverklaring genoemde doelen, zoals het plaatsen van een bestelling en het versturen van een nieuwsbrief.<sup>201</sup> De grondslag uit de AVG die voor het verwerken van de persoonsgegevens gebruikt wordt, is toestemming. Zoals in paragraaf 3.1.1 is toegelicht, moet Merford kunnen aantonen dat de betrokkene vrijwillig toestemming heeft gegeven voor de verwerking van de persoonsgegevens. Verder is het van belang dat Merford de betrokkene op de hoogte stelt dat de betrokkene het recht heeft om te allen tijde zijn toestemming in te trekken. Dit is niet terug te vinden in deze privacyverklaring.

### 3.2.2 Registreren

Voor bepaalde onderdelen is registratie verplicht. Na de registratie worden door Merford de gekozen gebruikersnaam en de opgegeven persoonsgegevens bewaard en eventueel de adresgegevens, indien de betrokkene dit invult. De gegevens worden niet aan derden verstrekt, tenzij dit noodzakelijk is in het kader van de uitvoering van de overeenkomst.<sup>202</sup> De grondslag uit de AVG die gebruikt wordt voor het verwerken van de persoonsgegevens, is noodzakelijkheid voor de uitvoering van de overeenkomst.<sup>203</sup> Het verstrekken van adresgegevens is bijvoorbeeld voor de transporteur van belang, omdat de transporteur anders de overeenkomst niet kan uitvoeren. Waarom en voor welke onderdelen registratie verplicht is, wordt niet nader toegelicht in de privacyverklaring.

### 3.2.3 Afhandelen bestelling

Indien de betrokkene een bestelling plaats in de webwinkel, wordt voor de afhandeling gebruik gemaakt van zijn persoonsgegevens. De persoonsgegevens kunnen ook aan derden worden verstrekt, indien dit nodig is voor een goede afhandeling. Toelichting hierover is verderop te vinden in de privacyverklaring.<sup>204</sup> Het is echter onduidelijk waar verderop in de

<sup>197</sup> Bijlage 1 Privacyverklaring Merford Holding B.V. (Zie paragraaf *Autoriteit Persoonsgegevens*).

<sup>198</sup> Engelfriet, Chew-Meij & Kager 2018, p. 78.

<sup>199</sup> Bijlage 2 Privacyverklaring Akoestiekwinkel.

<sup>200</sup> [www.akoestiekwinkel.nl](http://www.akoestiekwinkel.nl).

<sup>201</sup> Bijlage 2 Privacyverklaring Akoestiekwinkel (Zie paragraaf *Gebruik van persoonsgegevens*).

<sup>202</sup> Bijlage 2 Privacyverklaring Akoestiekwinkel (Zie paragraaf *Registreren*).

<sup>203</sup> Artikel 6 lid 1 sub b AVG.

<sup>204</sup> Bijlage 2 Privacyverklaring Akoestiekwinkel (Zie paragraaf *Afhandelen bestelling*).

privacyverklaring moet worden gezocht voor toelichting over verstrekking van persoonsgegevens aan derden. De persoonsgegevens worden gebruikt om ervoor te zorgen dat een correcte afhandeling van de bestelling kan plaatsvinden. Hier mag gebruik gemaakt worden van de persoonsgegevens, omdat dit noodzakelijk is voor het uitvoeren van de overeenkomst conform artikel 6 lid 1 sub b AVG.

#### 3.2.4 Reviews

Via de webwinkel kan de betrokkene uitgenodigd worden tot het schrijven van een review op de website of via de partner Kiyoh. Bij het schrijven van een recensie kan betrokkene zelf kiezen of hij zijn naam of andere gegevens deelt. Het wordt aangeraden om de relevante privacyverklaring van Kiyoh te lezen.<sup>205</sup> Met Kiyoh is een verwerkersovereenkomst afgesloten op 8 augustus 2018, die voldoet aan de AVG.<sup>206</sup> Voor Merford is het van belang hoe de betrokkene het product, contact en het bestelproces ervaren heeft. Indien het nodig is kan Merford haar werkwijze naar aanleiding van de reviews aanpassen. De betrokkene wordt niet verplicht tot het schrijven van een review. De grondslag uit de AVG die voor het verwerken van de persoonsgegevens gebruikt wordt, is toestemming.

#### 3.2.5 Deelname aan winacties

De persoonsgegevens die verwerkt worden voor winacties zijn naam en e-mailadres. Deze gegevens worden gebruikt om contact op te nemen met de winnaar(s) en voor het toezien van de levering van de gewonnen prijzen. Doordat de betrokkene kiest om deel te nemen aan de winactie, wordt ervan uitgegaan dat de betrokkene toestemming geeft voor de verwerking van zijn of haar persoonsgegevens. De betrokkene heeft te allen tijde het recht om de toestemming in te trekken voor verwerking van de persoonsgegevens. De gegevens worden dertig dagen na het einde van de winactie bewaard.<sup>207</sup> De grondslag uit de AVG die voor het verwerken van de persoonsgegevens gebruikt wordt, is toestemming. De betrokkene wil deelnemen aan een winactie en om hiervan gebruik te maken, moeten de naam en het e-mailadres worden doorgegeven. Het beginsel van dataminimalisatie wordt hier ook juist toegepast, er worden namelijk niet meer gegevens verzameld dan nodig is. Hier is het de vraag of het noodzakelijk is om de gegevens nog dertig dagen te bewaren na het einde van de winactie.

#### 3.2.6 Reclame

In de privacyverklaring van de webwinkel staat dat de betrokkene, naast de informatie op de website, ook op de hoogte gebracht kan worden van nieuwe producten en diensten per e-mail of via sociale media.<sup>208</sup> Hier geldt dat de betrokkene bij sociale media zelf kan bepalen of hij Merford wil volgen. In deze privacyverklaring is het niet duidelijk hoe de betrokkene zich moet aanmelden voor informatie per e-mail. Ook is het onduidelijk of nieuwsbrief en reclame wel of niet bij elkaar horen.

#### 3.2.7 Contactformulier en nieuwsbrief

Via de webwinkel wordt de mogelijkheid geboden om vragen te stellen middels een contactformulier. De gegevens die worden toegestuurd, worden bewaard zolang het naar de aard van het formulier of de inhoud van de e-mail nodig is voor een volledige beantwoording en afhandeling daarvan. Voor geïnteresseerden wordt een nieuwsbrief aangeboden. Iedere nieuwsbrief bevat een link voor afmelding. Het e-mailadres wordt met expliciete toestemming toegevoegd aan de lijst van abonnees.<sup>209</sup> Net zoals in paragraaf 3.1.3 is uitgelegd, kan ook hier de rechtmatigheid van de verwerking gekwalificeerd worden als noodzakelijk voor de belangenafweging. De persoonsgegevens worden namelijk verwerkt, om de vraag van de betrokkene te behandelen. De verplichte persoonsgegevens die de betrokkene in moet

<sup>205</sup> Bijlage 2 Privacyverklaring Akoestiekwinkel (Zie paragraaf *Reviews*).

<sup>206</sup> Bijlage 5 Verwerkersovereenkomst Kiyoh.

<sup>207</sup> Bijlage 2 Privacyverklaring Akoestiekwinkel (Zie paragraaf *Deelname aan winacties*).

<sup>208</sup> Bijlage 2 Privacyverklaring Akoestiekwinkel (Zie paragraaf *Reclame*).

<sup>209</sup> Bijlage 2 Privacyverklaring Akoestiekwinkel (Zie paragraaf *Contactformulier en nieuwsbrief*).

vullen, zijn: de voornaam, de achternaam, het telefoonnummer en het e-mailadres. Of hier is voldaan aan het beginsel van dataminimalisatie, is discutabel. Het is niet altijd nodig om een e-mailadres en een telefoonnummer te verwerken voor het opnemen van contact. Een keuze zou ook een optie kunnen zijn. Voor de nieuwsbrief geldt dat het e-mailadres van de betrokkene met expliciete toestemming wordt toegevoegd aan de lijst van abonnees. Het is echter niet duidelijk hoe de expliciete toestemming wordt verleend. Voor overige toelichting wordt verwezen naar paragraaf 3.1.3.

### 3.2.8 Locatiegegevens

Ook in de privacyverklaring van de webwinkel staat dat de locatiegegevens door Merford verzameld kunnen worden als dat nodig is voor de dienst.<sup>210</sup> De tekst uit de privacyverklaring van de webwinkel is identiek aan de tekst uit de privacyverklaring van Merford. Om deze reden wordt er verwezen naar paragraaf 3.1.4 voor een nadere toelichting.

### 3.2.9 Publicatie

Bij het gebruik van de webwinkel wordt door de betrokkene zelf opgegeven informatie gepubliceerd, met uitzondering van zoekmachines. De betrokkene kiest zelf welke informatie er wordt gepubliceerd en anonimiseren is mogelijk op verzoek.<sup>211</sup> De grondslag uit de AVG waarop de verwerking van deze persoonsgegevens is gebaseerd, is toestemming. De vereisten voor toestemming zijn eerder al besproken. Om wat voor soort informatie het gaat en waarom deze informatie wordt gepubliceerd, wordt niet duidelijk omschreven in de privacyverklaring.

### 3.2.10 Verstrekking aan derden

De persoonsgegevens kunnen worden doorgegeven aan de partners van de webwinkel. Deze partners zijn betrokken bij de uitvoering van de overeenkomst. Verder zijn op de website sociale media buttons opgenomen, waarmee de beheerder van deze diensten de persoonsgegevens van betrokkene verzamelt.<sup>212</sup> Het is niet duidelijk welke gegevens door de derden worden verzameld, waarom deze gegevens mogen worden verzameld en of dit geldt voor alle betrokkenen.

### 3.2.11 Cookies

Ook op de website van de webwinkel wordt gebruik gemaakt van cookies. Deze tekst is vrijwel identiek aan de tekst in de privacyverklaring van Merford. Een verschil is dat in deze privacyverklaring een toelichting wordt gegeven over de gegevens die een cookie bijhoudt tijdens een bezoek aan de website van de webwinkel.<sup>213</sup> Verder wordt op de website van de webwinkel apart uitleg gegeven over de cookies.<sup>214</sup> Voor verdere toelichting over de cookies wordt verwezen naar paragraaf 3.1.6.

### 3.2.12 Google Analytics

Om bij te houden hoe bezoekers de webwinkel gebruiken, wordt gebruik gemaakt van Google Analytics.<sup>215</sup> De tekst uit de privacyverklaring is identiek aan die van de privacyverklaring van Merford en daarom wordt voor verder toelichting verwezen naar het eerste gedeelte van paragraaf 3.1.7.

---

<sup>210</sup> Bijlage 2 Privacyverklaring Akoestiekwinkel (Zie paragraaf *Locatiegegevens*).

<sup>211</sup> Bijlage 2 Privacyverklaring Akoestiekwinkel (Zie paragraaf *Publicatie*).

<sup>212</sup> Bijlage 2 Privacyverklaring Akoestiekwinkel (Zie paragraaf *Verstrekking aan derden*).

<sup>213</sup> Bijlage 2 Privacyverklaring Akoestiekwinkel (Zie paragraaf *Cookies*).

<sup>214</sup> [www.akoestiekwinkel.nl/cookies](http://www.akoestiekwinkel.nl/cookies).

<sup>215</sup> Bijlage 2 Privacyverklaring Akoestiekwinkel (Zie paragraaf *Google Analytics*).

### 3.2.13 Beveiliging

De tekst over de beveiliging is vrijwel identiek aan het stukje uit de privacyverklaring van Merford. In deze privacyverklaring is toegevoegd dat de toegang tot persoonsgegevens wordt afgeschermd met een gebruikersnaam en wachtwoord.<sup>216</sup> Voor meer informatie over de beveiligingsmaatregelen wordt verwezen naar paragraaf 3.1.8.

### 3.2.14 Bewaartermijnen

De persoonsgegevens worden bewaard zolang de betrokkene een actieve klant is. Voor e-mail geldt dat de betrokkene als een inactieve klant wordt beschouwd, als de betrokkene het afgelopen jaar geen e-mail heeft geopend.<sup>217</sup> Op grond van artikel 5 lid 1 sub e AVG mogen de persoonsgegevens niet langer worden bewaard dan noodzakelijk is. Wanneer een klant als inactief wordt beschouwd wordt niet duidelijk omschreven, behalve voor e-mail. Waarom er voor de termijn van een jaar is gekozen wordt ook niet nader toegelicht. Verder is het nog de vraag of deze termijn noodzakelijk is.

### 3.2.15 Verwijdering van gegevens

Volgens artikel 17 AVG heeft de betrokkene het recht om op elk moment de door de webwinkel verwerkte persoonsgegevens te laten verwijderen. Hier zijn echter wel enkele uitzonderingen op.<sup>218</sup> De uitzonderingen zijn door Merford gebaseerd op artikel 17 lid 3 sub e AVG. De situaties wanneer persoonsgegevens niet verwijderd worden zijn logisch, veelal is dit in het belang van de organisatie of een onderzoek. De termijnen die erbij genoemd worden, kunnen als onlogisch ervaren worden. Waarom wordt bijvoorbeeld een termijn aangehouden van drie of vier jaar in bepaalde situaties?

### 3.2.16 Websites van derden

Deze privacyverklaring is niet van toepassing op de websites van derden die door middel van links met de webwinkel zijn verbonden.<sup>219</sup> Voor meer informatie, zie paragraaf 3.1.10.

### 3.2.17 Wijzigingen in deze privacyverklaring

Verder is in deze privacyverklaring opgenomen dat Merford het recht behoudt om wijzigingen aan te brengen in deze verklaring.<sup>220</sup> Dit is toegestaan, zolang de privacyverklaring niet in strijd is met de AVG.

### 3.2.18 Inzage en wijzigen van uw gegevens

De betrokkene kan een verzoek sturen om de gegevens in te zien, te wijzigen, te beperken of te verwijderen.<sup>221</sup> Deze rechten voor de betrokkene zijn vastgelegd in de artikelen 15 tot en met 18 AVG.

### 3.2.19 Autoriteit Persoonsgegevens

Merford helpt de betrokkene graag verder als hij een klacht heeft over de verwerking van zijn persoonsgegevens.<sup>222</sup> Dit recht is vastgelegd in artikel 13 lid 2 sub d de AVG. Voor verdere uitleg, zie paragraaf 3.1.13.

---

<sup>216</sup> Bijlage 2 Privacyverklaring Akoestiekwinkel (Zie paragraaf *Beveiliging*).

<sup>217</sup> Bijlage 2 Privacyverklaring Akoestiekwinkel (Zie paragraaf *Bewaartermijnen*).

<sup>218</sup> Bijlage 2 Privacyverklaring Akoestiekwinkel (Zie paragraaf *Verwijdering van gegevens*).

<sup>219</sup> Bijlage 2 Privacyverklaring Akoestiekwinkel (Zie paragraaf *Websites van derden*).

<sup>220</sup> Bijlage 2 Privacyverklaring Akoestiekwinkel (Zie paragraaf *Wijzigingen in deze privacyverklaring*).

<sup>221</sup> Bijlage 2 Privacyverklaring Akoestiekwinkel (Zie paragraaf *Inzage en wijzigen van uw gegevens*).

<sup>222</sup> Bijlage 2 Privacyverklaring Akoestiekwinkel (Zie paragraaf *Autoriteit Persoonsgegevens*).

### 3.3 Tussenconclusie

In dit hoofdstuk zijn de privacyverklaringen van Merford getoetst aan de AVG. In beide verklaringen is niet terug te vinden dat de betrokkene het recht heeft om zijn toestemming in te trekken. Zowel Merford als de webwinkel kunnen reclame verstrekken aan de betrokkene. Het is niet duidelijk of de betrokkene zich hiervoor moet aanmelden. Vragen kunnen gesteld worden via een contactformulier. De grondslag uit de AVG hiervoor is noodzakelijkheid voor belangenafweging. Verder worden door Merford en de webwinkel een nieuwsbrief aangeboden. Om een nieuwsbrief te ontvangen moet de betrokkene zich inschrijven en iedere nieuwsbrief bevat een link voor afmelding. In beide privacyverklaringen staat dat de locatiegegevens kunnen worden verzameld als het nodig is voor de dienst. Wat er met de gegevens gebeurt als ze niet meer nodig zijn en hoe lang de gegevens worden bewaard, is niet terug te vinden in de verklaringen. Derden verzamelen gegevens van de betrokkene via sociale media buttons. Welke gegevens dit zijn en waarom ze worden verzameld, is onduidelijk. Merford maakt ook gebruik van cookies. Om bij te houden hoe bezoekers de website van Merford en de webwinkel gebruiken, wordt Google Analytics gebruikt. Verder worden door Merford beveiligingsmaatregelen genomen, wat verplicht is conform artikel 32 AVG. De gegevens worden niet langer bewaard dan noodzakelijk voor het doel waarvoor ze zijn ontvangen. Merford en de webwinkel behouden het recht om wijzigingen aan te brengen in de privacyverklaringen. Het recht op inzage, correctie en verwijdering is ook opgenomen in beide privacyverklaringen. Net zoals het recht dat de betrokkene heeft om in bezwaar te gaan. Het recht van beperking ontbreekt echter in de privacyverklaring van Merford. De privacyverklaring van de webwinkel is uitgebreider. In deze privacyverklaring is onder andere opgenomen dat registratie verplicht is voor bepaalde onderdelen. Ook voor de afhandeling van de bestelling wordt gebruik gemaakt van de persoonsgegevens. Dit is noodzakelijk voor het uitvoeren van de overeenkomst. Verder kan de betrokkene worden uitgenodigd tot het schrijven van een review op de website of via de partner Kiyoh. Bij de webwinkel is het mogelijk om deel te nemen aan winacties. Hierbij worden minimale persoonsgegevens gebruikt, namelijk alleen een naam en een e-mailadres. De privacyverklaringen voldoen dus nog niet aan de AVG. De aanbevelingen op basis van dit hoofdstuk worden in hoofdstuk 5 besproken. Eerst wordt in het volgende hoofdstuk de huidige werkwijze van Merford getoetst aan de AVG.

## Hoofdstuk 4 Huidige werkwijze Merford versus de AVG

In dit hoofdstuk wordt de huidige werkwijze van Merford met betrekking tot de verwerking van de persoonsgegevens van haar klanten en leveranciers getoetst aan de AVG. Om erachter te komen wat de huidige werkwijze van Merford is, zijn verschillende medewerkers geïnterviewd. Zo zijn er medewerkers van de verkoopafdeling geïnterviewd, een applicatiebeheerder en een persoon van marketing. Om de huidige werkwijze te toetsen aan de AVG wordt er gekeken naar de verzameling en verwerking van de persoonsgegevens, de bewaartermijnen, de rechten van de betrokkene en naar privacy by design and privacy by default. Ook wordt er gekeken naar de beveiliging, het begrip datalek, de functionaris gegevens, doorgifte van persoonsgegevens en de samenwerking met landen buiten de EU. Ten slotte volgt de conclusie van dit hoofdstuk.

### 4.1 Verzameling en verwerking persoonsgegevens

Zoals in paragraaf 2.2.2 is besproken, moet elke verwerking van persoonsgegevens aan de zes basisbeginselen voldoen uit artikel 5 AVG. Het verzamelen van persoonsgegevens geschiedt op diverse manieren. De gegevens worden digitaal verzameld, per e-mail of via het contact door de klant zelf. Veelal is sprake van zakelijke klanten, maar er zijn ook particuliere klanten aanwezig.<sup>223</sup> De gegevens voor de website worden verzameld via het CMS-systeem, dat is de achterkant van de website. Hier stromen alle gegevens doorheen en die worden weer aan de juiste database gekoppeld. De contactformulieren gaan via MailCampaigns, waar op 9 maart 2018 een verwerkersovereenkomst mee is afgesloten. De verwerkersovereenkomst voldoet aan de AVG.<sup>224</sup>

Het is de bedoeling dat de medewerkers ervoor zorgen dat de gegevens juist zijn om contact op te nemen met de klanten en leveranciers. De gegevens die worden verwerkt, zijn onder andere NAW-gegevens, telefoonnummers, e-mailadressen en de gegevens uit de Kamer van Koophandel (hierna: KvK). Verder wordt de functienaam ook weleens verwerkt.<sup>225</sup> Voor de webwinkel worden ook nog betalingsgegevens verwerkt voor zowel particuliere als zakelijke klanten. Deze gegevens zijn specifiek bedoeld voor de webwinkel.<sup>226</sup>

*“Bij het factureren moeten de gegevens er goed in staan. Een typefoutje is zo gemaakt.”  
– Commercieel administratief medewerkster<sup>227</sup>*

Het systeem waar de gegevens voornamelijk verzameld en verwerkt worden, bestaat uit twee delen. Enerzijds het CRM-systeem, dat heet Synergy en daar worden veel relaties in aangemaakt. Anderzijds is er het ERP-systeem en dat heet Exact. Synergy en Exact zijn broer en zus van elkaar en zijn zo ingericht dat ze gegevens met elkaar uitwisselen. Voor de gegevens van klanten en leveranciers is het namelijk handiger om in een CRM-systeem te werken. Financiële handelingen gebeuren in het ERP-systeem. Beide pakketten worden gebruikt om de gegevens compleet te maken.<sup>228</sup>

Van Excel wordt zelden gebruik gemaakt.<sup>229</sup> Excel wordt niet als einddoel gebruikt.<sup>230</sup> Het is meestal de plek waar de gegevens tijdelijk worden verzameld, omdat dat handig is.

Via de website worden de betrokkene geïnformeerd over de verwerking van de persoonsgegevens en vanuit diverse plekken wordt verwezen naar de privacyverklaring.<sup>231</sup> De zakelijke klanten worden niet geïnformeerd over de verwerking van de gegevens.<sup>232</sup> Gelet op de beginselen van behoorlijke en transparante verwerking, moet de betrokkene op de hoogte worden gesteld van het feit dat er verwerking plaatsvindt en de doeleinden

<sup>223</sup> Bijlage 7 Interview 1, Bijlage 9 Interview 3, Bijlage 10 Interview 4 & Bijlage 11 Interview 5.

<sup>224</sup> Bijlage 6 Verwerkersovereenkomst MailCampaigns.

<sup>225</sup> Bijlage 7 Interview 1.

<sup>226</sup> Bijlage 10 Interview 4.

<sup>227</sup> Bijlage 7 Interview 1.

<sup>228</sup> Bijlage 8 Interview 2.

<sup>229</sup> Bijlagen 7-11 Interview 1-5.

<sup>230</sup> Bijlage 8 Interview 2.

<sup>231</sup> Bijlage 10 Interview 4.

<sup>232</sup> Bijlage 7 Interview 1, Bijlage 9 Interview 3 & Bijlage 11 Interview 5.

daarvan.<sup>233</sup> Dit geldt dus ook voor de zakelijke klanten waarvan persoonsgegevens worden verwerkt.

## 4.2 Bewaartermijnen

Het beginsel van opslagbeperking houdt in dat de persoonsgegevens niet langer mogen worden bewaard dan noodzakelijk is voor de verwerking ervan. Dit is uitgewerkt in paragraaf 2.2.2. Op dit moment is er geen vaste termijn voor het bewaren van de gegevens.<sup>234</sup> Voor de webwinkel geldt dat een wettelijke termijn wordt gehanteerd, omdat hier voornamelijk sprake is van verwerking van persoonsgegevens van particulieren.<sup>235</sup> De gegevens op Google Analytics worden vijftig maanden bewaard.<sup>236</sup> Hiervoor geldt dat er een keuze is uit het bewaren van 14, 24, 36 of 50 maanden. De keuze van vijftig maanden is willekeurig.<sup>237</sup> Hierbij is het de vraag of het noodzakelijk is om de gegevens vijftig maanden te bewaren. Indien de opslag van de gegevens van Google Analytics met minder maanden kan worden bewaard en hier is niet voor gekozen, dan is er niet voldaan aan het beginsel van opslagbeperking.

*“De gegevens worden in principe bewaard.” – Applicatiebeheerder<sup>238</sup>*

Indien een contactpersoon uit dienst is getreden bij een organisatie, wordt deze persoon op non-actief gezet.<sup>239</sup> De gegevens van (zakelijke) klanten en leveranciers worden niet actief verwijderd.<sup>240</sup> Dit is in strijd met het beginsel van opslagbeperking, omdat de gegevens langer worden bewaard dan noodzakelijk is voor de verwerking. De gegevens worden wel opgeschoond, maar het is niet bekend of hier vaste richtlijnen voor zijn. De medewerkers zien het als een punt van aandacht om een duidelijke procedure te hebben tegen vervuiling.<sup>241</sup> Het lastige van klanten en leveranciers is dat iemand een paar jaar geen producten kan afnemen of niks kan leveren, maar toch een potentiële klant blijft. Indien een klant of leverancier een lange tijd niets heeft besteld of heeft geleverd wordt die niet uit het systeem gezet.<sup>242</sup>

Voor de klantenservice van de webwinkel geldt dat de gegevens definitief worden verwijderd. De e-mail van de klantenservice van de webwinkel wordt om de zoveel tijd verwijderd. Hiervoor is geen specifieke termijn vastgesteld. Indien het om een klacht of vraag gaat, wordt de e-mail na afhandeling vrijwel direct verwijderd. De e-mails worden niet opgeslagen. Het is niet bekend of de gegevens van het contactformulier worden verwijderd, die gegevens komen automatisch bij betreffende managers terecht. Vaste regels voor de verwijdering van gegevens zijn er nog niet.<sup>243</sup>

## 4.3 Realisatie rechten van betrokkene

De betrokkene heeft recht op inzage, rectificatie, gegevenswissing en beperking van de verwerking. Deze rechten zijn vastgelegd in de artikelen 15 tot en met 18 AVG en in de privacyverklaringen van Merford. De partijen waar Merford mee samenwerkt hebben een bepaalde sectie opgebouwd, die ervoor zorgt dat indien het e-mailadres van iemand ingevuld wordt, dit e-mailadres dan ook overal wordt verwijderd. Dit geldt voor het uitschrijven van de nieuwsbrieven. Een verzoek op inzage, rectificatie en beperking van de verwerking is nog niet gedaan door een betrokkene. Het is nog onduidelijk hoe deze rechten gerealiseerd

---

<sup>233</sup> Overweging 60 AVG.

<sup>234</sup> Bijlage 7 Interview 1, Bijlage 8 Interview 2, Bijlage 9 Interview 3 & Bijlage 11 Interview 5.

<sup>235</sup> Bijlage 11 Interview 5.

<sup>236</sup> Bijlage 2 Privacyverklaring Akoestiekwinkel.

<sup>237</sup> Bijlage 10 Interview 4.

<sup>238</sup> Bijlage 8 Interview 2.

<sup>239</sup> Bijlage 11 Interview 5.

<sup>240</sup> Bijlage 7 Interview 1, Bijlage 8 Interview 2, Bijlage 9 Interview 3 & Bijlage 11 Interview 5.

<sup>241</sup> Bijlage 9 Interview 3.

<sup>242</sup> Bijlage 8 Interview 2.

<sup>243</sup> Bijlage 10 Interview 4.

zullen worden. Merford geeft aan dat aan het verzoek natuurlijk altijd zal worden voldaan. Indien de betrokkene een account heeft, dan kan hij de gegevens altijd inzien.<sup>244</sup>

#### 4.4 Beveiliging

In artikel 32 AVG is de beveiliging van de verwerking van persoonsgegevens uitgewerkt. De AVG noemt een viertal maatregelen die een organisatie ten minste moet nemen. Deze zijn uitgewerkt in paragraaf 2.2.5.8. De applicatiebeheerders van Merford weten wie toegang heeft tot het netwerk van Merford. Per persoon is een setje met rechten gekoppeld aan betreffende persoon. Voor de digitale mappen geldt dat vooraf toestemming wordt gevraagd aan de betreffende persoon en manager, voordat de toegang wordt verleend. Het principe is dat de kraan voornamelijk dicht zit en dat die alleen wordt opengedraaid waar het nodig is. Specifiek gebeurt dit op verzoek. Wanneer iemand een verzoek indient, kan het even duren voor hij een reactie krijgt. Dit komt omdat de informatie in principe niet openbaar is. Iemand die zich bezighoudt met financiën, krijgt bijvoorbeeld alleen toegang tot de betreffende map. Op programmaniveau of op applicatieniveau is ook sprake van rechtenuitdelingen. Er wordt altijd een grove scheidingslijn gemaakt tussen management, finance en human resource management. Dit zijn de drie categorieën waar iemand alleen toegang tot krijgt als dit zo is afgesproken, bijvoorbeeld vanwege de functie. Dit wordt allemaal ook vastgelegd. Een van de applicatiebeheerders probeert zelf direct actie te ondernemen, als iemand vanuit zijn beperkte rol meer kan zien dan de bedoeling is.<sup>245</sup>

*“De insteek is om qua beveiliging ook up-to-date te blijven.” – Applicatiebeheerder<sup>246</sup>*

De gegevens van de website worden versleuteld verstuurd, namelijk via SSL. De websites zijn ook beveiligd en dat is te zien aan de https. In het CMS-systeem kunnen gebruikersrollen worden toegewezen. Iemand krijgt dan een bepaalde rol, zodat diegene alleen bepaalde zaken achter de schermen kan zien en niet alles.<sup>247</sup>

De maatregelen die de organisatie ten minste moet nemen, zijn niet schriftelijk terug te vinden bij Merford. Aan een van de vier maatregelen wordt overigens nog niet voldaan. Er is namelijk nog geen vaste procedure om de beveiliging van de verwerking te testen, te beoordelen en te evalueren. Dit moet dus nog gerealiseerd worden. Verder worden de gegevens niet gepseudonimiseerd, maar dit is passend aangezien de gegevens versleuteld worden en minimale gegevens worden verwerkt.

Er wordt niet dagelijks beziggehouden met het beveiligen, maar het blijft in ontwikkeling. Als iets naar boven komt wat niet veilig lijkt, wordt er naar een oplossing gezocht.<sup>248</sup>

#### 4.5 Privacy by design and privacy by default

Privacy by design and privacy by default is geregeld in artikel 25 AVG. De begrippen zijn uitgewerkt in paragraaf 2.2.5.4 en zijn van belang voor de makers van het registratiesysteem van de persoonsgegevens. Voor Merford is het van belang dat het juiste systeem wordt gekozen, waarbij rekening moet worden gehouden met de privacy van de betrokkene en de vereisten uit de AVG. Dit geldt ook voor de maatregelen omtrent gegevensverwerking. Verder is het van belang voor Merford dat inbreuk op persoonsgegevens van de betrokkene zo veel mogelijk wordt beperkt. Dit betekent dat er in het systeem niet meer persoonsgegevens mogen worden verzameld dan noodzakelijk is. Met de software die Merford momenteel gebruikt, wordt rekening gehouden met de AVG. De software dateert van voor 25 mei 2018, maar de applicatiebeheerders houden rekening met de AVG en werken samen met de leverancier van de software, om de programma's zo te creëren dat niet iedereen bij de gegevens kan. Ook wordt ervoor gezorgd dat geen onnodige persoonsgegevens worden verwerkt door bepaalde velden uit te schakelen. Om naleving

---

<sup>244</sup> Bijlage 10 Interview 4.

<sup>245</sup> Bijlage 8 Interview 2.

<sup>246</sup> Bijlage 8 Interview 2.

<sup>247</sup> Bijlage 10 Interview 4.

<sup>248</sup> Bijlage 8 Interview 2.

van privacy by design and privacy by default aan te kunnen tonen, moet Merford interne beleidsmaatregelen nemen en maatregelen toepassen die voldoen aan de beginselen van gegevensbescherming door ontwerp en gegevensbescherming door standaardinstellingen.<sup>249</sup> De manager moet aangeven of iemand toegang mag krijgen tot het systeem en in welke mate diegene toegang mag krijgen.<sup>250</sup> Naar aanleiding van de interviews met de werknemers, is niet de indruk verkregen dat er onnodige persoonsgegevens worden verzameld van de betrokkenen.

#### 4.6 Datalekken

Indien een inbreuk in verband met persoonsgegevens heeft plaatsgevonden is er sprake van een datalek. De meldplicht van een datalek is uitgewerkt in de artikelen 33 en 34 AVG en in paragraaf 2.2.5.9 van dit onderzoeksrapport. Het is niet bekend of in het verleden datalekken zijn voorgekomen bij Merford. Dit wil niet zeggen dat het niet gebeurd is. De medewerkers kunnen momenteel weinig vertellen over de procedure van een datalek, wanneer sprake is van een datalek of wat onder een datalek valt.<sup>251</sup> Het is van belang dat de medewerkers weten wat een datalek is en wanneer er sprake is van een datalek. Een datalek kan namelijk resulteren in lichamelijke, materiële of immateriële schade voor de betrokkene, indien het probleem niet tijdig of op een passende wijze wordt aangepakt.<sup>252</sup>

*“Niet dat ik weet.” – Sales engineer<sup>253</sup>*

#### 4.7 Functionaris gegevensbescherming

Een FG kan vrijwillig worden aangesteld, maar in sommige gevallen is een FG verplicht. De FG is het eerste aanspreekpunt voor de betrokkene die vragen of klachten heeft met betrekking tot de verwerking van de persoonsgegevens.<sup>254</sup> Conform artikel 37 AVG is het voor Merford niet verplicht om een FG aan te stellen. In de verwerkersovereenkomsten wordt een medewerker als FG benoemd, zodat diegene als aanspreekpunt kan worden gezien, maar diegene is niet officieel aangesteld.

Betreffende persoon heeft ook geen (professionele) kennis van de AVG. In de toekomst wil Merford wel graag officieel een FG aanstellen.

#### 4.8 Doorgifte persoonsgegevens

Conform artikel 44 AVG mogen de verwerkte persoonsgegevens, slechts worden doorgegeven, mits aan de overige bepalingen van de AVG worden voldaan door de verwerker en de verwerkingsverantwoordelijke.

Het ligt niet voor de hand om gegevens extern uit te wisselen.<sup>255</sup> Op databaseniveau worden geen gegevens uitgewisseld met andere partijen. Het is handig als de transporteur, die een relatie is, de gegevens van de eind- of tussenklant of tussentransporteur te zien krijgt. Dit is gerelateerd aan de werkzaamheden.<sup>256</sup> De afdeling marketing wisselt wel gegevens uit met enkele externe partijen, maar met deze partijen zijn verwerkersovereenkomsten afgesloten.<sup>257</sup> Het is lastig om te controleren wat iemand exact doet. Momenteel zit er geen blokkade op het systeem om gegevens uit te wisselen. Het is een risico dat nog ingeperkt moet worden.<sup>258</sup>

*“De gegevens worden niet bewust uitgewisseld naar een ander bedrijf.”  
– Commercieel administratief medewerkster<sup>259</sup>*

---

<sup>249</sup> Overweging 78 AVG.

<sup>250</sup> Bijlage 8 Interview 2.

<sup>251</sup> Bijlagen 7-11 Interview 1-5.

<sup>252</sup> Overweging 85 AVG.

<sup>253</sup> Bijlage 9 Interview 3.

<sup>254</sup> Van der Sloot 2018, p. 96.

<sup>255</sup> Bijlage 9 Interview 3 & Bijlage 11 Interview 5.

<sup>256</sup> Bijlage 7 Interview 1 & Bijlage 8 Interview 2.

<sup>257</sup> Bijlage 10 Interview 4.

<sup>258</sup> Bijlage 8 Interview 2.

<sup>259</sup> Bijlage 7 Interview 1.

#### 4.9 Samenwerking met partijen buiten de EU

De AVG is conform artikel 3 AVG van toepassing op de verwerking van persoonsgegevens in het kader van de activiteiten van een vestiging van een verwerkingsverantwoordelijke of een verwerker in de EU. Wie in de EU gevestigd is als verwerkingsverantwoordelijke of verwerker valt onder de werkingssfeer van de AVG, dit geldt ook voor Merford.<sup>260</sup> De definitie van vestiging is terug te vinden in de begrippenlijst.

Er wordt met partijen samengewerkt die niet in de EU zitten. Een aantal van de business units handelen met partijen buiten de EU. Hierbij moet gedacht worden aan China, Zuid-Amerika en India. Voor zover het bekend is worden deze gegevens hetzelfde behandeld als die van de klanten in de EU.<sup>261</sup> De verwerking van gegevens van partijen buiten de EU, vindt binnen de EU plaats en dus is de AVG ook hierbij van toepassing.

Momenteel wordt er niet samengewerkt met leveranciers die buiten de EU zitten. Wat betreft leveranciers wordt er voornamelijk gericht op Nederland, België, Duitsland, Verenigd Koninkrijk en af en toe op Scandinavië.<sup>262</sup> Ook hier geldt weer dat de AVG voor Merford dan gewoon van toepassing is.

#### 4.10 Tussenconclusie

Uit dit hoofdstuk blijkt dat de gegevens voornamelijk digitaal worden verzameld, per e-mail of via het contact door de klant zelf. De contactformulieren gaan via MailCampaigns, waarmee een verwerkersovereenkomst is afgesloten. Excel wordt alleen af en toe gebruikt om gegevens tijdelijk te verzamelen. Zakelijke klanten worden niet geïnformeerd over de verwerking van de persoonsgegevens. Verder is er momenteel geen vaste bewaartermijn van de gegevens. Voor de webwinkel wordt aan de wettelijke termijn voldaan. Voor Google Analytics wordt een termijn van vijftig maanden gehanteerd. Deze termijn is willekeurig gekozen. Het is verder nog onbekend hoe de rechten van de betrokkene gerealiseerd zullen worden. De beveiligingsmaatregelen die een organisatie ten minste moet nemen, zijn niet schriftelijk terug te vinden bij Merford. Bovendien wordt aan één maatregel nog niet voldaan. Verder zijn de medewerkers onbekend met de procedure van een datalek en wat als een datalek gekwalificeerd dient te worden. Op dit moment is er door Merford geen officiële FG aangesteld. Het ligt niet voor de hand om persoonsgegevens extern uit te wisselen, tenzij het gerelateerd is aan de werkzaamheden. Vanuit de marketingafdeling worden wel gegevens uitgewisseld met enkele externe partijen, maar daarmee zijn verwerkersovereenkomsten afgesloten. Ten slotte wordt er ook samengewerkt met partijen buiten de EU. Ook bij deze relaties is de AVG gewoon van toepassing. Er kan geconcludeerd worden dat de huidige werkwijze van Merford nog niet volledig AVG-proof is. In het volgende hoofdstuk worden aanbevelingen gegeven aan Merford om AVG-proof te worden.

---

<sup>260</sup> Engelfriet, Chew-Meij & Kager 2018, p. 18.

<sup>261</sup> Bijlage 8 Interview 2 & Bijlage 9 Interview 3.

<sup>262</sup> Bijlage 11 Interview 5.

## Hoofdstuk 5 Wijzigingen om AVG-proof te worden

Naar aanleiding van de voorgaande hoofdstukken kan geconcludeerd worden dat Merford nog niet volledig aan de AVG voldoet. In dit hoofdstuk worden eerst aanbevelingen gegeven aan Merford om de privacyverklaring van Merford Holding B.V. AVG-proof te maken. Vervolgens worden aanbevelingen gegeven met betrekking tot de privacyverklaring van de webwinkel, zodat deze ook AVG-proof kan worden gemaakt. Hierna worden aanbevelingen gegeven over de werkwijze van Merford en vervolgens worden de overige aanbevelingen behandeld. Ten slotte volgt de conclusie van dit hoofdstuk.

### 5.1 Privacyverklaring Merford Holding B.V.

In deze paragraaf worden alleen de paragrafen uit de privacyverklaring behandeld waarbij iets toegevoegd of aangepast moet worden.

#### 5.1.1 Inleiding privacyverklaring

Zoals in paragraaf 2.2.3 is besproken, heeft de betrokkene te allen tijde het recht om zijn toestemming in te trekken. De betrokkene moet hiervan op de hoogte zijn alvorens hij de toestemming geeft. De AVG bepaalt niet hoe dit moet gebeuren, maar een vermelding in de privacyverklaring is het meest passend.<sup>263</sup> Het is dan ook aan te raden om de informatie over de intrekking van de toestemming op te nemen in het inleidende gedeelte van de privacyverklaring, zodat de betrokkene hiervan al op de hoogte is bij het lezen van de privacyverklaring.

#### 5.1.2 Reclame

Het is in de privacyverklaring onduidelijk hoe de betrokkene zich moet aanmelden voor reclame. Verder kan hierbij nog de vraag gesteld worden of reclame en nieuwsbrief bij elkaar horen. Dit kan niet duidelijk opgemaakt worden uit de privacyverklaring. Hier wordt niet in strijd gehandeld met de AVG. Het is echter goed om duidelijkheid te creëren.

#### 5.1.3 Contactformulier en nieuwsbrief

Voor de verwerking van de persoonsgegevens van het contactformulier wordt niet specifiek toestemming gegeven, maar de verwerking kan gekwalificeerd worden als noodzakelijk, zoals in paragraaf 3.1.3 is toegelicht. Het is aan te raden om specifiek toestemming te vragen voor de verwerking van de persoonsgegevens en hierbij aangeven dat, indien geen toestemming wordt gegeven, er dan geen contact met de betrokkene kan worden opgenomen. Dit creëert meer duidelijkheid bij de betrokkene. Dat kan bijvoorbeeld met een vakje die de betrokkene kan aanvinken bij het invullen van het contactformulier. Een double opt-in maakt de toestemming verlenen voor de nieuwsbrief AVG-proof. Bij een double opt-in ontvangt de betrokkene een bericht met het verzoek de inschrijving op de nieuwsbrief nogmaals te bevestigen. Bewijstechnisch kan het beste met een double opt-in gewerkt worden. Een double opt-in maakt het namelijk zeer lastig om te weerleggen dat de eigenaar van de mailbox de nieuwsbrief wilde ontvangen.<sup>264</sup> Bij afmelding van de nieuwsbrief is het de vraag of het e-mailadres ook automatisch wordt verwijderd uit de lijst van abonnees. Indien dit het geval is, is het verstandig om dit te vermelden in de privacyverklaring. Als dit nog niet het geval is, dan moet hiervoor actie worden ondernomen.

#### 5.1.4 Locatiegegevens

De tekst in deze paragraaf kan veel vragen oproepen. Het is niet duidelijk wat er met de gegevens gebeurd als ze niet meer nodig zijn, hoe lang de gegevens worden bewaard en hoe de gegevens verzameld worden. Het is aan te raden om dit duidelijker weer te geven in de privacyverklaring. Voor wat voor soort diensten locatiegegevens worden verzameld kan completer worden weergegeven door er een voorbeeld bij te geven.

<sup>263</sup> Engelfriet, Chew-Meij & Kager 2018, p. 53.

<sup>264</sup> Engelfriet, Chew-Meij & Kager 2018, p. 39.

#### 5.1.5 Verstrekking aan derden

De tekst in deze paragraaf is kort en krachtig, maar een toelichting ontbreekt. Dit kan ervoor zorgen dat de betrokkene diverse vragen over deze paragraaf heeft. De betrokkene kan zich afvragen of de verstrekking aan derden geldt voor alle betrokkenen, welke gegevens door de derden worden verzameld en waarom dit mag. Het is aan te raden om deze tekst uit te breiden en daarbij bovenstaande vragen in te verwerken, voor zover dit mogelijk is.

#### 5.1.6 Cookies

De reden voor gebruik van cookies is niet terug te vinden in deze privacyverklaring, maar wel in de privacyverklaring van de webwinkel. Het is aan te raden om de reden voor het gebruik van cookies ook te verwerken in deze privacyverklaring. Er zijn verschillende soorten cookies te onderscheiden, waaronder cookies die noodzakelijk zijn.<sup>265</sup> Het is geen verplichting volgens de AVG om dit op te nemen in de privacyverklaring, maar als dit wordt gerealiseerd, kan het voor helderheid zorgen. Verder is het aan te raden om bij het geven van toestemming voor gebruik van cookies op de website, erbij te vermelden dat dit wordt opgevat als toestemming voor het gebruik van cookies op de gehele website.

#### 5.1.7 Google Analytics en Hotjar

Het is aan te raden om de bezoekers van de website erop te wijzen dat Google een blokkademogelijkheid biedt voor het volgen van het bezoek aan de website met Google Analytics. Dit kan opgenomen worden in privacyverklaring.<sup>266</sup> Voor verdere informatie over de blokkademogelijkheid voor de gebruiker, kan doorverwezen worden naar het beleid van Google.

In de privacyverklaring staat hoe er bezwaar kan worden gemaakt tegen de gegevensverwerking door Hotjar. Als een betrokkene op de link klikt ziet hij ook staan dat er een opt-out optie is. Het is aan te raden om de opt-out optie ook in de privacyverklaring te benoemen.

#### 5.1.8 Bewaartermijnen

De persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk is. De vraag bij de bewaartermijn van de persoonsgegevens is waarom de gegevens nog een jaar worden bewaard. Is dit wel noodzakelijk? Kunnen de gegevens misschien niet al na een half jaar verwijderd worden. Indien dit het geval is dan moet daarvoor gekozen worden, omdat anders niet wordt voldaan aan het beginsel van opslagbeperking. Het is aan te raden om in de privacyverklaring kort toe te lichten waarom de persoonsgegevens van het contactformulier na een jaar worden verwijderd.

#### 5.1.9 Inzage en wijzigen van persoonsgegevens

De betrokkene heeft ook het recht op beperking van de verwerking, zoals in paragraaf 2.2.4.5 is besproken. In de privacyverklaring van de webwinkel is dit wel opgenomen, maar niet in de privacyverklaring van Merford. Aangezien het een recht van de betrokkene is, is het aan te raden om dit recht ook op te nemen in deze privacyverklaring.

### 5.2 Privacyverklaring Akoestiekwinkel

Voor deze paragraaf geldt, net zoals voor paragraaf 5.1, dat alleen de paragrafen uit de privacyverklaring behandeld worden, waarbij wat toegevoegd of aangepast moet worden.

---

<sup>265</sup> Berkvens, Vinken, Wiegerinck, Wolters, Reijner & Van Gerwen 2018, p. 197-202.

<sup>266</sup> Engelfriet, Chew-Meij & Kager 2018, p. 50.

### 5.2.1 Inleiding privacyverklaring

In deze privacyverklaring is niet opgenomen dat de betrokkene te allen tijde het recht heeft om zijn toestemming in te trekken. Zoals in paragraaf 5.1.1 is toegelicht, is het aan te raden om dit op te nemen in het inleidende gedeelte van de privacyverklaring. Hiermee is de betrokkene al bij het lezen van de privacyverklaring op de hoogte van zijn recht op intrekking van de toestemming.

### 5.2.2 Registratie

Het is onduidelijk waarom en voor welke onderdelen registratie verplicht is. Op grond van de AVG is het niet verplicht om dit te benoemen, maar in het kader van transparantie van gegevensverwerking kan een toelichting voor verheldering zorgen bij de betrokkene. Het is aan te raden om kort toe te lichten waarom voor bepaalde onderdelen registratie verplicht is en hierbij een voorbeeld te noemen.

### 5.2.3 Afhandelen bestelling

In deze paragraaf staat dat indien het nodig is voor een goede afhandeling, de persoonsgegevens aan derden kunnen worden verstrekt. Voor meer informatie wordt verwezen naar verderop in de privacyverklaring. Het is echter niet direct duidelijk waar verderop in de privacyverklaring moet worden gezocht. Het is geen verplichting uit de AVG, maar het is aan te raden om duidelijker te verwijzen naar waar de toelichting te vinden is.

### 5.2.4 Deelname aan winacties

In de privacyverklaring staat dat de persoonsgegevens van de winactie tot dertig dagen na einde van de wedstrijd worden bewaard. Hierbij kan de vraag gesteld worden of het noodzakelijk is om de gegevens dertig dagen te bewaren. Indien dit niet het geval is, moet dit aangepast worden zodat aan het beginsel van opslagbeperking wordt voldaan. Indien het noodzakelijk is om de persoonsgegevens dertig dagen te bewaren, kan eventueel in het kort worden toegelicht waarom de persoonsgegevens dertig dagen worden bewaard. Verder staat in deze paragraaf het zinnetje: "De verwerking van uw persoonsgegevens is gebaseerd op uw toestemming wanneer u ervoor kiest om deel te nemen aan een wedstrijd." Als tip kan meegegeven worden om iets explicieter te vermelden dat de betrokkene bij deelname toestemming geeft voor de verwerking van zijn persoonsgegevens.

### 5.2.5 Reclame

Ook voor deze paragraaf geldt, net zoals in paragraaf 5.1.2 is besproken, dat het onduidelijk is hoe de betrokkene zich moet aanmelden voor de reclame. Hier wordt niet in strijd gehandeld met de AVG, maar het is verstandig om duidelijkheid te creëren.

### 5.2.6 Contactformulier en nieuwsbrief

Voor het contactformulier geldt dat eventueel de keuze aan de betrokkene kan worden gegeven om of een e-mailadres of een telefoonnummer te verwerken, omdat beiden niet noodzakelijk zijn.

Voor de nieuwsbrief geldt dat het e-mailadres slechts met expliciete toestemming wordt toegevoegd aan de lijst van abonnees. Uit de tekst in de privacyverklaring wordt niet op voorhand duidelijk wat onder expliciete toestemming wordt verstaan. Indien mogelijk, kan dit duidelijker worden aangegeven in de privacyverklaring. Verder maakt een double opt-in het geven van toestemming voor de nieuwsbrief AVG-proof, zoals in paragraaf 5.1.3 is toegelicht.

### 5.2.7 Locatiegegevens

Deze tekst is identiek aan die van de privacyverklaring van Merford. Ook deze tekst kan dus veel vragen oproepen. Zoals in paragraaf 5.1.4 is aangegeven is het aan te raden om in de privacyverklaring duidelijker weer te geven hoe de gegevens verzameld worden, hoe lang en wat er met de gegevens gebeurt als ze niet meer nodig zijn.

### 5.2.8 Publicatie

In de privacyverklaring staat dat door de betrokkene zelf opgegeven informatie gepubliceerd wordt. Hierbij kan de vraag gesteld worden of dit voor alle informatie geldt, of dat er nog uitzonderingen zijn. Voor verheldering kan eventueel een voorbeeld toegevoegd worden. Verder is het niet duidelijk waarom de informatie gepubliceerd wordt. Dit kan nog toegevoegd worden in de privacyverklaring.

### 5.2.9 Verstrekking aan derden

Bij deze paragraaf ontbreekt de toelichting. Zie paragraaf 5.1.5 voor een nadere uitwerking. Het is aan te raden om deze tekst uit te breiden, voor zover dit mogelijk is. De uitbreiding zal ervoor zorgen dat de betrokkene minder vragen heeft.

### 5.2.10 Cookies

Zoals in paragraaf 5.1.6 is besproken, is het aan te raden om bij het geven van toestemming voor gebruik van cookies op de website te vermelden dat dit wordt opgevat als toestemming voor het gebruik van cookies op de gehele website.

### 5.2.11 Google Analytics

Deze tekst is identiek aan de tekst uit de privacyverklaring van Merford. Het is dus aan te raden om bezoekers te wijzen op de blokkademogelijkheid die Google aanbiedt. Voor verdere informatie over de blokkademogelijkheid kan in de privacyverklaring doorverwezen worden naar het beleid van Google.

### 5.2.12 Bewaartermijnen

De persoonsgegevens worden bewaard zolang de betrokkene een actieve klant is. Wanneer een betrokkene een inactieve klant is, kan niet afgeleid worden uit de privacyverklaring. Is dit al wanneer de betrokkene één week niets heeft besteld, of na één jaar? Voor e-mail wordt de betrokkene als inactieve klant beschouwd als hij het afgelopen jaar geen e-mail heeft geopend. De vraag die hierbij gesteld kan worden is of een termijn van één jaar noodzakelijk is of dat het bijvoorbeeld ook met een termijn van zes maanden kan.

### 5.2.13 Verwijdering van gegevens

De termijnen die gehanteerd worden voor de uitzonderingen van de verwijdering van de verwerkte persoonsgegevens kunnen als onduidelijk ervaren worden door de betrokkene. Het is niet verplicht op grond van de AVG om dit vast te leggen. Voor Merford is het van belang dat zij helder voor ogen heeft of de termijn een wettelijke basis heeft of goed is overwogen, zodat het te allen tijde toegelicht kan worden aan de betrokkene indien die daar om vraagt.

## 5.3 Werkwijze

In deze paragraaf wordt besproken hoe de werkwijze van Merford AVG-proof kan worden gemaakt. Het advies wordt gegeven aan de hand van het vorige hoofdstuk, waarin de huidige werkwijze is getoetst aan de AVG.

### 5.3.1 Verzameling en verwerking persoonsgegevens

De AVG in acht genomen, is er weinig aan te merken op de verzameling en verwerking van persoonsgegevens. Er wordt niet de indruk gewekt dat er onnodig gegevens worden verzameld of verwerkt. Door middel van de privacyverklaring wordt op de website aangegeven welke persoonsgegevens worden verwerkt en waarom. Het is aan te raden om tijdens een telefoongesprek of in een e-mail aan te geven welke persoonsgegevens worden verwerkt en waarom, zodat de betrokkene hier meteen van op de hoogte is. Uit de interviews blijkt niet dat dit momenteel gebeurt.<sup>267</sup>

---

<sup>267</sup> Bijlage 7 Interview 1, Bijlage 9 Interview 3 & Bijlage 11 Interview 5.

### 5.3.2 Bewaartermijnen

Indien het niet nodig is om de gegevens op Google Analytics vijftig maanden te bewaren, is het verstandig om dit aan te passen. Indien dit wordt aangepast, wordt er voldaan aan het beginsel van opslagbeperking. Verder wordt in strijd gehandeld met het beginsel van opslagbeperking, namelijk voor de verwijdering van de e-mails uit de mailbox. Hier is geen vaste termijn voor en de e-mails worden om de zoveel tijd verwijderd. Dit betekent dat gegevens langer worden bewaard dan noodzakelijk is. Het is aan te raden om hier een vaste procedure voor te hebben. Bijvoorbeeld na afhandeling van betreffende e-mail wordt de e-mail binnen één maand verwijderd. Wat betreft de persoonsgegevens van (zakelijke) klanten en leveranciers wordt er ook niet voldaan aan het beginsel van opslagbeperking. Het is zelfs zo dat de gegevens niet actief worden verwijderd. Ook hier is het aan te raden om een vaste procedure te hebben voor controle van de persoonsgegevens van klanten en leveranciers om te voorkomen dat de gegevens langer worden bewaard dan noodzakelijk is.

### 5.3.3 Realisatie rechten van betrokkene

De betrokkene die een account heeft kan altijd zijn gegevens inzien. Voor een betrokkene die geen account heeft, is het nog onduidelijk hoe zijn rechten gerealiseerd zullen worden. Hiervoor moet actie ondernomen worden, zodat aan het verzoek van de betrokkene kan worden voldaan. Het betreft hier het recht op inzage, rectificatie, gegevenswissing en beperking van de verwerking.

### 5.3.4 Beveiliging

Het is geen verplichting conform de AVG om de maatregelen die een organisatie ten minste moet nemen schriftelijk vast te leggen. Dit is echter wel verstandig, omdat zo schriftelijk aangetoond kan worden dat er passende technische en organisatorische maatregelen worden genomen om de beveiliging te waarborgen. Verder wordt nog niet voldaan aan de verplichte maatregel om een vaste procedure te hebben om de beveiliging van de verwerking te testen, te beoordelen en te evalueren. Het advies is dan ook om hiervoor een procedure te maken en deze ook regelmatig uit te voeren, zodat er voldaan wordt aan artikel 32 lid 1 sub d AVG.

### 5.3.5 Privacy by design and privacy by default

Privacy by design moet aangetoond kunnen worden. Dit wil zeggen dat in de ontwerpdocumentatie van de software overal privacyoverwegingen en beslissingen moeten zijn opgenomen. Het is aan te raden wanneer Merford nieuwe software aanschaft, de leverancier aan te laten tonen en te laten garanderen dat dit het geval is.<sup>268</sup> Met de software die Merford momenteel gebruikt, wordt rekening gehouden met de AVG, zoals in paragraaf 4.5 is besproken. De eisen van privacy by design and privacy by default gelden niet alleen voor de software die vanaf 25 mei op de markt is gekomen, maar ook de software van voor 25 mei 2018 moet aan de eisen voldoen.<sup>269</sup> Op dit moment wordt er wat betreft software rekening gehouden met de AVG. Het is echter aan te raden om de genomen en de te nemen interne beleidsmaatregelen op papier te zetten, zodat naleving controleerbaar is. Voor uitleg over de begrippen privacy by design and privacy by default wordt verwezen naar paragraaf 2.2.5.4.

---

<sup>268</sup> Engelfriet, Chew-Meij & Kager 2018, p. 87.

<sup>269</sup> Engelfriet, Chew-Meij & Kager 2018, p. 88.

### 5.3.6 Datalekken

De medewerkers kunnen momenteel weinig vertellen over een datalek en hebben op dit moment geen idee wat onder een datalek valt of wat een datalek is. Het is belangrijk dat er bewustwording rondom het begrip datalek wordt gecreëerd. Alle inbreuken in verband met persoonsgegevens moeten namelijk gedocumenteerd worden.<sup>270</sup> Hoe de bewustwording gecreëerd kan worden, wordt in paragraaf 5.3.9 besproken. Het is verder aan te raden om een procedure voor een datalek te schrijven. Deze procedure kan uitgewerkt worden in een processchema, zodat de medewerkers een schematisch overzicht hebben van een datalek.<sup>271</sup> Zo weten medewerkers hoe een datalek aangepakt moet worden en kan er gekeken worden naar hoe een datalek vermeden en voorkomen kan worden.

### 5.3.7 Functionaris gegevensbescherming

Zolang geen officiële FG is aangesteld, is het aan te raden om de paragraaf FG in een verwerkersovereenkomst leeg te laten, omdat het voor Merford ook niet verplicht is om een FG aan te stellen. In de toekomst wil Merford graag officieel een FG aanstellen. Een voordeel van vrijwillig een FG aanstellen is dat hiermee een signaal wordt afgegeven aan de markt en toezichthouder dat serieus wordt omgegaan met privacy. Indien een FG wordt aangesteld, is het aan te raden om een intern beleidsstuk of ander document op te stellen om de onafhankelijkheid van de FG te waarborgen. Hierin kan worden opgenomen op welke wijze de FG in staat wordt gesteld om zijn functie op een onafhankelijke wijze uit te oefenen.<sup>272</sup>

### 5.3.8 Doorgifte persoonsgegevens

Het ligt niet voor de hand dat gegevens extern worden uitgewisseld, maar momenteel zit er geen blokkade op het systeem voor gegevensuitwisseling. Het is een risico wat nog ingeperkt kan worden.

### 5.3.9 Bewustwording creëren

Het is belangrijk dat de medewerkers in grote lijnen weten wat de AVG inhoudt, omdat het in principe voor iedereen van toepassing is. Om bewustwording te creëren kunnen er diverse trainingen over de AVG worden aangeboden aan de medewerkers. Zo kunnen medewerkers een erkend certificaat behalen na afronding van een videotraining.<sup>273</sup> Verder is een online trainingsmodule beschikbaar, die maar vijftien minuten tijd in beslag neemt. Na afronding van de module krijgt de deelnemer een certificaat van deelname.<sup>274</sup> Ook is er een interactieve AVG game beschikbaar die medewerkers bewust maakt van de AVG en het belang van het correct omgaan met privacygevoelige gegevens.<sup>275</sup>

## 5.4 Overig

In deze paragraaf worden de overige wijzigingen besproken voor Merford om AVG-proof te zijn. Deze wijzigingen worden hier besproken, omdat ze los staan van de privacyverklaringen en niet aan bod zijn gekomen bij de interviews over de huidige werkwijze.

### 5.4.1 Gegevensbeschermingsbeleid

Zoals in paragraaf 2.2.5.3 is besproken, wordt van de verwerkingsverantwoordelijke verwacht dat de genomen maatregelen worden uitgewerkt in een beleid en dat dit beleid vervolgens ook daadwerkelijk in de praktijk wordt uitgevoerd. Momenteel is er nog geen beleid waar de technische en organisatorische maatregelen in staan om de gegevensbescherming te waarborgen, er is alleen een privacyverklaring. Het is aan te raden om dit te realiseren, zodat de maatregelen op papier staan en ook aantoonbaar zijn.

---

<sup>270</sup> Artikel 33 lid 5 AVG.

<sup>271</sup> Candel & Nouwt, *P&I* 2016, p. 10.

<sup>272</sup> Schaik & Abassi, *Bedrijfsjuridische Berichten* 2017/95, p. 324-325.

<sup>273</sup> [www.bol.com](http://www.bol.com) (zoek op AVG videotrainingen voor medewerkers).

<sup>274</sup> [www.nexttech.nl](http://www.nexttech.nl) (zoek op voorbereiden op de AVG).

<sup>275</sup> [www.denieuwezaak.nl/avg](http://www.denieuwezaak.nl/avg).

#### 5.4.2 Verwerkingsregister

In paragraaf 2.2.5.6 is geconcludeerd dat Merford de verplichting heeft om een verwerkingsregister bij te houden. Merford houdt nog geen verwerkingsregister bij, maar om AVG-proof te worden moet dit wel gerealiseerd worden. Indien dit niet gerealiseerd wordt, wordt in strijd gehandeld met de AVG en kan er dus door de AP sancties worden opgelegd zoals in paragraaf 2.2.8 is besproken. Welke informatie ten minste in het verwerkingsregister moet komen te staan, is te vinden in paragraaf 2.2.5.6.

#### 5.4.3 Data Privacy Impact Assessment

Voor Merford is een DPIA niet vereist.<sup>276</sup> Zoals in paragraaf 2.2.5.10 is uitgelegd, is het vaak nuttig om een DPIA als standaard te hanteren. Bij een DPIA gaat een organisatie na, voordat er begonnen wordt met een nieuw plan waarbij persoonsgegevens worden verwerkt, of aan alle eisen van de AVG is voldaan, of er risico's zijn verbonden aan het plan in relatie tot de verwerking van de persoonsgegevens en welke maatregelen er kunnen worden getroffen om die risico's te vermijden of te beperken.<sup>277</sup> Het is dus aan Merford of er wel of geen DPIA wordt gehanteerd. Het is volgens de AVG in ieder geval niet verplicht, maar wel raadzaam.

### 5.5 Tussenconclusie

Uit dit hoofdstuk blijkt dat Merford nog enkele wijzigingen moet doorvoeren om AVG-proof te zijn. Voor de privacyverklaring van Merford geldt dat de betrokkene gewezen moet worden op zijn recht op intrekking van de toestemming. Verder kan de nieuwsbrief van Merford AVG-proof worden gemaakt door een double opt-in. Verder is in deze privacyverklaring het recht van beperking van de verwerking voor de betrokkene niet opgenomen. Voor de privacyverklaring van de webwinkel geldt dat het de vraag is of bij deelname aan winacties en de bewaartermijnen voldaan is het aan het beginsel van opslagbeperking. Dit moet nog door Merford gecontroleerd worden en eventueel worden aangepast. Verder kan ook hier de nieuwsbrief AVG-proof worden gemaakt door een double opt-in. De overige paragrafen voldoen aan de AVG, maar zijn nog ietwat onduidelijk. Een verheldering is dan ook te raden. Voor de bewaartermijnen, beveiliging van de verwerking en datalekken, geldt dat een vaste procedure moet worden ontwikkeld. Verder moet gekeken worden naar hoe de rechten van de betrokkenen gerealiseerd worden. Ook is het belangrijk dat er bewustwording omtrent de AVG wordt gecreëerd bij de medewerkers van Merford. Merford moet nog een gegevensbeschermingsbeleid opstellen en een verwerkingsregister, dit is verplicht op grond van de AVG. Ten slotte kan Merford een DPIA hanteren indien ze dit wil. In het volgende en tevens het laatste hoofdstuk, worden conclusies getrokken en aanbevelingen gegeven.

---

<sup>276</sup> Artikel 35 lid 3 AVG.

<sup>277</sup> Van der Sloot 2018, p. 97.

## Hoofdstuk 6 Conclusies en aanbevelingen

Op basis van de in de voorgaande hoofdstukken gedane bevindingen, worden in dit hoofdstuk conclusies getrokken en aanbevelingen gegeven. De centrale vraag luidt als volgt: *“Welke aanbevelingen kunnen, gelet op de relevante bepalingen uit de AVG, aan Merford worden gegeven ten aanzien van de privacyverklaringen en de huidige werkwijze met betrekking tot de verwerking van de persoonsgegevens van haar klanten en leveranciers?”*

### 6.1 Privacyverklaring Merford Holding B.V.

Op de website van Merford is een algemene privacyverklaring te vinden welke dateert van 22 mei 2018. Merford wil graag weten of de huidige privacyverklaring voldoet aan de AVG. Hieronder zijn de conclusies en aanbevelingen weergegeven van het onderzoek hiernaar.

#### 6.1.1 Conclusies

Er kan geconcludeerd worden dat de privacyverklaring van Merford nog niet volledig AVG-proof is. Hieronder wordt in tabelvorm aangegeven welke paragrafen wel en welke niet voldoen aan de AVG. Verder wordt in de tabel aangegeven welke paragrafen voldoen aan de AVG, maar als onduidelijk kunnen worden ervaren door de betrokkene en daarom verder toegelicht kunnen worden. Als laatste is een kolom toegevoegd waarin de paragrafen staan die niet verplicht zijn conform de AVG, maar waarvan het handig is dat Merford dit in de privacyverklaring heeft staan. Dit schept namelijk duidelijkheid bij de betrokkenen.

| <b>Voldoet nog niet aan AVG</b>    | <b>Voldoet aan AVG, maar toelichting is aan te raden</b> | <b>Voldoet volledig aan AVG</b> | <b>Niet verplicht conform AVG</b>     |
|------------------------------------|----------------------------------------------------------|---------------------------------|---------------------------------------|
| Inleiding                          | Reclame                                                  | Autoriteit Persoonsgegevens     | Websites van derden                   |
| Contactformulier en nieuwsbrief    | Locatiegegevens                                          |                                 | Wijzigingen in deze privacyverklaring |
| Google Analytics                   | Verstreking aan derden                                   |                                 |                                       |
| Hotjar                             | Cookies                                                  |                                 |                                       |
| Inzage en wijzigen van uw gegevens | Bewaartermijnen                                          |                                 |                                       |

#### 6.1.2 Aanbevelingen

Om de privacyverklaring van Merford AVG-proof te maken, is het aan te raden om een aantal dingen te wijzigen of toe te voegen. Zo is het aan te raden om in de inleiding van de privacyverklaring het recht op intrekking van de toestemming op te nemen. De betrokkene moet namelijk hiervan op de hoogte zijn alvorens hij toestemming geeft.

Verder is het voor het contactformulier aan te raden om specifiek toestemming te vragen voor de verwerking van de persoonsgegevens en aan te geven dat indien geen toestemming wordt gegeven, het niet mogelijk is om contact op te nemen met de betrokkene. Dit zorgt voor duidelijkheid bij de betrokkene. Dit kan gerealiseerd worden door een vakje die de betrokkene kan aanvinken bij het invullen van het contactformulier. De nieuwsbrief kan AVG-proof worden gemaakt door te werken met een double opt-in. Een double opt-in is bewijstechnisch het beste. De betrokkene ontvangt dan namelijk een bericht met het verzoek de inschrijving op de nieuwsbrief nogmaals te bevestigen. Verder is het aan te raden om te onderzoeken of bij de afmelding van de nieuwsbrief, het e-mailadres direct of automatisch wordt verwijderd uit de lijst van abonnees. Indien dit het geval is, is het aan te raden om dit in de privacyverklaring te vermelden.

In de paragraaf Google Analytics is het aan te raden om te vermelden dat de Google een blokkademogelijkheid biedt voor het volgen van het bezoek aan de website met Google Analytics.

Voor Hotjar geldt dat er op de website een opt-out optie wordt aangeboden. Het is aan te raden om dit te vermelden in de privacyverklaring.

De betrokkene heeft het recht op beperking van de verwerking op grond van de AVG. Het is aan te raden om dit recht ook op te nemen in de privacyverklaring, in de paragraaf inzage en wijzigen van persoonsgegevens.

*“We hebben de accountmanagers erop gewezen, dat ze niet zomaar iemand mogen inschrijven voor een nieuwsbrief, maar dat je daar toestemming voor nodig hebt.” – Online Marketeer<sup>278</sup>*

Voor de bovengenoemde paragrafen die niet in strijd zijn met de AVG, maar wel onduidelijk kunnen zijn voor de betrokkenen, is het aan te raden om ze uit te breiden met een (korte) toelichting. Voor reclame geldt dat het onduidelijk is hoe de betrokkene zich hiervoor moet aanmelden en of reclame en nieuwsbrief bij elkaar horen.

De paragraaf locatiegegevens kan bij de betrokkene veel vragen oproepen. Het is aan te raden om aan te geven voor wat voor soort diensten locatiegegevens worden verzameld met eventueel een voorbeeld erbij.

Voor de paragraaf verstrekking aan derden is het onduidelijk of dit geldt voor alle betrokkenen, welke gegevens door derden worden verzameld en waarom dit mag. Het is aan te raden om dit toe te lichten.

Voor de paragraaf cookies geldt dat er verschillende soorten cookies zijn. Het is aan te raden om de redenen voor gebruik van cookies te verwerken in de privacyverklaring. Dit zorgt voor helderheid. Ook is het aan te raden om op de website te vermelden dat het geven van toestemming voor gebruik van cookies wordt opgevat als toestemming voor het gebruik van cookies op de gehele website.

Voor de bewaartermijnen geldt dat er onderzocht moet worden of de termijnen noodzakelijk zijn. Indien dit niet het geval is, moet dit aangepast worden. Als dit niet gerealiseerd wordt, wordt in strijd gehandeld met het beginsel van opslagbeperking en dus ook in strijd met de AVG.

## 6.2 Privacyverklaring Akoestiekwinkel

De webwinkel van de Akoestiekwinkel van Merford heeft een aparte privacyverklaring. De webwinkel verwerkt namelijk meer privacygevoelige gegevens, zoals betalingsgegevens. Deze privacyverklaring dateert van 22 mei 2018. Merford wil graag weten of deze privacyverklaring voldoet aan de AVG. Hieronder zijn de conclusies en aanbevelingen weergegeven van het onderzoek hiernaar.

### 6.2.1 Conclusies

Voor de privacyverklaring van de webwinkel kan geconcludeerd worden dat deze nog niet volledig AVG-proof is. Net zoals in de tabel van paragraaf 6.1.1 wordt een onderscheid gemaakt tussen voldoet wel of voldoet niet aan de AVG. Verder is er een kolom met voldoet aan de AVG, maar een toelichting is aan te raden. Ten slotte is er een kolom met niet verplicht conform de AVG, maar wel handig om in de privacyverklaring te hebben staan.

---

<sup>278</sup> Bijlage 10 Interview 4.

| Voldoet nog niet aan AVG        | Voldoet aan AVG, maar toelichting is aan te raden | Voldoet volledig aan AVG           | Niet verplicht conform AVG            |
|---------------------------------|---------------------------------------------------|------------------------------------|---------------------------------------|
| Inleiding                       | Registreren                                       | Reviews                            | Websites van derden                   |
| Contactformulier en nieuwsbrief | Afhandelen bestelling                             | Autoriteit Persoonsgegevens        | Wijzigingen in deze privacyverklaring |
| Google Analytics                | Deelname aan winacties                            | Inzage en wijzigen van uw gegevens |                                       |
|                                 | Reclame                                           |                                    |                                       |
|                                 | Locatiegegevens                                   |                                    |                                       |
|                                 | Publicatie                                        |                                    |                                       |
|                                 | Verstrekking aan derden                           |                                    |                                       |
|                                 | Cookies                                           |                                    |                                       |
|                                 | Bewaartermijnen                                   |                                    |                                       |
|                                 | Verwijdering van gegevens                         |                                    |                                       |

Voor de paragraaf contactformulier en nieuwsbrief geldt dat het e-mailadres expliciet wordt toegevoegd aan de lijst van abonnees. In de paragraaf van deelname aan winacties staat vermeld dat de betrokkene te allen tijde het recht heeft om de toestemming in te trekken voor de verwerking van de persoonsgegevens, dit is een pluspunt. Verder wordt in de paragraaf publicatie aangegeven dat anonimiseren mogelijk is op verzoek, het is goed dat dit vermeld wordt in de privacyverklaring. In de paragraaf cookies wordt toegelicht waarom een cookie gegevens bijhoudt van een bezochte website. Dit is ook verstandig om op te nemen in de privacyverklaring, want het creëert duidelijkheid bij de betrokkenen.

### 6.2.2 Aanbevelingen

Om de privacyverklaring van de webwinkel van Merford AVG-proof te maken, is het aan te raden om een aantal dingen te wijzigen of toe te voegen. Zo is het aan te raden om in de inleiding van de privacyverklaring het recht op intrekking van de toestemming op te nemen. Voor het invullen van het contactformulier geldt dat eventueel de keuze aan de betrokkene kan worden aangeboden om of een e-mailadres of een telefoonnummer op te geven. Indien dit toegepast wordt, wordt voldaan aan het beginsel van dataminimalisatie. De nieuwsbrief kan ook hier AVG-proof worden gemaakt, door te werken met een double opt-in. Verder is het ook voor deze privacyverklaring aan te raden om te vermelden dat Google een blokkademogelijkheid biedt voor het volgen van het bezoek aan de website met Google Analytics.

*“We bewaren de gegevens op Google Analytics vijftig maanden, dit is heel random eigenlijk.”  
– Online Marketeer<sup>279</sup>*

Voor de bovengenoemde paragrafen, die niet in strijd zijn met de AVG, is het aan te raden om deze uit te breiden met een (korte) toelichting.

Voor de paragraaf registreren is het onduidelijk waarom en voor welke onderdelen een registratie verplicht is. Een toelichting kan voor verheldering zorgen bij de betrokkene. Hier kan eventueel ook een voorbeeld bij gegeven worden.

In de paragraaf afhandelen bestelling wordt verwezen naar verderop in de privacyverklaring. Het is echter niet direct duidelijk waar in de privacyverklaring gezocht moet worden. Het is aan te raden om een duidelijkere verwijzing neer te zetten in deze paragraaf.

Voor deelname aan winacties staat vermeld, dat de persoonsgegevens tot dertig dagen na het einde van de wedstrijd worden bewaard. Hierbij moet gekeken worden of dit met minder

<sup>279</sup> Bijlage 10 Interview 4.

dagen kan. Zo ja, dan moet dit aangepast worden, zodat er aan het beginsel van opslagbeperking wordt voldaan. Verder is het aan te raden om expliciet te vermelden dat de betrokkene bij deelname toestemming geeft voor de verwerking van zijn persoonsgegevens. Voor reclame geldt dat het onduidelijk is hoe de betrokkene zich hiervoor moet aanmelden en of reclame en nieuwsbrief bij elkaar horen.

De tekst over locatiegegevens kan, net zoals bij de privacyverklaring van Merford, veel vragen oproepen bij de betrokkene. Ook hier is het aan te raden om aan te geven voor wat voor soort diensten locatiegegevens worden verzameld met een voorbeeld erbij.

De paragraaf publicatie kan de vraag oproepen voor de betrokkene of dit voor alle informatie geldt. Voor verheldering kan eventueel een voorbeeld worden toegevoegd. Ook is het aan te raden om kort toe te lichten waarom de informatie gepubliceerd wordt en wat de doeleinden hiervoor zijn.

In de paragraaf verstrekking aan derden is het onduidelijk of dit geldt voor alle betrokkenen, welke gegevens door derden worden verzameld en waarom dit mag.

Het is aan te raden om op de website van de webwinkel te vermelden dat verder gebruik van de website wordt opgevat als toestemming voor het gebruik van cookies.

Voor de bewaartermijnen geldt dat niet uit de privacyverklaring kan worden afgeleid wanneer een betrokkene als inactieve klant wordt aangemerkt. Dit kan worden uitgelegd in de privacyverklaring.

*“Als ik iets tegenkom wat niet klopt, geef ik dit door aan betreffende collega.” – Online marketeer<sup>280</sup>*

Voor de paragraaf verwijdering van gegevens geldt dat het onduidelijk is waarom de betreffende termijnen wordt gehanteerd. Dit hoeft overigens niet per se terug te vinden te zijn in de privacyverklaring. Voor Merford is het wel van belang dat ze weet of de termijn een wettelijke grondslag heeft of goed is overwogen. Zo kan Merford de termijnen te allen tijde toelichten aan de betrokkenen.

### 6.3 Huidige werkwijze

Om achter de huidige werkwijze van Merford te komen zijn vijf medewerkers van Merford geïnterviewd. Merford wil graag weten in hoeverre de huidige werkwijze voldoet aan de AVG. Hieronder zijn de conclusies en aanbevelingen weergegeven.

#### 6.3.1 Conclusies

Er kan geconcludeerd worden dat de huidige werkwijze van Merford nog niet voldoet aan de AVG. Hieronder wordt in een tabel weergegeven wat van de huidige werkwijze wel en niet (volledig) voldoet aan de AVG. Verder is een kolom toegevoegd in de tabel met punten uit de AVG die niet verplicht zijn voor Merford, maar wel aan te raden zijn.

| Voldoet nog niet aan AVG                   | Voldoet niet volledig aan AVG      | Voldoet volledig aan AVG                 | Niet verplicht, maar wel aan te raden |
|--------------------------------------------|------------------------------------|------------------------------------------|---------------------------------------|
| Verzameling en verwerking persoonsgegevens | Bewaartermijnen                    | Privacy by design and privacy by default | FG                                    |
| Beveiliging                                | Realisatie rechten van betrokkenen | Samenwerking met partijen buiten de EU   | DPIA                                  |
| Gegevens-beschermingsbeleid                | Uitwisseling gegevens              |                                          |                                       |
| Verwerkingsregister                        |                                    |                                          |                                       |

<sup>280</sup> Bijlage 10 Interview 4.

### 6.3.2 Aanbevelingen

Om volledig AVG-proof te worden, zal de huidige werkwijze aangepast moeten worden. Zo is het aan te raden om tijdens een telefoongesprek of in een e-mail aan te geven welke persoonsgegevens worden verwerkt en waarom. Dit zorgt voor duidelijkheid bij de betrokkene.

Voor de bewaartermijnen geldt dat onderzocht moet worden of het noodzakelijk is om de gegevens op Google Analytics vijftig maanden te bewaren. Indien dit niet noodzakelijk is, moet dit aangepast worden, zodat wordt voldaan aan het beginsel van opslagbeperking. Verder is het aan te raden om een vaste procedure te hebben voor het verwijderen van e-mails en persoonsgegevens. Zo kan worden voorkomen dat de persoonsgegevens langer worden bewaard dan noodzakelijk is.

*“Ik denk dat het wel een punt van aandacht is, om toch een duidelijke procedure te hebben om vervuiling tegen te gaan.” – Sales engineer<sup>281</sup>*

Verder is het aan te raden om voor de realisatie van de rechten van de betrokkenen een procedure op te stellen. Zo kan een verzoek van de betrokkene direct gerealiseerd worden. Het is geen verplichting volgens de AVG om de maatregelen voor beveiliging van de verwerking op papier te hebben staan, maar dit is wel aan te raden. Op deze manier kan er schriftelijk aangetoond worden dat er maatregelen worden genomen om de beveiliging te waarborgen. Verder is het voor Merford aan te raden om een vaste procedure te creëren om de beveiliging van de verwerking te testen, te beoordelen en te evalueren. Dit is namelijk verplicht volgens de AVG.

Op dit moment wordt met de software rekening gehouden met de AVG. Het is echter aan te raden om de genomen en de te nemen (interne) beleidsmaatregelen op papier te zetten, zodat naleving controleerbaar is. Het is verder aan te raden om bij aanschaf van nieuwe software, de leverancier aan te laten tonen en te laten garanderen dat in de ontwerpdocumentatie van de software privacyoverwegingen en welke beslissingen zijn opgenomen.

Verder is het van belang dat medewerkers op de hoogte zijn van het begrip datalek. Dit kan gerealiseerd worden door bij de medewerkers bewustwording te creëren omtrent de AVG. De AVG is immers voor iedere medewerker van toepassing. De bewustwording kan gecreëerd worden door het aanbieden van een online training, een videotraining of door middel van een AVG-game.

*“Ik ben me er niet bewust van dat er cases als datalek zijn bestempeld.” – Applicatiebeheerder<sup>282</sup>*

Verder is het aan te raden om de paragraaf FG in een verwerkersovereenkomst leeg te laten, zo lang er geen officiële FG is aangesteld. Verder is het een advies om in de toekomst officieel een FG aan te stellen. Dit laat namelijk zien dat er serieus wordt omgegaan met privacy.

Ondanks dat het niet voor de hand ligt om persoonsgegevens uit te wisselen, is het aan te raden om uit voorzorg een blokkade op het systeem te zetten voor gegevensuitwisseling. Verder is het aan te raden om een beleid op stellen waar de technische en organisatorische maatregelen in staan om de gegevensbescherming te waarborgen, ook wel een gegevensbeschermingsbeleid genoemd. Zo wordt er niet in strijd gehandeld met de AVG. Ten slotte wordt aangeraden om een verwerkingsregister bij te houden, zodat er niet in strijd wordt gehandeld met de AVG.

Een DPIA is niet vereist voor Merford, maar het is aan te raden om een DPIA als standaard te hanteren. Zo wordt, voordat er begonnen wordt aan een nieuw plan waarbij persoonsgegevens worden verwerkt, gecontroleerd of er risico's verbonden zijn aan de verwerking en welke maatregelen er kunnen worden getroffen.

---

<sup>281</sup> Bijlage 9 Interview 3.

<sup>282</sup> Bijlage 8 Interview 2.

## Bronnenlijst

### Handleidingen

#### **Schermer, Hagenauw & Falot 2018**

B.W. Schermer, D. Hagenauw & N. Falot, *Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming*, januari 2018.

### Internetbronnen

www.akoestiekwinkel.nl  
www.azquotes.com  
www.autoriteitpersoonsgegevens.nl  
www.bol.com  
www.denieuwezaak.nl  
www.europa.eu  
www.europadecentraal.nl  
www.merford.com  
www.nexttech.nl  
www.rijksoverheid.nl  
www.vandale.nl

### Jurisprudentie

HvJ EU 13 mei 2014, C-131/12 (*Google Spain SL, Google Inc t. Agencia Española de Protección de Datos, Mario Costeja González*).

HvJ EU 1 oktober 2016, C-230/14 (*Weltimmo*).

### Literatuur

#### **Berkvens, Vinken, Wiegerinck, Wolters Reijner & Van Gerwen 2018**

J.M.A. Berkvens, S.M.M.C. Vinken, S.R. Wiegerinck, S.W.G. Wolters, J. Reijner & M.J.M.G. van Gerwen, *Checklist privacy AVG: Privacybeleid in 46 checklists*, Amsterdam: Berghauser Pont Publishing 2018.

#### **Engelfriet, Chew-Meij & Kager 2018**

A. Engelfriet, L. Chew-Meij & P. Kager, *De Algemene Verordening Gegevensbescherming. Artikelsgewijs commentaar*, Amsterdam: Ius Mentis 2018.

#### **Engelfriet, Chew-Meij & Kager 2018**

A. Engelfriet, L. Chew-Meij & P. Kager, *Handboek AVG: Compliance in de praktijk*, Amsterdam: Ius Mentis 2018.

#### **Van den Eijnden, Jansen, Van den Bosch & Van de Pas 2018**

L. van den Eijnden, S. Jansen, R. van den Bosch & I. van de Pas, *De AVG: Alles over de verwerking van persoonsgegevens*, Alphen aan den Rijn: Vakmedianet 2018.

#### **Janssen 2018**

L. Janssen, *De Kleine Gids AVG. Privacy en beroepsgeheim in het sociale domein*, Deventer: Wolters Kluwer 2018.

**Van Schaaijk 2015**

G.A.F.M. van Schaaijk, *Praktijkgericht juridisch onderzoek*, Den Haag: Boom Juridische uitgevers 2015.

**Van der Sloot 2018**

B. van der Sloot, *De Algemene Verordening Gegevensbescherming in gewonemensentaal*, Amsterdam: Amsterdam University Press 2018.

**Versmissen, Terstegge & Krijgsman 2017**

K. Versmissen, J. Terstegge & N. Krijgsman, *Grip op de AVG: De nieuwe privacywet voor niet-juristen*, Deventer: Wolters Kluwer 2017.

Tijdschriften**Candel & Nouwt, P&I 2016, p. 10**

H. Candel & S. Nouwt, 'Help, een datalek!: een procedure voor het omgaan met datalekken', *Privacy & Informatie* 2016, afl. 1, p. 10.

**Hijmans, NJB 2018/356, p. 473**

H. Hijmans, 'De AVG en de UAVG', *Nederlands Juristenblad* 2018/356, afl. 7, p. 473.

**Holvast, P&I 2016/3, p. 98**

J. Holvast, 'Algemene verordening gegevensbescherming: veel gespin en weinig wol', *Privacy & Informatie* 2016, afl. 3, p. 98.

**De Jong, Ars Aequi 2016/10, p. 770 - 772**

J.P. de Jong, 'De Algemene verordening gegevensbescherming', *Ars Aequi* 2016/10, p. 770 - 772.

**Nouwt, P&I 2017/1, p. 6.**

J. Nouwt, 'Richtlijnen over de AVG', *P&I* 2018, afl. 1, p. 6.

**Van Schaik & Abassi, Bedrijfsjuridische berichten, 2017/95, p. 324 - 325**

R.E. van Schaik & I. Abassi, 'De verplichte aanstelling van een privacyduizendpoot: de Data Protection Officer', *Bedrijfsjuridische berichten* 2017/95, afl. 26, p. 324 - 325.

Wet- en regelgeving

Algemene Verordening Gegevensbescherming

Grondwet

Handvest van de grondrechten van de Europese Unie

Richtlijn betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen

Richtlijn betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens

Uitvoeringswet Algemene Verordening Gegevensbescherming

Verdrag betreffende de werking van de Europese Unie

Verdrag tot bescherming van personen met betrekking tot geautomatiseerde verwerking van persoonsgegevens