

AFSTUDEERSCRIPTIE

*Een onderzoek naar de invloed van de AVG op de
werkwijze van SchoeBroek Advocaten & Mediators*



Auteur: Kirsten van der Hauw

Instituut: Saxion Hogeschool

Afstudeerorganisatie: SchoeBroek advocaten & mediators

Datum: 31-05-2018

Titelpagina

Een onderzoek naar de invloed van de AVG op de werkwijze van SchoeBroek Advocaten & Mediators

Studentgegevens

Naam: Kirsten van der Hauw
Studentnummer: 405882
Klas: DSJ4VB
Email: 405882@student.saxion.nl
Telefoonnummer: 06-38295946

Opleidingsgegevens

Opleiding: Sociaal Juridische Dienstverlening voltijd
Instituut: Saxion Deventer
Eerste lezer: Coen de Heer
Tweede lezer: Christina van der Draaij

Organisatiegegevens

Organisatie: SchoeBroek Advocaten & Mediators
Praktijkcoach: M.J. Ellenbroek

Deventer, 31 mei 2018

Samenvatting

De Wet bescherming persoonsgegevens (Wbp) is per 25 mei 2018 vervangen voor de Algemene verordening gegevensbescherming (AVG). Een verordening die geldig is in de gehele Europese Unie. De verordening geldt voor alle organisaties die persoonsgegevens verwerken. SchoeBroek advocaten & mediators (hierna: SchoeBroek) is een kantoor in Deventer waar een combinatie van advocatuur en mediation wordt aangeboden. Zij richten zich op letselschade, personen- en familierecht en mediation, erfrecht, arbeidsrecht werknemer, arbeidsrecht werkgever en ondernemingsrecht (SchoeBroek, z.d.). Er wordt bij SchoeBroek dan ook veel gedaan met de verwerking van persoonsgegevens en daarom moeten zij per 25 mei 2018 voldoen aan de eisen die de AVG stelt. Het doel van dit onderzoeksrapport is om SchoeBroek te adviseren bij het aanpassen van hun werkwijze zodat zij voldoen aan de eisen die de AVG stelt. Binnen dit onderzoek is er een probleemstelling tot stand gekomen waar aan het einde van dit onderzoeksrapport een antwoord op wordt gegeven. De probleemstelling luidt als volgt: *“Wat is de invloed van de AVG op de werkwijze van SchoeBroek en welke veranderingen moeten er zo nodig plaatsvinden om te voldoen aan de eisen van de nieuwe verordening?”*

Om de probleemstelling te beantwoorden is er gebruik gemaakt van verschillende methoden. Allereerst is er praktijkgericht juridisch onderzoek gedaan. De Wbp is uiteengezet en vervolgens is de AVG in dezelfde volgorde uiteengezet. Op deze manier zijn de verschillen en de overeenkomsten naast elkaar gezet. Daarnaast zijn er semigestructureerde interviews afgenomen met de drie advocaten van SchoeBroek. Door het afnemen van de semigestructureerde interviews is naar voren gekomen welke gegevens er verwerkt worden en op welke wijze verwerking plaatsvindt.

De AVG brengt ten opzichte van de Wbp een aantal veranderingen met zich mee. Organisaties hebben een grotere verantwoordingsplicht gekregen en betrokkenen hebben meer rechten gekregen. Om aan de eisen te voldoen die de AVG aan de organisaties oplegt moeten er een aantal documenten worden opgesteld.

De invloed van de AVG op de werkwijze van SchoeBroek is dat zij in principe door kunnen gaan op de manier dat zij het deden volgens de Wbp, maar er moeten extra handelingen worden verricht om bij te houden welke gegevens zij verwerken om te voldoen aan de verantwoordingsplicht. Dit moet worden gedaan door middel van het bijhouden van een verwerkingsregister. Ook is SchoeBroek verplicht om een register bij te houden met alle datalekken. Een andere verandering binnen de werkwijze is dat SchoeBroek verwerkersovereenkomsten moet sluiten met iedere partij die in opdracht van SchoeBroek persoonsgegevens verwerkt. Naast de verantwoordingsplicht bestaat er de informatieplicht. SchoeBroek is verplicht om cliënten te informeren over wat er gebeurt met alle gegevens die zij verstrekken. Dit kan worden gedaan door middel van een privacyverklaring.

De aanbevelingen die worden gedaan binnen dit onderzoeksrapport zijn dan ook gericht op de verantwoordings- en informatieplicht. De eerste aanbeveling is om een register op te stellen waarin alle verwerkingen die gedaan worden binnen SchoeBroek worden vastgelegd. De tweede aanbeveling richt zich op datalekken. Ondanks dat SchoeBroek nog niet te maken heeft gehad met een datalek, is het van belang dat zij een register opstellen waarin eventuele datalekken gedocumenteerd kunnen worden. De derde aanbeveling heeft betrekking op de verwerkers waarmee gewerkt wordt. Er moet een verwerkersovereenkomst opgesteld worden en deze moet verstrekt worden aan verwerkers. De vierde en laatste aanbeveling is om een privacyverklaring op te stellen, zodat cliënten weten wat er met hun gegevens gebeurt. Aanbevolen wordt om deze toe te voegen aan de algemene voorwaarden en op de website te plaatsen.

Voorwoord

Voor u ligt het afstudeeronderzoek dat ik heb uitgevoerd in de periode van februari 2018 tot en met mei 2018. Ter afronding van mijn studie Sociaal Juridische Dienstverlening aan de Hogeschool Saxion te Deventer, heb ik een praktijk juridisch onderzoek uitgevoerd voor SchoeBroek. In overleg met SchoeBroek zijn we overeengekomen dat ik een onderzoek zou doen naar de AVG, die op 25 mei 2018 is in gegaan. Iedere organisatie waarbij persoonsgegevens worden verwerkt, moet voldoen aan de eisen van de nieuwe verordening, zo ook SchoeBroek.

Dit onderzoeksrapport is met name gericht aan de werknemers van SchoeBroek, zodat zij hun werkwijze waar nodig kunnen aanpassen en daarnaast met het onderzoeksrapport cliënten kunnen informeren over de nieuwe verordening.

Graag wil ik een aantal personen bedanken. Op de eerste plaats wil ik Marian Ellenbroek en Christa Schoemaker bedanken voor het feit dat zij mij de mogelijkheid hebben gegeven om mijn afstudeeronderzoek binnen hun organisatie te mogen uitvoeren. Naast dat zij mij de mogelijkheid hebben gegeven om het onderzoek bij hen uit te voeren, wil ik hen en de andere werknemers bij SchoeBroek bedanken voor de hulp en ondersteuning die zij geboden hebben gedurende de afstudeerperiode. Tevens wil ik meneer de Heer bedanken voor zijn begeleiding vanuit het Saxion gedurende de afstudeerperiode.

Deventer, 31 mei 2018

Kirsten van der Hauw

Inhoudsopgave

Hoofdstuk 1 <i>Aanleiding, doelstelling, probleemstelling en onderzoeksvragen</i>	7
1.1 Aanleiding	7
1.1.1 Betrokkenen en belanghebbenden	8
1.2 Doelstelling	8
1.3 Probleemstelling	9
1.4 Onderzoeksvragen	9
1.4.1 Operationalisering van begrippen	9
Hoofdstuk 2 <i>Methode en analysekader</i>	11
2.1 Dataverzamelmethode	11
2.2 Verantwoording geschiktheid methoden	11
Hoofdstuk 3 <i>Juridisch kader</i>	15
3.1 Verschil richtlijn en verordening	15
3.2 Wet bescherming persoonsgegevens	16
3.2.1 Wbp van toepassing?	16
3.2.2 Eisen Wbp gegevensverwerking	17
3.2.3 Verplichtingen verantwoordelijke en bewerker	18
3.2.4 Rechten van de betrokkene	20
3.2.5 Bijzondere persoonsgegevens	21
3.2.6 Gevolgen overtreden eisen Wbp	23
3.3 Algemene verordening gegevensbescherming	25
3.3.1 Belangrijke begrippen	25
3.3.2 AVG van toepassing?	25
3.3.3 Eisen AVG gegevensverwerking	28
3.3.4 Verplichtingen verwerkingsverantwoordelijke en verwerker	29
3.3.5 Rechten van de betrokkene	36
3.3.6 Bijzondere persoonsgegevens	39
3.3.7 Gevolgen overtreden eisen AVG	40
3.4 Verschillen Wbp en AVG	41
3.5 Conclusie	43
Hoofdstuk 4 <i>Verwerking persoonsgegevens bij SchoeBroek (getoetst aan de Wbp en AVG)</i>	45
4.1 Type persoonsgegevens	45
4.2 Verwerken persoonsgegevens	46

4.3 Betrokkenen	46
4.4 Bewerkers/verwerkers	46
4.5 Eisen aan de verwerking	47
4.6 Grondslagen	47
4.7 Beveiliging	48
4.8 Bewaartermijnen	48
4.9 Knelpunten	49
4.10 Conclusie	49
Hoofdstuk 5 <i>Stappen ondernemen binnen SchoeBroek</i>	51
5.1 Verantwoordingsplicht	51
5.1.1 Registerplicht (verwerkingen)	51
5.1.2 Register datalekken	52
5.2 Informatieplicht	52
5.3 Gevolgen niet (op tijd) voldoen aan de AVG	53
5.4 Conclusie	53
Hoofdstuk 6 <i>Conclusie</i>	55
Literatuurlijst	56
Bijlagen	59
Bijlage 1: Interviewlijst	59
Bijlage 2: Opzet register	61
Bijlage 3: Verklaring gebruikte hulpmiddelen	62

Hoofdstuk 1

Aanleiding, doelstelling, probleemstelling en onderzoeksvragen

In dit hoofdstuk wordt de aanleiding van het onderzoek beschreven. Vervolgens wordt er beschreven wie de belanghebbenden binnen dit onderzoek zijn, daarna wordt de doelstelling en probleemstelling beschreven en tot slot worden de onderzoeksvragen gepresenteerd.

1.1 Aanleiding

Elke lidstaat in de Europese Unie heeft tot 25 mei 2018 zijn eigen privacywet. Deze wetten zijn gebaseerd op de Europese privacyrichtlijn uit 1995; de periode dat internet nog maar net in opkomst was. (Autoriteit Persoonsgegevens, 2018) De digitalisering, de toename in het verzamelen en delen van gegevens en technologische ontwikkelingen zorgen voor extra risico's op het gebied van gegevensmisbruik. Om deze reden is het van belang dat persoonsgegevens goed beveiligd worden en dat iedereen het recht heeft om te weten voor welke doeleinden zijn of haar persoonsgegevens worden gebruikt. (Robidus, 2018) De ontwikkeling op het gebied van digitalisering en de grote mate van internetgebruik heeft ervoor gezorgd dat de huidige wet moest worden herzien. De bescherming van persoonsgegevens was voorheen uitgewerkt in Richtlijn 95/46/EG, waar de Wbp op gebaseerd is. (Engelfriet, Meij, Kager, 2017)

Vanaf 25 mei 2018 is de AVG van toepassing en deze verordening vervangt de Wbp, die op het moment van schrijven nog van toepassing is. Op 25 mei 2016 is de AVG in werking getreden. Dit betekent dat er twee jaar zit tussen de inwerkingtreding van de AVG en het moment dat deze wet daadwerkelijk van toepassing is. De AVG zal vanaf 25 mei 2018 in de gehele Europese Unie gelden. (Autoriteit Persoonsgegevens, 2018)

De AVG is opgesteld om de gegevensbescherming in de hele Europese Unie te reguleren. Het doel van de verordening is om twee belangen te waarborgen: de bescherming van natuurlijke personen in verband met de verwerking van hun gegevens en het vrije verkeer van persoonsgegevens binnen de Europese Unie. De AVG zal onder meer zorgen voor versterking en uitbreiding van privacy rechten en meer verantwoordelijkheden voor organisaties. Daarbij geldt een verantwoordingsplicht. De verantwoordingsplicht houdt in grote lijnen in dat organisaties de verantwoordelijkheid krijgen om aan te tonen dat zij aan de privacywetgeving voldoen. Organisaties moeten kunnen aantonen dat zij de juiste organisatorische en technische maatregelen hebben genomen om te voldoen aan de eisen die de AVG stelt. De nieuwe regels dwingen organisaties om goed na te denken over hoe persoonsgegevens worden verwerkt en beschermd. (Autoriteit Persoonsgegevens, 2018)

De AVG geldt voor alle bedrijven en organisaties die persoonsgegevens vastleggen van klanten, personeel of andere personen. SchoeBroek werkt met persoonsgegevens en daarom is de AVG bij hen ook van toepassing. Om deze redenen wil SchoeBroek een onderzoek laten doen in het kader van de AVG. Het onderzoek zal betrekking hebben op de invloed van de AVG op SchoeBroek en welke wijzigingen deze verordening met zich mee zal brengen. Vanaf 25

mei 2018 moeten zij voldoen aan de eisen van de nieuwe verordening en daarom is het van groot belang dat er een onderzoek gedaan wordt naar de veranderingen, zodat zij weten wat zij moeten veranderen aan hun werkwijze om te voldoen aan de nieuwe eisen en dat zij deze direct in de praktijk kunnen toepassen. Er wordt binnen dit onderzoek gekeken naar wat de AVG betekent voor zowel advocaten als voor mediators, omdat dit kantoor beiden betreft.

1.1.1 Betrokkenen en belanghebbenden

Dit onderzoek is gericht op één specifieke organisatie, waardoor er een kleine groep betrokkenen en belanghebbenden zijn in dit onderzoek.

De werknemers van SchoeBroek

In dit onderzoek zal het specifiek gaan om de invloed van de AVG op de werkwijze van SchoeBroek. Dit is de opdrachtgever van het onderzoek en daarom zijn zij betrokkenen en belanghebbenden in dit onderzoek. Dit onderzoek zal voor alle werknemers binnen deze organisatie van belang zijn, omdat iedere werknemer moet voldoen aan de eisen van de verordening. Er worden in het bedrijf zowel gegevens van cliënten als van de werknemers zelf verwerkt. Daarnaast is het van belang dat zij deze informatie kunnen doorgeven aan cliënten die hierover informatie willen ontvangen.

De cliënten van SchoeBroek

SchoeBroek is gespecialiseerd in meerdere rechtsgebieden, waarbij ze zowel particulieren als ondernemers van dienst kunnen zijn. Het is mogelijk dat cliënten advies willen over hoe zij met persoonsgegevens om moeten gaan, dus om deze reden zijn cliënten binnen de organisatie ook belanghebbenden. Om een concreter voorbeeld te noemen: het is mogelijk dat cliënten met een eigen bedrijf niet weten hoe zij om moeten gaan met het verwerken van gegevens, die nodig zijn in hun personeelsdossier. Denk aan naam, adres, woonplaats, het e-mailadres en het rekeningnummer van hun medewerkers.

1.2 Doelstelling

Het doel van dit onderzoek is om te weten te komen wat de invloed is van de AVG op de werkwijze die SchoeBroek op dit moment hanteert wat betreft de verwerking van persoonsgegevens. Door middel van dit onderzoek zal er in kaart gebracht worden welke veranderingen de AVG met zich meebrengt ten opzichte van de Wbp en op basis hiervan zullen er aanbevelingen worden gedaan. De aanbevelingen zijn gericht op de invloed van de AVG op de werkwijze die SchoeBroek op dit moment hanteert en de veranderingen die op grond van de nieuwe verordening zullen moeten plaatsvinden om te voldoen aan de eisen die de verordening stelt. Het is van groot belang dat SchoeBroek inzicht krijgt in de AVG zodat zij te weten komen wat de invloed is van de AVG en zij (waar nodig) hun werkwijze kunnen aanpassen. De resultaten en aanbevelingen die naar aanleiding van dit onderzoek worden gegeven kunnen zij toepassen in de praktijk. De verordening treedt op 25 mei 2018 in werking en daarom is het van belang dat er voor aanvang van die datum aangegeven kan worden welke grote veranderingen er nodig zijn om op tijd te voldoen aan de gestelde eisen, zodat er geen boete/sanctie wordt geriskeerd.

1.3 Probleemstelling

De probleemstelling die volgt uit de aanleiding en doelstelling, die gedurende dit onderzoek centraal staat luidt als volgt:

Wat is de invloed van de AVG op de werkwijze van SchoeBroek en welke veranderingen moeten er zo nodig plaatsvinden om te voldoen aan de eisen van de nieuwe verordening?

1.4 Onderzoeksvragen

Ter beantwoording van de probleemstelling zal deze opgedeeld worden in een aantal onderzoeksvragen. Beantwoording van de onderzoeksvragen zal leiden tot een antwoord op de probleemstelling.

1. Op welke wijze werkt SchoeBroek momenteel in de praktijk met persoonsgegevens?
2. Zijn er knelpunten op dit moment wat betreft de verwerking van persoonsgegevens bij SchoeBroek en welke risico's zitten eraan verbonden?
3. Welke veranderingen brengt de AVG met zich mee ten opzichte van de Wbp?
4. Welke stappen en maatregelen moet SchoeBroek nemen in de praktijk om te voldoen aan de AVG? Wat zijn de gevolgen als zij niet (op tijd) voldoen aan de AVG?

1.4.1 Operationalisering van begrippen

Ter verduidelijking van de probleemstelling en onderzoeksvragen worden een aantal begrippen toegelicht. De toelichting heeft betrekking op hoe begrippen tijdens dit onderzoek worden geïnterpreteerd, zodat zij worden afgebakend.

Werkwijze

Met werkwijze wordt bedoeld de manier waarop SchoeBroek om gaat met de verwerking van persoonsgegevens.

Invloed

De invloed van de AVG op de werkwijze van SchoeBroek wordt onderzocht. Tijdens dit onderzoek wordt met invloed bedoeld wat er uit de AVG voortkomt ten opzichte van de werkwijze die momenteel gehanteerd wordt. Dit kan zorgen voor veranderingen in de werkwijze die SchoeBroek op dit moment hanteert.

Wbp

De Wbp is de wet die voortkomt uit de Richtlijn 95/46/EG. Sinds 1 september 2001 is deze wet van toepassing en deze wet zal vanaf 25 mei 2018 worden vervangen door de AVG. De Wbp is op grond van art. 2 van voorgenoemde wet van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede de niet geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin opgenomen te worden.

AVG

De AVG is de vervanger voor de Wbp vanaf 25 mei 2018. Bij deze verordening worden regels vastgesteld betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van persoonsgegevens. (Engelfriet, Meij & Kager, 2017)

Hoofdstuk 2

Methode en analysekader

2.1 Dataverzamelmethode

Het onderzoek betreft een praktijkgericht juridisch onderzoek. Een praktijkgericht juridisch onderzoek heeft twee sporen: recht en praktijk (Schaaijk, 2015). De eerste twee onderzoeksvragen richten zich op de praktijk, de derde onderzoeksvraag richt zich op het recht en de vierde onderzoeksvraag richt zich op zowel recht als praktijk. Binnen dit onderzoek is er gebruik gemaakt van kwalitatieve methoden van dataverzameling. Het onderzoek richt zich op het beschrijven van de huidige werkwijze wat betreft het verwerken van persoonsgegevens en de wijzigingen die moeten plaatsvinden om te voldoen aan de AVG. Het gaat om een concreet onderwerp waarbij een juridische oplossing gevonden moet worden. Bij een onderzoek van de praktijk kan er gebruikgemaakt worden van bestaande gegevens en/of van gegevens die zelf verzameld worden (Schaaijk, 2015). Binnen dit onderzoek is van beide methoden gebruik gemaakt. Voor het onderzoek van recht ligt in een praktijkgericht juridisch onderzoek, een rechtsbronnen- en literatuuronderzoek het meest voor de hand (Schaaijk, 2015). Er is gebruik gemaakt van semigestructureerde interviews om zelf gegevens te verzamelen en van bestaand materiaal, waaronder wetgeving en literatuuronderzoek.

2.2 Verantwoording geschiktheid methoden

De gehanteerde onderzoeksmethoden worden beargumenteerd aan de hand van de eisen van bruikbaarheid, betrouwbaarheid en validiteit. Het is van belang dat de gebruikte bronnen valide en betrouwbaar zijn. 'Een van de standaardvragen bij de beoordeling van een argumentatie is of er redenen, eigenschappen of omstandigheden zijn die een andere conclusie rechtvaardigen. Is dat het geval, dan is de redenering niet valide', aldus Schaaijk (2015, p. 216). De eis van betrouwbaarheid brengt met zich mee dat de beweringen die de onderzoeker doet over de praktijk en het recht waar of aannemelijk moeten zijn. Zijn de argumenten oncontroleerbaar of wordt er te weinig of verkeerde informatie gegeven, dan is het niet betrouwbaar. (Schaaijk, 2015)

Interviews

Ter beantwoording van de eerste en tweede onderzoeksvraag, is er empirisch onderzoek gedaan. Dat wil zeggen een onderzoek waarbij een verschijnsel in de praktijk wordt waargenomen door o.a. ondervraging van personen of inhoudsanalyse van documenten (Schaaijk, 2015). De onderzoeksvragen zijn gericht op de praktijk en om deze reden zijn er semigestructureerde interviews gehouden met de advocaten van SchoeBroek. Doordat SchoeBroek een klein kantoor is met drie advocaten, was het mogelijk om iedere advocaat afzonderlijk te interviewen. Het afnemen van semigestructureerde interviews is geschikt voor kleine groepen, waardoor dit een geschikte methode was in dit onderzoek. Er is gekozen voor semigestructureerde interviews, omdat er op die manier naast vaststaande onderwerpen, voldoende ruimte was voor eigen inbreng van de respondenten. Ook maakten de semigestructureerde interviews het mogelijk om door te vragen, waardoor meer en

gedetailleerdere informatie naar voren kwam. De interviews zijn afgenomen in de vorm van een tweegesprek. (Verhoeven, 2014) Het doel van de interviews was het in kaart brengen van de werkwijze die gehanteerd wordt. De uitkomst is getoetst aan de eisen die de AVG met zich meebrengt, waardoor vervolgens geconcludeerd kon worden of er wijzigingen in de werkwijze moest plaatsvinden, en zo ja, welke wijzigingen. Deze informatie is meegenomen voor het doen van aanbevelingen. De interviews zijn niet bijgevoegd in de bijlage van dit onderzoeksrapport, maar de uitwerking van de interviews is op te vragen.

Betrouwbaarheid interviews

Om een onderzoek van de praktijk betrouwbaar te laten zijn, mogen er tijdens het onderzoek geen 'toevallige' fouten worden gemaakt door de onderzoeker en de respondenten. De betrouwbaarheid van het interview kan beïnvloed worden door toevallige fouten zoals bijvoorbeeld het geven van een verkeerd antwoord door respondenten en/of een verkeerde interpretatie door de onderzoeker. (Schaijk, 2015) Om dit te voorkomen, zijn er tijdens het interview een aantal onduidelijke begrippen gedefinieerd aan de hand van de begrippen die in dit onderzoeksrapport zijn gebruikt. De vragen in het semigestructureerde interview zijn gericht op feiten en niet op meningen, opvattingen of gevoelens. Hierdoor lag er geen druk op de respondenten, omdat het geven van een verkeerd antwoord niet mogelijk was. Daarnaast zijn de interviews opgenomen, zodat deze teruggeluisterd konden worden bij de verwerking van de interviews en er op die manier een controle heeft plaatsgevonden. Om deze redenen zijn de resultaten die uit de interviews zijn voortgekomen betrouwbaar.

Validiteit interviews

Bij validiteit gaat het om de vraag of de resultaten op de juiste wijze worden geïnterpreteerd. De semigestructureerde interviews die zijn afgenomen hebben betrekking op de werkwijze die de werknemers van SchoeBroek hanteren met betrekking tot de verwerking van persoonsgegevens. Door tijdens het interview de antwoorden die de respondenten gegeven hebben samen te vatten, is er direct gecontroleerd of de interpretatie juist was. De validiteit kan beïnvloed worden door het maken van systematische fouten. Doordat het interview gericht was op feiten, is de kans op systematische fouten klein. Ter controle is er gebruik gemaakt van het kantoorhandboek om de werkwijze, die door de respondenten tijdens de interviews is toegelicht, naast de beschreven werkwijze in het kantoorhandboek te leggen. Op die manier is de validiteit van de interpretatie van de antwoorden gewaarborgd. Tot slot kan de validiteit van het onderzoek beïnvloed zijn doordat er gebruik is gemaakt van een half-gestructureerd interview, omdat niet bij iedere respondent dezelfde vragen aan bod zijn gekomen. Dit zorgt ervoor dat de validiteit lager is dan bij een gestructureerd interview. (Verhoeven, 2014)

Bruikbaarheid interviews

Alle onderzoeksvragen tezamen zullen een antwoord geven op de probleemstelling. Hierdoor zijn de interviews niet direct bruikbaar voor de opdrachtgever, maar zullen de antwoorden wel bijdragen aan het volledig beantwoorden van de probleemstelling. Zonder het afnemen

van de interviews zal er geen antwoord gegeven kunnen worden op de eerste onderzoeksvraag, wat ertoe zal leiden dat het onduidelijk is wat SchoeBroek moet aanpassen in de werkwijze om te voldoen aan de eisen van de nieuwe verordening. Kortgezegd zijn de interviews niet direct bruikbaar voor de opdrachtgever, maar indirect wel.

Analyse interviews

Om antwoord te krijgen op hoe de werkwijze van SchoeBroek op dit moment is, zijn er interviews opgesteld. Zoals eerder gezegd zijn er semigestructureerde interviews afgenomen. Dit is gedaan door van tevoren de onderwerpen vast te stellen en per onderwerp een aantal vragen op te stellen, die in ieder geval gesteld moesten worden. Daarnaast was er genoeg ruimte voor inbreng van de respondenten. De interviews zijn niet afgenomen om te generaliseren (Verhoeven, 2014). Dit omdat er geen uitspraak gedaan wordt over een grote groep, maar specifiek over SchoeBroek. Om deze reden zijn de interviews niet geanalyseerd door te transcriberen en te coderen, maar is er een per onderwerp binnen het interview een korte samenvatting geschreven. Op deze manier werden de gegevens die het meest relevant zijn voor het onderzoek naar voren gebracht. De uitkomsten van de interviews zijn met elkaar vergeleken en er zijn verbanden gelegd (Schaijk, 2015). De overeenkomsten en de verschillen zijn hier duidelijk naar voren gekomen en verwerkt in de resultaten. Uit de drie korte samenvattingen is de relevante informatie samengevoegd tot een antwoord op de onderzoeksvragen. Op basis van het juridisch kader (zie hoofdstuk 3) is de werkwijze vergeleken met de eisen die de Wbp en de AVG stellen.

Praktijkgericht juridisch onderzoek

Er is op de derde en vierde onderzoeksvraag een antwoord gegeven worden door middel van praktijkgericht juridisch onderzoek. De reden dat er voor deze vraag gebruik gemaakt is van praktijkgericht juridisch onderzoek is omdat het gaat om het toepassen van bestaande kennis. Doordat er gebruik is gemaakt van bestaand materiaal, is de inhoud hiervan geanalyseerd. De informatie uit wetgeving die relevant is voor het onderzoek wordt geselecteerd en geïnterpreteerd. In een juridisch onderzoek wordt het geldend recht toegepast op een praktijksituatie om te beoordelen of de praktijk wel of niet in overeenstemming is met het recht. En wanneer dit niet het geval is, hoe dit in overeenstemming te brengen valt. (Schaijk, 2015)

Betrouwbaarheid praktijkgericht juridisch onderzoek

Het is voor de betrouwbaarheid van het onderzoek van groot belang dat de gegevens niet afhankelijk zijn van toeval en bij een herhaling van het onderzoek dezelfde antwoorden worden verkregen. Doordat er gebruik is gemaakt van bestaande wetgeving zullen dezelfde gegevens naar voren komen bij herhaling van het onderzoek, omdat het gaat om bestaand materiaal (Schaijk, 2015). De wetgeving die van belang is voor dit onderzoek is voor het grootste deel letterlijk overgenomen, waardoor de kans op toevallige fouten verkleind is, en daardoor is de betrouwbaarheid vergroot. (Verhoeven, 2014)

Validiteit praktijkgericht juridisch onderzoek

De juistheid van de gegevens op het gebied van wetgeving wordt gewaarborgd doordat er gebruik is gemaakt van meerdere bronnen. Door gebruik te maken van meerdere bronnen kon er een interpretatie gegeven worden aan de bedoelingen van de wetgever. Het is niet de bedoeling dat zinnen of zinsneden uit wetgeving of literatuur uit het verband getrokken worden omdat dat toevallig goed uitkomt voor het onderzoek. (Schaijk, 2015) Er is gebruik gemaakt van de Wbp, de AVG, de Memorie van Toelichting, de handleiding van zowel de Wbp als de AVG en de overwegingen. Doordat er gebruikt gemaakt wordt van verschillende databronnen, is de kans op valide onderzoeksgegevens groter (Baarda, 2013, p. 76-77).

Bruikbaarheid praktijkgericht juridisch onderzoek

Door in kaart te brengen wat de veranderingen zijn door de komst van de AVG ten opzichte van de Wbp, komt er naar voren waar de verschillen zitten en welke veranderingen er moeten plaatsvinden in de werkwijze van SchoeBroek. Om die reden is de derde onderzoeksvraag bruikbaar voor de organisatie. De resultaten op de derde onderzoeksvraag worden gebruikt om bij te dragen aan het aanpassen van de werkwijze van SchoeBroek. Het gaat hierbij om instrumentele bruikbaarheid (Verhoeven, 2014). Dit zal leiden tot een antwoord op de vierde onderzoeksvraag.

Analyse praktijkgericht juridisch onderzoek

Allereerst is de Wbp stapsgewijs uitgewerkt, vervolgens is de AVG op dezelfde wijze uitgewerkt. Door beide wetgeving op dezelfde manier langs te lopen, is het zeker dat van beide wetgevingen dezelfde soort informatie is geselecteerd. Vervolgens is er een tabel opgesteld waarin de meest opvallende en relevante verschillen en overeenkomsten tussen de Wbp en de AVG naar voren zijn komen. Door de tabel is het direct inzichtelijk waar de verschillen zitten en welke nieuwe eisen de AVG stelt. In de tabel is ook zichtbaar gemaakt aan welke plichten voldaan moet worden om aan de eisen van de AVG te voldoen.

Hoofdstuk 3

Juridisch kader

In dit hoofdstuk wordt het juridisch kader uiteengezet. Om in kaart te kunnen brengen wat de verschillen zijn tussen de Wbp en de AVG, is het van belang dat zowel de Wbp en de AVG uitgewerkt en vervolgens naast elkaar gelegd worden, zodat er vastgesteld kan worden waar de (grootste) verschillen zitten en waar de werkwijze van SchoeBroek aangepast moet worden om te voldoen aan de eisen van de AVG. Eerst zal het verschil tussen een richtlijn en een verordening worden toegelicht, vervolgens wordt de Wbp uiteengezet en ten slotte wordt de AVG op dezelfde wijze langsgelopen. Aan het einde van dit hoofdstuk zal er een antwoord gegeven worden op de derde onderzoeksvraag: *“Welke veranderingen brengt de AVG met zich mee ten opzichte van de Wbp?”*

3.1 Verschil richtlijn en verordening

De Wbp is gebaseerd op een richtlijn en de AVG is een verordening. Deze twee hebben allebei een verschillende werking. Op grond van het Verdrag betreffende de werking van de Europese Unie hebben de instellingen van de Europese Unie verschillende instrumenten (rechtshandelingen) om Europese regelgeving op te stellen. Richtlijnen en verordeningen zijn hier voorbeelden van. Het belangrijkste onderscheidende kenmerk is dat rechtshandelingen rechtstreeks of niet rechtstreeks bindend zijn. (De Nederlandsche Bank, 2011)

Richtlijn

Een richtlijn is een rechtshandeling die een bepaald doel vastlegt, die alle EU-landen moeten bereiken, maar zij mogen zelf de wetgeving vaststellen om dat doel te bereiken. Het beoogde resultaat staat dus vast, maar hoe een lidstaat daaraan voldoet niet. Lidstaten kunnen op deze manier rekening houden met de specifieke situatie in hun eigen land. Richtlijnen zijn niet direct toepasbaar, en moeten daarom omgezet worden in nationale wetgeving. (Europa Nu, z.d.)

Verordening

Een verordening is een bindende rechtshandeling die in de hele Europese Unie van toepassing is. Dit heet ook wel ‘rechtstreekse werking’. Het is vergelijkbaar met nationale wetten in de lidstaten, maar in geval van strijdigheid gaat de verordening boven de nationale wetgeving. Een verordening hoeft niet omgezet te worden in nationale wetgeving, omdat verordeningen direct toepasbaar zijn. Omdat een verordening dus niet door de lidstaten hoeft te worden uitgewerkt, moet een verordening in alle lidstaten van de Europese Unie op dezelfde manier worden ingevoerd en overal tot een gelijk resultaat leiden. Lidstaten zijn verplicht om verordeningen uit te voeren. (Europa Nu, z.d.)

De AVG is een verordening en heeft daarom rechtstreekse werking in de Europese Unie. Deze hoeft niet omgezet te worden in nationale wetgeving. De AVG zal in elke lidstaat op dezelfde manier worden ingevoerd en tot eenzelfde resultaat leiden.

3.2 Wet bescherming persoonsgegevens

De Wbp geeft tot 25 mei 2018 de regels voor het verwerken van persoonsgegevens in Nederland. Op het moment dat er persoonsgegevens verwerkt worden, gaat dat tot 24 mei 2018 volgens de regels van de Wbp. Om deze reden wordt er toegelicht wanneer de Wbp van toepassing is, welke eisen de Wbp stelt, welke plichten de verantwoordelijke heeft en welke rechten de betrokkene heeft.

3.2.1 Wbp van toepassing?

Om te beoordelen of de Wbp van toepassing is, is het van belang dat er twee vragen worden gesteld:

- 1) Zijn de gegevens persoonsgegevens?
- 2) Verwerk ik persoonsgegevens? (Handleiding Wet bescherming persoonsgegevens, 2002)

Persoonsgegevens

In art. 1 sub a Wbp worden persoonsgegevens omschreven als 'elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon'. Allereerst is het voor het begrip 'persoonsgegevens' relevant of de gegevens informatie over een persoon bevatten. Dit zal in veel gevallen uit de aard van de gegevens voortvloeien. In andere gevallen zal mede aandacht moeten worden besteed aan de context waarin het gegeven wordt vastgelegd en gebruikt. De begrippen 'geïdentificeerde' of 'identificeerbare persoon' houden in dat de identiteit van de persoon van wie de gegevens zijn, bekend is, of dat deze te achterhalen valt 'zonder onevenredige inspanning'. (MvT, Kamerstukken II 1997/98, 25892, 3) Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is. Dat het om een natuurlijke persoon moet gaan, houdt in dat gegevens van overleden personen of van organisaties geen persoonsgegevens zijn (Autoriteit Persoonsgegevens, 2018.).

Verwerking

In art. 1 sub b Wbp wordt het verwerken van persoonsgegevens als volgt omschreven: 'elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens'. Dit is dus een ontzettend ruim begrip waarbij het er eigenlijk op neerkomt dat iedere handeling die verricht wordt met persoonsgegevens onder verwerking valt.

Op het moment dat er is vastgesteld dat er sprake is van het verwerken van persoonsgegevens, is het van belang om vast te stellen wie er verantwoordelijk is voor de verwerking van persoonsgegevens.

- 3) Ben ik voor verantwoordelijk voor de verwerking? (Handleiding Wet bescherming persoonsgegevens, 2002)

Verantwoordelijke

De Wbp richt zich primair tot de verantwoordelijke voor de verwerking van persoonsgegevens. Op grond van art. 1 sub d Wbp is een verantwoordelijke 'de natuurlijk persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt'. De verantwoordelijke is dus met andere woorden een persoon of organisatie die het doel van en de middelen voor het gebruik van persoonsgegevens bepaalt (Autoriteit Persoonsgegevens, 2018). Deze persoon kan dit uitbesteden aan 'de bewerker'.

Bewerker

Een bewerker van persoonsgegevens is op grond van art. 1 sub e 'degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreekse gezag te zijn onderworpen'. De bewerker heeft geen zeggenschap over de verwerking, maar handelt naar de instructies en onder de verantwoordelijkheid van de verantwoordelijke. (Handleiding Wet bescherming persoonsgegevens, 2002)

Betrokkene

Op grond van art. 1 sub f Wbp is de betrokkene degene op wie een persoonsgegeven betrekking heeft.

3.2.2 Eisen Wbp gegevensverwerking*Zorgvuldig en behoorlijk*

Op grond van art. 6 Wbp moeten persoonsgegevens in overeenstemming met de wet en op zorgvuldige en behoorlijke wijze worden verwerkt. In de Memorie van Toelichting van de Wbp wordt nader toegelicht wat er bedoeld wordt met behoorlijkheid en zorgvuldigheid. Het komt erop neer dat dit artikel zich keert tegen het 'oneerlijk' verwerken van gegevens. Voorwaarde is dat de betrokkenen van het bestaan van de verwerking kennis kunnen hebben en daadwerkelijk en volledig worden geïnformeerd over de omstandigheden waaronder deze gegevens worden verkregen. (Autoriteit Persoonsgegevens, 2018)

Doelbinding

Op grond van art. 7 jo. art. 9 Wbp mogen persoonsgegevens alleen verzameld worden als daar een gerechtvaardigd doel voor is. Het doel moet welbepaald, uitdrukkelijk omschreven én gerechtvaardigd zijn. In art. 9 lid 1 Wbp is bepaald dat gegevens (vervolgens) niet mogen worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor de gegevens zijn verkregen. Welbepaald en uitdrukkelijk omschreven houdt in dat er geen persoonsgegevens verzameld mogen worden zonder een precieze doelomschrijving. Het doel moet bekend zijn voordat er tot verzamelen wordt overgegaan. (Katus & Zwenne, 2010) Verwerking van persoonsgegevens moet gebaseerd zijn op een van de zes grondslagen zoals genoemd in art. 8 Wbp.

Grondslagen

In art. 8 sub a t/m f Wbp wordt uitgewerkt wanneer er sprake is van gerechtvaardigde verwerkingsdoeleinden. Dit artikel bevat een limitatieve opsomming van gronden die de

gegevensverwerking rechtvaardigen. Dit houdt in dat persoonsgegevens alleen verwerkt mogen worden indien zij voldoen aan een van de in art. 8 Wbp genoemde voorbeelden. Art. 8 Wbp: Persoonsgegevens mogen slechts worden verwerkt indien:

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

Kwaliteitseisen

De Wbp bevat een algemene norm over de kwaliteit van de gegevensverwerking. Op grond van art. 11 lid 1 Wbp moeten persoonsgegevens, gelet op het doel toereikend, ter zake dienend en niet bovenmatig zijn. Het voorschrift dat persoonsgegevens toereikend dienen te zijn, beoogt te waarborgen dat de verantwoordelijke een compleet en juist beeld heeft van de betrokkene. Dat de persoonsgegevens ter zake dienend moeten zijn, dwingt tot een toets aan het doel waarvoor de gegevens verwerkt worden. Uitgaande van een gerechtvaardigd doel van de verwerking, mogen niet meer details over de persoon verwerkt worden dan noodzakelijk is. Niet bovenmatig wil zeggen dat de verantwoordelijke ook met minder gegevens het doel van de verwerking kan realiseren. (Katus & Zwenne, 2010)

In het tweede lid van art. 11 Wbp wordt tot slot genoemd dat de verantwoordelijke de nodige maatregelen treft om persoonsgegevens juist en nauwkeurig te verwerken. Dit wordt ook wel de inspanningsverplichting van de verantwoordelijke genoemd. (Katus & Zwenne, 2010) Met de nodige maatregelen wordt bedoeld de maatregelen die in redelijkheid van de verantwoordelijke kunnen worden gevegd.

3.2.3 Verplichtingen verantwoordelijke en bewerker

Meldplicht

Onder de Wbp had de verantwoordelijke een meldplicht. Bij de meldplicht moesten

organisaties aan de Autoriteit Persoonsgegevens (AP) melden als zij persoonsgegevens verwerkten. De meldplicht is vanaf 6 november 2017 aangepast. Organisaties hoeven geen melding meer te doen als zij persoonsgegevens verwerken, omdat de meldplicht vervalt met komst van de AVG (Autoriteit Persoonsgegevens, 2018). De AP handhaaft naleving op de meldplicht in principe niet meer sinds 6 november 2017, tenzij er sprake is van een gegevensverwerking met een bepaald risico. Het gaat om verwerkingen die naar het oordeel van de wetgever een grote inbreuk zijn op de persoonlijke levenssfeer van de betrokkene. Deze verwerkingen moeten wel gemeld worden, op grond van art. 31 Wbp. (Autoriteit Persoonsgegevens, 2018)

Informatieverstrekking aan betrokkenen

Een persoon wiens gegevens worden verwerkt, moet kunnen nagaan wat er met de gegevens gebeurt. De Wbp bevat daarom een regeling over informatieverstrekking aan de betrokkene (Handleiding Wet bescherming persoonsgegevens, 2002). De betrokkene hoeft niet geïnformeerd te worden indien de betrokkene al op de hoogte is van de informatie. Dit kan zijn wanneer de betrokkene zelf een formulier heeft ingevuld. Dat de betrokkene op de hoogte is, hoeft niet gecontroleerd te worden, er mag na toezending of uitreiking verwacht worden dat de betrokkene op de hoogte is.

In art. 33 lid 2 jo. 34 lid 2 wordt de verantwoordelijke verplicht om de betrokkene mede te delen wat zijn identiteit is en wat de doeleinden zijn van de verwerking waarvoor de gegevens zijn bestemd. De omvang van de informatieplicht hangt, op grond van art. 33 lid 3 jo. 34 lid 3 Wbp, af van wat nodig is om een behoorlijke en zorgvuldige gegevensverwerking te waarborgen. Hoe gevoeliger de gegevens liggen, hoe meer reden er is om de betrokkene gedetailleerd te informeren over de gegevensverwerking (Handleiding Wet bescherming persoonsgegevens, 2002).

Beveiligingsplicht

De verantwoordelijke heeft de plicht om technische en organisatorische maatregelen te treffen om gegevens op de juiste manier te beveiligen. Deze eisen dienen cumulatief (tezamen) getroffen te worden (Autoriteit Persoonsgegevens, 2018) en is opgenomen in art. 13 Wbp. De verplichting tot beveiliging richt zich tegen 'verlies' of 'onrechtmatige verwerkingen' van persoonsgegevens. Een voorbeeld van een organisatorische maatregel kan zijn dat er een beperkt aantal mensen toegang hebben tot een computersysteem (Handleiding Wet bescherming Persoonsgegevens, 2002). Ook kan er gedacht worden aan het gebruik van een bepaalde software, beveiliging met een 'password' (wachtwoord) en door middel van encryptie (versleutelen). In het artikel wordt ten slotte genoemd dat de maatregelen mede erop zijn gericht om onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

Bewaartermijn

Persoonsgegevens dienen niet langer bewaard te worden dan noodzakelijk is voor de verwezenlijking van de doeleinden waarvoor de persoonsgegevens zijn verzameld. Dit is

opgenomen in art. 10 Wbp. Indien persoonsgegevens worden bewaard voor historische, statistische of wetenschappelijke doeleinden, mogen persoonsgegevens langer bewaard worden. De Wbp noemt geen concrete bewaartermijnen voor persoonsgegevens, maar termijnen voor het bewaren van specifieke gegevens zijn in andere verschillende wetten opgenomen (bijvoorbeeld administratie belastingdienst 7 jaar) (Autoriteit Persoonsgegevens, 2018).

Meldplicht datalekken

Vanaf 1 januari 2016 geldt de meldplicht datalekken. In art. 34a Wbp staat de plicht van de verantwoordelijke om de AP onverwijld in kennis te stellen van een inbreuk op de beveiliging, die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens. De verantwoordelijke moet naast de AP ook de betrokkene onverwijld in kennis stellen van de inbreuk, indien dit ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene.

Uitzonderingen

In sommige gevallen hoeft er niet aan de eisen van de Wbp te worden voldaan. Het gaat om op grond art. 43 Wbp om de onderstaande verplichtingen:

- de verplichting om gegevens niet verder te verwerken op een wijze die onverenigbaar is met het doel waarvoor ze zijn verkregen;
- informatie- en inzageverplichtingen;
- de verplichting om inlichtingen te verstrekken over vrijgestelde gegevensverwerkingen. (Handleiding Wet bescherming persoonsgegevens, 2002)

Aan bovenstaande verplichtingen hoeft op grond van art. 43 Wbp niet worden voldaan indien het noodzakelijk is voor:

- a.** de veiligheid van de staat;
- b.** de voorkoming, opsporing en vervolging van strafbare feiten;
- c.** gewichtige economische en financiële belangen van de staat en andere openbare lichamen;
- d.** het toezicht op de naleving van wettelijke voorschriften die zijn gesteld ten behoeve van de belangen, bedoeld onder b en c, of
- e.** de bescherming van de betrokkene of van de rechten en vrijheden van anderen.

3.2.4 Rechten van de betrokkene

Informatieverzoek

De betrokkene heeft het recht om vrijelijk en met redelijke tussenpozen een informatieverzoek voor te leggen aan de verantwoordelijke. Dit recht is opgenomen in art. 35 lid 1 Wbp. Vrijelijk houdt in dat de betrokkene daarbij geen bijzonder belang hoeft aan te tonen (De Vries, 2001). Met redelijke tussenpozen impliceert dat de betrokkene de

verantwoordelijke niet meer dan gemiddeld en noodzakelijk mag benaderen met informatieverzoeken. De verantwoordelijke moet binnen vier weken schriftelijk reageren op een informatieverzoek (MvT, Kamerstukken II 1997/98, 25892, 3, p. 157-158).

Recht op inzage

In het tweede lid van art. 35 Wbp is het recht op inzage vastgelegd. Op het moment dat de gegevens inderdaad worden verwerkt, dan moet de verantwoordelijke de betrokkene hiervan op de hoogte stellen. De mededeling dient een volledig overzicht en in begrijpelijke vorm te zijn. De verantwoordelijke zal bij de voldoening aan de verplichting om aan de betrokkene een volledig overzicht van de verwerkte persoonsgegevens te verschaffen niet mogen volstaan met de verstrekking van globale informatie, maar zal alle relevante informatie over de betrokkene moeten verschaffen. (Handleiding Wet bescherming persoonsgegevens, 2002)

Correctierecht

In art. 36 Wbp staat het recht op verbetering, aanvulling, verwijdering en afscherming van gegevens voor de betrokkene. Dit wordt ook wel het correctierecht genoemd. De verantwoordelijke moet de gegevens verplicht corrigeren als de gegevens feitelijk onjuist, onvolledig of op andere wijze in strijd zijn met een voorschrift van de Wbp of een andere wet. De verantwoordelijke moet op grond van lid 2 van het artikel binnen vier weken na ontvangst van het verzoek aangeven of, en in hoeverre aan het correctieverzoek zal worden voldaan. Het weigeren van een correctieverzoek moet schriftelijk gemotiveerd worden (Handleiding Wet bescherming persoonsgegevens, 2002).

Recht van verzet

De betrokkene kan op grond van art. 40 Wbp verzet aantekenen tegen verwerkingen op grond van art. 8 sub e en f Wbp. Het gaat om verzet tegen verwerkingen die noodzakelijk zijn voor de vervulling van een publieke taak door een bestuursorgaan (art. 8 sub e Wbp) en verwerkingen die noodzakelijk zijn voor de behartiging van een gerechtvaardigd belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt (art. 8 sub f Wbp). Op basis van bijzondere persoonlijke omstandigheden is het mogelijk om verzet aan te tekenen (Handleiding Wet bescherming persoonsgegevens, 2002). Het recht van verzet is op grond van art. 40 lid 4 Wbp niet van toepassing op openbare registers die bij de wet zijn ingesteld.

3.2.5 Bijzondere persoonsgegevens

Het uitgangspunt van de Wbp is dat bijzondere persoonsgegevens niet verwerkt mogen worden. De Wbp kent een aantal algemene en specifieke uitzonderingen op dit verbod (Handleiding Wet bescherming persoonsgegevens, 2002, p. 47). In art. 16 Wbp staat het verbod op het verwerken van bijzondere persoonsgegevens.

Algemene uitzonderingen

De algemene uitzonderingen worden genoemd in art. 23 Wbp. In de volgende gevallen mogen bijzondere gegevens verwerkt worden:

- de betrokkene heeft uitdrukkelijk toestemming gegeven;
- de betrokkene heeft de gegevens zelf al duidelijk openbaar gemaakt;
- de verwerking is noodzakelijk voor het vaststellen, het uitoefenen of het verdedigen van een recht in een gerechtelijke procedure;
- de verwerking is noodzakelijk ter verdediging van de vitale belangen van de betrokkene of van een derde en het vragen van diens uitdrukkelijke toestemming is onmogelijk;
- de verwerking is noodzakelijk ter voldoening aan een volkenrechtelijke verplichting;
- de verwerking is noodzakelijk met het oog op een zwaarwegend algemeen belang.

In art. 17 t/m 22 Wbp worden de specifieke uitzonderingen genoemd wat betreft het verwerken van bijzondere persoonsgegevens. In deze gevallen mogen bijzondere persoonsgegevens wel worden verwerkt.

Godsdienst of levensovertuiging

Het verbod op het verwerken van gegevens over iemands godsdienst of levensovertuiging is op grond van art. 17 Wbp niet van toepassing indien het gaat om kerkgenootschappen of genootschappen op geestelijke grondslag of andere instellingen op godsdienstige of levensbeschouwelijke grondslag. Een verzorgingstehuis op islamitische grondslag en een katholieke universiteit zijn voorbeelden van 'andere instellingen' (Handleiding Wet bescherming persoonsgegevens, 2002).

Ras

In art. 18 Wbp worden de gronden uitgewerkt wanneer het verbod van persoonsgegevens betreffende iemands ras niet van toepassing is. Alleen in uitzonderlijk geval mogen gegevens over iemands ras verwerkt worden. Het is toegestaan op het moment dat het gebruikt wordt voor identificatiedoeleinden of met het doel om personen van een bepaalde etnische of culturele minderheidsgroep een bevoorrechte positie toe te kennen ten einde feitelijke nadelen verband houdende met de grond ras op te heffen of te verminderen, dus kortgezegd in het kader van voorkeursbeleid. Een voorbeeld van het verwerken van gegevens voor identificatiedoeleinden is een systeem van toegangspasjes van werknemers. Het gaat dan om verwerkingen die nodig zijn omdat bijvoorbeeld de omvang of de openbare toegankelijkheid van een bedrijf meebrengt dat identificatie met behulp van een foto noodzakelijk is. (Handleiding Wet bescherming persoonsgegevens, 2002)

Politieke gezindheid

Het verbod om persoonsgegevens betreffende iemands politieke gezindheid te verwerken, is niet van toepassing indien het gaat om een verwerking door instellingen op politieke grondslag betreffende hun leden of hun werknemers dan wel andere tot de instelling behorende personen, voor zover dit gelet op het doel van de instelling noodzakelijk is voor de verwezenlijking van haar grondslag, of met het oog op de eisen die met betrekking tot

politieke gezindheid in redelijkheid kunnen worden gesteld in verband met de vervulling van functies in bestuursorganen en adviescolleges, op grond van art. 19 Wbp. Het zal hierbij in de praktijk meestal gaan om ledenadministraties van politieke partijen, de administraties die worden gehouden van personen die in dienst zijn van een politieke partij en administraties van andere personen die gerekend kunnen worden tot een instelling op politieke grondslag (Gardeniers & Nouwt, 2009).

Gezondheidsgegevens

In art. 21 Wbp worden een aantal uitzonderingen genoemd, dat onder bepaalde voorwaarden gegevens over iemands gezondheid verwerkt mogen worden. Hulpverleners, instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening hebben een ontheffing van het verwerkingsverbod (Gardeniers & Nouwt, 2009). Daarnaast geldt voor verzekeraars dat indien het noodzakelijk is voor de beoordeling van het door de verzekeraar te verzekeren risico en indien dit noodzakelijk is voor de uitvoering van de overeenkomst van de verzekering. Ook zijn er uitzonderingen voor speciale scholen, reclasseringsinstellingen, de raad voor de kinderbescherming en voogdijinstellingen. (Handleiding Wet bescherming persoonsgegevens, 2002)

Strafrechtelijke persoonsgegevens

Art. 22 Wbp betreft de verwerking van strafrechtelijke persoonsgegevens door 'organen die krachtens de wet zijn belast met de toepassing van het strafrecht, alsmede door verantwoordelijkheden die deze hebben verkregen krachtens de Wet politiegegevens of de Wet justitiële en strafvorderlijke gegevens'. Het verbod geldt dus niet in deze gevallen. De uitzondering is niet van toepassing op de verwerking door de reguliere politie (Gardeniers & Nouwt, 2009). De bepaling regelt de verwerking van gegevens over personen die wegens gebleken of vermoede onregelmatigheden niet op gelijke voet als andere aan het maatschappelijke verkeer kunnen deelnemen of op wie de aandacht is gericht in verband met mogelijk verwijtbaar gedrag (Autoriteit Persoonsgegevens, 2018).

3.2.6 Gevolgen overtreden eisen Wbp

Toezicht

Op het moment dat er niet wordt voldaan aan de eisen van de Wbp zitten er gevolgen aan vast. Er wordt in Nederland toezicht gehouden op naleving van de Wbp door de AP. Dit wordt gedaan op grond van art. 51 lid 1 Wbp. Op het moment dat verwerking van persoonsgegevens niet conform de eisen van de wet wordt gedaan, is de AP bevoegd om een sanctie op te leggen.

Bestuursdwang

De AP is op grond van art. 65 Wbp bevoegd om een last onder bestuursdwang op te leggen. De basis voor deze maatregel is te vinden in art. 28 lid 3 van de Richtlijn (richtlijn 95/46/EG). Materieel gezien komt de bevoegdheid overeen met hetgeen in de Algemene wet bestuursrecht (Awb) valt onder last onder bestuursdwang, conform de omschrijving van art.

5:21 Awb. Last onder bestuursdwang is een sanctie die gericht is op herstel (Bitter, 2014). Onder last onder bestuursdwang wordt verstaan: de herstelsanctie, inhoudende:

- a. een last tot geheel of gedeeltelijk herstel van de overtreding, en
- b. de bevoegdheid van het bestuursorgaan om de last door feitelijk handelen ten uitvoer te leggen, indien de last niet of niet tijdig wordt uitgevoerd.

De last onder bestuursdwang geeft aan welke herstelmaatregelen er plaats moeten vinden en binnen welke termijn dit gedaan dient te worden (art. 5:24 Awb). Wordt dit niet gedaan, dan kan de AP zelf de herstelmaatregelen nemen. De kosten die hiervoor gemaakt worden zijn voor de overtreder (de verantwoordelijke). In plaats van bestuursdwang kan er een last onder dwangsom opgelegd worden (Autoriteit Persoonsgegevens, 2018).

Dwangsom

Op grond van art. 5:32 Awb kan een bestuursorgaan dat bevoegd is een last onder bestuursdwang op te leggen, in plaats daarvan een last onder dwangsom opleggen. Een last onder dwangsom is ook een herstelsanctie. In art. 5:31d Awb staat de beschrijving van de last onder dwangsom: Onder last onder dwangsom wordt verstaan: de herstelsanctie, inhoudende:

- a. een last tot geheel of gedeeltelijk herstel van de overtreding, en
- b. de verplichting tot betaling van een geldsom indien de last niet of niet tijdig wordt uitgevoerd.

De last onder dwangsom omschrijft de te nemen herstelmaatregelen en er wordt een termijn gesteld gedurende welke de overtreder de last kan uitvoeren zonder dat de dwangsom wordt verbeurd (art. 5:32a Awb). Een last onder dwangsom zal opgelegd worden wanneer de AP de overtreding niet gemakkelijk zelf kan herstellen (Handleiding Wet bescherming persoonsgegevens, 2002). De AP kan bijvoorbeeld opleggen dat binnen één week bepaalde gegevens verwijderd moeten worden, indien dit niet gedaan wordt kan er per dag dat er niet aan de last wordt voldaan een bedrag worden opgelegd.

Bestuurlijke boete

In een aantal gevallen kan er een bestuurlijke boete opgelegd worden door de AP. Tot 1 januari 2016 kon de AP slechts in een beperkt aantal gevallen een bestuurlijke boete opleggen van maximaal € 4.500,-. Per 1 januari 2016 is de bevoegdheid uitgebreid en is de maximale boete verhoogd. De maximale hoogte van de boete is afhankelijk van de ernst van de overtreding. In art. 66 lid 1 Wbp worden de artikelen genoemd wanneer de geldboete kan oplopen tot een bedrag van de vierde categorie van art. 23 lid 4 Sr, wat neerkomt op € 20.750,-. Op grond van de in art. 66 lid 2 Wbp genoemde overtredingen, kan de geldboete zelfs oplopen tot een bedrag van de zesde categorie van art. 23 lid 4 Sr, een bedrag van € 820.000,-.

3.3 Algemene verordening gegevensbescherming

Vanaf 25 mei 2018 moeten persoonsgegevens verwerkt worden volgens de regels van de AVG. In dit hoofdstuk zal de AVG uitgewerkt worden. Ondanks dat de AVG voor alle landen in de EU geldt, biedt de AVG op een aantal punten ruimte voor de landen om zelf regels nader te bepalen. De invulling van deze ruimte wordt vastgelegd in de zogeheten Uitvoeringswet AVG (UAVG). De wet is op het moment van schrijven nog niet vastgesteld, maar ervan uitgaande dat de UAVG aangenomen zal worden, wordt deze toegepast in het juridisch kader.

Er wordt in dit hoofdstuk ingegaan op het volgende: wanneer de AVG van toepassing is, welke eisen de AVG stelt aan de verwerking van persoonsgegevens, de verplichtingen voor de verwerkingsverantwoordelijke en de verwerker, de rechten van de betrokkene, hoe er moet worden omgegaan met de verwerking van bijzondere- en gevoelige persoonsgegevens en wat de gevolgen zijn bij het niet voldoen aan de eisen van de AVG.

3.3.1 Belangrijke begrippen

Betrokkene

De betrokkene is de (natuurlijke) persoon wiens gegevens verwerkt worden.

Verwerkingsverantwoordelijke

In de Wbp werd er gesproken over 'verantwoordelijke', dit is in de AVG vervangen door de 'verwerkingsverantwoordelijke. De verwerkingsverantwoordelijke is de (natuurlijke) persoon, rechtspersoon, overheidsinstantie die het doel van de verwerking en de middelen daarvoor vaststelt. In art. 4 lid 7 AVG wordt dit begrip nader toegelicht.

Verwerker

In de Wbp werd gesproken over 'bewerker', dit wordt in de AVG vervangen door 'verwerker'. In art. 28 AVG wordt het begrip nader toegelicht. De verwerker is op grond van art. 4 lid 8 AVG: de natuurlijke persoon of rechtspersoon, die namens de verwerkingsverantwoordelijke persoonsgegevens verwerkt. De verwerkingsverantwoordelijke bepaalt het doel en de middelen voor de verwerkingen, dat doet de verwerker niet.

3.3.2 AVG van toepassing?

Om te weten te komen of de verordening van toepassing is, moet het volgende vastgesteld worden:

- 1) Verwerk ik gegevens?
- 2) Zijn deze gegevens persoonsgegevens?
- 3) Verwerk ik deze gegevens geheel of gedeeltelijk geautomatiseerd, of zijn ze opgenomen in een bestand, dan wel bestemd om worden opgenomen te worden in een bestand? (Handleiding Algemene verordening gegevensbescherming, 2018)

Persoonsgegevens

In art. 4 lid 1 AVG wordt de definitie van persoonsgegevens in de AVG weergegeven. Wat direct opvalt is dat de definitie uitgebreider is dan in de Wbp. In het artikel staat namelijk het

volgende: ‘alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (“de betrokkene”); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identicator zoals een naam, een 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’. De reikwijdte van ‘identificeerbaar’ is vergroot ten opzichte van de Wbp. In overweging 26 Preambule wordt gesproken over wat identificeerbaar precies inhoudt. Om te bepalen of een natuurlijke persoon identificeerbaar is, moet er rekening worden gehouden met alle middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt door de verwerkingsverantwoordelijke of door een andere persoon om de natuurlijke persoon direct of indirect te identificeren.

Verwerking

In art. 4 lid 2 AVG wordt de definitie van ‘verwerking’ uitgelegd: ‘een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens’. De definitie van verwerking is nagenoeg gelijk gebleven zoals beschreven in de Wbp.

Indien de bovenstaande vragen met ‘ja’ beantwoord zijn, wordt er gekeken naar de volgende vragen:

- 4) Valt mijn verwerking binnen het toepassingsbereik van de verordening?
(Handleiding Algemene verordening gegevensbescherming, 2018)

Materiële toepasselijkheid van de AVG

In het tweede artikel van de AVG gaat het over de materiële toepasselijkheid van de AVG. Art. 2 lid 1 AVG stelt het volgende: ‘deze verordening is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.’

Een geautomatiseerde werking wil zeggen dat er middelen, methoden en/of technologieën worden gebruikt om verwerking van persoonsgegevens tot stand te laten komen. Op het moment dat er persoonsgegevens handmatig worden verwerkt is de AVG van toepassing. Een in het geheel niet geautomatiseerde verwerking valt slechts onder de AVG op het moment dat er sprake is van een bestand met persoonsgegevens. Een papieren kopie van een geautomatiseerde verwerking valt ook onder de definitie van een geautomatiseerde verwerking. (Engelfriet, Meij & Kager, 2017)

Uitzonderingen

In art. 2 lid 2 AVG worden uitzonderingen wat betreft de toepassing van de verordening genoemd. Zo is op grond van art. 2 lid 2 sub a de verordening niet van toepassing op de verwerking van persoonsgegevens in het kader van activiteiten die buiten de werkingssfeer van het Unierecht vallen. Sub b stelt dat de verordening niet van toepassing is op de verwerking van persoonsgegevens die door de lidstaten bij de uitvoering van activiteiten die binnen de werkingssfeer van titel V, hoofdstuk 2 van het Verdrag betreffende de Europese Unie (VEU) vallen. Dit hoofdstuk bevat specifieke bepalingen betreffende het gemeenschappelijk buitenlands en veiligheidsbeleid van de lidstaten. Vervolgens sluit sub c uit dat de verordening niet van toepassing is op de verwerking van persoonsgegevens door een natuurlijke persoon bij de uitoefeningen van een zuiver persoonlijke of huishoudelijke activiteit. Deze activiteiten dienen zodanig geen enkel verband te houden met een beroep- of handelsactiviteit (overweging 18 Preambule). Een voorbeeld van een zuiver huishoudelijke activiteit is cameratoezicht door particulieren bij een openbare ruimte. Ten slotte sluit sub d uit dat de verordening niet van toepassing is op de door de 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. (Engelfriet, Meij & Kager, 2017)

Territoriale toepasselijkheid

Het derde artikel van de AVG gaat over de territoriale toepasselijkheid van de AVG. Het artikel luidt als volgt: 'Deze verordening is van toepassing op de verwerking van persoonsgegevens in het kader van de activiteiten van een vestiging van een verwerkingsverantwoordelijke of een verwerker in de Unie, ongeacht of de verwerking in de Unie plaatsvindt.' Een voorbeeld van de brede reikwijdte van de AVG is het onderstaande voorbeeld.

Veel verwerkingen worden door Amerikaanse bedrijven verricht, denk aan Twitter of Google. Sommige van deze bedrijven hebben daarbij een Europese dochteronderneming opgezet, zoals Facebook of Microsoft, maar lang niet altijd. De AVG is van toepassing als men een vestiging in de EU heeft, ongeacht of deze dan ook verwerkingen uitvoert (Engelfriet, Meij & Kager, 2017, p. 18).

Tot slot moet er vastgesteld worden wat de juridische hoedanigheid is van de persoon die de verwerking van de persoonsgegevens uitvoert. Deze bepaalt namelijk welke regels van toepassing zijn. De laatste vraag luidt als volgt:

- 5) Ben ik de verwerkingsverantwoordelijke, of ben ik een verwerker? (Handleiding Algemene verordening gegevensbescherming, 2018)

Zie 3.3.1 van dit onderzoeksrapport voor de definitie van 'verwerkingsverantwoordelijke' en 'verwerker', om antwoord op deze vraag te kunnen geven.

3.3.3 Eisen AVG gegevensverwerking

Rechtmatigheid van de verwerking

Er moet sprake zijn van een wettelijke grondslag om 'gewone' persoonsgegevens te mogen verwerken. De AVG kent net als de Wbp zes grondslagen. De grondslagen zijn opgenomen in art. 6 AVG. De verwerking van persoonsgegevens is alleen voldaan indien er voor zover aan tenminste een van de onderstaande voorwaarden is voldaan:

- a. de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doelen;
- b. de gegevensverwerking is noodzakelijk voor de uitvoering van de overeenkomst;
- c. de gegevensverwerking is noodzakelijk voor het nakomen van een wettelijke verplichting;
- d. de gegevensverwerking is noodzakelijk ter bescherming van de vitale belangen;
- e. de gegevensverwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of uitoefening van openbaar gezag;
- f. de gegevensverwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen.

Beginselen inzake de verwerking van persoonsgegevens

De AVG gaat uit van zes basisbeginselen waaraan iedere verwerking moet voldoen. Deze staan verwerkt in art. 5 lid 1 sub a t/m f AGV. Artikel 10 Grondwet (Gw) legt de basis voor de verwerking van persoonsgegevens. In dit artikel staat namelijk het volgende:

Lid 1: Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer.

Lid 2: De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens.

Lid 3: De wet stelt regels inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens.

De beginselen waaraan iedere verwerking moet voldoen op grond van art. 5 AVG zijn de volgende:

Rechtmatig, behoorlijk en transparant

In sub a wordt het beginsel van rechtmatigheid, behoorlijkheid en transparantie genoemd. Dit houdt in dat het voor betrokkenen inzichtelijk moet zijn in hoeverre en op welke manier persoonsgegevens worden verwerkt. De informatie en communicatie dient eenvoudig toegankelijk en begrijpelijk te zijn. Dit betekent dat juridische taal zeer ongewenst is. (Engelfriet, Meij & Kager, 2017). Dit beginsel wordt aangevuld met overweging 39 en 58 Preambule. Ten opzichte van de eisen van de Wbp is 'zorgvuldigheid' vervangen voor het

woord 'transparant'. Het begrip transparant zorgt ervoor dat het recht op informatie van de betrokkene wordt gewaarborgd en sluit aan bij de verantwoordingsplicht van de verwerkingsverantwoordelijke.

Doelbinding

In sub b wordt het beginsel van doelbinding genoemd. Verwerking mag alleen gebeuren voor specifieke en gerechtvaardigde doeleinden. Er moet een reden zijn die de inperking van het grondrecht privacy rechtvaardigt. (Engelfriet, Meij & Kager, 2017).

Dataminimalisatie

In sub c wordt "minimale gegevensverwerking" genoemd, ook wel het beginsel van dataminimalisatie. Dit beginsel brengt met zich mee dat niet meer persoonsgegevens mogen verwerkt dan strikt nodig is voor het doel. Alleen de noodzakelijke gegevens mogen verwerkt worden. Persoonsgegevens dienen zo snel mogelijk gewist te of onherkenbaar gemaakt te worden. (Engelfriet, Meij & Kager, 2017).

Juistheid

Er moet voorkomen worden dat er wordt gewerkt met onjuiste of achterhaalde gegevens. Vandaar het beginsel van juistheid. Het beginsel in sub d eist dat gegevens juist en actueel moeten zijn. Op het moment dat gegevens onjuist of achterhaald zijn, moeten zij worden gewist. (Engelfriet, Meij & Kager, 2017).

Opslagbeperking

Het vijfde beginsel, sub e, is het beginsel van opslagbeperking. Dit beginsel dient ervoor te zorgen dat persoonsgegevens niet langer worden bewaard dan nodig is voor de verwerking. Er worden in de AVG geen concrete termijnen gegeven, maar verlangt van de verwerkingsverantwoordelijke dat deze gezien zijn beoogde verwerkingen zelf termijnen vaststelt voor het wissen van gegevens. (Engelfriet, Meij & Kager, 2017).

Integer en vertrouwelijk

Het laatste beginsel, sub f, is het beginsel van integriteit en vertrouwelijkheid. De verwerkingsverantwoordelijke moet de technische en organisatorische beveiligingsmaatregelen nemen om ongeoorloofde toegang tot of het ongeoorloofd gebruik van persoonsgegevens te voorkomen. (Engelfriet, Meij & Kager, 2017).

3.3.4 Verplichtingen verwerkingsverantwoordelijke en verwerker

In art. 24 van de AVG wordt de verantwoordelijkheid van de verwerkingsverantwoordelijke beschreven. De verwerkingsverantwoordelijke is verplicht passende en effectieve maatregelen te nemen om naleving van de AVG te borgen. Doordat een van de grootste veranderingen van de AVG ten opzichte van de Wbp vooral ziet op de versterkte rechten van betrokkene, worden de verplichtingen van de verwerkingsverantwoordelijke en de verwerker strenger. Allereerst wordt het toepassingsbereik van de verplichtingen uitgebreid: verwerkers dienen eveneens te voldoen aan de verplichtingen van de verordening. Daarnaast veranderen de materiële verplichtingen van de verwerkingsverantwoordelijke en de verwerker. De

voorafgaande meldingsplicht bij alle gegevensverwerkingen wordt vervangen door de registerplicht. (Nederlands juristenblad, 2018)

Verwerkersovereenkomst

Indien er gebruik wordt gemaakt van een verwerker of sub-verwerker, dienen de verwerkingsverantwoordelijke en de verwerker (of sub-verwerker) een overeenkomst sluiten. Ook als er eenmalig met een verwerker wordt gewerkt. De verwerkersovereenkomst dient in schriftelijke vorm te zijn, dit mag ook elektronisch zijn. Deze verplichting is opgenomen in art. 28 lid 3 AVG. In de verwerkingsovereenkomst wordt opgenomen: het onderwerp en de duur van de verwerking, de aard en het doel van de verwerking, het soort persoonsgegevens en de categorieën van betrokkenen en de rechten en plichten van de verwerkingsverantwoordelijke.

Naast bovenstaande verplichtingen dient er in de verwerkersovereenkomst te worden bepaald dat:

- a. de persoonsgegevens alleen verwerkt worden onder schriftelijke instructies van de verwerkingsverantwoordelijke;
- b. de overeenkomst waarborgt dat de toegang is beperkt tot de gemachtigde personen. Deze personen moeten gebonden zijn aan geheimhouding op grond van een overeenkomst of een wettelijke verplichting;
- c. de verwerker minimaal hetzelfde niveau van beveiliging van persoonsgegevens hanteert als de verwerkingsverantwoordelijke;
- d. op het moment dat er sprake is van een datalek, de verwerkersovereenkomst regelt dat de verwerker de verwerkingsovereenkomst bijstaat bij het nakomen van de verplichtingen;
- e. de verwerkingsverantwoordelijke alle mogelijke ondersteuning biedt aan de verwerker bij het nakomen van de verplichtingen met het oog op beantwoording van verzoeken rondom de rechten van betrokkenen;
- f. na beëindiging van de overeenkomst, gegevens worden gewist, teruggegeven en kopieën worden verwijderd;
- g. de verwerkingsverantwoordelijke alle informatie beschikbaar stelt die nodig is om aantoonbaar te maken dat er wordt voldaan aan de verplichtingen van de AVG;
- h. er afspraken met betrekking tot sub-verwerkers worden gemaakt.

Gezamenlijke verwerkingsverantwoordelijken

Wanneer twee partijen gezamenlijk het doel en de middelen voor de verwerking van persoonsgegevens hebben vastgesteld, maakt dit hen op grond van art. 26 AVG gezamenlijke verwerkingsverantwoordelijken. (Engelfriet, Meij, Kager, 2017).

Verantwoordingsplicht

In art. 24 staat dat de verwerkingsverantwoordelijke verplicht is om de technische en organisatorische maatregelen te treffen om te kunnen waarborgen dat aan de normen van de

AVG wordt voldaan. Anders dan in de Wbp, formuleert de AVG een open norm wat betreft de passende maatregelen (Engelfriet, Meij, Kager, 2017). De verwerkingsverantwoordelijke mag tijdens de verwerking rekening houden met de aard, de omvang, de context en het doel van de verwerking. En de ernst en waarschijnlijkheid van de risico's die uit de verwerking voortvloeien voor de rechten en vrijheden van natuurlijke personen. De verwerkingsverantwoordelijke heeft, afhankelijk van de hoogte van het risico voor de betrokkene, een grotere verantwoordelijkheidsplicht. Hoe groter het risico voor de betrokkene, hoe meer verplichtingen er gelden voor de verwerkingsverantwoordelijke. Het is dus niet nodig om steeds de zwaarste maatregel te nemen (Engelfriet, Meij, Kager, 2017). De verantwoordingsplicht houdt kortgezegd in dat de verwerkingsverantwoordelijke kan aantonen dat een verwerking aan de beginselen van verwerking voldoet wanneer de AP daar om vraagt (Handleiding algemene verordening gegevensbescherming 2018). In art. 5 lid 2 AVG staat dat de verwerkingsverantwoordelijke verplicht is voor naleving van art. 5 lid 1 AVG (de 6 beginselen). Dit valt onder de verantwoordingsplicht. De AVG geeft geen regels over hoe de verantwoordingsplicht concreet ingevuld dient te worden, maar geeft wel de maatregelen die getroffen moeten worden om invulling te geven aan de eisen die gesteld worden. Hieronder volgt een overzicht over de maatregelen die getroffen dienen te worden.

Registerplicht

De verwerkingsverantwoordelijke heeft op grond van art. 30 AVG de plicht om een register bij te houden van verwerkingsactiviteiten die onder zijn verantwoordelijkheid hebben plaatsgevonden. Een organisatie die minder dan 250 personen in dienst heeft, is vrijgesteld van het bijhouden van een register. Er zijn een aantal uitzonderingen op deze vrijstelling: wanneer de verwerking risico's inhoudt voor de betrokkenen en als er sprake is van verwerkingen die niet incidenteel zijn. Dit moet zelf door de verwerkingsverantwoordelijke ingeschat worden. Ondanks dat de verplichting in sommige situaties niet geldt, is het toch verstandig om een register bij te houden om transparantie te vergroten. Bij advocatenkantoren zijn verwerkingen bijna allemaal structureel en vaak is er risico voor betrokkenen. Advocaten hebben niet voor niets een geheimhoudingsplicht. Dat iemand een advocaat heeft ingeschakeld kan in sommige gevallen al gevoelige informatie zijn, aldus De Vries (2018).

Het register bevat de naam en de contactgegevens van de verwerkingsverantwoordelijke(n), de verwerkingsdoeleinden, een beschrijving van de categorieën van betrokkenen (bijvoorbeeld cliënten, werknemers) en van persoonsgegevens, de grondslag van de verwerking en indien mogelijk: de beoogde termijnen waarbinnen de verschillende categorieën van gegevens gewist moeten worden en een korte beschrijving van de beveiligingsmaatregelen die zijn genomen (de technische- en organisatorische beveiligingsmaatregelen). (Autoriteit Persoonsgegevens, 2018)

Functionaris gegevensbescherming

Op grond van art. 37 AVG is het in drie situaties verplicht om een functionaris voor de gegevensbescherming (FG) aan te stellen (ook bekend als de *data protection officer*).

Allereerst zijn overheden en publieke organisaties verplicht om een FG aan te stellen, ten tweede geldt de verplichting voor organisaties die het uitvoeren van regelmatige en stelselmatige observatie op grote schaal van betrokkenen als hoofdactiviteit hebben (bijv. recherchebureaus) en ten derde zijn organisaties verplicht als ze op grote schaal bijzondere persoonsgegevens verwerken. Het gaat dan met name om verwerking van veel bijzondere strafrechtelijke persoonsgegevens (De Vries, 2018). De FG is geen toezichthouder en heeft geen corrigerende bevoegdheden. De aanbevelingen die de FG doet wegen wel zwaar bij bepaling of een verwerking rechtmatig is (Engelfriet, Meij, Kager, 2017). Overweging 91 Preambule bepaalt dat verwerkingen van persoonsgegevens van cliënten door een individuele advocaat nooit als grootschalig mogen worden beschouwd, waardoor individuele advocaten geen FG aan hoeven te stellen. Of een advocatenkantoor een FG moet aanstellen, hangt dus af van de praktijk en van de omvang van het kantoor (De Vries, 2018).

Gegevensbeschermingseffectbeoordeling

De verwerkingsverantwoordelijke is vanuit het oogpunt van een zorgvuldige omgang met persoonsgegevens verplicht om een gegevensbeschermingseffectbeoordeling (ook wel bekend als: *privacy impact assessment*, PIA) uit te voeren voor verwerkingen die waarschijnlijk een verhoogd risico opleveren. Deze plicht is opgenomen in art. 35 AVG. De norm van een waarschijnlijk hoog risico is een open norm (Engelfriet, Meij, Kager, 2017, p. 148). Er zijn drie gevallen die specifiek worden genoemd als verwerkingen met een waarschijnlijk hoog risico in art. 35 lid 3 sub a t/m c AVG. Het is een niet-limitatieve opsomming.

Het eerste geval waarbij een gegevensbeschermingseffectbeoordeling in ieder geval verplicht is, (sub a) is bij situaties waarin grootschalig besluiten worden genomen gebaseerd op geautomatiseerde verwerkingen van persoonsgegevens, zoals bij profilering. De definitie van profilering wordt gegeven in art. 4 lid 4 AVG:

Profilering: elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.

De tweede situatie waarbij een gegevensbeschermingseffectbeoordeling in ieder geval verplicht is (sub b), is bij grootschalige verwerkingen van bijzondere categorieën van persoonsgegevens of van gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten. In overweging 91 Preambule wordt de definitie van grootschalig uitgelegd. Onder grootschalig wordt verstaan: een aanzienlijke hoeveelheid persoonsgegevens op regionaal, nationaal of supranationaal niveau.

De derde situatie (sub c) waarbij een gegevensbeschermingseffectbeoordeling in ieder geval nodig is, is voor de stelselmatig en grootschalige monitoring van openbaar toegankelijke ruimten. Een voorbeeld hiervan is bij bewaking door beveiligingscamera's.

Naast de drie genoemde situaties in de AVG, zijn er nog een aantal andere voorbeelden genoemd door de AP wanneer een gegevensbeschermingseffectbeoordeling nodig is. Er worden 9 criteria genoemd om te toetsen wanneer dit nodig is. De 9 criteria die genoemd worden door de AP zullen hierna kort genoemd worden, maar niet verder behandeld worden.

- Beoordelen van mensen op basis van persoonskenmerken;
- geautomatiseerde beslissingen (genoemd in de AVG);
- stelselmatige en grootschalige monitoring (genoemd in de AVG);
- gevoelige gegevens;
- grootschalige gegevensverwerkingen (genoemd in de AVG);
- gekoppelde databases;
- gegevens over kwetsbare personen;
- gebruik van nieuwe technologieën;
- blokkering van een recht, dienst of contract.

In drie stappen kan er beoordeeld worden of er sprake is van een verhoogd risico:

1. Bij iedere verwerking moet een korte beoordeling worden gemaakt van de risico's die kunnen bestaan. Dit wordt in het verwerkingsregister genoteerd.
2. Indien uit de eerste beoordeling volgt dat er waarschijnlijk een verhoogd risico kleeft aan de verwerking, dan moet daarop een gegevensbeschermingseffectbeoordeling uitgevoerd worden. Hierin moet elk risico benoemd worden en de mogelijkheden om het risico in te perken.
3. Als blijkt dat het risico niet kan worden beperkt met redelijke middelen, dan moet de toezichthouder om toestemming gevraagd worden. (Engelfriet, Chew-Meij, Kager, 2018)

Uit overweging 91 Preambule volgt dat de verwerking van een individuele advocaat niet gezien kan worden als een verwerking op grote schaal. Eenmanskantoren zouden in theorie daarom geen gegevensbeschermingseffectbeoordeling te hoeven doen (De Vries, 2018).

Voorafgaande raadpleging

Op het moment dat een gegevensbeschermingseffectbeoordeling laat zien dat een verwerking een hoog risico voor de betrokkene zou opleveren, ondanks dat er redelijke maatregelen zijn getroffen door de verwerkingsverantwoordelijke, is deze op grond van art. 36 AVG verplicht om voorafgaande toestemming te vragen aan de toezichthouder.

Gegevensbescherming door ontwerp en standaardinstellingen

Naast de algemene verplichting tot beveiliging van persoonsgegevens zoals bedoeld in art. 24 AVG, kent de AVG op grond van art. 25 AVG een plicht om verwerkingen zo in te richten dat rekening wordt gehouden met *privacy by design* en *privacy by default*. *Privacy by design* houdt in dat de voor verwerking gebruikte mechanismen zo zijn ontworpen dat zij zo veel mogelijk

rekening houden met de privacy van betrokkenen en de vereisten uit de AVG. Een voorbeeld hiervan is een systeem dat knoppen ingebouwd heeft waarmee betrokkenen inzake in hun persoonsgegevens kunnen krijgen. Er is sprake van *privacy by default* wanneer de standaardinstellingen zo zijn gekozen dat de privacy maximaal wordt gewaarborgd. Een voorbeeld hiervan, op het gebied van sociale media, is dat berichten standaard slechts aan 'directe vrienden' worden getoond, en pas na een actieve handeling van de gebruiker aan alle gebruikers of de gehele wereld. (Engelfriet, Meij, Kager, 2017) Een voorbeeld dat wordt genoemd in art. 25 AVG als passende technische en organisatorische maatregel is pseudonimisering. De definitie van pseudonimisering wordt gegeven in art. 4 lid 4 AVG:

Pseudonimisering: het zodanig aanpassen van persoonsgegevens dat zij niet meer aan een specifieke betrokkene gekoppeld kunnen worden zonder aanvullende gegevens.

Beveiliging van de verwerking

In art. 32 AVG worden de beveiligingsmaatregelen uitgewerkt. Er moet rekening gehouden worden met de stand van de techniek, de uitvoeringskosten, de aard, de omvang, de context van de verwerking en de qua waarschijnlijkheid en ernst van uiteenlopende risico's voor de rechten en vrijheden van personen passend zijn. Dit houdt in dat er een risico en maatregelen analyse moet worden gemaakt. Passende maatregelen zijn in ieder geval volgens art. 32 lid 1 sub a t/m d:

- a. de pseudonimisering en versleuteling van persoonsgegevens;
- b. het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
- c. het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
- d. een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

Ten opzichte van art. 13 Wbp zijn er dus een aantal elementen toegevoegd wat betreft de beveiliging van persoonsgegevens.

Meldplicht datalekken

Op het moment dat er sprake is van een inbreuk in verband met persoonsgegevens, oftewel een datalek, moet dit op grond van art. 33 AVG zonder vertraging gemeld worden aan de AP. Het gaat om het melden van een inbreuk en persoonsgegevens zijn vernietigd of verloren, gewijzigd, verstrekt of toegankelijk gemaakt op een manier die onrechtmatig is (Engelfriet, Meij, Kager, 2017). De melding moet in principe binnen 72 uur nadat er kennis is genomen van de inbreuk gedaan worden indien er een risico bestaat voor de betrokkene. Indien de melding niet binnen 72 uur na ontdekking gedaan wordt, zal de vertraging gemotiveerd

moeten worden. Wanneer het onwaarschijnlijk is dat de inbreuk een risico met zich meebrengt, hoeft er geen melding gedaan te worden maar moet de inbreuk wel gedocumenteerd worden, om in de toekomst erger te voorkomen (Engelfriet, Meij, Kager, 2017).

Een datalek kan tot gevolg hebben dat advocaten niet kunnen voldoen aan hun geheimhoudingsplicht, daarom moeten advocatenkantoren voldoende en de juiste beveiligingsmaatregelen nemen om dit te voorkomen. (De Vries, 2018)

Mededeling betrokkene

Naast de meldplicht aan de toezichthoudende autoriteit, bestaat er een meldplicht aan de betrokkene om wiens persoonsgegevens het gaat. Deze meldplicht is opgenomen in art. 34 AVG. De inbreuk moet gemeld worden aan de betrokkene indien de inbreuk waarschijnlijk een hoog risico inhoudt voor de rechten en de vrijheden van de betrokkene.

Er zijn een aantal uitzonderingen wanneer het niet nodig is om een datalek mede te delen aan de betrokkene. De uitzonderingen worden in art. 34 lid 3 sub a t/m c genoemd. Een melding is niet vereist op het moment dat:

- a. de persoonsgegevens onbegrijpelijk zijn gemaakt voor onbevoegden, bijvoorbeeld versleuteld;
- b. de verwerkingsverantwoordelijke na het datalek direct de maatregelen heeft genomen om de gevolgen van het datalek voor de betrokkene te voorkomen;
- c. het gaat om een groot aantal betrokkenen waardoor de melding onevenredig veel moeite kost. Een openbare mededeling kan in dat geval volstaan.

Toestemming betrokkene

Op de betreffende organisatie rust de bewijslast dat er toestemming is gegeven door een betrokkene. Toestemming moet vrijwillig zijn. Dit houdt in dat de betrokkene moet kunnen weigeren om toestemming te geven en dat er geen enkele dwang of tweederangs behandeling mag volgen als men weigert. Ten tweede moet toestemming specifiek gegeven zijn. De vraag moet in eenvoudige en duidelijke taal gesteld worden en mag niet verstopt zijn in een lap tekst zoals in de algemene voorwaarden of een privacyverklaring. Ten derde moet de betrokkene geïnformeerd zijn (vaak via privacyverklaring). Vervolgens moet de toestemming ondubbelzinnig zijn. Er mag dus geen twijfel bestaan voor het geven van toestemming voor de verwerking van de gegevens. Tot slot moet de toestemming op ieder moment in te trekken zijn, en wel net zo eenvoudig als waarop de toestemming gegeven is. (Engelfriet, Chew-Meij, Kager. 2018)

Informatieplicht

Privacyverklaring

De betrokkene heeft het recht op transparante informatie en communicatie en toegang tot persoonsgegevens. Om aan deze eis en daarmee direct aan de eis van transparantie te voldoen, is het van belang dat er een privacyverklaring binnen de organisatie wordt opgesteld

waar betrokkenen kennis van kunnen nemen, dit kan worden opgenomen in de algemene voorwaarden. In de privacyverklaring moet duidelijk worden aangegeven welke persoonsgegevens er verwerkt worden, voor welk specifiek doel dit gedaan wordt en of de gegevens gedeeld met of doorverkocht worden aan andere organisaties en zo ja, aan welke organisaties. Ook moet hierin worden vermeld: de identiteit en de contactgegevens van de verwerkingsverantwoordelijke, de bewaartermijn van de gegevens, de rechten van de betrokkene en de gevolgen als de gegevens niet verstrekt worden. (Autoriteit Persoonsgegevens, 2018).

3.3.5 Rechten van de betrokkene

De betrokkene is de persoon van wie de gegevens verwerkt worden. De rechten van de betrokkene komen deels overeen met de Wbp, maar zijn op een aantal punten uitgebreid. Zo is het recht om te worden vergeten en het recht om gegevens mee te nemen nieuw. Deels nieuw is het recht om niet onderworpen te worden aan geautomatiseerde individuele besluitvorming, waaronder proflering. (Nederlands juristenblad, 2018)

Recht op informatie

De betrokkene heeft op grond van art. 12 t/m 14 AVG recht op transparante informatie en communicatie en toegang tot persoonsgegevens. De verwerkingsverantwoordelijke is verplicht om passende maatregelen te nemen opdat de betrokkene de informatie en communicatie in verband met de verwerking van zijn persoonsgegevens zoals beschreven in art. 13 en 14 AVG in een beknopte, transparante en begrijpelijke en gemakkelijk toegankelijk vorm en in duidelijke en eenvoudige taal ontvangt. In de praktijk is een privacyverklaring de handigste manier om hieraan te voldoen (Autoriteit Persoonsgegevens, 2018).

De verwerkingsverantwoordelijke verstrekt de betrokkene onverwijld en in ieder geval binnen een maand nadat de betrokkene een verzoek heeft gedaan de informatie waarover het verzoek gaat. De termijn kan indien nodig, afhankelijk van de complexiteit van de verzoeken en van het aantal verzoeken verlengd worden met twee maanden. Indien er gebruik gemaakt wordt van deze langere termijn dient de verwerkingsverantwoordelijke dit binnen een maand aan de betrokkene mede te delen. De verwerkingsverantwoordelijke kan in beginsel het verzoek van de betrokkene niet weigeren en dient de rechten van de betrokkene te faciliteren. In art. 12 lid 2 AVG wordt de uitzondering opgenomen. Indien de verwerkingsverantwoordelijke aantoont dat hij niet in staat is om de betrokkene te identificeren, mag deze weigeren gevolg te geven aan het verzoek.

Recht op inzage

In art. 15 AVG is het recht op inzage voor de betrokkene opgenomen. Bij het recht op inzage is het van belang dat de verwerkingsverantwoordelijke de betrokkene informeert welke en waarom bepaalde persoonsgegevens verwerkt worden. Wanneer er persoonsgegevens verwerkt worden, heeft de betrokkene recht op inzage hiervan. Betrokkenen kunnen een kopie opvragen van de verwerkte persoonsgegevens. Daarnaast moet de

verwerkingsverantwoordelijke aangeven voor welke periode de persoonsgegevens worden bewaard. Op het moment dat dat niet precies aangegeven kan worden, moet duidelijk worden gemaakt welke criteria er gehanteerd worden om te bepalen wat de bewaartermijn is.

Correctierecht

De AVG geeft mensen het recht om onjuiste persoonsgegevens te laten wijzigen. Dit recht staat beschreven in art. 16 AVG als 'het recht op rectificatie'. De verwerkingsverantwoordelijke dient ervoor te zorgen dat de gegevens juist zijn en geactualiseerd worden indien dat nodig is. De betrokkene heeft het recht onjuiste en onvolledige gegevens aan te laten passen, onder meer door een aanvullende verklaring te verstrekken.

Recht op vergetelheid

De betrokkene heeft op grond van art. 17 AVG in een aantal gevallen het recht op gegevenswissing. Het recht op vergetelheid/gegevenswissing houdt in dat de betrokkene het recht heeft om van de verwerkingsverantwoordelijke zonder onredelijke vertraging verwijdering van hem betreffende persoonsgegevens te verkrijgen. Het gaat om betrokkenen zoals cliënten, wederpartijen en werknemers (De Vries, 2018). De verwerkingsverantwoordelijke is verplicht persoonsgegevens zonder onredelijke vertraging te wissen in de volgende gevallen:

- a. de persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor zij zijn verzameld of anderszins verwerkt;
- b. de betrokkene trekt de toestemming waarop de verwerking berust in en er is geen andere rechtsgrond voor de verwerking;
- c. de betrokkene maakt overeenkomstig art. 21 AVG, bezwaar tegen de verwerking en er zijn geen prevalerende dwingende gerechtvaardigde gronden voor de verwerking.
- d. de persoonsgegevens zijn onrechtmatig verwerkt;
- e. de persoonsgegevens moeten worden gewist om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;
- f. de persoonsgegevens zijn verzameld via internet of een app.

Het recht op vergetelheid is breder dan het correctierecht, omdat het recht niet meer beperkt is tot het verwijderen van objectief onjuiste gegevens, onvolledige of niet ter zake doende gegevens (Autoriteit Persoonsgegevens, 2018). In een aantal gevallen geldt het recht op vergetelheid niet. Deze uitzonderingen zijn opgenomen in art. 17 lid 3 AVG.

- a. de verwerking is noodzakelijk voor het uitoefenen van het recht op vrijheid van meningsuiting en informatie;
- b. de gegevens worden verwerkt om te voldoen aan een wettelijke verplichting;
- c. de gegevens worden verwerkt om openbaar gezag of een taak van algemeen belang uit te oefenen;

- d. de gegevens worden verwerkt voor een taak van algemeen belang op het gebied van de volksgezondheid;
- e. de gegevens zijn noodzakelijk voor een rechtsvordering.

Sub e is van groot belang voor de advocatuur. Als de verwerking nodig is voor uitoefening of onderbouwing van een rechtsvordering, geldt het recht op vergetelheid niet. Daarnaast kan de betrokkene dit recht niet uitoefenen als een verwerkingsverantwoordelijke wettelijk verplicht is om bepaalde persoonsgegevens te bewaren. Bijvoorbeeld verplichtingen uit de Advocatenwet kunnen niet zonder meer opzijgezet worden door dit recht, aldus De Vries (2018). Het is dus van groot belang om na te gaan welke gegevens noodzakelijk zijn om een wettelijke verplichting na te komen.

Recht op beperking

De betrokkene heeft in bepaalde situaties het recht op beperking van de verwerking. Het recht houdt in dat de betrokkene de mogelijkheid krijgt om de verwerking van hun persoonsgegevens tijdelijk 'stil' te laten zetten (Handleiding Algemene verordening gegevensbescherming, 2018). Dit recht is opgenomen in art. 18 AVG. De gegevens mogen dan alleen verwerkt worden met toestemming van de betrokkene, voor de instelling, uitoefening of onderbouwing van een rechtsvordering en ter bescherming van de rechten van anderen. De betrokkene kan het recht op beperking van de verwerking invoeren in onderstaande gevallen:

- a. de betrokkene betwist de juistheid van de persoonsgegevens;
- b. de verwerking is onrechtmatig en de betrokkene verzet zich tegen het wissen van de persoonsgegevens;
- c. de gegevens zijn niet meer nodig voor de verwerkingsdoeleinden;
- d. de betrokkene maakt bezwaar tegen de verwerking.

Dataportabiliteit

In de AVG is het recht op dataportabiliteit opgenomen, oftewel het recht om gegevens over te dragen. Dit recht staat in art. 20 AVG. Het recht houdt in dat de betrokkene het recht heeft om een kopie te krijgen van de persoonsgegevens die hij verstrekt. Advocaten hebben al te maken met gedragsregel 28, waarbij het dossier over moet naar een opvolgend advocaat als de cliënt daarom vraagt. Ook behoren cliënten al afschriften te ontvangen van correspondentie en stukken over hun dossier. Nu kunnen cliënten zich ook op de AVG beroepen (De Vries, 2018).

Recht van verzet

De betrokkene kan in drie gevallen bezwaar maken tegen (verdere) verwerking van zijn gegevens en het recht op verzet invoeren. Dit recht is opgenomen in art. 21 AVG. In de eerste situatie kan de betrokkene bezwaar maken tegen verwerking die noodzakelijk is voor de uitoefening van een taak van algemeen belang of openbaar gezag, vanwege persoonlijke omstandigheden. Ten tweede kan de betrokkene bezwaar maken tegen de verwerking van zijn persoonsgegevens met het oog op *direct marketing*, hier moet altijd gehoor aan gegeven

worden door de verwerkingsverantwoordelijke. De derde en tevens laatste situatie waarbij de betrokkene bezwaar kan maken tegen de verwerking van zijn persoonsgegevens is voor wetenschappelijk of historisch onderzoek of voor statistische doeleinden op grond van specifiek met zijn situatie verband houdende redenen. Ook aan dit bezwaar moet de verwerkingsverantwoordelijke gehoor geven, tenzij de verwerking noodzakelijk is voor de uitvoering van een taak van algemeen belang. (Handleiding Algemene verordening gegevensbescherming, 2018)

Recht om niet onderworpen te worden aan een geautomatiseerde besluitvorming

De betrokkene heeft op grond van art. 22 het recht niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking (zoals profilering) gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanzienlijke mate treft. Het houdt in dat een computer een beslissing neemt over iemand in plaats van een persoon. Deze bepaling valt onder een van de rechten van de betrokkene, maar is in feite een verbod voor de verwerkingsverantwoordelijke (Handleiding Algemene verordening gegevensbescherming, 2018).

3.3.6 Bijzondere persoonsgegevens

In de AVG wordt een onderscheid gemaakt tussen ‘gewone’ persoonsgegevens en gegevens die bijzonder van aard zijn. Het gaat om categorieën van persoonsgegevens die extra gevoelig zijn.

Bijzondere gegevens

Op grond van art. 9 lid 1 AVG zijn bijzondere categorieën van persoonsgegevens: gegevens waaruit ras of etnische afkomst blijkt, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, het lidmaatschap van een vakbond, genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, gegevens over gezondheid en gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid. De AVG is ten opzichte van de Wbp uitgebreid met categorieën bijzondere persoonsgegevens. Zo zijn ‘genetische gegevens’ en ‘biometrische gegevens’ nieuw in de AVG. In art. 4 lid 13 en 14 AVG worden genetische- en biometrische gegevens omschreven als volgt:

Genetische gegevens: persoonsgegevens die verband houden met de overgeërfde of verworven genetische kenmerken van een natuurlijke persoon die unieke informatie verschaffen over de fysiologie of de gezondheid van die natuurlijke persoon en die met name voortkomen uit een analyse van een biologisch monster van die natuurlijke persoon.

Biometrische gegevens: persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedrags-gerelateerde kenmerken van een natuurlijke persoon op grond waarvan

eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd, zoals gezichtsafbeeldingen of vingerafdrukgegevens.

In beginsel is verwerking van bijzondere categorieën persoonsgegevens verboden, tenzij er een uitzondering van toepassing is of de betrokkene uitdrukkelijk toestemming heeft gegeven voor de verwerking (Handleiding Algemene verordening gegevensbescherming, 2018). In art. 9 lid 2 sub a t/m j AVG worden de uitzonderingen genoemd, wanneer verwerking dus wel is toegestaan. Daarnaast wordt er een aanvulling gegeven in art. 22 t/m 30 UAVG over wanneer het verbod niet van toepassing is. De uitzonderingen komen in grote lijnen overeen met uitzonderingen die opgenomen zijn in de Wbp.

Strafrechtelijke persoonsgegevens

Persoonsgegevens van strafrechtelijke aard vallen niet onder de bijzondere persoonsgegevens als genoemd in art. 9 AVG, maar zijn dusdanig gevoelig, dat daarvoor een speciale regeling is opgenomen. De verwerking van persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen is alleen toegestaan als dat gebeurt onder toezicht van de overheid of als het specifiek bij de wet geregeld is, op grond van art. 10 AVG. Daarnaast worden er in art. 32 jo. 33 UAVG algemene en overige uitzonderingsgronden gegeven, wanneer verwerking van persoonsgegevens van strafrechtelijke aard is toegestaan. Met uitdrukkelijke toestemming van de betrokkene is verwerking van strafrechtelijke persoonsgegevens toegestaan.

BSN

In Nederland wordt gebruik gemaakt van het burgerservicenummer (BSN), dit is een uniek persoonsnummer. Het BSN valt buiten de categorie 'bijzondere persoonsgegevens', maar hier gelden wel speciale regels voor. Op grond van art. 87 AVG mogen de lidstaten zelf specifieke voorwaarden vaststellen voor het verwerken van het nationaal identificatienummer. In art. 46 UAVG is dit nader uitgewerkt. Dit nummer mag alleen verwerkt worden voor in de wet voorgeschreven doelen, in andere gevallen is verwerking hiervan niet toegestaan. De Nederlandse overheid mag het BSN-nummer gebruiken bij de verwerking van persoonsgegevens, erkende zorgverleners zijn verplicht het BSN te gebruiken en in het onderwijs wordt het persoonsgebonden nummer (PGN) gebruikt. (Rijksoverheid, z.d.)

3.3.7 Gevolgen overtreden eisen AVG

Toezicht

De toezichthoudende autoriteit is in Nederland, net als bij de Wbp, de AP op grond van art. 51 lid 1 AVG. De taken van de AP zijn opgenomen in art. 57 AVG. De belangrijkste taak van de AP is het monitoren en handhaven van de toepassing van de AVG (Handleiding Algemene verordening gegevensbescherming, 2018). Naast de taken, zijn de bevoegdheden opgenomen in art. 58 AVG. Een van de bevoegdheden van de AP is om sancties op te leggen aan organisaties bij het niet naleven van de AVG. Dit kan zowel in aanvulling op als in plaats van de andere bevoegdheden (o.a. onderzoeksbevoegdheden; controles verrichten, informatie

verkrijgen, corrigerende bevoegdheden; waarschuwingen geven, verwerkingen stopzetten) die de AP heeft.

Administratieve boete

De AP kan, in geval er niet aan de eisen van de AVG wordt voldaan, besluiten om een administratieve boete op te leggen aan zowel de verwerkingsverantwoordelijke als de verwerker. Er moet bij het opleggen van de boete rekening gehouden worden met doeltreffendheid van de boete, de boete moet evenredig zijn en hij moet afschrikkend werken. Hierbij moet er op grond van art. 83 lid 2 AVG meegewogen worden de aard, de ernst, de duur van de inbreuk, de omvang of het doel van de verwerking in kwestie, het aantal getroffen betrokkenen en de omvang van de door hen geleden schade. Verder wordt er o.a. rekening gehouden met of er sprake is van opzet of nalatigheid, eerdere inbreuken en de genomen maatregelen door de verwerkingsverantwoordelijke/verwerker om de geleden schade voor de betrokkene(n) te beperken. In art. 84 AVG wordt de mogelijkheid gegeven aan lidstaten om zelf sancties vast te stellen op het moment dat er sprake is van een inbreuk die niet aan administratieve geldboeten onderworpen zijn, overeenkomstig art. 83 AVG. In art. 16 t/m 18 UAVG is deze mogelijkheid nader uitgewerkt.

Er zijn twee boetecategorieën die de hoogte van de geldboete kunnen bepalen. In art. 83 lid 4 AVG is de eerste categorie opgenomen. In de eerste categorie vallen onder andere de inbreuken op de verplichtingen van de verwerkingsverantwoordelijke en de verwerker (overeenkomstig de artikelen 8, 11, 25 t/m 39, 42 en 43 AVG). Het gaat onder andere om overtredingen op het gebied van een gegevensbeschermingseffectbeoordeling of het niet doen van een melding in geval van een datalek. Deze gevallen kunnen worden gesanctioneerd met een administratieve boete van maximaal € 10.000.000,- of 2% van de totale (wereldwijde) jaaromzet van desbetreffend bedrijf, van het voorgaande boekjaar, indien dat cijfer hoger is. De tweede categorie is opgenomen in art. 83 lid 5 AVG. Inbreuken op de basisbeginselen inzake de verwerking, met inbegrip van de voorwaarden voor toestemming (overeenkomstig art. 5, 6, 7 en 9 AVG), de rechten van de betrokkenen (overeenkomstig art. 12 t/m 22 AVG), doorgifte van persoonsgegevens aan een ontvanger in een derde land (overeenkomstig art. 44 t/m 49 AVG) en alle verplichtingen genoemd in hoofdstuk IX AVG, worden gesanctioneerd met een geldboete tot € 20.000.000,- of 4% van de totale (wereldwijde) jaaromzet in het voorgaande boekjaar, indien dat cijfer hoger is.

3.4 Verschillen Wbp en AVG

In onderstaand tabel worden de verschillen in een tabel kort naast elkaar gezet. Op deze manier wordt er op een duidelijke manier inzicht gegeven in de verschillen.

	Wbp	AVG
Soort wetgeving	Richtlijn	Verordening
Waar van toepassing	Nederland	Europese Unie

Eisen	Zorgvuldig en behoorlijk Doelbinding Grondslagen Kwaliteitseisen: niet bovenmatig en ter zake dienend, juist en nauwkeurig	Rechtmatig, behoorlijk en transparant Doelbinding Grondslagen Dataminimalisatie Opslagbeperking Juistheid Integer en vertrouwelijk
Begrippen aangepast	Verantwoordelijke/bewerker	Verwerkingsverantwoordelijke/verwerker
Nieuwe begrippen		Profilering Pseudonimisering Genetische gegevens Biometrische gegevens
Plichten verwerkingsverantwoordelijke	Meldingsplicht Informatieverstrekking aan betrokkene(n) Beveiligingsplicht Bewaartermijn Meldplicht datalekken	Verwerkersovereenkomst opstellen en sluiten met verwerkers Voorafgaande raadpleging betrokkene <i>Privacy by default/privacy by design</i> Beveiliging van de verwerking Meldplicht datalekken Mededeling betrokkene(n) datalek Verantwoordingsplicht: • Registerplicht • Gegevensbeschermingseffectbeoordeling • Register datalekken • Toestemming betrokkene • Aanstellen FG (sommige gevallen) Informatieplicht: • Privacyverklaring opstellen en versturen naar betrokkene(n)
Meldplicht datalekken	De AP moet binnen 72 uur op de hoogte worden gesteld van elk datalek dat resulteert in een aanzienlijke kans op of ernstige nadele gevolgen heeft voor de bescherming van persoonsgegevens. Indien het waarschijnlijk is dat het datalek resulteert in nadelige gevolgen voor de betrokkene, dient deze op de hoogte te worden gesteld.	De verwerkingsverantwoordelijke moet in principe binnen 72 uur aan de AP het datalek melden. Indien dat niet lukt, zal er een verklaring gegeven moeten worden voor de vertraging. De meldplicht is niet van toepassing als de inbreuk geen hoog risico inhoudt voor de rechten en vrijheden van de betrokkene. De betrokkene moet ook geïnformeerd worden als het waarschijnlijk is dat de inbreuk resulteert in een hoog risico voor de rechten en de vrijheden van de betrokkene. Alle inbreuken moeten gedocumenteerd worden.

Rechten betrokkene	Recht op informatie Recht op inzage Correctierecht Recht op verzet	Recht op informatie Recht op inzage Correctierecht Recht op vergetelheid Recht op beperking Recht op dataportabiliteit Recht op verzet Recht om niet onderworpen te worden aan een geautomatiseerde besluitvorming
Hoogte boetes	Hoogste boete €820.000,-	Hoogste boete €20.000.000,- of 4% van de wereldwijde jaaromzet

Tabel 1: Wbp en AVG vergeleken

3.5 Conclusie

Onderzoeksvraag 3: “Welke veranderingen brengt de AVG met zich mee ten opzichte van de Wbp?”

De AVG heeft in tegenstelling tot de Wbp rechtstreekse werking, zonder dat er implementatie nodig is in Nederland, omdat het bij de AVG om een verordening gaat terwijl het bij de Wbp om een richtlijn ging. Er moet onder de AVG aan meer beginselen worden voldaan dan onder de Wbp, dit heeft te maken met de veranderende en vergrote materiële verplichtingen van de verwerkingsverantwoordelijke.

In de AVG zijn een aantal bestaande begrippen uit de Wbp aangepast. Het gaat concreet om de begrippen ‘verantwoordelijke’ en ‘bewerker’, die vervangen zijn voor ‘verwerkingsverantwoordelijke’ en ‘verwerker’. Ook zijn er een paar nieuwe begrippen toegevoegd aan de AVG, die onder de Wbp nog niet bestonden: profilering, pseudonimisering, genetische gegevens en biometrische gegevens.

De meldplicht datalekken was al opgenomen in de Wbp en is meegenomen naar de AVG. Echter, is de meldplicht datalekken onder de AVG veranderd. De Wbp had de verplichting om een melding te doen aan de AP als er sprake was van nadelige gevolgen voor de betrokkene. Onder de AVG is het verplicht om iedere datalek te melden aan de AP, tenzij er geen risico is voor de rechten en vrijheden van de betrokkene. Ook moeten volgens de AVG alle inbreuken worden gedocumenteerd.

Het was onder de Wbp verplicht om verwerkingen van persoonsgegevens te melden bij de AP. Deze plicht is sinds 6 november 2017 vervallen, in verband met de komst van de AVG. Het is dan ook niet meer verplicht onder de AVG om een melding te maken als een organisatie persoonsgegevens verwerkt.

Zoals in bovenstaande tabel wordt weergegeven zitten de meeste veranderingen van de AVG ten opzichte van de Wbp in het feit dat de verwerkingsverantwoordelijke meer verplichtingen heeft gekregen, het gaat hierbij om de verantwoordingsplicht. De verantwoordingsplicht houdt in dat er aangetoond kan worden dat verwerkingen binnen de organisatie aan de regels

van de AVG voldoen. Naast de uitbreiding van de verplichtingen van de verwerkingsverantwoordelijke, heeft de betrokkene extra rechten gekregen. Het recht op dataportabiliteit en het recht op vergetelheid zijn helemaal nieuw onder de AVG.

Op het moment dat er niet aan de eisen van de Wbp werd voldaan, was het voor de AP al mogelijk om boetes op te leggen. Onder de AVG zijn de boetes een stuk hoger geworden. De hoogste boete die opgelegd kon worden door de AP onder de Wbp was €820.000,-, terwijl de hoogste boete die opgelegd kan worden door de AP onder de AVG een bedrag van €20.000.000,- is, of 4% van de wereldwijde jaaromzet, mocht dat bedrag hoger zijn.

Hoofdstuk 4

Verwerking persoonsgegevens bij SchoeBroek (getoetst aan de Wbp en AVG)

In dit hoofdstuk wordt beschreven op welke wijze SchoeBroek op dit moment omgaat met (de verwerking van) persoonsgegevens. Op deze manier wordt er in dit hoofdstuk antwoord gegeven op de eerste en tweede onderzoeksvraag. De eerste onderzoeksvraag richt zich op de werkwijze die op dit moment gehanteerd wordt: *“Op welke wijze werkt SchoeBroek momenteel in de praktijk met persoonsgegevens?”* en de tweede onderzoeksvraag richt zich op de knelpunten die op dit moment spelen bij SchoeBroek: *“Zijn er knelpunten op dit moment wat betreft de verwerking van persoonsgegevens bij SchoeBroek en welke risico's zitten eraan verbonden?”*. Op deze vragen wordt een antwoord gegeven door de informatie die naar voren is gekomen tijdens het afnemen van de semigestructureerde interviews en waar nodig is het kantoorhandboek van SchoeBroek geraadpleegd.

4.1 Type persoonsgegevens

In het derde hoofdstuk van dit onderzoeksrapport staat beschreven wanneer een gegeven een persoonsgegeven is volgens de Wbp. Hierin staat dat het gaat om ‘elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon’. Er worden binnen SchoeBroek verschillende persoonsgegevens verwerkt. Het gaat om zowel ‘gewone’ als ‘bijzondere’ persoonsgegevens die gebruikt worden bij de verwerking. Tijdens het eerste contact wordt de cliënt gevraagd een intakeformulier in te vullen. Door het invullen van het intakeformulier wordt ervoor gezorgd dat SchoeBroek beschikt over de juiste gegevens van de cliënten. De cliënt vult op het intakeformulier de volgende gegevens in:

Gegevens cliënt	Gegevens partner
- achternaam;	- achternaam;
- voornaam;	- voornaam;
- geboortedatum;	- geboortedatum;
- (post)adres;	- BSN.
- postcode/woonplaats;	
- GBA-adres;	Minderjarige kinderen
- telefoonnummer;	- geboortedatum;
- e-mail;	- geboorteplaats.
- BSN;	
- paspoortnummer;	Gegevens wederpartij
- WSNP ja/nee;	- achternaam;
- burgerlijke staat.	- voornaam;
	- geboortedatum;
	- (post)adres;
	- postcode/woonplaats;
	- telefoonnummer.

Naast bovenstaande persoonsgegevens worden er onder andere bankrekeningnummers, IB-aangiftes, testamenten, huwelijkse voorwaarden, pensioengegevens en gegevens van kinderen verwerkt bij SchoeBroek indien dat nodig is voor de uitvoering van de overeenkomst. Naast de 'gewone' persoonsgegevens verwerkt SchoeBroek zoals eerder gezegd ook bijzondere persoonsgegevens. Bij het intakeformulier wordt de cliënt gevraagd om het BSN in te vullen, wat al buiten de categorie van 'gewone' persoonsgegevens valt. Daarnaast worden medische gegevens verzameld in letselschadezaken en dat valt onder de categorie 'bijzondere' persoonsgegevens.

4.2 Verwerken persoonsgegevens

De persoonsgegevens worden verwerkt op verschillende manieren. Zo worden de persoonsgegevens in ieder geval verzameld, vastgelegd, geordend, bijgewerkt, bewaard, gewijzigd en geraadpleegd. Iedere handeling met betrekking tot persoonsgegevens valt onder het verwerken, waardoor er nog meer relevante handelingen worden verricht binnen SchoeBroek.

Alle digitale verwerkingen van SchoeBroek komen terecht in het softwareprogramma 'Advocaat Centraal' (Hierna: AC). In AC worden alle belangrijke contactgegevens van cliënten en andere relaties opgeslagen. Om te corresponderen met cliënten wordt er gebruik gemaakt van Office 365. Naast de digitale verwerking van persoonsgegevens worden er fysieke dossiers bijgehouden. Deze zijn met name praktisch om in te werken en worden gebruikt als extra back-up, want AC zorgt ervoor dat er dagelijks (digitale) back-ups gemaakt worden.

4.3 Betrokkenen

Het grootste deel van het verwerken van persoonsgegevens bestaat bij SchoeBroek uit gegevens van haar cliënten. Naast de persoonsgegevens die van de cliënten worden verwerkt, worden van de wederpartijen dezelfde gegevens verwerkt. Hoeveel en welke gegevens dit zijn, is afhankelijk van wat er nodig is voor de uitvoering van de overeenkomst. Op het moment dat een persoon via de website contact zoekt met SchoeBroek, door het invullen van het contactformulier, geeft de potentiële cliënt een aantal persoonsgegevens door en deze worden dan verwerkt in de administratie van SchoeBroek. Tot slot worden er persoonsgegevens van iedere werknemer verwerkt, omdat dit nodig is voor de arbeidsovereenkomst.

4.4 Bewerkers/verwerkers

Er wordt bij SchoeBroek gewerkt met verschillende bewerkers. Allereerst wordt er gewerkt met het bedrijf AC. Dit bedrijf biedt zoals eerder beschreven een betaald softwareprogramma aan voor de advocatuur. Daarnaast wordt er gewerkt met 'Twinfield', een groot onlineboekhoudingsysteem waarmee verschillende advocatenkantoren werken. De combinatie van AC en Twinfield zorgt voor een eenvoudige boekhouding. In Twinfield worden financiële gegevens van cliënten verwerkt, voor de betalingen van cliënten aan SchoeBroek. Om in Twinfield te kunnen werken moet er ingelogd worden met een gebruikersnaam en wachtwoord. Voor het berekenen van alimentatie wordt er gebruik gemaakt van het betaalde

programma 'Split-Online'. In dit programma worden de achternaam van de cliënt en de geboortedatum van de kinderen van de cliënt verwerkt. Ook voor Split-Online geldt dat er alleen gebruik gemaakt kan worden van dit programma door in te loggen met een gebruikersnaam en wachtwoord. In het geval van letselschadezaken worden er medische adviseurs geraadpleegd, waarbij gegevens van de betreffende cliënt verstrekt worden. Tot slot wordt er gebruik gemaakt van deurwaarders aan wie persoonsgegevens van cliënten worden verstrekt.

Naast bovenstaande bewerkers/verwerkers, wordt er gewerkt met de Raad voor Rechtsbijstand. Echter, hebben zij aangegeven dat mediators, advocaten, bijzondere curatoren en andere bij de Raad ingeschreven dienstverleners zelf het doel en de middelen voor de verwerking van persoonsgegevens bepalen, evenals de Raad. Beide partijen zijn volgens hen daarom aan te merken als verantwoordelijke/verwerkingsverantwoordelijke en daarom zijn zij geen bewerkers/verwerkers. (Raad voor Rechtsbijstand, 2018)

Om de boekhouding te regelen voor de werknemers, wordt er gebruik gemaakt van 'Profijt Adviseurs' in Deventer. Aan hen worden de persoonsgegevens van de werknemers van SchoeBroek verstrekt. Het gaat hierbij om de naam, geboortedatum, adres, bankrekeningnummer, salaris en identiteitsbewijs/paspoort/rijbewijs. Naast het bedrijf voor de boekhouding, worden de persoonsgegevens van de werknemers verstrekt aan de Arbo-verzuim *servicedesk*.

4.5 Eisen aan de verwerking

Er worden een aantal eisen gesteld aan de verwerking van persoonsgegevens. Het is van belang dat verwerkingen zorgvuldig en behoorlijk worden gedaan en dat er aan de eis van doelbinding wordt voldaan. Daarnaast zijn er kwaliteitseisen verbonden aan de verwerkingen. Gegevens moeten juist en nauwkeurig verwerkt worden. SchoeBroek voldoet aan deze eisen. Persoonsgegevens worden niet 'oneerlijk' verwerkt. De cliënten van SchoeBroek weten welke gegevens van hen verwerkt worden, doordat deze door de cliënt zelf worden verstrekt. Bij het intakeformulier vullen cliënten zelf de gegevens en geven zelf de juiste informatie door. Er wordt bij SchoeBroek gewerkt met een kantoorhandboek, zodat iedere werknemer op dezelfde wijze te werk gaat. Daarnaast wordt er alleen om specifieke gegevens gevraagd als dit nodig is voor het uitvoeren van de overeenkomst. Er wordt dus bijvoorbeeld niet om medische gegevens gevraagd als dit niet nodig is. Hierdoor wordt aan de kwaliteitseisen voldaan. Aan de eis van doelbinding wordt voldaan, omdat er altijd aan een van de grondslagen wordt voldaan zoals genoemd in de Wbp en AVG.

4.6 Grondslagen

De wettelijke grondslagen waar een verwerking op moet berusten zijn in de AVG vrijwel gelijk gebleven met hoe ze in de Wbp geformuleerd waren. Hierdoor verwerkt SchoeBroek altijd persoonsgegevens op basis van een van de zes grondslagen. De meest voorkomende grondslagen waarop bij SchoeBroek verwerkingen worden gedaan zijn op basis van toestemming van de betrokkene, indien het noodzakelijk is voor de uitvoering van de

overeenkomst en om te voldoen aan een wettelijke verplichting. Doordat de betrokkene de toestemming kan intrekken, is het van belang dat een verwerking berust op een van de andere grondslagen.

4.7 Beveiliging

Om de beveiligingsplicht te waarborgen moeten er technische en organisatorische maatregelen getroffen worden, zodat persoonsgegevens op de juiste manier worden beveiligd. Bij SchoeBroek wordt er gewerkt met wachtwoorden op iedere computer/laptop die gebruikt wordt. Daarnaast zijn alle computers beveiligd met een firewall/virusscan om het systeem te beveiligen. Er worden geen gegevens en documenten op de computers/laptops opgeslagen. Alles wordt opgeslagen in AC en eens in de maand wordt er gecontroleerd of er inderdaad geen documenten op de computers/laptops zijn opgeslagen. Indien dit wel het geval is, worden de documenten verwijderd. Aan het einde van de dag gaan de laptops in een ladekast die op slot kan, zodat deze niet in het zicht liggen. De deuren van de kantoren worden aan het einde van de dag op slot gedaan zodat de ruimten alleen toegankelijk zijn voor werknemers van SchoeBroek.

Om in AC te kunnen, heeft iedere werknemer een eigen gebruikersnaam en wachtwoord. Op deze manier is er dus twee keer een beveiliging (op de computers/laptops en in de software). AC maakt dagelijks een back-up op de server, om te zorgen dat dossiers niet verloren gaan. Veiligheid heeft bij AC de hoogste prioriteit. Zij gebruiken altijd een versleutelde verbinding, werken met een ISO gecertificeerde provider en bieden standaard de mogelijkheid om specifieke IP-adressen toegang te verlenen tot de AC-administratie (Advocaat Centraal, z.d.).

Naast de digitale dossiers, wordt er zoals eerder beschreven, gebruik gemaakt van fysieke dossier. Fysieke dossiers dienen na gebruik direct in de dossierkast te worden opgeborgen. Dit dient in ieder geval aan het eind van een werkdag te gebeuren. De dossierkast bevindt zich in een ruimte die enkel toegankelijk is voor betrokken medewerkers die een geheimhoudingsverklaring hebben ondertekend. (Kantoorhandboek SchoeBroek, 2016) De dossierkasten zijn beveiligd met een sleutel. Op deze manier zijn de fysieke dossiers twee keer beveiligd. Naast de dossierkasten binnen het kantoor van SchoeBroek, is er een aparte archiefruimte in een ander kantoorpand. Op het moment dat de papieren dossiers volledig digitaal zijn verwerkt en niet meer nodig zijn, worden deze weggegooid in een afgesloten papiercontainer.

4.8 Bewaartermijnen

Alle dossiers en gegevensdragers dienen conform de wettelijke bewaartermijn te worden bewaard. Afhankelijk van de soort van de gegevens geldt er een andere termijn.

Type gegevens	Aantal jaar
Bewaartermijn van dossiers	10 jaar
Bewaartermijn van administratieve gegevens	7 jaar
Bewaartermijn gegevensdragers	7 jaar

Bewaartermijn op grond van de Algemene wet Inzake Rijksbelastingen (AWR)	7 jaar
---	--------

Tabel 2: Bewaartermijnen

(Kantoorhandboek SchoeBroek, 2016)

4.9 Knelpunten

Tijdens de semigestructureerde interviews is er gevraagd naar de knelpunten die op dit moment spelen bij SchoeBroek wat betreft de verwerking van persoonsgegevens. Er werd door iedere geïnterviewde hetzelfde antwoord gegeven. Op dit moment zijn er geen knelpunten wat betreft de verwerking van persoonsgegevens. Wel werd er aangegeven dat de komst van de AVG wellicht knelpunten zal opleveren, omdat de AVG nieuwe eisen met zich meebrengt waar zij aan moeten gaan voldoen.

4.10 Conclusie

Onderzoeksvraag 1: *“Op welke wijze werkt SchoeBroek momenteel in de praktijk met persoonsgegevens?”*

Er worden bij SchoeBroek persoonsgegevens verwerkt op verschillende wijzen. Dit komt omdat iedere handeling met betrekking tot persoonsgegevens al valt onder het verwerken. Dit kan dus zijn het verzamelen, raadplegen, opslaan, bijwerken, inzien, enzovoorts. Het gaat om zowel ‘gewone’ als ‘bijzondere’ categorieën van persoonsgegevens. In principe worden de gegevens die op het intakeformulier staan altijd verwerkt en extra gegevens worden opgevraagd indien dit nodig is voor de uitvoering van de overeenkomst.

De persoonsgegevens van cliënten worden zowel digitaal als fysiek verwerkt. Er worden dossiers aangemaakt in het programma AC en papieren dossiers zijn er als extra back-up en omdat dit praktisch is om in te werken. Naast de persoonsgegevens van de cliënten worden de persoonsgegevens van potentiële cliënten verwerkt (indien zij het contactformulier op de website invullen) en de persoonsgegevens van de werknemers van SchoeBroek.

SchoeBroek maakt gebruik van meerdere bewerkers/verwerkers om in opdracht van hen persoonsgegevens te verwerken. Het gaat om zowel bewerkers/verwerkers voor de gegevens van cliënten als de gegevens van de werknemers.

De Wbp en de AVG stellen eisen aan de verwerking van persoonsgegevens. De persoonsgegevens moeten voldoen aan de beginselen van zorgvuldigheid en behoorlijkheid en moeten voor een van tevoren bepaald doel verwerkt worden. Bij SchoeBroek wordt aan eisen voldaan en iedere verwerking berust op een van de zes grondslagen.

Het is van groot belang dat de juiste technische en organisatorische maatregelen getroffen worden om te waarborgen dat persoonsgegevens goed beveiligd zijn. Er zijn bij SchoeBroek verschillende maatregelen getroffen. Zowel voor de digitale dossiers als de fysieke dossiers. De computers/laptops zijn goed beveiligd met een wachtwoord, er wordt gebruik gemaakt van een firewall en virusscans. De software die gebruikt wordt door SchoeBroek om in te werken zijn allemaal beveiligd met een eigen gebruikersnaam en wachtwoord. De fysieke dossiers zijn alleen toegankelijk voor werknemers van SchoeBroek. Alle fysieke dossiers liggen achter slot en grendel.

SchoeBroek heeft in haar kantoorhandboek de termijnen staan voor het bewaren van dossiers. Dossiers worden 10 jaar na de sluiting van het dossier verwijderd en vernietigd.

Al met al kan er geconcludeerd worden dat SchoeBroek voldoet aan de eisen die de Wbp stelt. Hierdoor kunnen zij op dezelfde wijze omgaan met de verwerking van persoonsgegevens, maar zullen zij zich moeten richten op een aantal nieuwe verplichtingen die de AVG stelt, zodat zij gaan voldoen aan de eisen van de AVG. Waar zij zich op moeten richten zal toegelicht worden in hoofdstuk vijf van dit onderzoeksrapport.

Onderzoeksvraag 2: “Zijn er knelpunten op dit moment wat betreft de verwerking van persoonsgegevens bij SchoeBroek en welke risico’s zitten eraan verbonden?”

In de semigestructureerde interviews is aan de respondenten gevraagd of zij tegen knelpunten aanlopen wat betreft de verwerking van persoonsgegevens. Er zijn tijdens de semigestructureerde interviews geen knelpunten naar voren gekomen. De verwerkingen voldoen aan de eisen van de Wbp en hierdoor zijn er geen risico’s wat betreft sancties die opgelegd kunnen worden door de AP.

Tot slot werd er tijdens de interviews aangegeven dat de AVG wellicht knelpunten met zich mee zal brengen.

Hoofdstuk 5

Stappen ondernemen binnen SchoeBroek

In dit hoofdstuk wordt antwoord gegeven op de vierde onderzoeksvraag: “*Welke stappen en maatregelen moet SchoeBroek nemen in de praktijk om te voldoen aan de AVG? Wat zijn de gevolgen als zij niet (op tijd) voldoen aan de AVG?*”. Dit zijn gelijk de aanbevelingen en adviezen die gedaan worden aan SchoeBroek. De aanbevelingen die worden gedaan zijn op basis van de resultaten uit hoofdstuk 3.3 in combinatie met de resultaten van hoofdstuk vier van dit onderzoeksrapport opgesteld.

5.1 Verantwoordingsplicht

Vanaf 25 mei 2018 geldt de AVG en deze verordening brengt met zich mee dat de verwerkingsverantwoordelijke een verantwoordingsplicht heeft. De verplichte maatregelen die de AVG concreet noemt zodat er voldaan wordt aan de verantwoordingsplicht zijn:

- het bijhouden van een register van verwerkingsactiviteiten;
- het uitvoeren van een gegevensbeschermingseffectbeoordeling voor verwerkingen met een hoog risico;
- het bijhouden van een register datalekken;
- aantonen dat de betrokkene daadwerkelijk toestemming heeft gegeven voor een gegevensverwerking wanneer daar toestemming voor nodig is;
- opstellen/sluiten verwerkersovereenkomst;
- aanstellen functionaris voor gegevensbescherming (indien nodig).

Van de bovenstaande lijst worden de punten behandeld die nodig zijn bij SchoeBroek om te voldoen aan de verantwoordingsplicht.

5.1.1 Registerplicht (verwerkingen)

Zoals beschreven in hoofdstuk 3 van dit onderzoeksrapport is het niet verplicht om een register bij te houden als een organisatie minder dan 250 personen in dienst heeft. Er zijn een aantal uitzonderingen op deze vrijstelling. Indien het gaat om verwerkingen die risico's met zich meebrengen voor de betrokkenen en indien het gaat om verwerkingen die niet incidenteel zijn, moeten organisaties die minder dan 250 personen in dienst hebben ook aan de registerplicht voldoen. De persoonsgegevens die verwerkt worden bij SchoeBroek zijn niet incidenteel en daarom moeten zij zich aan de registerplicht houden. Op dit moment wordt er bij SchoeBroek nog geen register bijgehouden. Het advies is om een register op te stellen waarin alle verwerkingsactiviteiten gedocumenteerd worden. In bijlage 3 zit een register dat is opgesteld aan de hand van de eisen die de AVG stelt. Er wordt aan de registerplicht voldaan indien het format wordt ingevuld met de juiste gegevens. Naast de gegevens die in ieder geval opgenomen dienen te worden in het register, kan er in het register bijgehouden en beoordeeld worden of er sprake is van een hoog risico van de verwerking, zodat er indien dat het geval is, een gegevensbeschermingseffectbeoordeling uitgevoerd kan worden en kan er

bijgehouden worden of de betrokkenen zelf toestemming hebben gegeven voor het verwerken van de persoonsgegevens. De bewijslast van dat er toestemming is gegeven ligt namelijk bij de organisatie en door de toestemming te documenteren, kan er achteraf worden laten zien dat de verwerkingen plaatsvinden onder legaal gegeven toestemming.

5.1.2 Register datalekken

Er hebben bij SchoeBroek geen datalekken plaatsgevonden, dus hiervoor hadden zij nog geen register opgesteld. Onder de AVG is het verplicht om datalekken te documenteren. Op de website van de Nederlandse Orde van Advocaten (NOvA) is een document gepubliceerd die opgeslagen kan worden en indien er sprake is van een datalek, kan dit document ingevuld worden. (Nederlandse Orde van Advocaten, 2018). SchoeBroek hoeft dus zelf geen register op te stellen voor datalekken, maar het advies is om het document op te slaan zodat indien er sprake is van een datalek dit document direct ingevuld kan worden.

5.1.3 Verwerkersovereenkomst

SchoeBroek schakelt andere partijen in om persoonsgegevens voor hen te verwerken en daarom moet er met de betreffende partijen een verwerkersovereenkomst gesloten worden. Het gaat om gevallen waarbij SchoeBroek de andere partij de opdracht geeft om persoonsgegevens te verwerken waar zij verantwoordelijk voor zijn. (Autoriteit Persoonsgegevens, 2018)

Het is daarom een advies om een verwerkersovereenkomst op te stellen, zodat deze verstuurd kan worden naar de betreffende partijen. Het gaat in ieder geval om de bewerkers die genoemd zijn in hoofdstuk 4.4 van dit onderzoeksrapport.

De inhoud waaraan de verwerkersovereenkomst moet voldoen wordt toegelicht in hoofdstuk 3.3.4 van dit onderzoeksrapport.

5.2 Informatieplicht

Onder de AVG heeft een organisatie de informatieplicht. Dit geldt ook voor SchoeBroek. Bestaande en nieuwe cliënten moeten duidelijk geïnformeerd worden over wat er binnen SchoeBroek met de persoonsgegevens wordt gedaan en om welke reden.

5.2.1 Privacyverklaring

Om aan de informatieplicht te voldoen, moet er een privacyverklaring opgesteld worden. Het advies is om een privacyverklaring op te stellen en bestaande cliënten hiervan op de hoogte te stellen. In de privacyverklaring moet in ieder geval de volgende informatie worden gegeven:

- de contactgegevens van de verwerkingsverantwoordelijke binnen SchoeBroek;
- de doeleinden en de rechtsgrond van de verwerking;
- de ontvangers van de persoonsgegevens;
- of de gegevens buiten de EU worden doorgegeven;
- de gehanteerde bewaartermijn;

- de rechten van de betrokkene;
- dat en waar de betrokkene een klacht kan indienen;
- of en waarom de betrokkene verplicht is de persoonsgegevens te verstrekken en wat de gevolgen zijn als de gegevens niet worden verstrekt;
- of er gebruik gemaakt wordt van geautomatiseerde besluitvorming;
- als de gegevens van een andere organisatie zijn verkregen: de bron waar de persoonsgegevens vandaan komen. (Autoriteit Persoonsgegevens, 2018)

Om er zeker van te zijn dat nieuwe cliënten de privacyverklaring zien, is het van belang dat deze wordt toegevoegd aan de algemene voorwaarden. Cliënten krijgen de algemene voorwaarden te zien als zij het intakeformulier invullen en op deze manier hebben cliënten direct inzicht in wat er met hun gegevens gaat gebeuren. Daarnaast is het van belang dat de privacyverklaring op de website wordt geplaatst, zodat potentiële cliënten deze kunnen inzien, voordat zij het contactformulier invullen dat op de website staat. Zodra het contactformulier wordt ingevuld en verstuurd, worden de gegevens verwerkt. Bestaande cliënten kunnen op de hoogte gesteld worden van de nieuwe privacyverklaring door hen een e-mail te sturen met de privacyverklaring.

5.3 Gevolgen van het niet (op tijd) voldoen aan de AVG

De AVG kent hele strenge sanctiemogelijkheden voor de verwerkingsverantwoordelijke. Deze zijn reeds toegelicht in hoofdstuk 3.3.7 van dit onderzoeksrapport, maar worden nog kort behandeld in dit hoofdstuk. De AVG kent twee boetecategorieën: een lage categorie bij een overtreding van administratieve bepalingen en een hoge categorie voor meer fundamentele overtredingen. Laag houdt in: €10.000.000,- of 2% van de wereldwijde jaaromzet, hoog houdt in €20.000.000,- of 4% van de wereldwijde jaaromzet. (Engelfriet, Chew-Meij, Kager, 2018)

Regel	Maximale boete
Niet geldig toestemming vragen	Hoge categorie
Het BSN gebruiken als dat niet verplicht is	Hoge categorie
Een onduidelijke privacyverklaring publiceren	Hoge categorie
Een datalek veroorzaken door slechte beveiliging	Lage categorie
Een datalek niet melden (ongeacht de kwaliteit van de beveiliging)	Lage categorie
Weigeren een kopie van iemands dossier af te geven	Hoge categorie
Geen verwerkingsregister hebben	Lage categorie
Gegeven niet wissen als deze verouderd zijn	Hoge categorie

Tabel 3: Hoogte boetes

(Engelfriet, Chew-Meij, Kager 2018)

5.4 Conclusie

Onderzoeksvraag 4: “Welke stappen en maatregelen moet SchoeBroek nemen in de praktijk om te voldoen aan de AVG? Wat zijn de gevolgen als zij niet (op tijd) voldoen aan de AVG?”

- opstellen en bijhouden van verwerkingsactiviteiten in een register. Hierin moet ook aangetoond worden dat de betrokkene toestemming heeft gegeven voor de verwerking en moet er aangetoond worden of de verwerking een verhoogd risico betreft (zie 3.3.4 onder ‘registerplicht’). Uit het onderzoek is niet gebleken dat SchoeBroek op grote schaal

gegevens verwerkt met een verhoogd risico, om die reden is er geen aanbeveling gedaan over het doen van een gegevensbeschermingseffectbeoordeling, omdat dat simpelweg niet nodig is (zie 3.3.4 onder 'gegevensbeschermingseffectbeoordeling');

- opstellen en bijhouden van een register van de datalekken (zie 3.3.4 onder 'register datalekken');
- opstellen van verwerkersovereenkomst en deze toezenden aan de verwerkers (zie 3.3.4 onder 'verwerkersovereenkomst');
- opstellen van een privacyverklaring zodat de betrokkene weet wat er gebeurt met de persoonsgegevens die opgevraagd worden door SchoeBroek (zie 3.3.4 onder 'privacyverklaring');
- het aanstellen van een FG is niet nodig, omdat SchoeBroek geen overheid of publieke organisatie is, er niet regelmatig en stelselmatig op grote schaal observaties wordt uitgevoerd en er niet op grote schaal bijzondere persoonsgegevens wordt verwerkt (zie 3.3.4 onder 'functionaris gegevensbescherming');
- indien er niet (op tijd) aan de eisen van de AVG wordt voldaan heeft dat als gevolg dat er sancties opgelegd kunnen worden door de AP. De hoogte van de maximale boete is afhankelijk van de soort van de overtreding (zie tabel 3).

Hoofdstuk 6

Conclusie

In dit hoofdstuk zal er een antwoord worden gegeven op de probleemstelling die binnen dit onderzoeksrapport centraal staat. De probleemstelling luidt als volgt: *“Wat is de invloed van de AVG op de werkwijze van SchoeBroek en welke veranderingen moeten er zo nodig plaatsvinden om te voldoen aan de eisen van de nieuwe verordening?”*

Om een antwoord te kunnen geven op de probleemstelling zijn er vier onderzoeksvragen opgesteld. Bij beantwoording van de onderzoeksvragen is per onderzoeksvraag een conclusie geschreven, wat heeft geleid tot een antwoord op de probleemstelling.

Op de eerste en tweede onderzoeksvraag is in het vierde hoofdstuk van dit onderzoeksrapport een antwoord gegeven. Bij beantwoording van de eerste onderzoeksvraag is naar voren gekomen dat SchoeBroek op dit moment voldoet aan de eisen die de Wbp stelt (zie hoofdstuk 4.10). Hierdoor hoeven zij zich niet meer te richten op de eisen die zijn meegenomen van de Wbp naar de AVG, maar kunnen zij zich volledig richten op de nieuwe eisen. De tweede onderzoeksvraag richt zich op de knelpunten. Er is naar voren gekomen dat er geen knelpunten zijn wat betreft de verwerking van persoonsgegevens onder de eisen van de Wbp. Er kan geconcludeerd worden dat dat juist is, omdat de werkwijze getoetst is aan de Wbp en hierin naar voren is gekomen dat zij voldoen aan de eisen.

De derde onderzoeksvraag is behandeld in het derde hoofdstuk van dit onderzoeksrapport. De verschillen en overeenkomsten tussen de Wbp en de AVG zijn naast elkaar gelegd (zie hoofdstuk 3.4) en vervolgens is er vastgesteld dat de grootste veranderingen plaatsvinden op het gebied van de verplichtingen die worden opgelegd aan de verwerkingsverantwoordelijke en het aantal rechten dat de betrokkene heeft gekregen onder de AVG. Dit zorgt voor veranderingen in de werkwijze van SchoeBroek, die worden behandeld bij de vierde onderzoeksvraag.

Tot slot is de vierde onderzoeksvraag beantwoordt in het vijfde hoofdstuk van dit onderzoeksrapport, dit is direct het hoofdstuk met de aanbevelingen. In dit hoofdstuk is geconcludeerd dat SchoeBroek meerdere stappen moet ondernemen om te voldoen aan de eisen van de AVG. De stappen die concreet moeten worden ondernomen zijn te vinden in hoofdstuk 5.4 van dit onderzoeksrapport. De gevolgen die het niet voldoen aan de AVG met zich meebrengt is te vinden in tabel 3.

De AVG heeft als invloed op de werkwijze van SchoeBroek dat naast de werkwijze die op dit moment gehanteerd wordt, zij er extra plichten bij krijgen. Er ligt een grotere verantwoordelijkheid bij SchoeBroek om aan de tonen dat zij voldoen aan de eisen die de AVG stelt. Hoe aan deze extra verplichtingen kan worden voldaan, is beschreven in hoofdstuk vijf van dit onderzoeksrapport. Er moet daarnaast rekening gehouden worden met de extra plichten die de cliënten van SchoeBroek hebben gekregen (zie hoofdstuk 5.1). De cliënten dienen gewezen te worden op de rechten die zij hebben. Dit kan gedaan worden door middel van het opstellen en verstrekken van de privacyverklaring (zie hoofdstuk 5).

Literatuurlijst

Advocaat Centraal. (z.d.) *Veiligheid*. Geraadpleegd op 22 mei 2018, van <https://www.advocaatcentraal.nl/home>

Autoriteit Persoonsgegevens. (2018). AVG Nieuwe Europese privacywetgeving. *Algemene informatie AVG*. Geraadpleegd op 26 februari 2018, van <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/algemene-informatie-avg>.

Autoriteit Persoonsgegevens. (2018). AVG Nieuwe Europese privacywetgeving. *Overwegingen*. Geraadpleegd op 26 februari 2018, van https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/verordening_2016_-_679_definitief.pdf.

Autoriteit Persoonsgegevens. (2018). AVG Nieuwe Europese privacywetgeving. *Verantwoordingsplicht*. Geraadpleegd op 26 februari 2018, van <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/verantwoordingsplicht>.

Autoriteit Persoonsgegevens. (2018). Melden verwerking persoonsgegevens. Geraadpleegd op 1 mei 2018, van <https://autoriteitpersoonsgegevens.nl/nl/melden/melden-verwerking-persoonsgegevens>

Autoriteit Persoonsgegevens. (2018). AVG Nieuwe Europese privacywetgeving. *Rechten van betrokkenen*. Geraadpleegd op 2 mei 2018, van <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving/rechten-van-betrokkenen#hoe-stelt-u-een-privacyverklaring-op-6255>

Baarda, B. (2013). *Basisboek Kwalitatief onderzoek. Handleiding voor het opzetten en uitvoeren van kwalitatief onderzoek*. Groningen: Noordhof Uitgevers.

Bitter, C.M. (2014). Module Privacy en persoonsgegevens. *Bestuursdwang*. Geraadpleegd op 5 april 2018, van https://www.navigator.nl/document/dae61c68ecd455545364253a1ec8c2381d3?ctx=WKNL_CSL_493

De Nederlandsche Bank. (2011). *De werking van Europese regelgeving*. Geraadpleegd op 12 maart 2018, van <http://www.toezicht.dnb.nl/2/50-202428.jsp#>.

Ellenbroek. M.J., Schoemaker, C.A.F. (2016). *Kantoorhandboek*. Deventer: SchoeBroek advocaten & mediators.

Engelfriet, A. Meij, L., Kager, P. (2017). *De Algemene verordening gegevensbescherming. Artikelsgewijs commentaar*. Amsterdam: Ius Mentis.

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

Europa Nu. (z.d.). *Verordeningen*. Geraadpleegd op 12 maart 2018, van <https://www.europa-nu.nl/id/vh7bhpblc5za/verordening>.

Europa Nu. (z.d.). *Richtlijn*. Geraadpleegd op 12 maart 2018, van <https://www.europa-nu.nl/id/vh7bhovynh7/richtlijn>.

Gardeniers, H.J.M., Nouwt, J. (2009). *Module Privacy en persoonsgegevens. Politieke gezindheid, gezondheidsgegevens en strafrechtelijke gegevens*. Geraadpleegd op 22 maart, van https://www.navigator.nl/document/da439210041606728a73e9f594f394f1943?ctx=WKNL_CSL_493

ICT Recht. (2018). *Factsheets. Het register van verwerkingen van persoonsgegevens*. Geraadpleegd om 20 mei 2018, van <https://ictrecht.nl/factsheets/het-register-van-verwerkingen-van-persoonsgegevens/>

Katus, S.H., Zwenne, G.J. (2010). *Module Privacy en persoonsgegevens. Doelbinding en kwaliteitseisen*. Geraadpleegd op 22 maart 2018, van https://www.navigator.nl/document/da5e72765f7652551c9030b7ea659172803?ctx=WKNL_CSL_493

Nederlandse Orde van Advocaten. (2018). *Modellen AVG. Register datalekken*. Geraadpleegd op 24 mei 2018, van <https://www.advocatenorde.nl/modellen-avg>

Overheid. (1998). *Regels inzake bescherming van persoonsgegevens. Memorie van toelichting*. Geraadpleegd op 5 maart 2018, van <https://zoek.officielebekendmakingen.nl/kst-25892-3.html>.

Raad voor Rechtsbijstand. (2018). *Nieuws. Verwerkersovereenkomst voor privacywetgeving niet noodzakelijk*. Geraadpleegd op 22 mei 2018, van <https://www.rvr.org/nieuws/2018/april/verwerkersovereenkomst-voor-privacywetgeving-niet-noodzakelijk.html>

Rijksoverheid. (2018). *Handleiding Algemene verordening gegevensbescherming*. Geraadpleegd op 13 maart 2018, van <https://www.rijksoverheid.nl/documenten/rapporten/2018/01/22/handleiding-algemene-verordening-gegevensbescherming>.

Rijksoverheid. (2018). Wetsvoorstel Uitvoeringswet Algemene verordening gegevensbescherming. Geraadpleegd op 23 april 2018, van <https://www.rijksoverheid.nl/documenten/kamerstukken/2017/12/13/wetsvoorstel-uitvoeringswet-algemene-verordening-gegevensbescherming>

Rijksoverheid. (z.d.). Privacy en persoonsgegevens. *Burgerservicenummer*. Geraadpleegd op 24 april 2018, van <https://www.rijksoverheid.nl/onderwerpen/privacy-en-persoonsgegevens/burgerservicenummer-bsn>

Robidus Whitepaper. (2017). Privacy wetgeving: wat verandert er in 2018? Geraadpleegd op 28 februari 2018.

Sauerwein, L.B., Linneman, J.J. (2002). Ministerie van Justitie. Handleiding voor verwerkers van persoonsgegevens. Geraadpleegd op 5 maart 2018.

Schaaik. G.A.F.M. (2015). Praktijkgericht juridisch onderzoek. Den Haag: Boom Juridische uitgevers.

SchoeBroek. (z.d.). Wat doen wij? Geraadpleegd op 29 mei 2018, van <https://www.schoebroek.nl/wat-doen-wij>

Verhoeven, N. (2014). Wat is onderzoek? *Praktijkboek voor methoden en technieken*. Den Haag: Boom Lemma.

Vries, E. de. (2018). *De AVG voor advocaten*. Amersfoort: Boom Juridisch

Vries, H.H. de (2001). Telecommunicatie- en privacywet. *Vrijelijk*. Geraadpleegd op 15 maart 2018, van https://www.navigator.nl/document/inod743503b7a3d6050cd6407f1e70aa46fb?ctx=WKNL_CSL_584

Zwenne, G.J., Mommers, L. (2016). Tijdschrift voor Compliance. *De tien belangrijkste veranderingen die de Algemene verordening gegevensbescherming gaat brengen*.

Geraadpleegd van

https://openaccess.leidenuniv.nl/bitstream/handle/1887/46378/2016.08.00_GJZ_LM_De_tien_belangrijkste_veranderingen_Tijdschrift_voor_compliance%5bBR-3528943%5d.pdf?sequence=1.

Bijlagen

Bijlage 1: Interviewlijst

Interviewlijst met voorbeeldvragen per onderwerp

Persoonsgegevens

- 1. Welke persoonsgegevens worden verwerkt bij SchoeBroek?*
- 2. Op welke wijze worden de gegevens verwerkt*?*
- 3. Worden er 'bijzondere' persoonsgegevens verwerkt?*
- 4. Worden er strafrechtelijke persoonsgegevens verwerkt?*

Verantwoordelijke

- 1. Wie is bij SchoeBroek de verantwoordelijke voor de verwerking van persoonsgegevens?*
- 2. Wordt er gewerkt met een handboek/beleid, zodat iedere werknemer op dezelfde wijze omgaat met verwerking van persoonsgegevens?*
- 3. Worden verwerkingen van persoonsgegevens gemeld bij de AP?*
- 4. Hoe wordt er omgegaan met de informatieplicht naar de betrokkene toe?*
- 5. Wordt er gewerkt met een 'bewerker'?*
- 6. Wie zijn de 'bewerkers'?*
- 7. Wordt er gewerkt met een 'sub-verwerker'?*

Eisen Wbp

- 1. Hoe wordt er voor gezorgd dat aan de eisen van 'zorgvuldigheid', 'behoorlijkheid' en 'doelbinding' wordt voldaan?*
- 2. Op welke wijze wordt er voor gezorgd dat er aan de kwaliteitseisen wordt voldaan? (juist en nauwkeurig) (niet te veel, niet te weinig gegevens).*

Meldplicht datalekken

1. *Hoe wordt de beveiligingsplicht gewaarborgd? (welke technische- en organisatorische maatregelen** zijn er getroffen om gegevens op de juiste manier te beveiligen)*
2. *Wordt er op dit moment vastgelegd welke persoonsgegevens er worden verwerkt?*

Knelpunten

1. *Zijn er op dit moment knelpunten wat betreft de verwerking van persoonsgegevens?*

Opmerkingen/aanmerkingen

Bijlage 2: Opzet register

Organisatie:		Contactpersoon		
		Straat:		
		Postcode + plaats		
		Telefoon:		
		Email:		
		Datum:	24-5-2018	
# Procedure	Procedure naam	Naam verantwoordelijke	Betrokken personen	Type persoonsgegevens die (mogelijk) betrokken zijn bij de verwerking
1				
2				
3				

Gezamenlijke Verwerkingsverantwoordelijke:		
Bijzondere persoonsgegevens	Doel van de verwerking	De grondslag voor het verzamelen

Rechtstreeks verkregen of indirect van de betrokkene	Gebruikte technologie	Omschrijving van de technische en organisatorische beveiligingsmaatregelen die genomen zijn.	Termijn van bewaren / maximale termijn van bewaren	Incidenten	Hoog Risico?

(ICT Recht, 2018)

Bijlage 3: Verklaring gebruikte hulpmiddelen

Academie Bestuur & Recht



Hierbij verklaar ik, dat ik het voor u liggende werkstuk/project zelfstandig en zonder gebruik van andere dan de aangegeven hulpmiddelen geschreven heb; De uit andere bronnen direct of indirect overgenomen teksten zijn op enigerlei wijze in de door mij geschreven tekst expliciet met bronvermelding verantwoord. Het werkstuk werd tot nu toe nog niet in dezelfde of in vergelijkbare vorm aan een examiner of examencommissie voorgelegd. Ook is het werkstuk niet eerder in het openbaar verschenen.

Naam, achternaam: Kirsten van der Hauw

Plaats, datum: Deventer, 31-05-2018

Handtekening: