

Voorwoord

Eindelijk is het moment daar: Het inleveren van mijn scriptie. Voor u ligt mijn afstudeeronderzoek dat in opdracht van mijn werk- en opdrachtgever KBS Advocaten is uitgevoerd. Het afstudeeronderzoek is het resultaat van mijn vierjarige opleiding HBO-Rechten. Ondanks dat de laatste weken pittig waren, kan ik boven alles stellen dat ik met ontzettend veel plezier aan het onderzoek heb gewerkt. Het onderzoeksrapport zou er niet zo hebben uitgezien, zoals het er nu uit ziet, zonder de steun van anderen. Ik wil diegene graag in dit voorwoord bedanken.

Allereerst wil ik al mijn collega's van KBS Advocaten bedanken voor hun belangstelling en interesse in mijn onderzoek. Gedurende de afstudeerperiode hebben jullie mij gemotiveerd, gesteund en gerustgesteld om het onderzoek tot een goed einde te brengen. In het bijzonder wil ik Niels van den Burg bedanken. Verschillende keren ben ik door jou meegenomen naar bijeenkomsten over de AVG, zoals het congres van Medilex over de AVG voor zorgprofessionals en de seminars over de AVG. Hierdoor heb ik niet alleen de AVG bestudeerd, maar heb ik ook kunnen zien hoe de praktijk om gaat met de AVG en tegen wat voor problemen men aanloopt bij de implementatie van de AVG. Zonder deze kijk op de praktijk en zonder jouw duidelijke uitleg, kritische vragen, het juiste steuntje in de rug, jouw opmerkingen en aanvullingen op mijn conceptversies, had mijn onderzoeksrapport er niet uitgezien zoals het nu is. Niels, bedankt!

Verder wil ik de drie personen die ik heb mogen interviewen in het kader van mijn onderzoek, Rogier de Snoo, Niels van de Burg en Erik Luijendijk, bedanken. Nogmaals dank voor jullie inzet, tijd en het delen van jullie kennis met mij.

Daarnaast wil ik graag de heer Verstuijf en de heer Kuiper bedanken. Beiden hebben een grote rol in mijn afstudeeronderzoek gespeeld. De heer Verstuijf door ervoor te zorgen dat ik een goede basis had voor het schrijven van mijn afstudeeronderzoek en de heer Kuiper door de leerzame feedbackgesprekken, de opbeurende schouderklopjes wanneer het even iets minder ging en bovenal het vertrouwen in mij als student.

Tot slot wil ik de mensen in mijn persoonlijke omgeving bedanken voor hun steun, luisterend oor en vertrouwen in mij. Mama, zusje, Ad, vriend en vriendinnen: enorm bedankt!

Lisa van Leeuwen, 27 mei 2018

Woerden

Samenvatting

In 1995 is de Europese privacyrichtlijn 95/46.EG (Richtlijn) tot stand gekomen om de privacy van burgers te waarborgen, waarna in Nederland de Richtlijn in de Wet bescherming persoonsgegevens (Wbp) is geïmplementeerd. Door de snelle technologische ontwikkelingen van de afgelopen jaren en de opkomst van de sociale media voldeed de bestaande wet- en regelgeving niet meer. Reden waarom op 27 april 2016 de Algemene verordening gegevensbescherming (AVG) tot stand is gekomen. De AVG vervangt de Richtlijn (en dus ook de Wbp). De AVG is vanaf 25 mei 2018 rechtstreeks van toepassing in alle lidstaten. Gezien het voorstaande is de wet- en regelgeving over het verwerken van persoonsgegevens door organisaties volop in beweging, waardoor organisaties wijzigingen moeten doorvoeren, zo ook KBS Advocaten (KBS). Het is voor KBS vooralsnog onvoldoende inzichtelijk wat de komst van de AVG betekent voor de verwerkingen van persoonsgegevens, en in het bijzonder gezondheidspersoonsgegevens, zoals die plaatsvinden bij KBS. KBS heeft behoefte aan een compleet overzicht van de belangrijkste wijzigingen op het gebied van verwerkingen van persoonsgegevens, en in het bijzonder gezondheidspersoonsgegevens, binnen het kantoor.

Om bovenstaand probleem te onderzoeken zijn een doelstelling en een centrale vraag geformuleerd. Het doel van het onderzoek is allereerst om KBS inzicht te geven over hoe zij haar werkwijze met betrekking tot het verwerken van persoonsgegevens, en in het bijzonder gezondheidspersoonsgegevens, moet aanpassen, om zo aan de AVG te voldoen. De centrale vraag luidt als volgt: *“Welk advies kan er aan de hand van wetsanalyse, literatuuronderzoek en interviews aan KBS Advocaten worden gegeven over de implementatie van het privacybeleid en het verwerken van persoonsgegevens, en in het bijzonder gezondheidspersoonsgegevens, zodat KBS voldoet aan de vereisten van de Algemene verordening gegevensbescherming (AVG)?”* Om de doelstelling van het onderzoek te behalen en de centrale vraag te beantwoorden, is gebruik gemaakt van de onderzoeksmethoden, zoals genoemd in de centrale vraag.

In het onderzoeksrapport is de AVG opgesplitst in verschillende categorieën, waarbij bij elke categorie is gekeken hoe KBS hieraan invulling dient te geven. De volgende categorieën zijn achtereenvolgens in het onderzoeksrapport aan bod gekomen: De toepassing van de AVG, de rechtmatige verwerking van persoonsgegevens, de positie van verwerkingsverantwoordelijke en verwerker, de verplichtingen voor verwerkingsverantwoordelijken vanuit de AVG, de rechten van betrokkenen en de mate van kennis van de advocaten van KBS.

Het belangrijkste resultaat dat is behaald uit zowel de wetsanalyse, literatuuronderzoek als de interviews, is als volgt: De AVG is op KBS van toepassing. Hierdoor moeten de gegevensverwerkingen binnen KBS voldoen aan de AVG. Voor wat betreft de rechtmatige verwerking van persoonsgegevens, is gebleken dat KBS verschillende betrokkenen kent, waarbij zowel gewone als bijzondere persoonsgegevens, namelijk gezondheidspersoonsgegevens, worden verwerkt. De verwerkte persoonsgegevens zijn te baseren op een grondslag (en een voorwaarde voor het verwerken van bijzondere persoonsgegevens) van de AVG, zodat de gegevensverwerking rechtmatig is.

Verder is uit het onderzoek gebleken dat KBS kan worden aangemerkt als verwerkingsverantwoordelijke. Reden waarom de verantwoordingsplicht op KBS rust. KBS moet voldoen aan de verplichtingen van de AVG en aantonen dat zij hieraan voldoet. KBS moet voldoen aan de registerplicht, de verplichting van privacy by design & default, de meldplicht datalekken, het treffen van beveiligingsmaatregelen en het maken van afspraken met verwerkers. Daarnaast heeft KBS een informatieplicht. KBS heeft hieraan voldaan door een privacystatement op te stellen voor externe betrokkenen en een privacyprotocol voor interne betrokkenen. De verplichting om een FG aan te stellen en de verplichting om een DPIA uit te voeren, zijn (vooralsnog) niet op KBS van toepassing. Bij deze verplichtingen bestaat nog een grijs gebied. Reden waarom 100% zekerheid (nog) niet kan worden gegeven. Daarnaast is uit de resultaten gebleken dat KBS de rechten van betrokkenen moet waarborgen, waarbij zij in bepaalde gevallen geen gehoor mag en dus hoeft te geven aan een verzoek van recht op inzage en/of het recht op verwijdering. Tot slot is uit het onderzoeksrapport gebleken dat de advocaten van KBS op de hoogte zijn van de AVG, maar dat er nog enige onduidelijkheid bestaat over de invulling van bepaalde verplichtingen uit de AVG, hetgeen voornamelijk te maken heeft met grijze gebieden binnen de AVG.

De eindconclusie van het onderzoek is allereerst dat KBS een verantwoordingsplicht heeft, waardoor zij verplicht is om de beginselen en verplichtingen voor verwerkingsverantwoordelijken van de AVG in acht te nemen en de rechten van betrokkenen te waarborgen. Daarnaast is KBS verplicht om aan te tonen dat zij aan deze verantwoordingsplicht voldoet, hetgeen door KBS wordt gedaan in een privacystatement, zowel voor interne als voor externe betrokkenen. Daarnaast blijkt uit het onderzoeksrapport dat over een aantal onderdelen van de AVG, zoals de invulling van de criteria voor een FG of DPIA, nog onduidelijkheid bestaat. KBS zal de ontwikkelingen hierover moeten volgen om deze vervolgens te kunnen toepassen op de organisatie en wellicht aanpassingen te treffen binnen de organisatie om zo te voldoen aan de AVG.

Uit de hierboven genoemde eindconclusie vloeien diverse aanbevelingen voort. Per categorie van de AVG zijn aanbevelingen gedaan: de positie van verwerkingsverantwoordelijke, de rechtmatige verwerking van persoonsgegevens, de verplichtingen voor verwerkingsverantwoordelijken en de rechten van betrokkenen. Alle aanbevelingen zijn erop gericht om de privacy binnen de organisatie van de opdrachtgever te optimaliseren, hiermee te voldoen aan de AVG en dus als organisatie "AVG compliant" te zijn.

Inhoudsopgave

Samenvatting	3
Afkortingen	7
Begrippenlijst	8
Hoofdstuk 1: Inleiding	11
1.1 Achtergrondinformatie, probleemstelling en analyse	11
1.2 Doelstelling	13
1.3 Centrale vraag & deelvragen	14
1.3.1 De theoretisch-juridische deelvragen	14
1.3.2 De praktijkgerichte deelvragen	15
1.4 Operationaliseren van begrippen	16
1.5 Onderzoeksmethodiek	16
1.5.1 Het theoretisch-juridisch onderzoeksgedeelte	17
1.5.2 Het praktijkgericht onderzoeksgedeelte	17
1.6 Leeswijzer	18
Hoofdstuk 2: De reikwijdte en de beginselen van de AVG	19
2.1 De reikwijdte van de AVG	19
2.2 De beginselen van de AVG	20
Hoofdstuk 3: De legitieme gegevensverwerking van de AVG	22
3.1 Het onderscheid tussen gewone persoonsgegevens en bijzondere persoonsgegevens	22
3.2 De grondslagen voor het rechtmatig verwerken van persoonsgegevens	22
3.2.1 Het rechtmatig verwerken van gewone persoonsgegevens	22
3.2.2 Het rechtmatig verwerken van bijzondere persoonsgegevens	25
3.2.2.1 De definitie van gezondheidspersoonsgegevens	25
3.2.2.2 Het rechtmatig verwerken van gezondheidspersoonsgegevens	25
3.3 Deelconclusie	26
Hoofdstuk 4: Verwerkingsverantwoordelijke versus verwerker	28
4.1 Het onderscheid tussen verwerkingsverantwoordelijke en verwerker	28
4.1.1 De verwerkingsverantwoordelijke	28
4.1.2 De gezamenlijke verwerkingsverantwoordelijken	29
4.1.3 De verwerker	29
4.2 De verplichtingen voor de verwerkingsverantwoordelijke	30
4.3 De verplichtingen voor de verwerker	34
4.4 De Functionaris voor de Gegevensbescherming	34
4.5 De gegevensbeschermingseffectbeoordeling (DPIA)	37
4.6 Deelconclusie	39
Hoofdstuk 5: De rechten van betrokkenen	42
5.1 De rechten van de betrokkenen	42
5.2 Het recht op inzage tegenover het beroepsgeheim van een advocaat	44
5.2.1 Het recht op inzage	44
5.2.2 Het beroepsgeheim van een advocaat	45
5.2.3 Het recht op inzage tegenover het beroepsgeheim van een advocaat	45
5.3 Het recht op verwijdering tegenover de dossierplicht van een advocaat	46
5.3.1 Het recht op verwijdering	46
5.3.2 De dossierplicht van een advocaat	48

5.3.3	Het recht op verwijdering tegenover de dossierplicht van een advocaat	48
5.4	Deelconclusie	49
Hoofdstuk 6: Het toezicht op de naleving van de AVG		51
Hoofdstuk 7: Resultaten		52
7.1	De verwerkte persoonsgegevens binnen KBS	52
7.2	De werkwijze m.b.t. het verwerken van persoonsgegevens binnen KBS	54
7.3	De verwerkingsverantwoordelijke en de verwerkers binnen KBS	56
7.4	De invulling van de verplichtingen binnen KBS	58
7.5	De invulling van de rechten van de betrokkenen binnen KBS	61
7.6	De mate van kennis over de AVG bij de advocaten van KBS	62
Hoofdstuk 8: Conclusie		64
8.1	De AVG is van toepassing op KBS	64
8.2	De grondslagen voor het rechtsgeldig verwerken van persoonsgegevens binnen KBS	64
8.3	De rolverdeling binnen KBS	65
8.4	De invulling van de verplichtingen van de AVG bij KBS	65
8.5	Het waarborgen van de rechten van betrokkenen bij KBS	66
8.6	De kennis van de advocaten van KBS	67
Hoofdstuk 9: Aanbeveling		67
Literatuurlijst		73
Bijlagenoverzicht		75
Bijlage I	Schematisch overzicht over de reikwijdte van de AVG	76
Bijlage II	Schematisch overzicht over de rechtmatige verwerking van persoonsgegevens	
Bijlage III	Schematisch overzicht verwerkingsverantwoordelijke versus verwerker	77
Bijlage IV	Schematisch overzicht recht op inzage versus beroepsgeheim	78
Bijlage V	Schematisch overzicht recht op verwijdering versus dossierplicht	79
Bijlage VI	Schematisch overzicht van de verwerkte persoonsgegevens binnen KBS Advocaten	80
Bijlage VII	Transcriptie interview de heer R. de Snoo	84
Bijlage VIII	Transcriptie interview [REDACTED]	105
Bijlage IX	Transcriptie interview de heer mr. E. Luijendijk	124
Bijlage X	Resultaten enquête (mentimeter)	140

Afkortingen

Artikel 29 Werkgroep	Groep Gegevensbescherming Artikel 29
AP	Autoriteit Persoonsgegevens
AVG	Algemene verordening gegevensbescherming
AWR	Algemene Wet inzake Rijksbelastingen
BW	Burgerlijk Wetboek
DPIA	Data protection impact assessment
EVRM	Europees Verdrag voor de Rechten van de Mens
FG	Functionaris voor de gegevensbescherming
HR	Hoge Raad
HvJ EU	Hof van Justitie van de Europese Unie
KBS	KBS Advocaten
MvT	Memorie van Toelichting
Richtlijn	Richtlijn 95/46/EG
UAVG	Uitvoeringswet algemene verordening gegevensbescherming
Wbp	Wet bescherming persoonsgegevens
Wlb	Wet op de loonbelasting
Wmd	Wet meldplicht datalekken
WWFT	Wet ter voorkoming van witwassen en financieren van terrorisme

Begrippenlijst

Betrokkene	Waar in het onderzoeksrapport wordt gesproken over betrokkene, wordt de definitie van artikel 4 lid 1 AVG bedoeld, namelijk: <i>"De persoon op wie de persoonsgegevens betrekking hebben."</i>
Bijzondere persoonsgegevens	Waar in het onderzoeksrapport wordt gesproken over bijzondere persoonsgegevens, wordt de definitie van artikel 9 lid 1 AVG bedoeld, namelijk: <i>"(...) persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid (...)."</i>
Persoonsgegevens	Waar in het onderzoeksrapport wordt gesproken over persoonsgegevens, wordt de definitie artikel 4 lid 1 AVG bedoeld, namelijk: <i>"Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon."</i> ¹
Gevoelige gegevens	Waar in het onderzoeksrapport wordt gesproken over gevoelige gegevens, wordt de definitie bedoeld, zoals de Handleiding AVG en UAVG van het Ministerie Van Justitie & Veiligheid dit beschrijven namelijk: <i>"(...) Bijzondere persoonsgegevens of strafrechtelijke persoonsgegevens, maar ook gegevens die niet 'bijzonder' in de zin van de Verordening zijn, kunnen gevoelig zijn. Denk hierbij bijvoorbeeld aan financiële data of locatiegegevens."</i>

¹ Wanneer gegevens van een rechtspersoon worden verwerkt, is er dus geen sprake van een persoonsgegevens. Echter, wanneer de gegevens van een contactpersoon van de rechtspersoon worden verwerkt, is er wel sprake van een persoonsgegeven. De gegevens hebben dan immers betrekking op een natuurlijk persoon binnen de rechtspersoon. Verder is er bij een onderneming dat geen rechtspersoon is, bijvoorbeeld in het geval van een maatschap, ook sprake van het verwerken van persoonsgegevens. Dit aangezien de persoonsgegevens van de maten van de maatschap in dat geval worden verwerkt en deze zijn aan te merken als natuurlijk persoon.

De maatregelen die u moet nemen om persoonsgegevens te beschermen zijn mede afhankelijk van de gevoeligheid van de gegevens en het risico dat zij kunnen vormen voor de betrokkene bij verkeerd gebruik of misbruik.”².

Gewone persoonsgegevens

Waar in het onderzoeksrapport wordt gesproken over gewone persoonsgegevens, wordt de definitie bedoeld, zoals de Handleiding AVG en UAVG van het Ministerie van Justitie & Veiligheid dit beschrijven, namelijk: *“De persoonsgegevens die niet zijn thuis te brengen onder de categorie bijzondere persoonsgegevens zoals bedoeld in artikel 9 lid 1 AVG of gegevens van strafrechtelijke aard zoals bedoeld in artikel 10 AVG.”³*

Gezondheidspersoonsgegevens

Waar in het onderzoeksrapport wordt gesproken over gezondheidspersoonsgegevens, wordt de definitie van artikel 4 lid 15 bedoeld, namelijk: *“Persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven.”.*

Verwerken

Waar in het onderzoeksrapport wordt gesproken over verwerken, wordt de definitie van artikel 4 lid 2 AVG bedoeld, namelijk: *“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.”.*

² Schermer, Hagenauw & Falot, 2018, p.26.

³ Schermer, Hagenauw & Falot, 2018, p.26.

Verwerker	Waar in het onderzoeksrapport wordt gesproken over verwerker, wordt de definitie van artikel 4 lid 8 AVG bedoeld, namelijk: <i>"Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat namens de verwerkingsverantwoordelijke persoonsgegevens verwerkt."</i>
Verwerkingsverantwoordelijke	Waar in het onderzoeksrapport wordt gesproken over verwerkingsverantwoordelijke, wordt de definitie van artikel 4 lid 7 AVG bedoeld, namelijk: <i>"De bevoegde autoriteit die, alleen of samen met anderen, de doeleinden van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doeleinden van en de middelen voor die verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen."</i> ⁴

⁴ Waar de Richtlijn spreekt over "verantwoordelijke" en "bewerker", spreekt de AVG over "verwerkingsverantwoordelijke" en "verwerker". Het begrip "verwerkingsverantwoordelijke" wordt in de praktijk afgekort als "verantwoordelijke". Om in het onderzoek de begrippen van de Richtlijn en de AVG van elkaar gescheiden te houden, is in het onderzoek gesproken over "verwerkingsverantwoordelijke" waar het de AVG betreft en "verantwoordelijke" waar het de Richtlijn betreft.

Hoofdstuk 1: Inleiding

1.1. Achtergrondinformatie, probleemstelling en analyse

Eenieder in Nederland heeft ingevolge artikel 8 EVRM en artikel 10 Grondwet recht op eerbiediging van zijn persoonlijke levenssfeer, hetgeen kort gezegd betekent dat iedereen recht heeft op privacy.⁵ Het vastleggen en verwerken van persoonsgegevens valt onder privacy. Het recht op gegevensbescherming en het recht op privacy houden in zekere zin verband met elkaar. Het recht op privacy wordt immers gewaarborgd door op een rechtmatige manier persoonsgegevens vast te leggen en te verwerken.⁶

Om privacy te waarborgen is er door de Europese Unie wet- en regelgeving opgesteld. In 1995 is de Europese privacyrichtlijn 95/46.EG (hierna te noemen: Richtlijn) tot stand gekomen, waarna in Nederland de Richtlijn in de Wet bescherming persoonsgegevens (hierna te noemen: Wbp) is geïmplementeerd. De Richtlijn had twee kerndoelen: enerzijds het beschermen van fundamentele vrijheden en rechten, waarbij in het bijzonder het beschermen van de persoonlijke levenssfeer, en anderzijds het bevorderen en waarborgen van het vrije verkeer van persoonsgegevens als onderdeel van de interne markt.⁷

Door de snelle technologische ontwikkelingen van de afgelopen jaren en de opkomst van de sociale media voldeed de bestaande wet- en regelgeving niet meer.⁸ Reden waarom de Europese Unie op 25 januari 2012 op basis van artikel 16 lid 2 van het Verdrag betreffende de werking van de Europese Unie (hierna te noemen: VWEU) een voorstel deed voor nieuwe wet- en regelgeving. Er is gekozen voor een verordening. De wens om te komen tot een Europese harmonisatie op het terrein van de bescherming van persoonsgegevens was een reden voor dit voorstel.⁹ De keuze voor een verordening lag in het volgende: Een verordening heeft rechtstreeks werking in de lidstaten, waardoor de keuzeruimte voor nationale wetgevers bij de uitvoering meer wordt beperkt, dan bij de implementatie van een richtlijn het geval was.

Gedurende een periode van vier jaar is onderhandeld, waarna op 27 april 2016 de Algemene verordening gegevensbescherming (hierna te noemen: AVG) tot stand is gekomen.¹⁰ De AVG vervangt de Richtlijn (en dus ook de Wbp). Ondanks dat de AVG al op 25 mei 2016 in werking is getreden, is de AVG pas vanaf 25 mei 2018 rechtstreeks van toepassing in alle lidstaten. Organisaties en toezichthouders hebben hierdoor twee jaar de tijd gekregen om zich voor te bereiden.¹¹

⁵ Van der Jagt, 2013, p. 163.

⁶ Van der Jagt, 2013, p. 163.

⁷ Van Balen & Nijveld, 2017, p. 608.

⁸ Van der Jagt, 2013, p. 163.

⁹ Van Balen & Nijveld, 2017, p. 608.

¹⁰ De AVG heet oorspronkelijk General Data Protection Regulation (GDPR). AVG is de Nederlandse vertaling hiervoor. In het onderzoeksrapport wordt gesproken over de AVG.

¹¹ Van Balen & Nijveld, 2017, p. 608.

Hoewel de AVG een bindend karakter kent, heeft de AVG op een aantal plaatsen ruimte vrij gelaten voor de nationale wetgever om keuzes te maken. In dit kader heeft de regering op 16 mei 2018 de Uitvoeringswet Algemene verordening gegevensbescherming (hierna te noemen: UAVG) opgesteld en gepubliceerd.¹² Ondanks dat de Wbp is komen te vervallen, worden bij de UAVG de regels van de Wbp zoveel mogelijk gehandhaafd, tenzij dit in strijd is met de AVG.¹³

Het onderzoek wordt uitgevoerd in opdracht van KBS Advocaten (hierna te noemen: KBS). KBS is een middelgroot advocatenkantoor in Utrecht en is werkzaam voor organisaties, instellingen en individuele beroepsbeoefenaren in de individuele gezondheidszorg, ondernemingen, verzekeringsmaatschappijen, maatschappelijke instellingen en particulieren. KBS richt zich hiermee op de medische wereld. Naast de medische wereld richt KBS zich tevens voornamelijk op het insolventierecht.

Gezien het voorstaande is de wet- en regelgeving over het verwerken van persoonsgegevens voor organisaties volop in beweging, waardoor organisaties wijzingen moeten doorvoeren, zo ook KBS. Het is voor KBS vooralsnog onvoldoende inzichtelijk wat de komst van de AVG betekent voor de verwerkingen van persoonsgegevens, en in het bijzonder gezondheidspersoonsgegevens, zoals die plaatsvinden bij KBS. KBS heeft dan ook behoefte aan een algemeen overzicht van de belangrijkste wijzigingen op het gebied van verwerkingen van persoonsgegevens, en in het bijzonder gezondheidspersoonsgegevens, binnen het kantoor. Gezien de onduidelijkheid over de gevolgen van de AVG voor het verwerken van (gezondheids) persoonsgegevens binnen KBS, is in het onderzoeksrapport onderzocht of KBS op het gebied van het verwerken van (gezondheids) persoonsgegevens voldoet aan de AVG.

KBS heeft behoefte aan een algemeen overzicht, waarbij de AVG in begrijpelijke taal wordt beschreven en wordt toegespitst op KBS. Aangezien de AVG een grote omvang kent en het uitdrukkelijk weergeven van alle onderwerpen van de AVG zou leiden tot een te grote omvang van het onderzoek, heeft KBS voorts aangegeven over welke onderwerpen van de AVG zij expliciet wil worden voorgelicht. Aan deze onderwerpen is in het onderzoeksrapport extra aandacht gegeven. Gelet op het feit dat KBS gezondheidspersoonsgegevens verwerkt, is bij KBS de vraag ontstaan of zij verplicht is om een Functionaris voor de Gegevensbescherming (hierna te noemen: FG) aan te stellen en een gegevensbeschermingseffectbeoordeling (hierna te noemen: DPIA) uit te voeren. De AVG maakt verder een onderscheid tussen verwerkingsverantwoordelijke en verwerker met elk verschillende verplichtingen, hetgeen bij KBS heeft geleid tot onduidelijkheid over welke positie KBS inneemt bij de invulling van deze begrippen. Tot slot heeft een betrokkene met de komst van de AVG het recht op inzage en het recht op verwijdering, hetgeen bij KBS heeft geleid tot de vraag of en hoe zij hieraan invulling moeten geven, mede gelet op het beroepsgeheim en de dossierplicht van advocaten. In het onderzoeksrapport is expliciet ingegaan op deze - door KBS benadrukte - onderwerpen.

¹² Kamerstukken I 2017/18, 34 851, nr. 144.

¹³ Van Balen & Nijveld, 2017, p. 608.

Gezien het feit dat de opdracht toeziet op het weergeven van een algemeen beeld van de AVG voor het verwerken van persoonsgegevens, en in het bijzonder gezondheidspersoonsgegevens, geeft het onderzoeksrapport allereerst een algemeen beeld van de AVG weer, waarbij de AVG kort is afgezet tegen KBS. Daarna is op de door KBS expliciete onderwerpen van de AVG (positie van verwerkingsverantwoordelijke en verwerker, FG, DPIA en recht op inzage en -verwijdering) ingegaan.

Om de advocaten van KBS meer bewust te laten worden van de gevolgen van de AVG voor de gegevensverwerkingen binnen het kantoor, is in het onderzoek tot slot onderzocht in welke mate de kennis van de AVG bij de advocaten van KBS aanwezig is. Aan de hand van de resultaten is in het onderzoeksrapport aansluiting gezocht bij de mate van kennis over de AVG bij de advocaten van KBS. Dit kan vervolgens worden meegenomen bij het implementeren van het privacybeleid¹⁴ binnen KBS. Het onderzoeksrapport kan vervolgens worden geraadpleegd door de advocaten van KBS, die willen worden voorgelicht over de (gevolgen van de) AVG voor de gegevensverwerkingen binnen KBS.¹⁵

Aangezien de afdeling insolventie een geheel eigen werkwijze kent en het weergeven van beide gebieden (medische wereld en insolventie) zou resulteren in een te grote omvang van het onderzoek, is in het onderzoek niet ingegaan op het verwerken van persoonsgegevens bij de afdeling insolventie. Het onderzoek beperkt zich tot het analyseren van het verwerken van persoonsgegevens, en in het bijzonder gezondheidspersoonsgegevens, binnen KBS.

Volledigheidshalve wordt verder vermeld dat het onderzoeksrapport geen weergave geeft van het juridisch kader van de Richtlijn en de Wbp. Reden hiervoor is dat de Richtlijn en de Wbp met de komst van de AVG komen te vervallen en het weergeven van het juridisch kader dan ook niet van belang is voor de verwerking van (gezondheids) persoonsgegevens binnen KBS Advocaten.

1.2 Doelstelling

Het bovenstaande heeft geresulteerd in de volgende doelstelling voor het onderzoeksrapport:

"Het doel van het onderzoek is allereerst om KBS Advocaten inzicht te geven over hoe zij haar werkwijze met betrekking tot het verwerken van persoonsgegevens, en in het bijzonder gezondheidspersoonsgegevens, moet aanpassen, om zo aan de vereisten van de Algemene verordening gegevensbescherming (AVG) te kunnen voldoen. Om dit te onderzoeken wordt wetsanalyse en literatuuronderzoek gedaan en worden interviews afgenomen bij de medewerkers van KBS Advocaten die toezien op de privacy binnen het kantoor.

¹⁴ Voor een inhoudelijke uitleg over wat er in het onderzoeksrapport wordt verstaan onder "privacybeleid" wordt hierbij volledigheidshalve verwezen naar paragraaf 1.4 van het onderzoeksrapport.

¹⁵ Niet geheel onbelangrijk om te vermelden, is dat er onderzoek is gedaan naar de kennis van de advocaten en niet naar de kennis van andere medewerkers van KBS (boekhouding, secretaresses, etc.). Dit aangezien KBS behoefte heeft aan een groeiende bewustwording van de AVG onder de advocaten en niet onder de andere medewerkers binnen het kantoor. Reden hiervoor is dat de andere medewerkers altijd in opdracht van een advocaat werken, waardoor de advocaat verantwoordelijk is voor een correcte gegevensverwerking en de medewerker enkel de opdracht naar behoren dient uit te voeren.

Het onderzoek resulteert in een advies over de wijzigingen die KBS Advocaten moet doorvoeren om zo aan de Algemene verordening gegevensbescherming (AVG) te voldoen. Verder heeft het onderzoek als doel om de bewustwording van de gevolgen van de AVG onder de advocaten van KBS Advocaten te vergroten. Om de kennis van de AVG van de advocaten van KBS Advocaten te onderzoeken wordt een enquête (via mentimeter) bij de advocaten van KBS Advocaten afgenomen. De resultaten geven inzicht in de mate waarin de advocaten van KBS Advocaten kennis hebben van de AVG. De resultaten kunnen worden meegenomen bij de implementatie van het privacybeleid binnen KBS Advocaten.”

1.3 Centrale vraag & deelvragen

Uit de genoemde doelstelling volgt de volgende vraagstelling:

“Welk advies kan er aan de hand van wetsanalyse, literatuuronderzoek en interviews aan KBS Advocaten worden gegeven over de implementatie van het privacybeleid en het verwerken van persoonsgegevens, en in het bijzonder gezondheidspersoonsgegevens, zodat KBS Advocaten voldoet aan de vereisten van de Algemene verordening gegevensbescherming (AVG)?”

Om antwoord te kunnen geven op de centrale onderzoeksvraag, zijn de volgende deelvragen geformuleerd:

1.3.1 De theoretische-juridische deelvragen

Deelvraag 1

Wat is het juridische kader voor het verwerken van persoonsgegevens gelet op de AVG?

Zoals eerder is aangegeven, ziet de opdracht van KBS toe op het weergeven van een algemeen beeld van de AVG voor het verwerken van persoonsgegevens. Hierdoor geeft deelvraag 1 een algemeen beeld van de AVG weer. KBS heeft verder in haar opdracht aangegeven expliciet behoefte te hebben aan een weergave van het juridisch kader voor het verwerken van gezondheidspersoonsgegevens. Tot slot heeft KBS een aantal onderwerpen van de AVG benoemd, waarover zij expliciet wil worden voorgelicht. Reden waarom bij de beantwoording van deelvraag 1 een algemeen beeld van de AVG is weergegeven en deze deelvraag vervolgens bij de deelvragen 2 t/m 6 is geëxpliciteerd. Bij de deelvragen 2 t/m 6 is ingegaan op de door KBS expliciet benoemde onderwerpen van de AVG. Hierdoor kan er enige overlap zijn tussen de beantwoording van deelvraag 1 en de beantwoording van deelvragen 2 t/m 6.

Deelvraag 2

Wat is het juridisch kader voor het verwerken van bijzondere persoonsgegevens, specifiek gezondheidspersoonsgegevens, gelet op de AVG?

Deelvraag 3

Wat is het juridisch kader om vast te stellen of er sprake is van een verwerkingsverantwoordelijke of verwerker gelet op de AVG?

Deelvraag 4

Wat is het juridisch kader voor het aanstellen van een Functionaris voor de Gegevensbescherming gelet op de AVG?

Deelvraag 5

Wat is het juridisch kader voor het uitvoeren van een gegevensbeschermingseffectbeoordeling (DPIA) gelet op de AVG?

Deelvraag 6

Hoe verhoudt het recht op inzage of gegevenswissing zich tot het beroepsgeheim en de dossierplicht van een advocaat?

1.3.2 De praktijkgerichte deelvragen

Deelvraag 7

Wat voor persoonsgegevens verwerkt KBS?

- a) Wat voor gewone persoonsgegevens verwerkt KBS?
- b) Wat voor gezondheidspersoonsgegevens verwerkt KBS?

Deelvraag 8

Wat is de werkwijze van KBS met betrekking tot het verwerken van persoonsgegevens?

- a) Wat is de werkwijze van KBS met betrekking tot het verwerken van gewone persoonsgegevens?
- b) Wat is de werkwijze van KBS met betrekking tot het verwerken van gezondheidspersoonsgegevens?

Deelvraag 9

In welke hoedanigheid kan KBS worden beschouwd gelet op de posities verwerkingsverantwoordelijke en verwerker zoals bedoeld in de AVG?

Deelvraag 10

In hoeverre is KBS verplicht om een Functionaris voor de Gegevensbescherming aan te stellen?

- a) In hoeverre is er bij KBS sprake van verwerkingen, die vanwege hun aard, omvang en/of doeleinden, regelmatige en stelselmatige observatie op grote schaal van betrokkenen vereisen?
- b) In hoeverre is er bij KBS sprake van een hoofdzakelijke belasting met het grootschalig verwerken van bijzondere categorieën van persoonsgegevens?

Deelvraag 11

In hoeverre is KBS verplicht om een gegevensbeschermingseffectbeoordeling (DPIA) te verrichten?

Deelvraag 12

Wat is de werkwijze van KBS bij het verzoek van een cliënt of andere betrokkene bij het inzien of verwijderen van een dossier?

Deelvraag 13

In welke mate is de kennis van de AVG bekend bij de advocaten van KBS?

1.4 Operationaliseren van begrippen

In de begrippenlijst van het onderzoeksrapport is een aantal begrippen beschreven die voor het verdere verloop van het onderzoeksrapport van belang zijn. Hieronder worden enkel begrippen geoperationaliseerd, zoals die in de probleemanalyse, doelstelling, centrale vraag en deelvragen zijn opgenomen, en die van belang zijn voor het onderzoek. Aangezien de begrippen de rest van het onderzoek zijn gebruikt, wordt hieronder de inhoud van de begrippen weergegeven.

Belangrijkste	Onder belangrijkste wordt in het onderzoeksrapport verstaan: Wat het meeste impact heeft (in dit geval op de bedrijfsvoering).
Huidige	Onder huidige wordt in het onderzoeksrapport verstaan: De manier en/of werkwijze zoals die op dit moment binnen een organisatie verloopt.
Privacybeleid	Onder privacybeleid wordt in het onderzoeksrapport verstaan: Een op schrift gesteld document, waarbij de procedures, beleidsregels en activiteiten op het gebied van de informatiebeveiliging binnen een organisatie zijn beschreven met als doel om medewerkers van de organisaties en betrokkenen te voorlichten over de gegevensverwerking binnen de organisatie.
Zaakdossier	Onder zaakdossier wordt in het onderzoeksrapport verstaan: Het dossier dat een advocaat van een cliënt aanmaakt, bijhoudt en archiveert.

1.5 Onderzoeksmethodiek

Om tot beantwoording van de deelvragen te komen, zijn diverse methoden van onderzoek gehanteerd. De methoden van onderzoek worden hieronder kort weergegeven, waarbij een onderscheid wordt gemaakt tussen de theoretisch-juridische deelvragen en de praktijkgerichte deelvragen.

1.6 Leeswijzer

Het onderhavige hoofdstuk betreft de inleiding. In hoofdstuk 2 t/m 6 van het onderzoeksrapport worden de theoretisch-juridische deelvragen beantwoord (deelvraag 1 t/m deelvraag 6). Deelvraag 1 wordt beantwoord in hoofdstuk 2 t/m hoofdstuk 6. De deelvragen 2 t/m 6 worden elk in een afzonderlijk hoofdstuk in de hoofdstuk 2 t/m 6 beantwoord. Hoofdstuk 2 beschrijft de reikwijdte en de beginselen van de AVG. Hoofdstuk 3 beantwoordt deelvraag 2 en ziet toe op de rechtmatige verwerking van persoonsgegevens. Hoofdstuk 4 geeft vervolgens het antwoord op deelvragen 3 t/m 5 en beschrijft het onderscheid tussen de verwerkingsverantwoordelijke en de verwerker, evenals de verplichtingen voor de verwerkingsverantwoordelijke en de verwerker. Hoofdstuk 5 beantwoordt deelvraag 6 en ziet toe op de rechten van betrokkene. Hoofdstuk 6 beschrijft het toezicht op de naleving van de AVG. In hoofdstuk 7 van het onderzoeksrapport worden de praktijkgerichte deelvragen (deelvraag 7 t/m 13) beantwoord en worden de resultaten van het onderzoek weergegeven. In hoofdstuk 8 van het onderzoeksrapport volgt een conclusie, waarna in hoofdstuk 9, tevens het laatste hoofdstuk van het onderzoeksrapport, een aanbeveling wordt gegeven. De conclusie en de aanbeveling geven een antwoord op de centrale vraag van het onderzoeksrapport.

Hoofdstuk 2 – De reikwijdte en de beginselen van de AVG

In hoofdstuk 2 wordt, alvorens in te gaan op de verplichtingen van de AVG, in paragraaf 2.1 de reikwijdte van de AVG besproken. In paragraaf 2.2. komen de beginselen van de AVG aan bod. Hiermee wordt (deels) antwoord gegeven op deelvraag 1.

2.1 De reikwijdte van de AVG

Alvorens inhoudelijk in te gaan op de AVG, is van belang om te kijken wanneer de AVG van toepassing is op een organisatie. Om als organisatie te kunnen achterhalen of de AVG op de organisatie van toepassing is, dient allereerst te worden gekeken naar de manier waarop een organisatie persoonsgegevens verwerkt. Zo is de AVG niet van toepassing op elke verwerking van persoonsgegevens. De AVG is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede op de verwerking van de in een bestand opgenomen persoonsgegevens of persoonsgegevens die zijn bestemd om in een bestand te worden opgenomen.¹⁶ Bij een geautomatiseerde verwerking gaat het om een verwerking van persoonsgegevens, waarbij gebruik wordt gemaakt van methoden en middelen van geautomatiseerde gegevensverwerking, zoals het gebruik van een computer.¹⁷ Daartegenover staat de niet geautomatiseerde verwerking, hetgeen inhoudt dat er een handmatige verwerking van persoonsgegevens plaatsvindt, bijvoorbeeld het gebruik van een archiefkast.¹⁸ Naast deze twee vormen, is ook een gedeeltelijke geautomatiseerde verwerking mogelijk, waarbij er zowel gebruik wordt gemaakt van middelen en methoden van geautomatiseerde gegevensverwerking, evenals handmatige verwerking van persoonsgegevens.¹⁹

Kortom, wil een organisatie onder de reikwijdte van de AVG vallen, dan dient er dus sprake te zijn van een (gedeeltelijke) geautomatiseerde verwerking van persoonsgegevens en/of van verwerkte persoonsgegevens die (bestemd) zijn (om te worden) opgenomen in een bestand.

De AVG kent – naast het hiervoor genoemde criterium - het criterium van het toepassingsbereik. De AVG is slechts van toepassing op een organisatie wanneer een organisatie onder het toepassingsbereik van de AVG valt. Om te kunnen bepalen of de verwerking van persoonsgegevens onder het toepassingsbereik van de AVG valt, moet worden vastgesteld of de verwerking van persoonsgegevens valt binnen het materiële- en territoriale toepassingsbereik van de AVG. Het materiële toepassingsbereik gaat over de vraag waarop de AVG van toepassing is. Het territoriale toepassingsbereik gaat over de vraag binnen welk gebied de AVG van toepassing is.²⁰

Ad 1) Het materiële toepassingsbereik van de AVG

De AVG is van toepassing op het verwerken van persoonsgegevens, tenzij er sprake is van een van de uitzonderingen, waarbij de regels niet van toepassing zijn op de verwerking van persoonsgegevens (artikel 2 lid 3 AVG).

¹⁶ Zwenne & Mommers, 2016, p. 182 - 189

¹⁷ *Kamerstukken II 1997/98*, 25892, nr. 3, p. 69 (MvT)

¹⁸ *Kamerstukken II 1997/98*, 25892, nr. 3, p. 69 (MvT)

¹⁹ *Kamerstukken II 1997/98*, 25892, nr. 3, p. 69 (MvT)

²⁰ Schermer, Hagenauw & Falot, 2018, p.28.

De regels van de AVG zijn niet van toepassing op:

- De verwerking van persoonsgegevens in het kader van activiteiten die buiten de werkingssfeer van het Unierecht vallen;
- De verwerking van persoonsgegevens door lidstaten bij de uitvoering van activiteiten voor de openbare veiligheid, de staatsveiligheid, defensie en dergelijke;
- De verwerking van persoonsgegevens door de bevoegde autoriteiten met het oog op het onderzoek, voorkoming, opsporing en vervolging van strafbare feiten of de tenuitvoerlegging van straffen;
- De verwerking van persoonsgegevens door natuurlijke personen bij de uitoefening van een huishoudelijke of persoonlijke activiteit.²¹

Ad 2) Het territoriale toepassingsbereik van de AVG

De AVG geldt niet voor de gehele wereld. De AVG beperkt zich tot de volgende situaties:

- Personen en organisaties, die persoonsgegevens verwerken, en in de Europese Unie zijn gevestigd;
- Personen en organisatie, die gegevens verwerken van personen in de Europese Unie, maar die niet in de Europese Unie zijn gevestigd.²²

2.2 De beginselen van de AVG

Wanneer de AVG op een organisatie van toepassing is, dan dient elke verwerking van persoonsgegevens binnen die organisatie te voldoen aan de beginselen van de AVG. De beginselen van de AVG zijn neergelegd in artikel 5 AVG en worden nader geconcretiseerd in diverse bepalingen uit de AVG.²³

Elke verwerking van persoonsgegevens moet voldoen aan de volgende beginselen:

- Rechtmatigheid, behoorlijkheid en transparantie;
- Doelbinding;
- Minimale gegevensverwerking;
- Juistheid;
- Opslagbeperking;
- Integriteit en vertrouwelijkheid.

De beginselen zijn cumulatief, reden waarom een organisatie bij het verwerken van persoonsgegevens aan alle beginselen moet voldoen. De beginselen worden hieronder toegelicht.

Ad 1) Rechtmatigheid, behoorlijkheid en transparantie

Het uitgangspunt is dat persoonsgegevens slechts mogen worden verwerkt voor gerechtvaardigde doeleinden. De gegevensverwerking is rechtmatig, wanneer deze niet in strijd is met het Europese- en het nationale recht.²⁴

²¹ Zwenne & Mommers, 2016, p. 182 - 189

²² Schermer, Hagenauw & Falot, 2018, p. 29.

²³ Schermer, Hagenauw & Falot, 2018, p. 21.

²⁴ Vermissen, Terstegge & Krijgsman, 2018, p. 55.

De gegevensverwerking is rechtmatig wanneer deze voldoet aan een van de grondslagen voor het verwerken van persoonsgegevens. De grondslagen worden in paragraaf 3.2 weergegeven. Wanneer is geconstateerd dat de gegevensverwerking rechtmatig is, dan moet de gegevensverwerking vervolgens verantwoord worden uitgevoerd. Tot slot moet duidelijk zijn voor welke doeleinden de persoonsgegevens worden verwerkt en op welke wijze dit gebeurt.²⁵

Ad 2) Doelbinding

Het uitgangspunt is dat persoonsgegevens slechts mogen worden verwerkt voor een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel.²⁶ Indien men persoonsgegevens op een andere manier wil gebruiken, dan is dit toegestaan, mits de doeleinden van de verdere verwerking verenigbaar zijn met de oorspronkelijke doeleinden waarvoor de persoonsgegevens zijn verzameld.²⁷

Ad 3) Minimale gegevensverwerking

Het uitgangspunt is dat er niet meer persoonsgegevens worden verwerkt, dan noodzakelijk is voor het doel van de gegevensverwerking.²⁸

Ad 4) Juistheid

Het uitgangspunt is dat de persoonsgegevens correct en actueel zijn. Gegevens die niet correct, dan wel actueel zijn, dienen te worden gecorrigeerd of te worden verwijderd.²⁹ Een 100% juistheid is niet te realiseren. Reden waarom er een afweging mag worden gemaakt over hoe actueel persoonsgegevens moeten zijn, gelet op waarvoor de persoonsgegevens voor worden gebruikt.³⁰

Ad 5) Opslagbeperking

Het uitgangspunt is dat de persoonsgegevens niet langer worden bewaard dan noodzakelijk is voor het doel van de verwerking.³¹

Ad 6) Integriteit en vertrouwelijkheid.

Het uitgangspunt is dat persoonsgegevens worden beschermd tegen onrechtmatige of ongeoorloofde verwerking en tegen onopzettelijk verlies, beschadiging of vernietiging.³²

²⁵ Schermer, Hagenauw & Falot, 2018, p. 22.

²⁶ Schermer, Hagenauw & Falot, 2018, p. 22.

²⁷ Vermissen, Terstegge & Krijgsman, 2018, p. 56.

²⁸ Schermer, Hagenauw & Falot, 2018, p. 22.

²⁹ Schermer, Hagenauw & Falot, 2018, p. 22.

³⁰ Vermissen, Terstegge & Krijgsman, 2018, p. 59.

³¹ Schermer, Hagenauw & Falot, 2018, p. 22.

³² Schermer, Hagenauw & Falot, 2018, p. 22.

Hoofdstuk 3 - De legitieme gegevensverwerking van de AVG

Hoofdstuk 3 gaat in op de grondslagen voor het rechtmatig verwerken van persoonsgegevens. Hiermee wordt antwoord gegeven op deelvraag 1 en deelvraag 2. In paragraaf 3.1 wordt het onderscheid tussen gewone persoonsgegevens en bijzondere persoonsgegevens beschreven. Paragraaf 3.2 beschrijft de grondslagen voor het rechtmatig verwerken van persoonsgegevens. Tot slot wordt in paragraaf 3.3 een deelconclusie gegeven.

3.1 Het onderscheid tussen gewone persoonsgegevens en bijzondere persoonsgegevens

De AVG onderscheidt twee soorten persoonsgegevens: gewone persoonsgegevens en bijzondere categorieën van persoonsgegevens (hierna te noemen: bijzondere persoonsgegevens). Bij gewone persoonsgegevens kan men bijvoorbeeld denken aan de NAW-gegevens van een betrokkene. Bij bijzondere persoonsgegevens kan men bijvoorbeeld denken aan gegevens over iemands gezondheidstoestand. Voor een volledige definitie van de begrippen gewone persoonsgegevens en bijzondere persoonsgegevens, wordt hierbij verwezen naar de begrippenlijst.

3.2 De grondslagen voor het rechtmatig verwerken van persoonsgegevens.

In paragraaf 3.2.1 wordt ingegaan op het rechtmatig verwerken van gewone persoonsgegevens. In paragraaf 3.2.2 wordt ingegaan op het rechtmatig verwerken van bijzondere persoonsgegevens.

3.2.1 Het rechtmatig verwerken van gewone persoonsgegevens

Zoals in paragraaf 2.2 is weergegeven, is een van de beginselen van de AVG dat het verwerken van persoonsgegevens rechtmatig moet zijn, oftewel: het doel voor de verwerking moet rechtvaardig zijn. De gegevensverwerking is gerechtvaardigd, indien het doel van de verwerking kan worden gebaseerd op één van de zes grondslagen van artikel 6 AVG. De grondslagen zijn limitatief. Het aanvoeren van een andere rechtsgrond is dus niet mogelijk. Verder zijn de grondslagen niet cumulatief. Er hoeft slechts aan één van de grondslagen te zijn voldaan om de gegevensverwerking te rechtvaardigen.³³

De AVG kent in artikel 6 de volgende zes grondslagen:

1. Toestemming;
2. Overeenkomst;
3. Wettelijke verplichting;
4. Vitale belangen;
5. Algemeen belang;
6. Gerechtvaardigd belang.

De grondslagen 2 t/m 6 zijn "noodzakelijkheidsgrondslagen", hetgeen inhoudt dat de gegevensverwerking slechts gerechtvaardigd is indien de verwerking noodzakelijk is voor de in de grondslagen genoemde doelen. In de vraag of gegevensverwerking noodzakelijk is, ligt de eis van proportionaliteit en subsidiariteit besloten.

³³ Schermer, Hagenauw & Falot, 2018, p. 36.

De gegevensverwerking dient allereerst proportioneel te zijn: de gegevensverwerking moet effectief zijn, oftewel het moet het gestelde doel kunnen bereiken. Daarnaast moet de gegevensverwerking evenredig zijn, oftewel het nagestreefde legitieme doel moet in verhouding staan tot de daarvoor te verwerken persoonsgegevens.³⁴ Voorts moet de gegevensverwerking voldoen aan het vereiste van subsidiariteit. Het vereiste van subsidiariteit bepaalt dat het doel op de minst ingrijpende wijze moet worden bereikt.³⁵ Ook bij gegevensverwerking op grond van toestemming van de betrokkene moeten de vereisten subsidiariteit en proportionaliteit in acht worden genomen.³⁶

Een organisatie hoeft niet altijd toestemming te vragen aan een betrokkene om persoonsgegevens te verwerken. Wanneer een organisatie kan aantonen dat gegevensverwerking noodzakelijk is op grond van de onder 2 t/m 6 genoemde rechtvaardigingsdoelen, is toestemming van de betrokkene niet vereist.

Hieronder worden de zes grondslagen nader toegelicht.

Ad 1) Toestemming

De gegevensverwerking mag plaatsvinden indien de betrokkene hiervoor toestemming heeft gegeven. De toestemming moet aan een aantal elementen voldoen:

- De toestemming dient vrij te zijn gegeven;
De betrokkene moet de keuze hebben om – zonder negatieve consequenties – te weigeren.
- De toestemming dient geïnformeerd en specifiek te zijn;
De verwerkingsverantwoordelijke moet duidelijk informatie verschaffen over de doeleinden van de gegevensverwerking.
- De toestemming dient ondubbelzinnig te zijn.
Er mag geen twijfel bestaan over de toestemming van de betrokkene. Een vakje kunnen aanvinken leidt bijvoorbeeld tot ondubbelzinnige toestemming.³⁷

Ad 2) Overeenkomst

De gegevensverwerking mag plaatsvinden indien dit noodzakelijk is voor de uitvoering van de overeenkomst. De betrokkene moet zelf partij zijn bij de overeenkomst. De overeenkomst hoeft niet te zijn gericht op het verwerken van persoonsgegevens, maar de gegevensverwerking moet wel een noodzakelijk uitvloeisel zijn.³⁸ Een voorbeeld is dat een arts gezondheidsgegevens verwerkt van zijn patiënt om zo zorg te kunnen verlenen.

Ad 3) Wettelijke verplichting

De gegevensverwerking mag plaatsvinden indien dit noodzakelijk is om aan een wettelijke plicht te kunnen voldoen. Om deze grondslag te kunnen aanwenden, moet het niet mogelijk zijn om aan de wettelijke plicht te kunnen voldoen zonder de gegevensverwerking.

³⁴ Schermer, Hagenauw & Falot, 2018, p. 37.

³⁵ Schermer, Hagenauw & Falot, 2018, p. 37.

³⁶ Schermer, Hagenauw & Falot, 2018, p. 37.

³⁷ Schermer, Hagenauw & Falot, 2018, p. 37.

³⁸ Schermer, Hagenauw & Falot, 2018, p. 38.

De wettelijke plicht moet voorts en grondslag hebben in het recht van de Europese Unie of van de lidstaat.³⁹ Een voorbeeld is dat werkgevers verplicht zijn om een kopie van het identiteitsbewijs van de werknemers te overleggen aan de Belastingdienst.⁴⁰

Ad 4) Vitale belangen

De gegevensverwerking mag plaatsvinden indien dit noodzakelijk is ter bescherming van vitale belangen van de betrokkene of van een ander natuurlijk persoon. De gegevensverwerking op grond van deze grondslag is slechts toegestaan, indien de gegevensverwerking niet op een van de andere grondslagen kan worden gebaseerd. Een voorbeeld is wanneer iemand buiten bewustzijn is, maar men acuut dringend noodzakelijke medische hulp moet verlenen aan de betrokkene.⁴¹

Ad 5) Algemeen belang

De gegevensverwerking mag plaatsvinden indien het noodzakelijk is voor de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen of ter vervulling van een taak in het algemeen belang. De gegevensverwerking moet in dit geval een grondslag hebben in het recht van de Europese Unie of van de lidstaat.⁴² Een voorbeeld is wanneer de gemeente camera's plaats voor cameratoezicht.⁴³

Ad 6) Gerechtvaardigd belang

De gegevensverwerking mag plaatsvinden indien dit noodzakelijk is ter behartiging van het gerechtvaardigd belang van de verwerkingsverantwoordelijke of een derde, mits de vrijheden, rechten en belangen van de betrokkene niet zwaarder wegen. Een voorbeeld is wanneer de gegevensverwerking noodzakelijk is ter voorkoming van fraude.⁴⁴ Een ander voorbeeld is direct marketing. De AP geeft aan dat direct marketing mogelijk is op grond van de grondslag "gerechtvaardigd belang".⁴⁵ Om als organisatie direct marketing te baseren op de grondslag "gerechtvaardigd belang", moet aangetoond worden dat het belang van de organisatie groter is dan het belang van de betrokkene. Wanneer er geen gerechtvaardigd belang is, is direct marketing slechts toegestaan op grond van de grondslag "toestemming".⁴⁶

Van belang om te vermelden is dat het verwerken van het nationaal identificatienummer verboden is, tenzij het verwerken ervan is toegestaan voor bij een in de wet voorgeschreven doel. Een voorbeeld hiervan is de Wet algemene bepalingen Burgerservicenummer of de Wet ter voorkoming van witwassen en financieren van terrorisme.⁴⁷

³⁹ Schermer, Hagenauw & Falot, 2018, p. 38.

⁴⁰ Schermer, Hagenauw & Falot, 2018, p. 38.

⁴¹ Schermer, Hagenauw & Falot, 2018, p. 39.

⁴² Schermer, Hagenauw & Falot, 2018, p. 39.

⁴³ Autoriteit Persoonsgegevens, "Mag u persoonsgegevens verwerken?", bekeken op 13 mei 2018

⁴⁴ Schermer, Hagenauw & Falot, 2018, p. 39.

⁴⁵ Schermer, Hagenauw & Falot, 2018, p.39. & Bijlage IX, Interview mr. E. Luijendijk, p. 124 t/m 139.

⁴⁶ Bijlage IX, Interview mr. E. Luijendijk, p. 124 t/m 139.

⁴⁷ Schermer, Hagenauw & Falot, 2018, p. 26.

3.2.2. Het rechtmatig verwerken van bijzondere persoonsgegevens

Het verwerken van bijzondere persoonsgegevens is in beginsel verboden, tenzij men zich kan beroepen op één van de specifieke voorwaarden van artikel 9 lid 2 AVG én op één van de zes grondslagen voor het verwerken van gewone persoonsgegevens van artikel 6 lid 1 AVG.⁴⁸ Het betreft dus een en-en-situatie.

In hoofdstuk 1 is aangegeven dat het onderzoeksrapport toeziet op het verwerken van gewone persoonsgegevens en het verwerken van bijzondere persoonsgegevens, waarbij wordt gekeken naar het verwerken van gezondheidsgegevens. Reden waarom in het vervolg slechts op de vereisten voor een rechtmatige verwerking van gezondheidspersoonsgegevens wordt ingegaan.

3.2.2.1 De definitie van gezondheidspersoonsgegevens

Alvorens in te gaan op de vereisten voor het rechtmatig verwerken van gezondheidspersoonsgegevens, dient duidelijk te zijn wat de AVG onder gezondheidspersoonsgegevens verstaat. Zoals tevens in de begrippenlijst vermeld, wordt ingevolge artikel 4 lid 15 AVG onder “gegevens over gezondheid” – in het onderzoeksrapport aangeduid als gezondheidspersoonsgegevens – het volgende verstaan: *“persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven.”*.

Gezien deze definitie zouden bijna alle persoonsgegevens over iemands gezondheidstoestand onder gezondheidspersoonsgegevens vallen. Er zijn echter uitzonderingen denkbaar. Zo heeft de Hoge Raad in haar arrest bepaald dat een medisch advies, althans een analyse van gezondheidspersoonsgegevens, geen persoonsgegevens zijn in de zin van de Richtlijn en de Wbp. Hierdoor komen de rechten van betrokkene vanuit de Richtlijn niet aan de betrokkene toe voor wat betreft de medische analyse.⁴⁹ Weliswaar ziet de uitspraak van de Hoge Raad toe op de oude wetgeving, maar gezien de recente datum van de uitspraak kan worden verwacht dat het medisch advies in de zin van een analyse van gezondheidspersoonsgegevens ook niet als persoonsgegevens in de zin van de AVG zal worden aangemerkt.

3.2.2.2 Het rechtmatig verwerken van gezondheidspersoonsgegevens

Het verwerken van gezondheidspersoonsgegevens is in beginsel verboden.⁵⁰ De AVG kent in artikel 9 lid 2 tien verschillende voorwaarden, waarbij bijzondere persoonsgegevens wel mogen worden verwerkt. Ondanks het verwerkingsverbod mogen bijzondere persoonsgegevens (en dus ook gezondheidspersoonsgegevens) worden verwerkt, indien er sprake is van (een):

1. Uitdrukkelijke toestemming van de betrokkene;
2. Noodzakelijke verwerking voor het uitvoeren van regels op het gebied van arbeids- en sociale zekerheidsrecht;

⁴⁸ Schermer, Hagenauw & Falot, 2018, p. 41.

⁴⁹ Gerechtshof Amsterdam, 13 september 2016, ECLI:NL:GHAMS:2016:3739, Hoge Raad, 16 maart 2018, ECLI:NL:HR:2018:365 & Parket bij de Hoge Raad, 12 januari 2018, ECLI:NL:PHR:2018:45.

⁵⁰ Comijs, 2017, p. 4

3. Noodzakelijke verwerking in verband met het beschermen van vitale belangen van de betrokkene dan wel andere natuurlijke personen;
4. Verwerking uitgevoerd door een vereniging, stichting of andere instantie zonder winstoogmerk die werkzaam is op levensbeschouwelijk, politiek, godsdienstig of vakbondsgebied;
5. Verwerking van persoonsgegevens betrekking hebbend op persoonsgegevens die kennelijk zelf door de betrokkene openbaar zijn gemaakt;
6. Noodzakelijke verwerking voor instelling, uitoefening, dan wel onderbouwing van een rechtsvordering;
7. Noodzakelijke verwerking in verband met een zwaarwegend belang;
8. Noodzakelijke verwerking in verband met algemene belangen voor de volksgezondheid;
9. Noodzakelijke verwerking in verband met archivering in algemeen belang, historisch of wetenschappelijk onderzoek of statistische doeleinden.

De UAVG kent aan de bovengenoemde voorwaarden van de AVG specifieke regels, voorwaarden en beperkingen per categorie bijzondere persoonsgegevens toe (artikel 22 en 23 UAVG). Aangezien deze niet van toepassing zijn op KBS, wordt hierop niet nader ingegaan.

Voor een schematisch overzicht wordt hierbij verwezen naar bijlage II

3.3. Deelconclusie

De AVG maakt een onderscheid tussen gewone persoonsgegevens en bijzondere persoonsgegevens. Elke verwerking van persoonsgegevens (zowel gewone als bijzondere persoonsgegevens) binnen een organisatie moet aan de beginselen van artikel 5 lid 1 AVG voldoen, onder meer aan het beginsel van rechtmatigheid. Voor dit beginsel geldt ten aanzien van persoonsgegevens het volgende: Om hieraan te kunnen voldoen, moet het doel van de verwerking van persoonsgegevens binnen een organisatie rechtmatig zijn. Het doel van een verwerking van gewone persoonsgegevens is rechtmatig, indien het doel van de verwerking van gewone persoonsgegevens ten minste aan één van de grondslagen van artikel 6 lid 1 AVG voldoet: toestemming, overeenkomst, wettelijke verplichting, vitale belangen, algemeen belang of gerechtvaardigd belang. Wanneer aan één van deze grondslagen wordt voldaan, is er sprake van een rechtmatige verwerking van gewone persoonsgegevens binnen een organisatie. Wordt niet aan één van de grondslagen voldaan, dan is het verwerken van de desbetreffende gewone persoonsgegevens onrechtmatig en mag deze niet plaatsvinden. Naast dat de verwerking aan een van de zes grondslagen moet voldoen, dient de verwerking te voldoen aan het proportionaliteits- en het subsidiariteitsbeginsel.

Voor wat betreft het rechtmatig verwerken van bijzondere persoonsgegevens geldt het volgende: Op het verwerken van bijzondere persoonsgegevens rust in beginsel ingevolge artikel 9 lid 1 AVG een verwerkingsverbod. Bijzondere persoonsgegevens mogen niet worden verwerkt. Er zijn echter voorwaarden opgesteld en, in het geval daarvan sprake is, mogen bijzondere persoonsgegevens wel worden verwerkt. Zowel de AVG als de UAVG geven voorwaarden voor het verwerken van bijzondere persoonsgegevens.

Het verwerken van bijzondere persoonsgegevens (en dus het verwerken van gezondheidspersoonsgegevens) is toegestaan – en dus rechtmatig – wanneer de verwerking is te baseren op één van de grondslagen voor het verwerken van gewone persoonsgegevens (artikel 6 lid 1 AVG) en op één van de voorwaarden voor het verwerken van bijzondere persoonsgegevens (artikel 9 lid 2 AVG / artikel 22 en 23 UAVG).

Hoofdstuk 4: Verwerkingsverantwoordelijke versus verwerker

In de begrippenlijst zijn de begrippen verwerkingsverantwoordelijke en verwerker al kort benoemd. In paragraaf 4.1 wordt dieper ingegaan op het onderscheid tussen de verwerkingsverantwoordelijke en de verwerker. Het onderscheid is van belang in verband met de (verschillende) verplichtingen voor de verwerkingsverantwoordelijke en de verwerker. Wanneer duidelijk is wie welke verplichting heeft, is duidelijk wie waarvoor verantwoordelijk is. In paragraaf 4.2 worden vervolgens de verplichtingen voor de verwerkingsverantwoordelijke weergegeven en in paragraaf 4.3 de verplichtingen voor de verwerker. In paragraaf 4.1 t/m paragraaf 4.3 wordt antwoord gegeven op deelvraag 3. In paragraaf 4.4 wordt nader ingegaan op de FG en in paragraaf 4.5 op de DPIA. Hiermee wordt antwoord gegeven op deelvraag 4 en deelvraag 5. In paragraaf 4.6 wordt tot slot een deelconclusie gegeven.

4.1 Het onderscheid tussen verwerkingsverantwoordelijke en verwerker

Allereerst wordt ingegaan op de verwerkingsverantwoordelijke, vervolgens de gezamenlijke verwerkingsverantwoordelijken en tot slot de verwerker.

4.1.1 De verwerkingsverantwoordelijke

De verwerkingsverantwoordelijke is een natuurlijk persoon of rechtspersoon (een stichting, bedrijf, overheidsorgaan, etc.), die - tezamen met anderen of alleen - het doel en de middelen voor de verwerking van persoonsgegevens vaststelt.⁵¹ Oftewel de verwerkingsverantwoordelijke is diegene die bepaalt welke persoonsgegevens worden verzameld, voor welk doel persoonsgegevens worden verzameld en op welke manier de verwerking van persoonsgegevens plaatsvindt.⁵²

Bij het beoordelen wie als verwerkingsverantwoordelijke kan worden aangemerkt, kunnen grofweg drie categorieën van elkaar worden onderscheiden:

1. De verwerkingsverantwoordelijkheid op basis van een uitdrukkelijke juridische bevoegdheid;
2. De verwerkingsverantwoordelijkheid op basis van een impliciete bevoegdheid;
3. De verwerkingsverantwoordelijkheid op basis van een feitelijke invloed.⁵³

Ad 1) De verwerkingsverantwoordelijkheid op basis van een uitdrukkelijke juridische bevoegdheid

De situatie van een uitdrukkelijke juridische bevoegdheid doet zich voor wanneer een bepaalde gegevensverwerking expliciet is opgedragen aan de verwerkingsverantwoordelijke, bijvoorbeeld de Belastingdienst bij het verwerken van persoonsgegevens.⁵⁴

Ad 2) De verwerkingsverantwoordelijkheid op basis van een impliciete bevoegdheid

De situatie van een impliciete bevoegdheid doet zich voor wanneer er voor de gegevensverwerking niet expliciet een bevoegdheid bestaat, maar op grond van het maatschappelijk verkeer aan een

⁵¹ Schermer, Hagenauw & Falot, 2018, p.32

⁵² Schermer, Hagenauw & Falot, 2018, p.32

⁵³ Schermer, Hagenauw & Falot, 2018, p.32.

⁵⁴ Schermer, Hagenauw & Falot, 2018, p.32.

natuurlijke persoon of rechtspersoon de verwerkingsverantwoordelijkheid toekomt, bijvoorbeeld de werkgever die de verwerking van gegevens van zijn medewerkers doet.⁵⁵

Ad 3) De verwerkingsverantwoordelijkheid op basis van een feitelijke invloed

De situatie van een feitelijke invloed doet zich voor, wanneer de invloed die partijen kunnen uitoefenen op de verwerking van persoonsgegevens, leidt tot verwerkingsverantwoordelijkheid. Het gaat er hierbij om wie feitelijk bepaalt wat er met persoonsgegevens gebeurt en wie daadwerkelijk de beslissingen neemt. Zo wordt de rechtspersoon aangemerkt als verwerkingsverantwoordelijke, als de persoonsgegevens ten behoeve van de rechtspersoon worden verwerkt. De individuele werknemer kent dan geen verwerkingsverantwoordelijkheid (intern beheer).⁵⁶

4.1.2 De gezamenlijke verwerkingsverantwoordelijken

Wanneer de verwerkingsverantwoordelijke het doel en de middelen samen met anderen bepaalt, dan spreekt men van gezamenlijke verantwoordelijkheid.⁵⁷ Een voorbeeld hiervan is wanneer een fitnessbedrijf en een computerfabrikant samen een smartwatch ontwikkelen, die de gezondheidsgegevens registreert en beide partijen samen bepalen waarom en hoe de gezondheidsgegevens worden verwerkt.⁵⁸

4.1.3 De verwerker

Een verwerkingsverantwoordelijke schakelt vaak organisaties of personen in die persoonsgegevens voor hen verwerken. Wanneer men persoonsgegevens verwerkt ten behoeve van een verwerkingsverantwoordelijke, zonder dat men aan diens rechtstreekse gezag is onderworpen, dan spreekt men van een verwerker.⁵⁹

Om te kunnen spreken van het verwerken van persoonsgegevens ten behoeve van de verwerkingsverantwoordelijke (ook wel verwerkerschap genoemd), zijn er concreet drie vereisten:

1. De verwerking van persoonsgegevens vindt plaats ten behoeve van de verwerkingsverantwoordelijke (primaire opdracht);
2. Degene die persoonsgegevens verwerkt heeft geen zeggenschap over de verwerking;
3. De verwerker is niet onderworpen aan het rechtstreekse gezag van de verwerkingsverantwoordelijke of aan een andere hiërarchische verhouding.⁶⁰

Ad 1) De verwerking van persoonsgegevens vindt plaats ten behoeve van de verwerkingsverantwoordelijke (primaire opdracht).

De verwerking van persoonsgegevens moet de primaire opdracht betreffen. Oftewel: de dienstverlening moet erop zijn gericht om de persoonsgegevens te verwerken ten behoeve van de verwerkingsverantwoordelijke.

⁵⁵ Schermer, Hagenauw & Falot, 2018, p.32.

⁵⁶ Schermer, Hagenauw & Falot, 2018, p.32.

⁵⁷ Schermer, Hagenauw & Falot, 2018, p.32.

⁵⁸ Schermer, Hagenauw & Falot, 2018, p.32.

⁵⁹ Schermer, Hagenauw & Falot, 2018, p.33.

⁶⁰ Schermer, Hagenauw & Falot, 2018, p.33.

Wanneer het verwerken van persoonsgegevens niet de primaire opdracht is, maar een uitvloeisel van een andere vorm van dienstverlening, dan is men als dienstverlener zelf de verwerkingsverantwoordelijke voor deze verwerking en niet de verwerker.⁶¹ Kortom, het enkele feit dat men van de verwerkingsverantwoordelijke een opdracht krijgt, is onvoldoende om te kunnen spreken van verwerkerschap. De opdracht moet gericht zijn op het verwerken van persoonsgegevens.

Een voorbeeld ter verduidelijking: Een administratiekantoor doet de salarisadministratie namens een bedrijf. In dat geval is de opdracht aan het administratiekantoor om de salarisadministratie uit te voeren, hetgeen inhoudt dat zij de persoonsgegevens van de medewerkers moeten verwerken. In dat geval is het administratiekantoor de verwerker en is diegene die de opdracht verstrekt de verwerkingsverantwoordelijke.⁶²

Ad 2) Degene die persoonsgegevens verwerkt heeft geen zeggenschap over de verwerking.

De verwerker mag geen zeggenschap hebben over de verwerking. De verwerker mag slechts handelen onder de verantwoordelijkheid van de verwerkingsverantwoordelijke en naar diens instructies. Wanneer de verwerker zelfstandig beslissingen neemt over doelen van de verwerking en de middelen, dan wordt de verwerker zelf verantwoordelijk voor de verwerking en is men zelf verwerkingsverantwoordelijke.

Een voorbeeld ter verduidelijking: De zorgaanbieders leveren in opdracht van de gemeente zorg. De zorgaanbieder handelt hier weliswaar in opdracht van de gemeente, maar zij bepaalt zelf het doel en de middelen voor de concrete invulling van de zorgtaken. De zorgaanbieder is dan zelf de verwerkingsverantwoordelijke.⁶³

Ad 3) De verwerker is niet onderworpen aan het rechtstreekse gezag van de verwerkingsverantwoordelijke of aan een andere hiërarchische verhouding.

Men mag niet ondergeschikt zijn aan de verwerkingsverantwoordelijke, bijvoorbeeld in het geval van detachering of werknemerschap. In dat geval is er sprake van intern beheer⁶⁴

Voor een schematisch overzicht wordt hierbij verwezen naar bijlage III.

4.2 De verplichtingen voor de verwerkingsverantwoordelijke

Zoals in hoofdstuk 2 is aangegeven, kent de AVG een aantal beginselen. Elke verwerking van persoonsgegevens moet aan deze beginselen voldoen. De verantwoordelijkheid om aan de beginselen te voldoen én om aan te tonen dat aan de beginselen is voldaan, ligt bij de verwerkingsverantwoordelijke. Kortom, de verwerkingsverantwoordelijke heeft een verantwoordingsplicht voor het naleven van de AVG, ook wel accountability genoemd.⁶⁵

⁶¹ Schermer, Hagenauw & Falot, 2018, p.33.

⁶² Schermer, Hagenauw & Falot, 2018, p.33.

⁶³ Schermer, Hagenauw & Falot, 2018, p.33.

⁶⁴ Schermer, Hagenauw & Falot, 2018, p.33.

⁶⁵ Vermissen, Terstegge & Krijgsman, 2018, p. 38.

De verantwoordingsplicht komt neer op vier verplichtingen voor de verwerkingsverantwoordelijke, namelijk:

- Waarborgen dat de verwerking in overeenstemming met de AVG worden uitgevoerd;
- Kunnen aantonen dat de verwerking in overeenstemming met de AVG worden uitgevoerd;
- Passende technische en organisatorische maatregelen nemen om de verwerking te waarborgen;
- De genomen passende technische en organisatorische maatregelen evalueren en actualiseren.⁶⁶

Het is raadzaam om de genomen maatregelen op te nemen binnen een privacybeleid.⁶⁷

Om invulling te geven aan de verantwoordingsplicht, geeft de AVG concrete eisen waaraan een verwerkingsverantwoordelijke onder bepaalde voorwaarden moet voldoen, namelijk:

- Registerplicht;
- Functionaris voor de Gegevensbescherming (FG);
- Gegevensbeschermingseffectbeoordeling (DPIA);
- Voorafgaande raadpleging;
- Privacy door ontwerp en standaardinstellingen (privacy by design en privacy by default);
- Beveiligingsmaatregelen;
- Meldplicht datalekken;
- Afspraken met verwerkers.⁶⁸

De verplichtingen voor de verwerkingsverantwoordelijke worden hieronder beschreven. Zoals in hoofdstuk 1 van het onderzoeksrapport is beschreven, heeft KBS onder andere behoefte aan een expliciete voorlichting over de verplichtingen van de FG en de DPIA. Reden waarom hieronder allereerst kort op alle verplichtingen wordt ingegaan en vervolgens FG in paragraaf 4.4 en de DPIA in paragraaf 4.5 nader worden beschreven.

Ad 1) Registerplicht

Ingevolge artikel 30 AVG dient de verwerkingsverantwoordelijke, om aantoonbaar te kunnen maken dat aan de verplichtingen van de AVG wordt voldaan, een register bij te houden van de verwerkingsactiviteiten waarvoor men verantwoordelijk is. Het register van verwerkingsactiviteiten betreft een op schrift gestelde opsomming van de belangrijkste informatie over het verwerken van persoonsgegevens, waarin in ieder geval de contactgegevens van de organisatie (en de FG) moeten worden vermeld, evenals de verwerkingsdoeleinden, de verschillende soorten persoonsgegevens die worden verwerkt, de betrokkenen en ontvangers, informatie over doorgifte van persoonsgegevens aan andere landen, de bewaartermijn van de persoonsgegevens en een beschrijving van de beveiliging van de persoonsgegevens.⁶⁹

⁶⁶ Vermissen, Terstegge & Krijgsman, 2018, p. 38.

⁶⁷ Schermer, Hagenauw & Falot, 2018, p. 51.

⁶⁸ Schermer, Hagenauw & Falot, 2018, p. 51.

⁶⁹ Schermer, Hagenauw & Falot, 2018, p. 52.

Elke organisatie is verplicht om een register bij te houden, tenzij het een organisatie betreft met minder dan 250 personen in dienst. In dat geval geldt geen verplichting om een register bij te houden, tenzij één van de volgende situaties zich voordoet:

- De verwerking van persoonsgegevens brengt een hoog risico mee voor betrokkenen;
- Er vindt een verwerking van bijzondere persoonsgegevens plaats, dan wel een verwerking van gegevens betreffende strafbare feiten of strafrechtelijke veroordelingen.⁷⁰

Ad 2) Functionaris voor Gegevensbescherming

De AVG verplicht verwerkingsverantwoordelijken en verwerkers om in bepaalde gevallen een FG aan te wijzen.⁷¹ In paragraaf 4.4 wordt nader ingegaan op de FG.

Ad 3) DPIA

De verwerkingsverantwoordelijke is ingevolge artikel 35 AVG verplicht om voorafgaand aan het verwerken van persoonsgegevens een DPIA uit te voeren, indien er sprake is van een hoog risico voor de vrijheden en rechten van betrokkenen.⁷² De DPIA staat voor Data Protection Impact Assessment en wordt ook wel Privacy Impact Assessment (PIA) of gegevensbeschermingseffectbeoordeling genoemd. In paragraaf 4.5 wordt nader ingegaan op de DPIA.

Ad 4) Voorafgaande raadpleging

Wanneer uit een DPIA blijkt dat er een hoog risico voor betrokkenen is én het risico niet kan worden weggenomen door het treffen van maatregelen, dan moet de verwerkingsverantwoordelijke ingevolge artikel 36 AVG de verwerking bij de AP voorleggen. De AP moet vervolgens een positief oordeel uitbrengen, voordat een organisatie mag beginnen aan de verwerking.⁷³

Ad 5) Privacy door ontwerp en standaardinstellingen (privacy by design en privacy by default)

In de praktijk worden privacymaatregelen vaak pas aan het einde van ontwerpproces van nieuwe producten, processen en diensten meegenomen.⁷⁴ Om dit voortaan te voorkomen hanteert de AVG het beginsel van privacy door ontwerp en door standaardinstellingen, in de praktijk ook wel Privacy by Design en Privacy by Default genoemd. Kort gezegd houdt dit in dat de verwerkingsverantwoordelijke vanaf het begin van het ontwerpproces van nieuwe systemen of nieuw beleid de gegevensbescherming en privacy meeneemt, door over de benodigde technische en organisatorische maatregelen na te denken en deze in te bouwen in de nieuwe processen en systemen. De verwerkingsverantwoordelijke moet ervoor zorgen dat er een zo klein mogelijke inbreuk wordt gemaakt op de persoonlijke levenssfeer van betrokkenen.⁷⁵

⁷⁰ Schermer, Hagenauw & Falot, 2018, p. 52.

⁷¹ Groep Gegevensbescherming Artikel 29, 2017, p. 6.

⁷² Schermer, Hagenauw & Falot, 2018, p. 54

⁷³ Schermer, Hagenauw & Falot 2018, p. 60

⁷⁴ Vermissen, Terstegge & Krijgsman, 2018, p. 46.

⁷⁵ Schermer, Hagenauw & Falot 2018, p. 61

Ad 6) Beveiligingsmaatregelen

Ingevolge artikel 32 AVG is de verwerkingsverantwoordelijke verplicht om verwerkte persoonsgegevens te beveiligen. Hiertoe moeten passende organisatorische en technische maatregelen worden genomen. De maatregelen moeten een op het risico afgestemd beschermingsniveau waarborgen.

Ad 7) Meldplicht datalekken

Een datalek is een inbreuk op de beveiliging, die leidt tot verlies, wijziging, vernietiging, ongeoorloofde toegang tot of verstrekking van opgeslagen of op een andere manier verwerkte gegevens.⁷⁶ De verwerkingsverantwoordelijke is ingevolge artikel 33 AVG verplicht om elke datalek bij te houden in een register, waarin de details worden genoemd, evenals de gevolgen voor de betrokkene en de corrigerende maatregelen die zijn genomen.⁷⁷ De meldplicht datalekken van de AVG houdt in dat de verwerkingsverantwoordelijke in beginsel alle datalekken moet melden aan de AP en, in sommige gevallen, aan de betrokkene.

Een datalek moet binnen 72 uur, nadat de verwerkingsverantwoordelijke bekend is geworden met een datalek, worden gemeld aan de AP, tenzij een datalek geen risico's met zich meebrengt voor de vrijheden en rechten van betrokkenen.⁷⁸ Het risico is per geval verschillend en zal dan ook per geval moeten worden bekeken.

Ingevolge artikel 34 AVG moet een datalek, naast de melding aan de AP, ook worden gemeld aan de betrokkene, indien het datalek een hoog risico voor de vrijheden en rechten van de betrokkene met zich meebrengt.⁷⁹ Een datalek hoeft niet aan een betrokkene te worden gemeld, indien:

- De persoonsgegevens zijn versleuteld;
- Het verhoogde risico doet zich niet meer voor door de achteraf genomen maatregelen;
- Het melden brengt een onevenredige inspanning met zich mee.⁸⁰

Ad 8) Afspraken met verwerkers

Indien de verwerkingsverantwoordelijke gebruikmaakt van verwerkers, dan moet de verwerking geregeld zijn in een schriftelijke overeenkomst of andere bindende rechtshandeling.⁸¹ In de verwerkingsovereenkomst moet ingevolge artikel 28 AVG in ieder geval het volgende zijn geregeld:

- De onderwerpen, duur en doeleinden van de verwerking;
- De verschillende soorten persoonsgegevens;
- De plichten en rechten van de verwerkingsverantwoordelijke;
- De waarborging dat slechts gemachtigde personen toegang hebben tot de gegevens;
- De mogelijke ondersteuning bij verzoeken van betrokkenen;
- De bijstand bij eventuele datalekken;
- De regeling wat er gebeurt na het beëindigen van de verwerkingsovereenkomst;

⁷⁶ Vermissen, Terstegge & Krijgsman, 2017, p. 49

⁷⁷ Vermissen, Terstegge & Krijgsman, 2017, p. 50

⁷⁸ Vermissen, Terstegge & Krijgsman, 2017, p. 50

⁷⁹ Vermissen, Terstegge & Krijgsman, 2017, p. 51

⁸⁰ Vermissen, Terstegge & Krijgsman, 2017, p. 51

⁸¹ Schermer, Hagenauw & Falot, 2018, p. 66.

- De benodigde informatie wordt aantoonbaar gemaakt;
- De eventuele afspraken met subverwerkers.⁸²

4.3 De verplichtingen voor de verwerker

Aangezien de verwerkingsverantwoordelijke het doel en de middelen voor de verwerking bepaalt, is de AVG voor het merendeel van de verplichtingen op de verwerkingsverantwoordelijke gericht. In de onderlinge verhouding tussen verwerkingsverantwoordelijke en verwerker betekent dit dat de verwerker op basis van de instructies van de verwerkingsverantwoordelijke handelt. Hierdoor heeft de verwerker bij het helpen van het uitvoeren ook te maken met sommige van de plichten. Daarnaast zijn er enkele plichten die zelfstandig aan de verwerker zelf toekomen.⁸³

De AVG kent de volgende verplichtingen toe aan de verwerkers van persoonsgegevens:

- Het uitsluitend handelen in opdracht van de verwerkingsverantwoordelijke;
- Het bijhouden van een overzicht van alle persoonsgegevens die ten behoeve van de verwerkingsverantwoordelijke worden verwerkt (registerplicht);
- Het treffen van passende organisatorische en technische beveiligingsmaatregelen met het oog op het risico van gegevensverwerking voor betrokkenen;
- De verwerker is niet bevoegd tot het inschakelen van sub-verwerkers zonder toestemming van de verwerkingsverantwoordelijke;
- De verwerkingsverantwoordelijke onverwijld op de hoogte te brengen van een datalek;
- Het meewerken aan een verzoek van de AP in het kader van de uitoefening van de taken van de AP;
- Het in bepaalde gevallen aanstellen van een FG.⁸⁴

4.4 De functionaris voor de gegevensbescherming

Ingevolge artikel 37 AVG is de verwerkingsverantwoordelijke onder bepaalde omstandigheden verplicht een Functionaris voor Gegevensbescherming (hierna te noemen: FG) aan te stellen. De FG adviseert over de toepassing en naleving van de AVG binnen een organisatie, houdt intern toezicht op de naleving van de AVG binnen de organisatie en is het aanspreekpunt voor betrokkenen.⁸⁵

Ingevolge artikel 37 AVG moeten organisaties een FG aanstellen als de organisatie aan minstens één van de volgende drie voorwaarden voldoet:

- Het betreft een overheidsorganisatie;
- Het betreft een organisatie die hoofdzakelijk is belast met verwerkingen, die vanwege hun omvang, aard en/of hun doeleinden, regelmatige, grootschalige en stelselmatige observatie op grote schaal van betrokkenen vereist;
- Het betreft een organisatie die hoofdzakelijk is belast met grootschalige verwerking van strafrechtelijke of bijzondere persoonsgegevens.

⁸² Schermer, Hagenauw & Falot, 2018, p. 67.

⁸³ Schermer, Hagenauw & Falot, 2018, p. 69.

⁸⁴ Schermer, Hagenauw & Falot, 2018, p. 16.

⁸⁵ Schermer, Hagenauw & Falot, 2018, p. 53.

Ad 1) Het betreft een overheidsorganisatie

Ingevolge 37 lid 1 sub a AVG is iedere overheidsorgaan- of instantie verplicht tot het aanstellen van een FG. Hierbij moet men denken aan de rijksoverheid, gemeenten en provincies. Gerechten hoeven geen FG aan te stellen.⁸⁶

Ad 2) Het betreft een organisatie die hoofdzakelijk is belast met verwerkingen, die vanwege hun omvang, aard en/of hun doeleinden, regelmatige, grootschalige en stelselmatige observatie op grote schaal van betrokkenen vereist

De verwerkingsverantwoordelijke is verplicht tot het aanstellen van een FG, wanneer hij hoofdzakelijk belast is met verwerken van persoonsgegevens, die bestaan uit het stelselmatig en regelmatig observeren van betrokkenen op grote schaal.

Met "hoofdzakelijk belast" wordt bedoeld op het kernactiviteiten. De Groep Gegevensbescherming Artikel 29 (hierna te noemen: Artikel 29 Werkgroep), het samenwerkingsverband van Europees toezichthouders, heeft het begrip kernactiviteiten gedefinieerd als de processen die tot de hoofdtaken van de organisatie horen of die essentieel zijn voor het bereiken van de doelen van de organisatie.⁸⁷ Bij een "kernbezigheid" gaat het niet alleen om de dingen dat een organisatie doet, maar ook om wat daarmee onlosmakelijk is verbonden. Zo is bij een ziekenhuis de kernbezigheid het behandelen van patiënten, maar het bijhouden van een medisch dossier is daarmee onlosmakelijk verbonden.⁸⁸

Voor wat betreft "regelmatige en stelselmatige observatie" wordt bedoeld op een planmatig, systematisch of strategische observatie, die herhaald of continu plaatsvindt. Het begrip moet breed worden opgevat. Zo valt het profileren en volgen van internetgebruikers hieronder, evenals het aanbieden van telecommunicatiediensten, klantenkaarten, controleren van welzijn en beveiligingscamera's.⁸⁹

Ad 3) Het betreft een organisatie die hoofdzakelijk is belast met grootschalige verwerking van strafrechtelijke of bijzondere persoonsgegevens

De verwerkingsverantwoordelijke is verplicht tot het aanstellen van een FG als de van de organisatie hoofdzakelijk is belast met het grootschalig verwerken van persoonsgegevens van strafrechtelijke aard of bijzondere categorieën persoonsgegevens.⁹⁰

Wat er moet worden verstaan onder "hoofdzakelijk belast" is onder ad 2 weergegeven en verschilt bij het derde criterium niet van betekenis. De AVG geeft verder geen definitie van wat er moet worden verstaan onder "verwerking op grote schaal". De verwerkingsverantwoordelijke moet zelf oordelen of er sprake is van een verwerking op grote schaal.

⁸⁶ Schermer, Hagenauw & Falot, 2018, p. 53.

⁸⁷ Schermer, Hagenauw & Falot, 2018, p. 54.

⁸⁸ Groep Gegevensbescherming Artikel 29, 2017a, P. 10.

⁸⁹ Groep Gegevensbescherming Artikel 29, 2017a, p. 8.

⁹⁰ Schermer, Hagenauw & Falot, 2018, p. 54.

Om dit te kunnen beoordelen, adviseert Artikel 29 Werkgroep om te kijken naar de volgende criteria:

- Het aantal betrokkenen;
- De hoeveelheid aan verwerkte persoonsgegevens;
- Het permanente karakter of de duur van het verwerken van persoonsgegevens;
- De omvang van de verwerking van persoonsgegevens.⁹¹

Artikel 29 Werkgroep geeft een voorbeeld: zo is een ziekenhuis grootschalig, maar een solistische huisarts niet. Daartussen ligt een grijs gebied.⁹² Dit gebied zal nog nader door de Europese toezichthouders worden ingevuld. Nu moet iedereen zelf een afweging maken, zo bijvoorbeeld ook de Landelijke Huisartsenvereniging (hierna te noemen: LHV). Zij adviseert haar leden dat zij geen FG hoeven aan te stellen, omdat zij – gelet op het aantal patiënten in vergelijking met het aantal patiënten van een ziekenhuis – niet op grootschalige wijze bijzondere persoonsgegevens verwerken.⁹³

Opmerking verdient dat de AP uiteindelijk met duidelijkere criteria zal komen over de invulling van de criteria voor het aanstellen van een FG.⁹⁴ De AP zal in de loop der tijd meer toelichtingen publiceren, zo heeft de AP op 31 mei 2018 al een toelichting gegeven over de invulling van de criteria voor het aanstellen van een FG, waarin onder andere is bepaald dat een gegevensverwerking van gezondheidspersoonsgegevens als grootschalig valt aan te merken, wanneer de gezondheidspersoonsgegevens van meer dan 10.000 patiënten of meer worden verwerkt.⁹⁵

Wanneer een organisatie niet verplicht is om een FG aan te stellen, dan mag zij dit wel vrijwillig doen.⁹⁶ Wanneer een organisatie een FG vrijwillig aanstelt, moet de FG wel aan dezelfde eisen voldoen als wanneer een FG verplicht wordt aangesteld. Wanneer een organisatie of een bedrijf concludeert geen FG nodig te hebben en ook niet vrijwillig een FG aanstelt, dan is het verstandig om de redenering goed te documenteren, voor het geval de AP vragen stelt.⁹⁷

Een FG moet – zowel bij een verplichte als een vrijwillige aanstelling – gekwalificeerd zijn, kennis hebben van de organisatie en haar gegevenswerkende processen en verstand hebben van privacywetgeving om de hieronder genoemde taken uit te voeren. De FG heeft in ieder geval ingevolge artikel 39 AVG de volgende taken:

- Het informeren en adviseren over wet- en regelgeving over privacy;
- Het toezien op de naleving van de privacywet- en regelgeving en het interne beleid en op de uitvoering van de DPIA's;
- Het fungeren als een aanspreekpunt voor betrokkenen en de AP.

⁹¹ Schermer, Hagenauw & Falot, 2018, p. 54

⁹² Groep Gegevensbescherming Artikel 29, 2017a, p. 7.

⁹³ Landelijke Huisartsen Vereniging, "Analyse LHV: Functionaris Gegevensbescherming voor meeste praktijken niet noodzakelijk", bekeken op 20 mei 2018

⁹⁴ Kamerstukken II 2017/18, 34 851, nr. 21

⁹⁵ Autoriteit Persoonsgegevens, "AP geeft uitleg over grootschalige gegevensverwerking in de zorg", bekeken op 7 juni 2018

⁹⁶ Schermer, Hagenauw & Falot, 2018, p. 54

⁹⁷ Groep Gegevensbescherming Artikel 29, 2017a, p. 4.

De FG moet een onafhankelijke positie hebben, waarbij er dus geen instructies voorafgaand aan de FG worden gegeven en de FG achteraf geen nadeel ondervindt van anderen bij de door haar ingenomen standpunten. Tot slot moet de FG aan de hoogste leidinggevende in de organisatie een verslag uitbrengen. De verantwoordelijke blijft immers verantwoordelijk voor de het naleven van de AVG en dus niet de FG.

Tot slot is van belang om op te merken dat elke organisatie iemand (in de organisatie) zal moeten aanwijzen, die toeziet op de privacy binnen de organisatie. Een betrokkene moet immers weten tot wie hij zich moeten wenden, als hij gebruik wil maken van zijn rechten. Hierdoor is het verstandig om als organisatie – ook in het geval waarin zij niet is verplicht om een FG aan te stellen – iemand in de organisatie te benoemen als contactpersoon. Dit kan de keuze zijn voor een vrijwillige FG, maar kan bijvoorbeeld ook een privacyofficer zijn.

4.5 De gegevensbeschermingseffectbeoordeling (DPIA)

Ingevolge artikel 35 AVG is de verwerkingsverantwoordelijke verplicht om voorafgaand aan het verwerken van persoonsgegevens een DPIA uit te voeren. Door het voorafgaand uitvoeren van een DPIA kunnen de effecten van de gegevensverwerking voor betrokkenen in kaart worden gebracht en worden beoordeeld.⁹⁸ Op basis hiervan kunnen vervolgens maatregelen worden genomen om de effecten voor betrokkenen weg te nemen dan wel te verkleinen.

Organisaties hoeven niet voor elke gegevensverwerking een DPIA uit te voeren. Een organisatie hoeft enkel een DPIA uit te voeren, als een gegevensverwerking waarschijnlijk een hoog privacyrisico voor de betrokkene oplevert.⁹⁹ Hiervan is in ieder geval sprake, wanneer een organisatie:

- Persoonlijke aspecten systematisch en uitvoerig evalueert, waaronder profilering;
- Het op grote schaal verwerken van bijzondere persoonsgegevens;
- Het op grote schaal en systematisch volgen van mensen in een publiek toegankelijk gebied.¹⁰⁰

Artikel 29 Werkgroep heeft criteria opgesteld om te kunnen beoordelen of er sprake is van een hoog risico. Als vuistregel kan men hanteren dat een organisatie een DPIA moet uitvoeren, wanneer de verwerking aan twee of meer van de onderstaande negen criteria voldoet:

1. Het beoordelen van mensen op basis van persoonskenmerken;
2. Het nemen van geautomatiseerde beslissingen;
3. Het stelselmatig en grootschalig monitoren;
4. Het verwerken van gevoelige gegevens;
5. Het grootschalig verwerken van persoonsgegevens;
6. Het hebben van gekoppelde databases;
7. Het verwerken van gegevens van kwetsbare personen;
8. Het gebruikmaken van nieuwe technologieën;

⁹⁸ Schermer, Hagenauw & Falot, 2018, p. 54

⁹⁹ Schermer, Hagenauw & Falot, 2018, p. 54

¹⁰⁰ Schermer, Hagenauw & Falot, 2018, p. 54

9. Het blokkeren van een contract, dienst of recht.¹⁰¹

Ad 1) Het beoordelen van mensen op basis van persoonskenmerken

De AVG doelt hierbij onder meer op profilering en het maken van prognoses op basis van kenmerken, zoals iemands economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen en beroepsprestaties.¹⁰²

Voorbeeld: Een bedrijf dat profielen van mensen opstelt aan de hand van de bezoeker van de website.

Ad 2) Het nemen van geautomatiseerde beslissingen

De AVG doelt hierbij op beslissingen die rechtsgevolgen hebben voor de betrokkene. Gegevensverwerkingen met een gering of geen gevolg vallen hier niet onder.

Voorbeeld: Gegevensverwerking kan ertoe leiden dat iemand wordt gediscrimineerd.¹⁰³

Ad 3) Het stelselmatig en grootschalig monitoren

De AVG doelt hierbij op het monitoren van openbaar toegankelijke ruimten, waarbij persoonsgegevens worden verzameld zonder dat de betrokkene hiervan afweet.¹⁰⁴

Voorbeeld: Cameratoezicht.

Ad 4) Het verwerken van gevoelige gegevens

De AVG doelt hierbij op bijzondere persoonsgegevens, zoals in artikel 9 AVG, en strafrechtelijke persoonsgegevens, zoals in artikel 10 AVG.¹⁰⁵

Voorbeeld: Persoonsgegevens over iemands ras.

Ad 5) Het grootschalig verwerken van persoonsgegevens

De AVG voorziet niet in een definitie van grootschalig. Zie hiervoor paragraaf 4.4.

Ad 6) Het hebben van gekoppelde databases

De AVG doelt hierbij op gegevensverzamelingen, die aan elkaar kunnen worden gekoppeld of met elkaar kunnen worden gecombineerd.¹⁰⁶

Voorbeeld: twee of meer verschillende gegevensverwerkingen met verschillende doeleinden en uitgevoerd door verschillende verwerkingsverantwoordelijken worden aan elkaar gekoppeld op een manier die voor een betrokkene niet is te verwachten.

¹⁰¹ Groep gegevensbescherming artikel 29, 2017b, p. 10.

¹⁰² Groep gegevensbescherming artikel 29, 2017b, p. 10.

¹⁰³ Groep gegevensbescherming artikel 29, 2017b, p. 11.

¹⁰⁴ Groep gegevensbescherming artikel 29, 2017b, p. 11.

¹⁰⁵ Groep gegevensbescherming artikel 29, 2017b, p. 11.

¹⁰⁶ Groep gegevensbescherming artikel 29, 2017b, p. 12.

Ad 7) Het verwerken van gegevens van kwetsbare personen

De AVG doelt hierbij op een ongelijke machtsverhouding tussen de betrokkene en de verwerkingsverantwoordelijke met het gevolg dat de betrokkene niet in al haar vrijheid toestemming zou kunnen geven of weigeren voor het verwerken van persoonsgegevens.¹⁰⁷

Voorbeeld: werknemers, kinderen, patiënten, etc.

Ad 8) Het gebruikmaken van nieuwe technologieën

De AVG doelt hierbij op nieuwe manieren waarmee gegevens worden verzameld en gebruikt met mogelijk grote privacyrisico's als gevolg. Een DPIA kan inzicht geven in het risico van een nieuwe manier.¹⁰⁸

Ad 9) Het blokkeren van een contract, dienst of recht

De AVG doelt hierbij op gegevensverwerkingen, waarbij betrokkene een recht niet kan uitoefenen, een contract niet kan afsluiten of een dienst niet kan gebruiken.

Voorbeeld: Bank wil persoonsgegevens van iemand verzamelen om al dan niet te kunnen vaststellen of zij een lening aan diegene verstrekken.¹⁰⁹

Opmerking verdient dat de AP uiteindelijk met een lijst van verwerkingen zal komen, waarvoor een DPIA verplicht is.¹¹⁰ Tot op heden is deze lijst nog niet bekend.

Wanneer een organisatie niet aan twee of meer van de negen criteria voldoet, hoeft een organisatie in beginsel geen DPIA uit te voeren. Echter, ondanks dat een DPIA niet verplicht is, moet een organisatie in het kader van de verantwoordingsplicht alsnog goed kunnen onderbouwen waarom zij geen DPIA uitvoert.¹¹¹

Indien een organisatie heeft geconstateerd dat het uitvoeren van een DPIA noodzakelijk, dan wel raadzaam is, dan dient de DPIA te resulteren in een beschrijving van de verwerking en de doeleinden voor die verwerking, een oordeel over de noodzaak en evenredigheid van de verwerking ten opzichte van het vastgestelde doel, een oordeel over de risico's voor de betrokkene en de noodzakelijke maatregelen om de risico's voor betrokkene weg te nemen.¹¹²

4.6 Deelconclusie

Het onderscheid tussen de verwerkingsverantwoordelijke en de verwerker is van belang in verband met de positie omtrent de verantwoordelijkheid voor het naleven van de AVG.

¹⁰⁷ Groep gegevensbescherming artikel 29, 2017b, p. 12.

¹⁰⁸ Groep gegevensbescherming artikel 29, 2017b, p. 12.

¹⁰⁹ Groep gegevensbescherming artikel 29, 2017b, p. 12.

¹¹⁰ *Kamerstukken II 2017/18*, 34 851, nr. 21

¹¹¹ Groep gegevensbescherming artikel 29, 2017b, p. 13.

¹¹² Schermer, Hagenauw & Falot, 2018, p. 59.

De verwerkingsverantwoordelijke is diegene die bepaalt welke persoonsgegevens er worden verzameld, voor welk doel persoonsgegevens worden verzameld en op welke manier de verwerking van de persoonsgegevens plaatsvindt. De rol van verwerkingsverantwoordelijke kan worden toegewezen aan de hand van een juridische bevoegdheid, een impliciete bevoegdheid of een feitelijke invloed.

Op de verwerkingsverantwoordelijke rust een verantwoordingsplicht. Om invulling te geven aan de verantwoordingsplicht, geeft de AVG concrete eisen waaraan een verwerkingsverantwoordelijke onder bepaalde voorwaarden aan moet voldoen, namelijk:

- Registerplicht;
- Functionaris voor de Gegevensbescherming (FG);
- Gegevensbeschermingseffectbeoordeling (DPIA);
- Voorafgaande raadpleging;
- Privacy door ontwerp en standaardinstellingen (privacy by design en privacy by default);
- Beveiligingsmaatregelen;
- Meldplicht datalekken;
- Afspraken met verwerkers.

De verwerker is degene die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. Hierbij dient het verwerken van de persoonsgegevens de primaire opdracht te zijn en niet een uitvloeisel van een andere opdracht. Voorts dient de verwerker geen zeggenschap te hebben over de verwerking. De zeggenschap ligt bij de verwerkingsverantwoordelijke. Tot slot is de verwerker niet onderworpen aan het rechtstreekse gezag van de verwerkingsverantwoordelijke.

De verwerkingsverantwoordelijke is onder bepaalde voorwaarden verplicht om een FG aan te stellen en/of een DPIA uit te voeren. Hieraan is in het onderzoek meer aandacht besteed.

Een FG is een functionaris die toeziet op de privacy binnen een organisatie. Een verwerkingsverantwoordelijke is verplicht om een FG aan te stellen, wanneer een organisatie een overheidsorganisatie betreft, de organisatie hoofdzakelijk is belast met verwerkingen, die vanwege hun omvang, aard en/of hun doeleinden, regelmatige, grootschalige en stelselmatige observatie op grote schaal van betrokkenen vereist, of wanneer de organisatie hoofdzakelijk is belast met grootschalige verwerking van strafrechtelijke of bijzondere persoonsgegevens. De AVG geeft tot op heden geen duidelijke omschrijving van de invulling van deze drie criteria, maar Artikel 29 Werkgroep heeft enige handvaten overlegd, waarin meer toelichting wordt gegeven. Ondanks deze toelichting is er nog steeds een grijs gebied. Hierdoor kan een organisatie twijfelen of zij verplicht zijn om een FG aan te stellen. Indien een organisatie besluit om geen FG aan te stellen, dan is het van belang dat deze keuze wordt gemotiveerd in het privacybeleid, zodat dit voor de AP en de betrokkene is terug te vinden. Indien er geen FG wordt aangesteld, is het raadzaam om als organisatie een contactpersoon te benoemen die toeziet op de privacy binnen de organisatie. Betrokkenen weten hierdoor bij wie zij vragen kunnen stellen / een verzoek bij kunnen indienen over hun privacyrechten.

Een DPIA geeft inzicht in de effecten van de gegevensverwerking voor betrokkenen en beoordeelt deze gegevensverwerking. Een verwerkingsverantwoordelijke is verplicht om een DPIA uit te voeren, wanneer er sprake is van een hoog risico voor betrokkenen. De AVG bepaalt dat er in ieder geval sprake is van een hoog risico voor betrokkenen wanneer er sprake is van profilering, wanneer de organisatie bijzondere persoonsgegevens op grote schaal verwerkt en/of wanneer een organisatie mensen op grote schaal en systematisch in publiek toegankelijke gebieden volgt. Ook hierbij geeft de AVG geen duidelijke omschrijving van de invulling van deze verplichting en heeft Artikel 29 Werkgroep een nadere toelichting gegeven. Ondanks deze toelichting is er ook hierbij sprake van een grijs gebied. Reden waarom het ook bij het in acht nemen van deze verplichting raadzaam is om het besluit om wel of geen DPIA uit te voeren te onderbouwen in het privacybeleid. Wanneer een organisatie besluit om geen DPIA uit te voeren, is het wel van belang dat er is gekeken naar het risico voor betrokkenen en dat de organisatie beveiligingsmaatregelen treft om de rechten van betrokkenen te beschermen. Het treffen van beveiligingsmaatregelen is immers – ondanks dat er wellicht geen sprake is van een hoog risico – een verplichting vanuit de AVG.

Hoofdstuk 5: De rechten van betrokkenen

De privacyrechten van de Richtlijn zijn in de AVG uitgebreid en de AVG voorziet in een aantal nieuwe rechten. In paragraaf 5.1 worden de rechten van betrokkenen weergegeven. In paragraaf 5.2 wordt het recht op inzage afgezet tegen de dossierplicht van advocaten. Vervolgens is in paragraaf 5.3 het recht op verwijdering afgezet tegen het beroepsgeheim van advocaten.

5.1 De rechten van betrokkenen

Een betrokkene heeft de volgende rechten vanuit de AVG:

- Het recht op inzage;
- Het recht op rectificatie;
- Het recht op beperking van de verwerking;
- Het recht op geautomatiseerde besluitvorming en verwerking;
- Het recht om bezwaar te maken;
- Het recht op duidelijke informatie;
- Het recht op dataportabiliteit;
- Het recht op verwijdering.¹¹³

Ad 1) Het recht op inzage

De betrokkene heeft ingevolge artikel 15 AVG het recht om de verwerkte persoonsgegevens in te zien.

In paragraaf 5.2 wordt hier nader op ingegaan.

Ad) 2 Het recht op rectificatie

De betrokkene heeft ingevolge artikel 16 AVG het recht om de verwerkingsverantwoordelijke te verzoeken om onverwijld een rectificatie van de onjuiste persoonsgegevens te verkrijgen. De gegevens van betrokkenen moeten, indien betrokkene terecht aangeeft dat de verwerkte persoonsgegevens onjuist zijn, worden verbeterd of, indien de persoonsgegevens onvolledig zijn, worden aangevuld.¹¹⁴

Ad) 3 Het recht op beperking van de verwerking

De betrokkene heeft ingevolge artikel 18 AVG het recht om de verwerkingsverantwoordelijke te verplichten om het verwerken van persoonsgegevens als het ware te pauzeren. Men mag dan niet verder gaan met het verwerken van persoonsgegevens.¹¹⁵

Het recht op beperking geldt slechts wanneer er sprake is van één van de volgende situaties:

- De gegevens zijn mogelijk onjuist;
- De verwerking is onrechtmatig;
- De persoonsgegevens zijn niet meer nodig;
- De betrokkene maakt bezwaar.

¹¹³ Vermissen, Terstegge & Krijgsman, 2017, p. 73.

¹¹⁴ Vermissen, Terstegge & Krijgsman, 2017, p. 73.

¹¹⁵ Schermer, Hagenauw & Falot, 2018, p. 80.

Ad) 4 Het recht op geautomatiseerde besluitvorming en verwerking

Het recht op geautomatiseerde besluitvorming en verwerking wordt ook wel het recht op een menselijke blik bij besluiten genoemd. De betrokkene heeft ingevolge artikel 22 AVG het recht om niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit, waaraan rechtsgevolgen voor de betrokkene zijn verbonden of dat de betrokkene anderszins in aanmerkelijke mate treft. Een voorbeeld hiervan is de verwerking van sollicitaties via het internet zonder een menselijke tussenkomst.¹¹⁶ Indien de betrokkene een beroep doet op dit recht, dan moet de verwerkingsverantwoordelijke een nieuw besluit nemen, waarbij een mens de persoonsgegevens beoordeelt.

Ad) 5 Het recht om bezwaar te maken

De betrokkene heeft ingevolge artikel 21 AVG het recht om bezwaar te maken tegen de verwerking van de persoonsgegevens, indien de organisatie de persoonsgegevens verwerkt op grond van een taak van algemeen belang of op grond van een gerechtvaardigd belang. De betrokkene moet worden geïnformeerd over het recht om bezwaar te kunnen maken. Wanneer de betrokkene bezwaar maakt, moet men stoppen met het verwerken van de persoonsgegevens, tenzij er dwingende gerechtvaardigde gronden aanwezig zijn voor het verwerken van de persoonsgegevens en die gronden zwaarder wegen dan de belangen, vrijheden en rechten van de betrokkene of die te maken hebben met een rechtsoverweging. Wanneer de persoonsgegevens worden gebruikt voor direct marketing, dan heeft de betrokkene te allen tijde het recht om hiertegen bezwaar te maken. De verwerking van persoonsgegevens moeten in dat geval direct worden gestopt.¹¹⁷

Ad) 6 Het recht op duidelijke informatie

De betrokkene heeft ingevolge 13 AVG het recht om te worden geïnformeerd over wat er met de persoonsgegevens gebeurt. De verwerkingsverantwoordelijke heeft een informatieplicht, hetgeen inhoudt dat bestaande en nieuwe klanten moeten worden geïnformeerd over wat er gebeurt met hun persoonsgegevens. De informatie moet schriftelijk aan betrokkene worden medegedeeld. Het opstellen van een privacyverklaring is dan ook de meest eenvoudige manier om aan deze verplichting te voldoen.¹¹⁸

De volgende informatie moet aan betrokkene worden medegedeeld:

- De identiteit en contactgegevens van de organisatie en de eventuele FG;
- De doeleinden, bewaartermijnen en grondslagen voor het verwerken van persoonsgegevens;
- De soorten ontvangers aan wie persoonsgegevens worden verstrekt;
- Of men contractueel of wettelijk verplicht is tot het verstrekken van de persoonsgegevens en de mogelijke gevolgen van het niet verstrekken van de persoonsgegevens.¹¹⁹

Indien de organisatie de persoonsgegevens van de betrokkene zelf verkrijgt, dan moet de betrokkene worden geïnformeerd op het moment dat de gegevens wordt verstrekt.

¹¹⁶ Schermer, Hagenauw & Falot, 2018, p. 81.

¹¹⁷ Autoriteit Persoonsgegevens, "Rechten van betrokkenen", bekeken op 25 februari 2018

¹¹⁸ Autoriteit Persoonsgegevens, "Rechten van betrokkenen", bekeken op 25 februari 2018

¹¹⁹ Vermissen, Terstegge & Krijgsman, 2017, p. 71.

Indien de persoonsgegevens van een andere partij dan de betrokkene zelf worden verkregen, dan moet de betrokkene binnen een redelijke termijn door de organisatie worden geïnformeerd.¹²⁰

De betrokkene hoeft niet geïnformeerd te worden, indien:

- De betrokkene de informatie al heeft;
- Het informeren onmogelijk is;
- De doeleinden van de verwerking ernstig in het gedrang kunnen komen;
- De verwerking is wettelijk verplicht;
- De persoonsgegevens berusten op een beroepsgeheim.¹²¹

Ad) 7 Het recht op dataportabiliteit

De betrokkene heeft ingevolge artikel 20 AVG het recht op dataportabiliteit, oftewel het recht op overdraagbaarheid van persoonsgegevens. Betrokkene heeft hiermee het recht om persoonsgegevens te ontvangen die de organisatie van de betrokkene heeft, indien de persoonsgegevens worden verwerkt op basis van toestemming van de betrokkene of op basis van een overeenkomst met de betrokkene, de persoonsgegevens door de betrokkene zelf aan de verwerkingsverantwoordelijke zijn verstrekt en het gaat om digitale persoonsgegevens.¹²²

Ad) 8 Het recht op verwijdering

De betrokkene heeft ingevolge artikel 17 AVG het recht op verwijdering, hetgeen inhoudt dat een organisatie in een aantal gevallen persoonsgegevens moet verwijderen, indien een betrokkene hierom verzoekt.

In paragraaf 5.3 wordt hier nader op ingegaan.

5.2 Het recht op inzage tegenover het beroepsgeheim van advocaten

Allereerst zal het recht op inzage in paragraaf 5.2.1 nader worden toegelicht. In paragraaf 5.2.2 wordt het beroepsgeheim van advocaten besproken. In paragraaf 5.2.3 wordt het recht op inzage afgezet tegen het beroepsgeheim van advocaten.

5.2.1 Het recht op inzage

De betrokkene heeft ingevolge artikel 15 AVG het recht om de persoonsgegevens in te zien. Indien de betrokkene daartoe een verzoek doet, dan dient een kopie van alle gegevens, die over de betrokkene zijn verwerkt, aan de betrokkene te worden verstrekt.¹²³ Wanneer een betrokkene een inzageverzoek doet, dan dient het volgende aan de betrokkene te worden vermeld:

- De reden waarom bepaalde gegevens worden verwerkt;
- De soorten verzamelde persoonsgegevens;
- De bewaartermijn van persoonsgegevens;
- De privacyrechten van de betrokkene;

¹²⁰ Vermissen, Terstegge & Krijgsman, 2017, p. 72.

¹²¹ Vermissen, Terstegge & Krijgsman, 2017, p. 72.

¹²² Vermissen, Terstegge & Krijgsman, 2017, p. 75.

¹²³ Vermissen, Terstegge & Krijgsman, 2017, p. 72.

- Het recht van betrokkene om een klacht in te dienen bij de AP;
- Indien van toepassing: De organisaties waarvan de persoonsgegevens zijn ontvangen indien deze niet zelf zijn verzameld bij de betrokkene;
- Indien van toepassing: de organisaties waaraan de persoonsgegevens zijn doorgegeven;
- Indien van toepassing: De logica van een geautomatiseerd besluit.

5.2.2 Het beroepsgeheim van advocaten

Ingevolge artikel 10a Advocatenwet draagt een advocaat in het belang van een goede rechtsbedeling zorg voor de rechtsbescherming van zijn cliënt. Een advocaat is hiertoe bij de uitoefening van zijn beroep onder andere vertrouwenspersoon en neemt geheimhouding in acht binnen de door het recht en de wet gestelde eisen. Artikel 11a Advocatenwet geeft een nadere invulling aan het beroepsgeheim en bepaalt dat een advocaat, uitzonderingen daargelaten, tot geheimhouding is verplicht ten aanzien van al hetgeen hij uit hoofde van zijn beroepsuitoefening als zodanig kennis neemt. Deze verplichting geldt tevens voor medewerkers en personeel van de advocaat, alsmede andere bij de beroepsuitoefening betrokken personen. De geheimhoudingsplicht blijft voortbestaan na beëindiging van de beroepsuitoefening of de betrekking waarin de werkzaamheden zijn verricht.

In regel 3 van de Gedragsregels Advocatuur wordt een verdere invulling gegeven van het beroepsgeheim van advocaten. Ingevolge regel 3 Gedragsregels Advocatuur dient een advocaat te zwijgen over bijzonderheden van de door hem behandelde zaak, de persoon van zijn cliënt en de aard en omvang van diens belangen. Om aan deze verplichting gehoor te geven, dient een advocaat passende maatregelen te nemen.

Ondanks het beroepsgeheim staat het een advocaat vrij om vertrouwelijk verkregen kennis naar buiten toe te gebruiken, mits er is voldaan aan alle drie de volgende voorwaarden:

- Het rechtvaardigt een juiste uitvoering van de aan de advocaat opgedragen taak;
- De cliënt heeft desgevraagd geen bezwaar;
- Het is in overeenstemming met de goede beroepsuitoefening.

5.2.3 Het recht op inzage tegenover het beroepsgeheim van advocaten

Ingevolge artikel 15 AVG heeft de betrokkene het recht om uitsluitel te verkrijgen van de verwerkingsverantwoordelijke over de van hem verwerkte persoonsgegevens en hiervan inzage te krijgen. De betrokkene bij een advocatenkantoor in het geval van een juridische kwestie betreft vaak de (potentiële) cliënt of de wederpartij. Wanneer de (potentiële) cliënt een verzoek doet om inzage, dan zal er doorgaans geen probleem ontstaan. Het beroepsgeheim geldt immers niet ten opzichte van de cliënt en een advocaat heeft op grond van regel 16 Gedragsregels Advocatuur een informatieplicht jegens de cliënt. Een cliënt moet op de hoogte worden gehouden van de zaak en een afschrift krijgen van (belangrijke) stukken. Een advocaat kan dus, uitzonderingen daargelaten, zonder gevolgen het verzoek om inzage van een cliënt honoreren.

Echter, in het geval dat een wederpartij of een andere betrokkene om inzage verzoekt, is de verplichting om gehoor te geven aan het recht op inzage in strijd met het beroepsgeheim dat op een advocaat rust.

In dit geval biedt artikel 23 AVG uitkomst, waarin is bepaald dat het recht op inzage niet absoluut is en dus kan worden beperkt, onder meer wanneer de beperking ter waarborging is van de bescherming van de betrokkene of van de rechten en vrijheden van anderen. In overweging 63 van de AVG is dit nader toegelicht: *“Het recht op inzage mag geen afbreuk doen aan de rechten of vrijheden van anderen met inbegrip van het zakengeheim (...) De overweging mag er niet toe leiden dat de betrokkene alle informatie wordt onthouden. De betrokkene moet in dat geval de kans krijgen om een gericht verzoek te doen, waarin hij uitlegt welke gegevens hij precies wil weten. In dat geval dient de verwerkingsverantwoordelijke te kijken of het verzoek dan wel mogelijk is en dus geen afbreuk doet aan de rechten van anderen.”* Wanneer een wederpartij of een andere betrokkene aan een advocaat een verzoek om inzage doet, dan is de wederpartij “de betrokkene” en “de andere” betreft de cliënt, zoals bedoeld in artikel 23 lid 1 sub I AVG. Wanneer het verzoek om inzage van de wederpartij wordt gehonoreerd, dan kunnen de rechten en vrijheden van de cliënt in het geding komen. Reden waarom een advocaat het verzoek om recht op inzage door een wederpartij moet afwijzen op grond van artikel 23 lid 1 sub I AVG, namelijk het beschermen van de rechten en vrijheden van anderen, en op grond van het beroepsgeheim. Het beroepsgeheim van een advocaat maakt het voor een advocaat onmogelijk om inhoudelijk in te gaan op een verzoek om inzage van de wederpartij. Het enkel aangeven welke persoonsgegevens van de wederpartij worden verwerkt, zou al een schending van het in artikel 10a Advocatenwet neergelegde beroepsgeheim zijn. Reden waarom een advocaat, gezien zijn beroepsgeheim en gezien de beperking van artikel 23 lid 1 sub I AVG, geen gehoor mag en hoeft te geven aan het verzoek van de wederpartij om inzage en zich hierover niet inhoudelijk mag uitlaten. Een enkele reactie als “Gezien mijn beroepsgeheim, kan ik geen gehoor geven aan uw verzoek” is voldoende.

Voor een schematisch overzicht wordt hierbij verwezen naar bijlage IV.

5.3. Het recht op verwijdering tegenover de dossierplicht van advocaten

Allereerst zal het recht op verwijdering in paragraaf 5.3.1 nader worden toegelicht. In paragraaf 5.3.2 komt de dossierplicht van advocaten aan bod. In paragraaf 5.3.3 wordt het recht op verwijdering afgezet tegen de dossierplicht van advocaten.

5.3.1 Het recht op verwijdering

Het recht op verwijdering, ook wel het recht op gegevenswissing, het recht op vergetelheid of “the right to be forgotten” genoemd, komt voort uit een arrest van het Europese Hof van Justitie, waarin het hof heeft geoordeeld dat een burger – in bepaalde omstandigheden – het recht heeft om vergeten te worden. Volgens het Hof is dit met name het geval wanneer de informatie over een persoon onjuist, irrelevant, onvoldoende of buitensporig is.¹²⁴

¹²⁴ HvJ EU, 13 mei 2014, C-131/12, ECLI:EU:C:2014:317 (*Google Spanje SL, Google Inc. / Agencia Espanola de Proteccion de Datos, Mario Costeja Gonzalez*)

De AVG heeft het recht om vergeten te worden uitgewerkt in artikel 17, waarin is bepaald dat een betrokkene het recht heeft om een verzoek te doen aan de verwerkingsverantwoordelijke, waarbij de verwerkingsverantwoordelijke zonder onredelijke vertraging de persoonsgegevens van de betrokkene moet verwijderen. Naast het recht op verwijdering heeft de betrokkene onder bepaalde omstandigheden tevens het recht om te worden “vergeten”. Het recht om vergeten te worden ligt in het verlengde van het recht op verwijdering van persoonsgegevens.

Wanneer een betrokkene een beroep doet op haar recht op verwijdering dan wel het recht om vergeten te worden, dan dient de verwerkingsverantwoordelijke de persoonsgegevens zo snel mogelijk te wissen, mits er sprake is van één van de volgende situaties:

- De persoonsgegevens zijn niet meer nodig;
- De betrokkene trekt de toestemming voor het verwerken van persoonsgegevens in;
- De betrokkene maakt bezwaar tegen het verwerken van persoonsgegevens;
- Er is sprake van een onrechtmatige verwerking van persoonsgegevens;
- De wettelijk bepaalde bewaartermijn is verstreken;
- Er zijn persoonsgegevens verzameld middels een website of een app van een kind jonger dan 16 jaar en het kind betreft de betrokkene.¹²⁵

Het recht op verwijdering van persoonsgegevens en het recht om vergeten te worden kennen beperkingen en zijn hiermee niet absoluut. Het recht van de betrokkene dient te worden afgewogen tegenover andere belangen. Zo hoeft de verwerkingsverantwoordelijke geen gehoor te geven aan het verzoek om verwijdering, dan wel het verzoek om vergeten te worden, als er sprake is van één van de volgende situaties:

- De gegevensverwerking is noodzakelijk voor het recht op vrijheid van meningsuiting en informatie;
- De gegevensverwerking is noodzakelijk voor het nakomen van een wettelijke verplichting;
- De gegevensverwerking is noodzakelijk voor het vervullen van een taak van algemeen belang of uitoefening van openbaar gezag;
- De gegevensverwerking is noodzakelijk voor het belang van de volksgezondheid;
- De gegevensverwerking is noodzakelijk voor onderzoek, statistiek of archivering;
- De gegevensverwerking is noodzakelijk voor het instellen, uitoefenen of onderhouden van een rechtsvordering.¹²⁶

Niet geheel onbelangrijk om te vermelden, is dat, wanneer een organisatie persoonsgegevens heeft gedeeld met andere partijen, verwerkingsverantwoordelijke de partijen op de hoogte moet brengen van het verzoek van betrokkene om verwijdering van persoonsgegevens, dan wel van het verzoek om vergeten te worden.¹²⁷

¹²⁵ Schermer, Hagenauw & Falot, 2018, p. 79

¹²⁶ Vermissen, Terstegge & Krijgsman, 2017, p. 74.

¹²⁷ Schermer, Hagenauw & Falot, 2018, p. 80

5.3.2 De dossierplicht van advocaten

De Nederlandse Orde van Advocaten geeft in de handleiding "archivering op het advocatenkantoor" met betrekking tot het bewaren van documenten de bewaartermijnen aan. Ingevolge artikel 7:412 BW dienen advocaten zaakdossier minstens vijf jaar na afsluiting van de zaak te bewaren. Administratieve gegevens, waaronder de financiële administratie, dienen advocaten ingevolge artikel 52 lid 2 AWR zeven jaar te bewaren. Bij het bewaren van zaakdossiers moeten advocaten rekening houden met de aansprakelijkheid van advocaten voor beroepsfouten.¹²⁸

De verjaringstermijn voor beroepsfouten van advocaten betreft vijf jaar en de verjaringstermijn voor aansprakelijkheid betreft ingevolge artikel 3:310 BW twintig jaar. Advocaten dienen bij het bewaren van dossiers rekening te houden met deze verjaringstermijnen. De Nederlandse Orde van Advocaten adviseert hierdoor om alle zaakdossier minstens twintig jaar na afsluiting van de zaak te bewaren in een archiefruimte.¹²⁹ Wanneer de bewaartermijn van archiefbestanden is verstreken, komen de dossiers in aanmerking voor vernietiging.

5.3.3 Het recht op verwijdering versus de dossierplicht van advocaten

Bij een juridische kwestie, zowel enkel een juridisch advies dan wel een gerechtelijke procedure, zijn vaak twee partijen betrokken: de cliënt en de wederpartij. In het zaakdossier zijn hierdoor vaak persoonsgegevens over de cliënt terug te vinden, maar ook persoonsgegevens van de wederpartij (en eventuele derden).

Om de vraag te kunnen beantwoorden of een advocaat gehoor moet geven aan een verzoek van een betrokkene om verwijdering van (bepaalde stukken uit) het dossier, geldt het volgende: ingevolge artikel 17 AVG kan een betrokkene de verwerkingsverantwoordelijke verzoeken om verwijdering van zijn persoonsgegevens, indien onder meer de betrokkene de toestemming intrekt, de betrokkene bezwaar maakt tegen de verwerking en/of de wettelijke bewaartermijn is verstreken.¹³⁰ Indien de betrokkene¹³¹ voldoet aan een van deze situaties en hij vervolgens een verzoek doet aan de verwerkingsverantwoordelijke, in dit geval een advocaat, zal een advocaat in beginsel gehoor moeten geven aan het verzoek.

Echter, ingevolge artikel 17 lid 3 sub e AVG hoeft de verwerkingsverantwoordelijke geen gehoor te geven aan het recht op verwijdering, indien de verwerking noodzakelijk is voor onder meer het instellen, uitoefenen of onderbouwen van een rechtsvordering. Het verwerken van persoonsgegevens van een ander dan de betrokkene, bijvoorbeeld de wederpartij, is noodzakelijk voor het instellen, uitoefenen, dan wel het onderbouwen van een rechtsvordering, waardoor er wordt voldaan aan de voorwaarde op het verwerkingsverbod van bijzondere persoonsgegevens van artikel 9 lid 2 AVG.

¹²⁸ Nederlandse Orde van Advocaten, 2004, p. 6.

¹²⁹ Nederlandse Orde van Advocaten, 2004, p. 6.

¹³⁰ Het verwerken van persoonsgegevens van een wederpartij zal vaak niet te baseren zijn op de grondslag "toestemming", "wettelijke bepaling" of "overeenkomst" maar op "gerechtvaardigd belang". Dit omdat er geen wettelijke verplichting bestaat voor een advocaat om persoonsgegevens van een wederpartij te verzamelen. Voorts zal een advocaat niet vaak om toestemming vragen aan een wederpartij, daar dit erg omslachtig kan zijn en zelfs in bepaalde gevallen nadelig. Toestemming kan daarnaast worden ingetrokken, hetgeen nadelig kan zijn.

¹³¹ De wederpartij is in beginsel een betrokkene, zoals in de zin van artikel 4 lid 1 AVG, aangezien het gegevens betreffen over een identificeerbaar natuurlijk persoon. Wanneer de wederpartij een rechtspersoon betreft, dan zal de contactpersoon van de rechtspersoon de betrokkene zijn.

Hierdoor komt het recht op verwijdering van de wederpartij te vervallen. De advocaat hoeft geen gehoor te geven aan het verzoek. Een advocaat zal het weigeren van het verzoek wel moeten onderbouwen, met inachtneming van het beroepsgeheim.

Niet geheel onbelangrijk om te vermelden is dat het niet is toegestaan om (gezondheids) persoonsgegevens te verwerken, die niet noodzakelijk zijn voor de overeenkomst en het instellen, uitoefenen of onderbouwen van de rechtsvordering, dit in verband met het beginsel van minimale gegevensverwerking en opslagbeperking, genoemd in artikel 5 AVG.

Daarnaast is het denkbaar dat een juridische procedure tot een einde is gekomen (en er geen vervolgprocedure komt) en een advocaat zich niet meer kan baseren op de uitzonderingsgrond "instelling, uitoefening of onderbouwing van een rechtsvordering". In dit geval biedt artikel 17 lid 3 sub b AVG uitkomst. Hierin is namelijk bepaald dat een verwerkingsverantwoordelijke geen gehoor hoeft te geven aan het verzoek van een betrokkene om het verwijderen van zijn persoonsgegevens, indien de verwerking van de persoonsgegevens noodzakelijk is voor het nakomen van een onder andere in het Unierecht of lidstatelijk recht neergelegde wettelijke verwerkingsverplichting die op de verwerkingsverantwoordelijke rust.

Zoals in paragraaf 5.3.2 is beschreven heeft een advocaat een dossierplicht, waarbij zaakdossiers vijf jaar dienen te worden bewaard en administratieve dossiers zeven jaar. In bepaalde gevallen, omschreven in paragraaf 5.3.2 kan de bewaarplicht zelfs oplopen tot 20 jaar.

Gezien het voorstaande kan een advocaat bij een verzoek van een betrokkene om verwijdering zich beroepen op de uitzonderingsgrond van artikel 17 lid 3 sub b AVG en verwijzen naar zijn dossierplicht. Een advocaat zal ook in dit geval geen gehoor hoeven geven aan het verzoek om verwijdering van persoonsgegevens.

Niet geheel onbelangrijk om te vermelden is dat een advocaat altijd – en dus ook in dit geval – de beslissing om te weigeren op het verzoek om persoonsgegevens te verwijderen met inachtneming van het beroepsgeheim zal moeten onderbouwen.

Voor een schematisch overzicht wordt hierbij verwezen naar bijlage V.

5.4 Deelconclusie

Gezien het voorstaande kan het recht op inzage en het recht op verwijdering haaks staan op het beroepsgeheim en de dossierplicht van advocaten.

In het geval een betrokkene een verzoek doet om inzage bij een verwerkingsverantwoordelijke, dan dient een verwerkingsverantwoordelijke hieraan in beginsel gehoor te geven. Echter, in het geval dat het gehoor geven aan het verzoek de rechten en vrijheden van de betrokkene of een ander kan schaden, dan kan een verwerkingsverantwoordelijke het verzoek afwijzen. In het geval van een advocaat zal een wederpartij of een cliënt het verzoek om inzage kunnen doen.

Wanneer een cliënt het verzoek om inzage doet, zal dit geen problemen opleveren, daar het beroepsgeheim van een advocaat niet geldt ten opzichte van de cliënt en een advocaat een informatieplicht heeft jegens zijn cliënt. In het geval een wederpartij om inzage verzoekt, dan is dit wel in strijd met het beroepsgeheim van een advocaat. Het gehoor geven aan een verzoek om inzage van de wederpartij leidt tot schending van het beroepsgeheim en tot schade aan de rechten en vrijheden van de cliënt, hetgeen ingevolge artikel 23 AVG een van de uitzonderingen is om een verzoek tot inzage te kunnen weigeren. Een advocaat moet dan ook het verzoek om inzage van de wederpartij weigeren.

In het geval een betrokkene een verzoek om verwijdering doet bij de verwerkingsverantwoordelijke, dan dient de verwerkingsverantwoordelijke hieraan in beginsel gehoor te geven. Echter, de verwerkingsverantwoordelijke hoeft geen gehoor te geven aan het recht op verwijdering, indien de verwerking noodzakelijk is voor onder meer het instellen, uitoefenen of onderbouwen van een rechtsvordering. Wanneer een juridische kwestie nog voortduurt, dan kan een advocaat bij een verzoek van de betrokkene om verwijdering van (bepaalde stukken uit) het dossier weigeren, waarbij hij zich beroept op de uitzondering "noodzakelijk i.v.m. rechtsvordering". In het geval dat de juridische kwestie al is beëindigd, dan kan een advocaat zich niet scharen op de uitzondering "noodzakelijk i.v.m. rechtsvordering". Echter, een advocaat kan ook in dat geval het verzoek om verwijdering weigeren, en wel op de uitzondering "noodzakelijk is voor het nakomen van een onder andere in het Unierecht of lidstatelijk recht neergelegde wettelijke verwerkingsverplichting die op de verwerkingsverantwoordelijke rust", namelijk de dossierplicht van een advocaat. Voor beide uitzonderingen geldt uiteraard dat een advocaat het weigeren van het verzoek zal moeten onderbouwen, met inachtneming van het beroepsgeheim.

Hoofdstuk 6: Het toezicht op de naleving van de AVG.

Hoofdstuk 6 ziet toe op het toezicht op de naleving van de AVG. Voor de volledigheid van de beantwoording van deelvraag 1 wordt het toezicht op de naleving van de AVG hier kort uiteen gezet. De manier waarop de Autoriteit Persoonsgegevens (hierna te noemen: AP) toezicht houdt op de naleving van de AVG, onderstreept het belang van het in acht nemen van de AVG. Gelet op de forse boetes die de AP een organisatie namelijk kan opleggen, zou het buitenbeschouwing laten van de toezicht op de AVG, afbreuk doen aan de opdracht van KBS.

Elke lidstaat van de Europese Unie heeft één of meer toezichthouders aangesteld om toezicht te houden op de naleving van de AVG en om de AVG te stimuleren. In Nederland is het de AP die toezicht houdt op de naleving van de AVG.¹³² Wanneer een organisatie volgens de AP niet aan de AVG voldoet, dan is de AP bevoegd om een administratieve boete op te leggen. Men kent twee soorten boetes: een boete van ten hoogste 10 miljoen euro of 2% van de wereldwijde jaaromzet van de verwerkingsverantwoordelijke of de verwerker (artikel 83 lid 4 AVG) of een boete van ten hoogste 20 miljoen euro of 4% van de wereldwijde omzet (artikel 83 lid 5 AVG). Onder de eerste boetecategorie vallen overtredingen van informatieverplichtingen en de verplichting om te voldoen aan verbeterings- en inzagerechten, het recht op vergetelheid en de verplichting om voor een gegevensbescherming door ontwerp en door standaardinstellingen zorg te dragen. Onder de tweede boetecategorie vallen de overige overtredingen, zoals de verplichting om persoonsgegevens slechts te verwerken overeenkomstig de gegevensverwerkingsbeginselen (zorgvuldig, behoorlijk transparant, doelbinding en op grond van een toereikende verwerkingsrechtsgrondslag).¹³³ Kort gezegd geldt dat de boete van de eerste categorie geldt voor het niet nakomen van de verplichtingen van de AVG en de boete van de tweede categorie voor het niet in acht nemen van beginselen van de AVG en/of de rechten van betrokkenen. Naast boetes, kent de AVG ook sancties die gericht zijn op het beëindigen van overtredingen of het herstellen van nadelige gevolgen voortvloeiende uit de overtredingen.¹³⁴

Naast de AP kunnen ook betrokkenen actie ondernemen, indien zij van mening zijn dat een organisatie hun persoonsgegevens in strijd met de geldende wet- en regelgeving verwerkt. Hiertoe hebben zij verschillende mogelijkheden:

- Het recht op een klacht bij de toezichthouder;
- Het recht op een voorziening in rechte tegen de verwerkingsverantwoordelijke;
- Het recht op vertegenwoordiging;
- Het recht op schadevergoeding.¹³⁵

¹³² Schermer, Hagenauw & Falot, 2018, p. 90.

¹³³ Zwenne & Mommers, 2016, p. 182 - 189

¹³⁴ Schermer, Hagenauw & Falot, 2018, p. 90.

¹³⁵ Schermer, Hagenauw & Falot, 2018, p. 90.

Hoofdstuk 7: Resultaten

In hoofdstuk 7 van het onderzoeksrapport worden de praktijkgerichte deelvragen (deelvraag 7 t/m 13) beantwoord en worden de resultaten van het onderzoek weergegeven.

De praktijkgerichte deelvragen zijn beantwoord aan de hand van drie interviews en een enquête. De interviews zijn aan de hand van een topiclijst en een lijst met algemene voorbeeldvragen afgenomen. De afgenomen interviews zijn te kwalificeren als een half open gestructureerd interview. De topics en voorbeeldvragen waren gericht op de manier waarop persoonsgegevens binnen KBS worden verwerkt en de manier waarop KBS invulling geeft aan de AVG. De interviews zijn afgenomen bij drie medewerkers van KBS die toezien op de privacy binnen kantoor, namelijk:

- De officemanager van KBS (de heer De Snoo)
- De advocaten binnen KBS die voorlichting geven over de AVG (de heer Van den Burg en de heer Luijendijk)

De transcripties van de interviews zijn opgenomen in bijlage VIII t/m bijlage IX. De enquête is afgenomen onder de advocaten van KBS en de resultaten hiervan zijn opgenomen in bijlage X.

In paragraaf 7.1 t/m 7.5 worden de resultaten van de interviews weergegeven en in paragraaf 7.6 de resultaten van de enquête.

7.1 De verwerkte persoonsgegevens binnen KBS

KBS kent verschillende betrokkenen binnen haar organisatie, namelijk de (potentiële) cliënt, de wederpartij, de eventuele advocaat of andere vertegenwoordiger van de wederpartij (hierna te noemen: advocaat wederpartij), leveranciers, bezoekers, (potentiële) werknemers, studentstagiaires en leden van de nieuwsbrief.¹³⁶ KBS verwerkt zowel gewone persoonsgegevens als bijzondere persoonsgegevens, namelijk gezondheidsgegevens.¹³⁷ Voor een volledig overzicht wordt hierbij naar Bijlage VI verwezen, waarin een overzicht is weergegeven van alle verwerkte persoonsgegevens, zowel gewone- als bijzondere persoonsgegevens, per betrokkene.

Ad 1) De verwerkte gewone persoonsgegevens

Voor wat betreft de gewone persoonsgegevens wordt van elke betrokkene NAW gegevens¹³⁸ en contactgegevens verwerkt.¹³⁹ In het geval van de (potentiële) cliënt zijn zowel natuurlijke personen als rechtspersonen cliënt bij KBS. In het geval er gegevens worden verwerkt van rechtspersonen, dan is er geen sprake van het verwerken van persoonsgegevens in de zin van de AVG. Het betreft immers geen gegeven over een natuurlijk persoon (zie hiervoor de begrippenlijst).



Echter, KBS verwerkt doorgaans de persoonsgegevens van de contactpersoon van de rechtspersoon, hetgeen wel een natuurlijk persoon betreft.¹⁴⁰ Daarnaast staat KBS - naast natuurlijke personen en rechtspersonen - ondernemingen bij die niet als rechtspersoon kunnen worden aangemerkt, bijvoorbeeld een eenmanszaak. In dit geval is er tevens sprake van persoonsgegevens en die worden door KBS verwerkt.¹⁴¹

Naast de NAW gegevens worden bij bepaalde betrokkenen meer gewone persoonsgegevens verwerkt, zo wordt bij een (potentiële) cliënt het identificatienummer verwerkt op grond van de WWFT en wordt bij werknemers een kopie van het paspoort / ID op grond van de Wlb verwerkt.¹⁴² Verder is bij de ingang van het kantoor een camera gevestigd, zodat bij bezoekers van KBS - naast NAW gegevens - tevens camerabeelden worden verwerkt.¹⁴³

Ad 2) De verwerkte gezondheidspersoonsgegevens

Voor wat betreft het verwerken van gezondheidspersoonsgegevens, verwerkt KBS niet bij elke categorie betrokkene gezondheidspersoonsgegevens, maar slechts bij de categorie betrokkene "wederpartij", "(potentiële) cliënt" en de categorie "werknemers".

In het geval van de wederpartij geldt het volgende: KBS staat in een juridisch medische kwestie de zorginstelling (en dus de desbetreffende hulpverlener) bij. De wederpartij betreft de patiënt. Om de rechtsvordering te kunnen onderbouwen, overlegt een zorginstelling het patiëntendossiers aan KBS. In het patiëntendossiers zijn gezondheidspersoonsgegevens over de patiënt terug te vinden, hetgeen bij KBS doorgaans de wederpartij betreft. Gezondheidspersoonsgegevens van de (potentiële) cliënt staan hier niet in en deze verwerkt KBS dan ook in die gevallen niet.

Het komt echter ook weleens voor dat er gezondheidsgegevens van de cliënt worden verwerkt, bijvoorbeeld bij een aansprakelijkheidskwestie. In dat geval worden ook gezondheidsgegevens van de cliënt verwerkt.¹⁴⁴ Een cliënt overlegt het gehele patiëntendossier (met wellicht zowel gezondheidsgegevens van hemzelf als van de wederpartij). Reden hiervoor is dat een advocaat van KBS het gehele patiëntendossiers moet inzien om zo een afweging te kunnen maken welke medische stukken relevant zijn ten aanzien van het uitoefenen van een rechtsvordering.¹⁴⁵ De cliënt maakt geen selectie van "relevante medische stukken". De omvang van het patiëntendossiers hangt af van de cliënt.¹⁴⁶ Zo overlegt een huisarts vaak het gehele medische dossier, waarbij wellicht psychische klachten als fysieke klachten zijn terug te lezen, terwijl een ziekenhuis "slechts" het patiëntendossiers van de desbetreffende afdeling overlegt.¹⁴⁷

[Redacted text block]

In het geval van de werknemer worden niet altijd gezondheidspersoonsgegevens verwerkt. Dit is pas het geval, wanneer een medewerker wegens ziekte is verhinderd om te werken. In dat geval worden onder andere correspondentie en rapporten van de bedrijfsarts verwerkt. Daarnaast worden gezondheidsgegevens verwerkt in het geval van zwangerschap, namelijk gegevens ten behoeve van de zwangerschapsuitkeringen.¹⁴⁸

7.2 De werkwijze met betrekking tot het verwerken van persoonsgegevens binnen KBS

Zojuist is aangegeven welke betrokkenen KBS kent en welke persoonsgegevens KBS van de betrokkenen verwerkt. Relevant hierbij is op welke manier de desbetreffende persoonsgegevens worden verwerkt en op welke grondslag van de AVG KBS zich baseert voor het verwerken van de desbetreffende persoonsgegevens.

Ad 1) De werkwijze van KBS met betrekking tot het verwerken van persoonsgegevens.

In het geval KBS persoonsgegevens verwerkt, dan worden de persoonsgegevens zowel digitaal (Fortuna) als in het papieren dossier verwerkt.¹⁴⁹ De wens en het doel van KBS is om volledig digitaal te gaan werken, maar de verwachting is dat het nog een aantal jaar zal duren voordat de papieren dossiers volledig verleden tijd zijn.¹⁵⁰ Naast Fortuna en het papieren dossier, heeft elke medewerker een persoonlijke map op de K-schijf. Ondanks dat het protocol binnen KBS voorschrijft dat de K-schijf enkel is bedoeld voor persoonlijke documenten (denk aan scholingsdocumenten)¹⁵¹ en dat de advocaten in het papieren dossier en in Fortuna moeten werken wanneer het een zaak betreft, wordt een aantal stukken van het zaakdossier soms op de K-schijf verwerkt.¹⁵² Ook dit probeert KBS tegen te gaan. De wens en het doel is om zo snel mogelijk alles van de K-schijf in Fortuna te verwerken.¹⁵³

Ad 2) De grondslagen voor het verwerken van persoonsgegevens binnen KBS

Eerder zijn de verschillende betrokkenen en de daarbij behorende verwerkte persoonsgegevens weergegeven (bijlage VI).

De grondslag voor het verwerken van gewone persoonsgegevens is bij KBS over het algemeen de grondslag van artikel 6 lid 1 sub b AVG: Het kunnen uitvoeren van de overeenkomst. In enkele gevallen baseert KBS zich op de grondslag van artikel 6 lid 1 sub f AVG: Gerechtvaardigd belang.¹⁵⁴

Het verwerken van gezondheidspersoonsgegevens is in beginsel verboden, tenzij er sprake is van een voorwaarde om bijzondere persoonsgegevens te verwerken.

¹⁴⁸ De Arboarts heeft een beroepsgeheim, zo ook tegenover de werkgever van de desbetreffende werknemer. De Arboarts correspondeert met de werkgever. Hierin wordt bijvoorbeeld aangegeven welke werkzaamheden een werknemer kan verrichten en welke niet. Ook dit soort gegevens zeggen iets over iemands gezondheidstoestand en zijn dus aan te merken als gezondheidspersoonsgegevens.

[Redacted text block]

KBS beroept zich bij het verwerken van gezondheidspersoonsgegevens inzake de (potentiële) cliënt en/of de wederpartij op de voorwaarde “instelling, uitoefening en onderbouwing van de rechtsvordering”.¹⁵⁵ Voor wat betreft het verwerken van gezondheidspersoonsgegevens inzake de werknemer, beroept KBS zich de voorwaarde “uitvoering van arbeids- en sociaalzekerheidsrechtelijke rechten van de verwerkingsverantwoordelijke”.¹⁵⁶

Uit de resultaten is gebleken dat er onzekerheid is over de grondslag “gerechtvaardigd belang” bij direct marketing en over de vraag of het verwerken van camerabeelden als een gewoon persoonsgegeven of als een bijzonder persoonsgegeven moet worden aangemerkt. Gelet op deze onduidelijk wordt hieronder kort op beide punten ingegaan en volgt een korte juridische uitleg.

Ad 1) Direct marketing

Voor een inhoudelijke uitleg over direct marketing, wordt hierbij verwezen naar hoofdstuk 3. Om als organisatie direct marketing te baseren op de grondslag “gerechtvaardigd belang”, moet aangetoond worden dat het belang van de organisatie groter is dan het belang van de betrokkene. KBS zal moeten aantonen dat haar belang groter is dan het belang van de betrokkene. Men kan hierover van mening verschillen. Om zeker te zijn van een rechtmatige verwerking, is het verstandig om – naast de grondslag gerechtvaardigd belang – de grondslag toestemming te hanteren en de leden van de nieuwsbrief om toestemming te vragen.

Ad 2) Cameratoezicht

Uit de resultaten van het onderzoek bleek dat er verwarring mogelijk is over de vraag of het verwerken van camerabeelden valt te kwalificeren onder gewone persoonsgegevens of bijzondere persoonsgegevens.¹⁵⁷ Dit in verband met het feit dat op camerabeelden de fysieke kenmerken van personen zichtbaar zijn. Zo is bijvoorbeeld zichtbaar of iemand een hoofddoek draagt (wat iets zou kunnen zeggen over een godsdienstige overtuiging) of dat iemand een bril draagt (wat iets kan zeggen over de visuele gezondheid). Daarnaast zou iemands ras kunnen worden afgeleid van de camerabeelden.¹⁵⁸

Wanneer het verwerken van camerabeelden wordt aangemerkt als het verwerken van iemands godsdienst, gezondheidstoestand of ras, dan zou dit strikt genomen betekenen dat alle camerabeelden bijzondere persoonsgegevens zijn en het verwerken van camerabeelden dus verboden is, tenzij er sprake is van een van de voorwaarden de persoonsgegevens te verwerken.

¹⁵⁸ Kamerstukken II 1997/98, 25 892, nr. 3, p. 105, Hoge Raad, 23 maart 2010, ECLI:NL:HR:2010:BK6331, R.O. 2.6 & Parket bij de Hoge Raad, 23 maart 2010, ECLI:NL:PHR:2010:BK6331

Ingevolge de rechtspraak is dit niet de bedoeling geweest van de wetgever.¹⁵⁹ De uitspraak is gedaan in de tijd van de Richtlijn, maar ook de AVG beaamt dit en heeft de kwestie in overweging 51 van de AVG genuanceerd: “*The processing of photographs will not systematically be a sensitive processing (...)*”. De AP beschouwt camerabeelden van een persoon hierdoor niet als bijzondere persoonsgegevens, indien: Het doel van de verwerking niet is gericht op het verwerken van bijzondere persoonsgegevens of het maken van onderscheid op grond van bijzondere persoonsgegevens; Het voor een verwerkingsverantwoordelijke niet voorzienbaar is dat de verwerking zal leiden tot het op grond van bijzondere persoonsgegevens maken van onderscheid, en het verwerken van bijzondere persoonsgegevens onvermijdelijk is bij de verwerking.¹⁶⁰

Wanneer deze criteria worden toegespitst op KBS, dan geldt het volgende: Het doel van het cameratoezicht betreft de beveiliging en niet het vastleggen van godsdienstige gegevens, rasgegevens of gezondheidsgegevens van de bezoekers. Daarnaast wordt er middels het cameratoezicht geen onderscheid gemaakt op basis van de godsdienstige gegevens, rasgegevens of gezondheidsgegevens van de bezoekers. Vervolgens is het voor KBS redelijkerwijs niet voorzienbaar dat het cameratoezicht zal leiden tot het maken van een onderscheid. Voorts is het verwerken van eventuele godsdienstige gegevens, rasgegevens of gezondheidsgegevens onvermijdelijk bij de inzet van cameratoezicht bij KBS. Tot slot leidt het verwerken van de camerabeelden niet tot identificatie. Reden waarom kan worden geconcludeerd dat het verwerken van camerabeelden niet valt aan te merken als bijzondere persoonsgegevens, maar als gewone persoonsgegevens. De grondslag voor het verwerken van de camerabeelden betreft in dit geval de grondslag “gerechtvaardigd belang”.¹⁶¹

7.3 De verwerkingsverantwoordelijke en verwerkers binnen KBS

Zoals in hoofdstuk 4 aan bod is gekomen, maakt de AVG een onderscheid tussen de verwerkingsverantwoordelijke en de verwerker.

Ad 1) De positie van KBS

Het kantoor “KBS Advocaten N.V.” is volgens KBS de verwerkingsverantwoordelijke, aangezien het kantoor het doel en de middelen voor het verwerken van persoonsgegevens van de zojuist genoemde betrokkenen bepaalt.¹⁶² Voor wat betreft het verwerken van persoonsgegevens van de cliënt is ruimte voor discussie.¹⁶³ Men kan twijfelen over het feit of het advocatenkantoor of de individuele advocaat binnen het advocatenkantoor als verwerkingsverantwoordelijke kan worden aangemerkt. Een advocaat bepaalt bij KBS immers zelf wat voor persoonsgegevens hij van een cliënt verwerkt. Gezegd kan worden dat een advocaat wellicht hierdoor het doel en de middelen bepaalt voor de verwerking.¹⁶⁴

¹⁵⁹ Hoge Raad, 21 december 2010, ECLI:NL:HR:2010:BL7688 & Parket bij de Hoge Raad, 21 december 2010, ECLI:NL:PHR:2010:BL7688.

¹⁶⁰ College bescherming persoonsgegevens, 2016, 2.11

¹⁶¹ Op 6 juni 2018 stond er op de website van de AP nog geen verwijzing naar deze beleidsregels.

Desalniettemin beschouwt KBS een advocatenkantoor, in dit geval "KBS Advocaten N.V.", als verwerkingsverantwoordelijke en niet een individuele advocaat van een advocatenkantoor.¹⁶⁵ KBS is van mening dat het onwenselijk is om de individuele advocaat als verwerkingsverantwoordelijke te benoemen. KBS verwijst hierbij naar de Opinion van Artikel 29 Werkgroep, waarin is aangegeven dat de voorkeur ernaar uit moet gaan dat een onderneming of een orgaan als verwerkingsverantwoordelijke wordt aangemerkt en niet de natuurlijke persoon binnen die onderneming of dat orgaan.¹⁶⁶ Gelet op de Opinion van Artikel 29 Werkgroep ligt het volgens KBS voor de hand dat een advocatenkantoor, en dus de onderneming "KBS Advocaten N.V." als verwerkingsverantwoordelijke wordt aangemerkt en niet (ook) de advocaat die aan KBS is verbonden.¹⁶⁷ Een cliënt sluit immers een overeenkomst van opdracht met het kantoor en niet met de individuele advocaat. Een advocaat verwerkt dan de persoonsgegevens ten behoeve van het kantoor.¹⁶⁸

Uit de resultaten van het onderzoek is verder terug te zien dat er binnen KBS onduidelijkheid bestaat over wie er verantwoordelijk is voor het verwerken van de camerabeelden (verhuurder van het kantoorpand, het andere bedrijf in het kantoorpand (Talent & Pro) of KBS).¹⁶⁹ De verhuurder van het kantoorpand van KBS heeft de camera opgehangen.¹⁷⁰ De camerabeelden worden bekeken – en dus verwerkt – door KBS en Talent & Pro.¹⁷¹ KBS heeft hier vooralsnog geen duidelijkheid over.¹⁷² Gezien de onzekerheid, wordt hier tevens kort op ingegaan. In de beleidsregels cameratoezicht, college bescherming persoonsgegevens komt naar voren dat ten aanzien van het verwerken van camerabeelden degene die beslist over de inzet van cameratoezicht kan worden aangemerkt als de verantwoordelijke in de zin van de Richtlijn en de Wbp.¹⁷³ Gezien het feit dat de verhuurder van het kantoorpand de camera heeft opgehangen, beslist de verhuurder de inzet van het cameratoezicht. De verhuurder heeft het doel (beveiliging van het pand) en de middelen (de camera's) bepaald en is hiermee aan te merken als verwerkingsverantwoordelijke. Het feit dat KBS live de beelden bekijkt, doet hier mijns inziens niet aan af. Hierdoor is KBS niet aan te merken als verwerkingsverantwoordelijke. Daarnaast kan KBS niet worden aangemerkt als verwerker, aangezien de verhuurder geen opdracht tot het verwerken van de camerabeelden aan KBS heeft gegeven.

Ad 2) De verwerkers binnen KBS

KBS maakt gebruik van verschillende verwerkers, namelijk: ICT Concept voor het beheer van de ICT systemen en ETL voor de salarisadministratie.¹⁷⁴

¹⁶⁶ ARTICLE 29 DATA PROTECTION WORKING PARTY, 2010, p. 15.

¹⁷² Bijlage VII, Interview R. de Snoo, p. 84 t/m 104.

¹⁷³ College bescherming persoonsgegevens, 2016, 2.3

Met beide verwerkers is een verwerkersovereenkomst gesloten.¹⁷⁵ Daarnaast gaat KBS een nieuwe verwerkersovereenkomst aan, namelijk met ZIVVER.¹⁷⁶ ZIVVER biedt KBS de mogelijkheid om e-mails via een beveiligd platform te versturen. Reden waarom ZIVVER data van KBS verwerkt. Verder gaat KBS mogelijk een verwerkersovereenkomst aan met MailChimp voor het versturen van de nieuwsbrief.¹⁷⁷ Dit is nog niet zeker.¹⁷⁸ Tot slot zal KBS een verwerkersovereenkomst aangaan met een bedrijf dat het archief voor KBS zal beheren.¹⁷⁹ Hierover wordt nog onderhandeld en het is nog onduidelijk welk bedrijf dit gaat worden. Het doel is om dit voor 2019 te hebben geregeld.¹⁸⁰

7.4 De invulling van de verplichtingen binnen KBS

In hoofdstuk 4 van het onderzoeksrapport zijn de verschillende verplichtingen voor een verwerkingsverantwoordelijke en een verwerker beschreven. In hoofdstuk 1 van het onderzoeksrapport is aangegeven dat de opdracht van KBS toeziet op het weergegeven van een algemeen beeld van de AVG, waarbij expliciet wordt ingezoomd op twee verplichtingen vanuit de AVG, namelijk de verplichting om een FG aan te stellen en de verplichting om een DPIA uit te voeren. De twee verplichtingen worden hieronder afgezet tegen KBS.

Ad 1) De verplichting om een Functionaris voor de Gegevensbescherming aan te stellen.

Zoals eerder in hoofdstuk 4 van het onderzoeksrapport is beschreven, stelt de AVG de verwerkingsverantwoordelijke in bepaalde gevallen verplicht om een FG aan te stellen. Wanneer KBS de criteria toepast op haar organisatie, komt KBS tot de conclusie dat zij met kracht kan betogen dat zij niet is verplicht om een FG aan te stellen.¹⁸¹ De afweging hierbij is als volgt: Het eerste criterium is niet op KBS van toepassing, aangezien KBS geen overheidsorganisatie betreft.

Voor wat betreft de invulling van het tweede criterium beargumenteren de medewerkers op het gebied van privacy van KBS dat zij niet hoofdzakelijk zijn belast met verwerkingen, die vanwege hun omvang, aard en/of hun doeleinden, regelmatige, grootschalige en stelselmatige observatie op grote schaal van betrokkenen vereisen. KBS analyseert immers geen persoonsgegevens op basis van gedrag van personen.¹⁸² Hierdoor is geen sprake van het volgen van mensen in publiek toegankelijke ruimtes of van profilering.¹⁸³ Reden waarom volgens KBS niet is voldaan aan het twee criterium.

Het derde criterium kent drie onderdelen: bijzondere persoonsgegevens of strafrechtelijke persoonsgegevens, hoofdzakelijk belast en verwerking op grootschalige wijze. KBS heeft naar de invulling van deze onderdelen gekeken. Allereerst concludeert KBS dat zij bijzondere persoonsgegevens verwerkt, namelijk gezondheidspersoonsgegevens, en dus zal binnen KBS moeten worden gekeken naar de invulling van het derde criterium.¹⁸⁴



Wanneer het derde criterium vervolgens wordt afgezet tegen KBS, dan zijn de medewerkers op het gebied van privacy binnen KBS van mening dat KBS niet hoofdzakelijk zijn belast met het verwerken van gezondheidspersoonsgegevens en dat, al zou KBS dat wel zijn, dit niet gebeurt op een grootschalige wijze.¹⁸⁵ Eerder is aangegeven dat met “hoofdzakelijk belast” wordt bedoeld op de kernactiviteit van de desbetreffende organisatie. In het geval van KBS is de kernactiviteit het verlenen van juridische bijstand en niet het verwerken van gezondheidspersoonsgegevens.¹⁸⁶ Zoals in hoofdstuk 4 uiteen is gezet, stelt de AP zich op het standpunt dat het verwerken van gezondheidspersoonsgegevens bij een ziekenhuis wellicht geen kernactiviteit is, maar dat een zorginstelling (ziekenhuis dan wel solistische huisarts) toch hoofdzakelijk is belast met het verwerken van gezondheidspersoonsgegevens, simpelweg omdat dit een uitvloeisel is van hun kernactiviteit: het verlenen van zorg.¹⁸⁷ Echter, in het geval van KBS is het verwerken van gezondheidspersoonsgegevens geen “uitvloeisel” van hun kernbezigheid. Het is immers niet zo dat KBS in alle juridische kwesties gezondheidspersoonsgegevens verwerkt om juridische bijstand te verlenen.¹⁸⁸ KBS verwerkt immers niet bij elke zaak gezondheidspersoonsgegevens. KBS is namelijk niet alleen actief in de medische wereld, maar is ook actief op andere rechtsgebieden, zoals arbeidsrecht, ondernemingsrecht en insolventie.¹⁸⁹ Reden waarom zij ook over veel dossiers beschikt die geen gezondheidspersoonsgegevens bevatten. Het verwerken van gezondheidspersoonsgegevens zal wellicht bij hoogstens 50% het geval zijn. Gezien deze beargumentering is KBS van mening dat zij niet hoofdzakelijk is belast met het verwerken van gezondheidspersoonsgegevens.¹⁹⁰

Het tweede onderdeel van het derde criterium betreft de vraag of KBS – indien zij toch hoofdzakelijk zou zijn belast met het verwerken van gezondheidspersoonsgegevens – gezondheidspersoonsgegevens op een grootschalige manier verwerkt. Zoals in hoofdstuk 4 is aangegeven, dient bij de invulling van het begrip “grootschalig” te worden gekeken naar de hoeveelheid verwerkte persoonsgegevens, de duur van de verwerking en de omvang van de verwerking. De AP heeft aangegeven dat een ziekenhuis als grootschalig wordt aangemerkt, maar een solistische huisarts niet. KBS verwerkt de gezondheidspersoonsgegevens niet langer dan een zorginstelling. Zo heeft een zorginstelling een bewaarplicht van 15 jaar, wat wellicht wordt verhoogd naar 20 jaar¹⁹¹, en hebben advocaten een dossierplicht van 5 jaar, waarbij de Orde van Advocaten een termijn van 20 jaar adviseert.¹⁹² De geografische reikwijdte verschilt niet in die zin dat KBS ook gezondheidspersoonsgegevens van personen van het gehele land verwerkt, maar het aantal waarop dit gebeurt, is aanzienlijk minder dan dat van een zorginstelling.¹⁹³ De omvang van de verwerking is dan ook relevant.¹⁹⁴

¹⁸⁷ Groep Gegevensbescherming Artikel 29, 2017a, p. 8.

Zoals in hoofdstuk 4 is beschreven, adviseert de LHV huisartsen geen FG aan te stellen, aangezien een solistische huisarts op jaarbasis van 2.168 patiënten persoonsgegevens¹⁹⁵ verwerkt en dit niet als grootschalig kan worden aangemerkt.¹⁹⁶ Daarnaast is onlangs door de AP aangegeven dat een huisarts een FG moet aanstellen, wanneer hij beschikt over meer dan 10.000 patiënten¹⁹⁷ (zie hoofdstuk 4). KBS heeft daarentegen op jaarbasis maximaal 400 medisch juridische kwesties, waardoor zij ongeveer op jaarbasis van 400 personen gezondheidspersoonsgegevens verwerkt.¹⁹⁸ Wanneer KBS wordt afgezet tegen een solistische huisarts, dan verwerkt KBS aanzienlijk minder gezondheidspersoonsgegevens dan een solistische huisarts. Volgens de AP is een solistische huisarts niet grootschalig en dus is een solistische huisarts niet verplicht om een FG aan te stellen. Gezien het feit dat KBS aanzienlijk minder gezondheidspersoonsgegevens verwerkt dan een solistische huisarts, is er bij KBS dus ook geen sprake van grootschalige verwerking van gezondheidspersoonsgegevens en dus is tevens niet voldaan aan het derde criterium om een FG aan te stellen.¹⁹⁹

Gezien het voorstaande is KBS van mening dat zij met kracht kan betogen dat zij niet voldoet aan één van de drie criteria om een FG aan te stellen. Reden waarom KBS niet verplicht is om een FG aan te stellen en zij dit dan ook niet zal doen.

Ad 2) De verplichting om een DPIA uit te voeren

Zoals in hoofdstuk 4 van het onderzoeksrapport is aangegeven, is een verwerkingsverantwoordelijke in bepaalde gevallen verplicht om een DPIA uit te voeren, namelijk: als een gegevensverwerking waarschijnlijk een hoog privacyrisico voor de betrokkene oplevert.²⁰⁰ Hiervan is in ieder geval sprake, wanneer een organisatie:

- Persoonlijke aspecten systematisch en uitvoerig evalueert, waaronder profilering;
- Het op grote schaal verwerken van bijzondere persoonsgegevens;
- Het op grote schaal en systematisch volgen van mensen in een publiek toegankelijk gebied.²⁰¹

Om te beoordelen of er sprake is van een hoog risico, heeft Artikel 29 Werkgroep negen punten benoemd. Wanneer aan twee of meer van deze punten is voldaan, dan is er sprake van een hoog risico. Voor een volledig overzicht hiervan wordt verwezen naar paragraaf 4.6 van het onderzoeksrapport.

Zoals hiervoor onder ad 1 van de onderhavige paragraaf is aangegeven, stelt KBS zich op het standpunt dat zij geen persoonsgegevens analyseert op het gedrag van personen.

¹⁹⁵ Kursten, 13 juli 2017, p. 3.

¹⁹⁶ Landelijke Huisartsenvereniging, "Analyse LHV: Functionaris Gegevensbescherming voor meeste praktijken niet noodzakelijk", bekeken op 13 mei 2018

¹⁹⁷ Autoriteit Persoonsgegevens, "AP geeft uitleg over grootschalige gegevensverwerking in de zorg", bekeken op 7 juni 2018



²⁰⁰ Schermer, Hagenauw & Falot, 2018, p. 54

²⁰¹ Schermer, Hagenauw & Falot, 2018, p. 54

Reden waarom er geen sprake is van profilering.²⁰² Verder volgt KBS geen personen in een publiek toegankelijk gebied.²⁰³ Reden waarom het eerste criterium en het derde criterium niet op KBS van toepassing zijn.²⁰⁴ Voor de invulling van het tweede criterium geldt het volgende: KBS verwerkt bijzondere persoonsgegevens, namelijk gezondheidspersoonsgegevens, maar zij verwerkt dit niet op grote schaal.²⁰⁵ Een inhoudelijke uitleg over de beargumentering waarom KBS geen gezondheidspersoonsgegevens verwerkt op grote schaal, is terug te lezen onder ad 1 van de onderhavige paragraaf. Hierdoor is niet voldaan aan twee van de negen punten opgesteld door Artikel 29 Werkgroep en is er hierdoor niet voldaan aan de zojuist genoemde criteria voor het verplicht uitvoeren van een DPIA. KBS is dan ook van mening dat zij met kracht kan betogen dat zij niet is verplicht om een DPIA uit te voeren.²⁰⁶

Ondanks het feit dat KBS van mening is dat zij geen DPIA moet uitvoeren, is KBS zich bewust van het feit dat zij gevoelige persoonsgegevens (gezondheidspersoonsgegevens) verwerkt.²⁰⁷ Reden waarom KBS zowel technische als organisatorische beveiligingsmaatregelen treft om zo de privacy van betrokkenen te beschermen. KBS neemt onder andere de volgende beveiligingsmaatregelen: clean-desk-policy, dossierkasten op slot, sleutels van dossierkast in een kastje voorzien van een toegangscode, protocol over dossier meenemen naar huis, beveiligd e-mailen via ZIVVER, archief slechts toegankelijk met sleutel, container in garage in plaats van op straat, inloggen via een beveiligde server om bij digitale dossier te kunnen komen, geheimhoudingsverklaringen voor ondersteunend personeel en het opruimen van K-schijf en Outlook en deze bestanden overzetten naar de beveiligde server.²⁰⁸

7.5 De invulling van de rechten van betrokkenen binnen KBS

In hoofdstuk 5 van het onderzoeksrapport zijn de verschillende rechten voor een betrokkene beschreven. In hoofdstuk 1 van het onderzoeksrapport is aangegeven dat de opdracht van KBS toeziet op het weergegeven van een algemeen beeld van de AVG, waarbij expliciet wordt ingezoomd op twee rechten van betrokkene vanuit de AVG, namelijk het recht op inzage tegenover het beroepsgeheim van een advocaat en het recht op verwijdering tegenover de dossierplicht van een advocaat.

Ad 1) Het recht op inzage tegenover het beroepsgeheim van een advocaat

De advocaten van KBS hebben vanuit hun ambt een beroepsgeheim en de overige medewerkers van KBS hebben een geheimhoudingsverklaring ondertekend om het beroepsgeheim te waarborgen. In het geval de cliënt zelf een verzoek tot inzage doet, dan wordt hier gehoor aan gegeven.²⁰⁹



Een cliënt heeft immers recht op inzage van zijn dossier. Een cliënt kan het dossier bijvoorbeeld willen ontvangen met het doel om over te stappen naar een andere advocaat. Aantekeningen van de advocaat worden wel uit het dossier verwijderd.²¹⁰ Wanneer een ander dan de cliënt om inzage van het zaakdossier vraagt, dan wordt dit strikt geweigerd. Dit in verband met het beroepsgeheim van een advocaat en om de rechten van de cliënt te beschermen.²¹¹ Voor een inhoudelijke uitleg over een afwijzing van het verzoek om verwijdering van een ander dan de cliënt, wordt hierbij verwezen naar hoofdstuk 5 van het onderzoeksrapport.

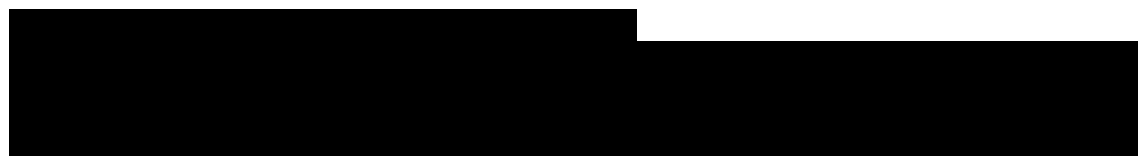
Ad 2) Het recht op verwijdering tegenover de dossierplicht van een advocaat

KBS bewaart zaakdossiers na sluiting van het dossier voor een periode van zeven jaar.²¹² Dit in verband met de dossierplicht. De Orde van Advocaten adviseert echter om zaakdossiers 20 jaar te bewaren in verband met de verjaringstermijn voor een tuchtklacht. KBS bewaart de zaakdossiers nu nog voor een periode van zeven jaar, maar er wordt overwogen om dit te verhogen naar 20 jaar gelet op de wettelijke verjaringstermijn.²¹³ In hoofdstuk 5 is uiteen gezet dat een advocaat gelet op de dossierplicht en het eigen belang om een zaakdossier te bewaren, bijvoorbeeld bij de angst voor een tuchtklacht, geen gehoor hoeft te geven aan het verzoek van een betrokkene om het dossier te verwijderen. Voor een volledige uitleg wordt hierbij tevens verwezen naar hoofdstuk 5 van het onderzoeksrapport. De medewerkers op het gebied van privacy van KBS hebben aangegeven dat het verzoek om verwijdering per geval zal worden bekeken, maar dat het belang van de cliënt of het belang van de advocaat voorop staat.²¹⁴ Hierdoor zal niet tot verwijdering van het dossier worden overgegaan.

7.6 De mate van kennis over de AVG bij de advocaten van KBS

Om in het advies in het onderzoeksrapport te kunnen aansluiten bij het kennisniveau van de advocaten van KBS en om de advocaten meer bewust te laten worden met de AVG, is middels een enquête onderzocht in welke mate de kennis van de AVG bij de advocaten van KBS bekend is. De resultaten zijn terug te vinden in bijlage X. In de resultaten is terug te zien dat de meeste vragen (7/11) met meer dan 50% goed zijn beantwoord en slechts enkele vragen met minder dan 50% (4/11) goed zijn beantwoord. Hiermee is 63,63% van de vragen correct beantwoord en is slechts 36,36% fout beantwoord.

De vragen die fout zijn beantwoord, gingen over tot nu toe nog onduidelijke termen van de AVG, zoals "grootschalige verwerking" en "hoog risico". In de AVG zijn deze termen niet gedefinieerd. Artikel 29 Werkgroep heeft geprobeerd de begrippen middels criteria enigszins te verduidelijken, maar 100% zekerheid is er nog niet. De praktijk met de AVG zal dit later moeten aantonen. De tot nu toe nog heersende onduidelijkheid over de invulling van de begrippen zou een reden kunnen zijn waarom er bij de advocaten van KBS nog onvoldoende duidelijkheid heerst over het invullen van deze begrippen.



Tijdens de enquête zijn criteria gegeven om een dergelijk geval te kunnen beoordelen. Voorts is aangegeven dat er nog geen 100% duidelijkheid is, maar dat dit hoogst waarschijnlijk wel zal komen.²¹⁵ Zodra het zover is, worden de advocaten hiervan op de hoogte gebracht. In het onderzoeksrapport is ingegaan op de “vage termen” van de AVG, zodat hierover meer duidelijkheid en kennis bij de advocaten van KBS ontstaat.

²¹⁵ *Kamerstukken II 2017/18, 34 851, nr. 21*

Hoofdstuk 8: Conclusie

Hoofdstuk 8 geeft een antwoord op de centrale vraag van dit onderzoek en geeft tevens de eindconclusie van het voorliggend rapport weer. In het onderstaand kader is de centrale vraag herhaald.

“Welk advies kan er aan de hand van wetsanalyse, literatuuronderzoek en interviews aan KBS Advocaten worden gegeven over de implementatie van het privacybeleid en het verwerken van persoonsgegevens, en in het bijzonder gezondheidspersoonsgegevens, zodat KBS voldoet aan de vereisten van de Algemene verordening gegevensbescherming (AVG)?”

Om antwoord te kunnen geven op de onderzoeksvraag zijn dertien deelvragen opgesteld en in de voorgaande hoofdstukken beantwoord. In dit hoofdstuk worden conclusies getrokken en advies gegeven. De conclusies en daarmee het advies zijn gebaseerd op de onderzoeksresultaten. De onderzoeksresultaten hebben geleid tot een duidelijk beeld omtrent de gevolgen van de AVG voor KBS. De indeling van de voorgaande hoofdstukken is terug te zien in de indeling van de paragrafen.

8.1 De AVG is van toepassing op KBS

De AVG ziet toe op het verwerken van persoonsgegevens van betrokkenen. KBS kent een aantal betrokkenen binnen haar organisatie: de (potentiële) cliënt, de (advocaat van de) wederpartij, de leveranciers, de bezoekers, de (potentiële) werknemers, de studentstagiaires en de leden van de nieuwsbrief. Van deze betrokkenen verwerkt KBS persoonsgegevens, waaronder gewone persoonsgegevens, zoals NAW gegevens, alsmede in bepaalde gevallen bijzondere persoonsgegevens, namelijk gezondheidspersoonsgegevens. Er is bij KBS sprake van een gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, namelijk digitale dossiers en papieren dossiers. De verwerkte persoonsgegevens worden daarnaast binnen de Europese Unie verwerkt. Voorts is er geen sprake van een van de uitzonderingen van artikel 2 lid 3 AVG. Reden waarom KBS onder het toepassingsbereik van de AVG valt en KBS aan de formaliteiten van de AVG moet voldoen.

8.2 De grondslagen voor het rechtsgeldig verwerken van persoonsgegevens binnen KBS

Een van de beginselen van de AVG is het rechtmatig verwerken van persoonsgegevens. Om hieraan te voldoen, moet de gegevensverwerking voldoen aan de vereisten van de AVG voor het rechtmatig verwerken van persoonsgegevens. KBS voldoet aan dit vereiste.

Om gewone persoonsgegevens rechtmatig te verwerken, moet zijn voldaan aan een van de grondslagen van de AVG. In het geval van KBS wordt bij elke gegevensverwerking voldaan aan een van de grondslagen van de AVG, namelijk de grondslag “overeenkomst” of de grondslag “gerechtvaardigd belang”. In het geval de persoonsgegevens worden verwerkt van de (potentiële) cliënt, de leveranciers, de (potentiële) werknemers en de studentstagiaires, dan wordt de gegevensverwerking gebaseerd op de grondslag “overeenkomst”.

In het geval de persoonsgegevens worden verwerkt van de (advocaat van de) wederpartij, de bezoekers (waaronder camerabeelden) of de leden van de nieuwsbrief (waaronder direct marketing), dan wordt de gegevensverwerking gebaseerd op de grondslag "gerechtvaardigd belang".

KBS verwerkt naast gewone persoonsgegevens ook bijzondere persoonsgegevens. Het verwerken van bijzondere persoonsgegevens is in beginsel bij de AVG verboden, tenzij men zich op een van de grondslagen voor het verwerken van gewone persoonsgegevens en op een voorwaarde voor het verwerken van bijzondere persoonsgegevens kan scharen. KBS verwerkt gezondheidspersoonsgegevens van de (potentiële) cliënt en/of de wederpartij. In dit geval kan KBS zich bij de (potentiële) cliënt beroepen op de grondslag "overeenkomst" en bij de wederpartij op de grondslag "gerechtvaardigd belang" en bij beide op de voorwaarde "instelling, onderbouwing, uitoefening van de rechtsvordering".

In het geval KBS gezondheidspersoonsgegevens van een werknemer verwerkt, dan kan zij dit baseren op de grondslag "overeenkomst" en de voorwaarde "Uitvoering van arbeids- en sociaalzekerheidsrechtelijke rechten van de verwerkingsverantwoordelijke".

8.3 De posities van verwerkingsverantwoordelijke en verwerker binnen KBS

Gezien het feit dat KBS het doel en de middelen voor de gegevensverwerking bepaalt, namelijk het verlenen van juridische bijstand, wordt KBS aangemerkt als verwerkingsverantwoordelijke.²¹⁶ Uit het onderzoek is gebleken dat het onwenselijk is om een individuele advocaat van een advocatenkantoor als verwerkingsverantwoordelijke aan te merken. Reden waarom KBS Advocaten N.V. de verwerkingsverantwoordelijke betreft en niet de advocaten van KBS. KBS maakt daarnaast gebruik van verschillende verwerkers, waarmee verwerkersovereenkomsten zijn gesloten of worden gesloten. Voor wat betreft het cameratoezicht kan worden geconcludeerd dat KBS geen verwerkingsverantwoordelijke en geen verwerker is. De verhuurder is de verwerkingsverantwoordelijke en het camerabedrijf de verwerker.

8.4 De invulling van de verplichtingen van de AVG bij KBS

Gezien het feit dat KBS verwerkingsverantwoordelijke is, rust er een verantwoordingsplicht op KBS. Hierdoor moet KBS voldoen en kunnen aan de verplichtingen van de AVG en moet zij dit aantonen. De verplichtingen voor de verwerkingsverantwoordelijke vanuit de AVG worden hieronder afgezet tegenover KBS.



Verplichting vanuit de AVG	Moet KBS hieraan voldoen?	Toelichting
Registerplicht	Ja	Ondanks dat KBS minder dan 250 medewerkers heeft, moet zij toch – aangezien er bijzondere persoonsgegevens worden verwerkt - aan de registerplicht voldoen.
FG	Nee	KBS is geen overheidsorganisatie. Verder is er binnen KBS geen sprake van een regelmatige en stelselmatige observatie. Tot slot is KBS niet hoofdzakelijk belast met het verwerken van bijzondere persoonsgegevens
DPIA	Nee	Er is bij de gegevensverwerking geen hoog risico voor de betrokkenen van KBS. Dit aangezien er geen sprake is van profilering, observatie of grootschalige verwerking van bijzondere persoonsgegevens
Voorafgaande raadpleging	Nee	Aangezien KBS geen DPIA hoeft uit te voeren, hoeft zij geen voorafgaande raadpleging uit te voeren
Privacy by design & default	Ja	In het geval KBS kiest voor nieuwe technologieën, bijvoorbeeld een ander digitaal systeem dan Fortuna, moet zij van tevoren rekening houden met de privacy van betrokkenen
Beveiligingsmaatregelen	Ja	KBS moet beveiligingsmaatregelen treffen om de persoonsgegevens te beschermen. Zeker aangezien KBS gevoelige persoonsgegevens (gezondheidspersoonsgegevens) verwerkt, neemt zij beveiligingsmaatregelen, zoals genoemd in hoofdstuk 7.
Meldplicht datalekken	Ja	KBS moet in beginsel elk datalek aan de AP melden, tenzij het risico voor de betrokkene onwaarschijnlijk is.
Afspraken met verwerkers	Ja	KBS maakt gebruik van verwerkers en moet hiermee verwerkersovereenkomsten afsluiten

8.5 Het waarborgen van de rechten van betrokkenen bij KBS

KBS moet de rechten van betrokkenen waarborgen. Zo moet KBS onder meer voldoen aan de informatieplicht.

KBS geeft hieraan invulling op twee manieren: een privacystatement op de website voor de betrokkenen buiten de organisatie: cliënt, (advocaat van de) wederpartij, leveranciers, bezoekers en leden van de website) en een privacyprotocol voor de betrokkenen binnen de organisatie (werknemers en studentstagiaires). Wanneer een betrokkene zijn rechten wil uitoefenen, dan kan diegene zich richten tot Niels van den Burg of Erik Luijendijk.

In het onderzoek is specifiek ingegaan op de invulling van twee rechten: het recht op inzage en het recht op verwijdering. In het geval een betrokkene anders dan de cliënt een verzoek doet om inzage van het dossier, dan mag KBS hieraan, mede gelet op het beroepsgeheim van een advocaat en het beschermen van de rechten en vrijheden van de cliënt, geen gehoor geven. In het geval een cliënt om inzage verzoekt, geldt deze beperking niet en kan KBS gehoor geven aan het verzoek. In het geval een betrokkene een verzoek doet om verwijdering van het dossier, dan hoeft KBS hieraan geen gehoor te geven. In het geval een juridische procedure voortduurt, kan KBS zich namelijk baseren op de uitzondering "noodzakelijk i.v.m. rechtsvordering". In het geval een juridische kwestie is beëindigd, kan KBS zich baseren op de uitzondering "wettelijke plicht tot verwerken", namelijk haar dossierplicht en het belang om het dossier te bewaren. Bij een verzoek van een ander dan de cliënt om inzage dan wel verwijdering dient bij een reactie rekening te worden gehouden met het beroepsgeheim van een advocaat.

8.6 De kennis van de advocaten van KBS

Tot slot is in het onderzoek gekeken naar de mate waarin de kennis over de AVG bij de advocaten van KBS aanwezig is. Gezien het hoge resultaat van goed beantwoorde vragen (rond 70%), kan worden geconcludeerd dat de advocaten van KBS op de hoogte zijn van de veranderingen en de gevolgen van de AVG. Wel is er vraag naar duidelijke handvaten over de vage termen van de AVG.

Hoofdstuk 9 – Aanbevelingen

Hoofdstuk 9 ziet toe op de aanbevelingen die naar aanleiding van het onderzoeksrapport aan KBS kunnen worden gegeven. Op grond van de conclusies van hoofdstuk 8 kunnen de volgende aanbevelingen aan KBS worden gedaan.²¹⁷

²¹⁷ De AVG geldt vanaf 25 mei 2018 rechtstreeks voor alle lidstaten. Wanneer het onderzoeksrapport – en hiermee dus ook de aanbevelingen – aan KBS Advocaten worden overhandigd, is de AVG al rechtstreeks van toepassing. KBS Advocaten zal dan ook eigenlijk al vanaf 25 mei 2018 aan de AVG moeten voldoen. De aanbevelingen vloeien voort uit de conclusie. Het is mogelijk dat KBS Advocaten al aan de AVG voldoet, waardoor de aanbevelingen wellicht overbodig zijn. Desondanks is gekozen om een volledige overzicht van aanbevelingen te geven. Indien namelijk nog niet aan (een bepaalde categorie van de) AVG is voldaan, dan is het raadzaam dat KBS Advocaten zo spoedig mogelijk hieraan voldoet en de aanbevelingen (alsnog) in acht neemt.

Onderdeel vanuit de AVG	Situatie binnen KBS	Aanbeveling
De positie van verwerkingsverantwoordelijke	KBS is de verwerkingsverantwoordelijke	Gezien het feit dat KBS de verwerkingsverantwoordelijke is, is het raadzaam om in een privacystatement aan te geven hoe KBS invulling geeft aan de AVG en waarom zij voor bepaalde afwegingen heeft gekozen. Op deze manier kan, indien nodig, verantwoording worden afgelegd aan de AP.
Informatieplicht	KBS heeft een informatieplicht ten opzichte van de betrokkenen	Om aan de informatieplicht te voldoen, is het raadzaam om een privacystatement op te nemen. Een privacystatement kan op de website worden geplaatst voor de externe betrokkenen. Een privacystatement kan worden overhandigd aan de interne betrokkenen en kan worden opgenomen in het kantoorhandboek.
Grondslagen voor verwerkingen	KBS heeft bij elke categorie betrokkene een grondslag (en een voorwaarde in het geval bijzondere persoonsgegevens) om de desbetreffende persoonsgegevens te verwerken	Het is raadzaam om de grondslagen in de privacystatement te benoemen, evenals de beargumentering van de afweging die is gemaakt. Op deze manier voldoet KBS niet alleen aan de verplichting dat zij een grondslag moet hebben, maar toont zij tevens aan waarop zij deze grondslag baseert (verantwoordingsplicht). Voor de volledigheid wordt aanbevolen om de verhuurder als verwerkingsverantwoordelijke voor het cameratoezicht te beschouwen en deze keuze op te nemen in de privacystatement. Voor wat betreft het versturen van de nieuwsbrief (direct marketing), wordt zekerheidshalve aanbevolen om, naast de grondslag gerechtvaardigd belang, toestemming te vragen aan de leden van de nieuwsbrief.
Privacy by design & default	KBS is verplicht om voorafgaand aan nieuwe processen en/of technologieën de privacy mee te nemen in het ontwerpproces	Het is raadzaam om, in het geval er nieuwe processen / technologieën komen (bijvoorbeeld een nieuw digitaal systeem) om samen met Niels van den Burg en Erik Luijendijk te kijken hoe hierbij met de privacy kan worden omgegaan.

Onderdeel vanuit de AVG	Situatie binnen KBS	Aanbeveling
FG	KBS is niet verplicht om een FG aan te stellen	Het is raadzaam om iemand in de organisatie te benoemen die toeziet op de privacy. Gezien het feit dat Niels van den Burg en Erik Luijendijk zich bezighouden met de AVG en de privacystatement hebben geschreven, is het raadzaam om hen als contactpersoon te benoemen. Zowel interne als externe betrokkenen kunnen zich dan tot hen wenden en zij kunnen een verzoek afhandelen. Een uitzondering hierop is als volgt: gezien de gezagsverhoudingen binnen de organisatie, is het raadzaam dat de aandeelhouders toezien op het naleven van de privacyregels binnen KBS, zoals de beveiligingsmaatregelen. Gezien het feit dat er een grijs gebied bestaat over de invulling van de criteria over het aanstellen van een FG, is het raadzaam om de ontwikkelingen hierover te blijven volgen en naar aanleiding van eventuele nieuwe criteria opnieuw te bekijken of een FG noodzakelijk is. Niels van den Burg en Erik Luijendijk dienen dit te volgen en de rest van het kantoor van updates te voorzien.
DPIA	KBS is niet verplicht om een DPIA uit te voeren	Aangezien KBS gevoelige persoonsgegevens verwerkt, is het raadzaam om passende beveiligingsmaatregelen te treffen. De aanbevolen beveiligingsmaatregelen worden hieronder weergegeven. Het is raadzaam om – net zoals bij de FG – de ontwikkelingen te blijven volgen, aangezien het nog niet duidelijk is wat er in de AVG precies wordt verstaan onder “hoog risico”. Hiervoor geldt dezelfde aanbeveling als bij de FG.
Voorafgaande raadpleging	KBS is niet verplicht om een voorafgaande raadpleging te treffen	Indien in de toekomst blijkt dat KBS wel een DPIA moet uitvoeren, is het raadzaam om te kijken of KBS in dat geval wel een voorafgaande raadpleging moet doen.

Onderdeel vanuit de AVG	Situatie binnen KBS	Aanbeveling
Meldplicht datalekken	KBS is in beginsel verplicht om iedere datalek aan de AP te melden, tenzij er een onwaarschijnlijk hoog risico is voor de betrokkene	Het is raadzaam om binnen de organisatie een protocol op te stellen, waarin wordt aangegeven dat elke datalek (van welke omvang dan ook) aan Niels van den Burg en/of Erik Luijendijk moet worden gemeld. De vraag of er sprake is van een "hoog risico voor de betrokkene" verschilt per geval. Het is raadzaam om deze afweging te laten nemen door de aandeelhouders samen met Niels van den Burg en Erik Luijendijk. Bij twijfel is het raadzaam om het datalek te melden aan de AP. In dat geval is immers in ieder geval aan de verplichting voldaan.
Afspraken met verwerkers	KBS maakt gebruik van verwerkers	Het is raadzaam om met elke verwerker een verwerkersovereenkomst aan te gaan. In het geval er een nieuwe verwerker komt, dient bij het aangaan van de overeenkomst tevens de verwerkersovereenkomst te worden aangegeven.
Rechten van betrokkenen	KBS moet de rechten van betrokkenen in acht nemen en aangegeven dat zij hieraan voldoet	Het is raadzaam om in het privacystatement (zowel extern als intern) op te nemen bij wie een betrokkene een verzoek kan doen voor het uitoefenen van zijn rechten. Het is raadzaam om dit verzoek door te sturen naar Niels van den Burg en/of Erik Luijendijk. Zij kunnen het verzoek af handelen in overleg met de betrokkene (en de desbetreffende advocaat).

Gelet op de gevoelige gegevens (gezondheidspersoonsgegevens) die KBS verwerkt en om de privacy van betrokkenen te waarborgen, worden de volgende passende technische en organisatorische maatregelen binnen KBS Advocaten aanbevolen:

- Het is raadzaam het volgende op te nemen in een protocol aan de advocaten van KBS Advocaten:
 - Advocaten moeten erop toezien dat zijn of haar secretaresse werkt ingevolge het privacyprotocol met betrekking tot zaakdossiers;
 - Advocaten moeten communiceren met cliënten en andere betrokkene via de professionele wijze, bijvoorbeeld via zakelijke e-mail, en niet via privé e-mail of WhatsApp;
 - Advocaten mogen het zaakdossier mee naar huis nemen, maar mogen deze niet laten rondslingeren. Denk hierbij aan veilig opbergen, zodat anderen niet bij het dossier kunnen;
 - Advocaten mogen enkel werken via het beveiligde systeem (Fortuna) en dus niet via een ander digitaal systeem;
 - Advocaten mogen enkel hun zakelijke e-mail op hun telefoon, wanneer de telefoon is voorzien van een wachtwoord;
 - Advocaten mogen niet werken vanaf een onbekend Wifi-netwerk.
- Het is raadzaam alle medewerkers te verplichten om alle dossiers en inhoudelijke stukken aan het einde van de werkdag in de dossierkast op te ruimen en de dossierkasten op slot te doen;
- Het is raadzaam om een sleutelkastje aan te schaffen, zodat de sleutels van de dossierkasten kunnen worden opgeborgen. Het sleutelkastje kan enkel met een code worden geopend.
- Het is raadzaam om alle medewerkers te verplichten om e-mails met inhoudelijke (en gevoelige) informatie, zoals concept dagvaarding, voortaan via een beveiligde manier te versturen (ZIVVER);
- Het is raadzaam om alle medewerkers te verplichten om documenten met betrekking tot zaakdossier alleen digitaal te verwerken in Fortuna en niet meer in de K-schijf of in Outlook. Om deze verplichting daadwerkelijk tot uitvoering te laten komen, is het raadzaam hier een termijn aan te stellen, bijvoorbeeld twee maanden. Alle documenten na de termijn worden verwijderd;
- Het is raadzaam om het wachtwoord te blijven veranderen, bijvoorbeeld maandelijks een melding krijgen dat het wachtwoord dient te worden veranderd;
- Het is raadzaam om een mogelijkheid te creëren om verzonden e-mails in te trekken, bijvoorbeeld wanneer een e-mail (met gevoelige inhoud) naar de verkeerde persoon is verzonden. Dit zou wellicht kunnen worden besproken met ZIVVER;
- Het is raadzaam om in plaats van e-mail op privételefoon te activeren, een zaaktelefoon te hebben;
- Het is raadzaam om de mogelijkheid te hebben om de gegevens van een (zaak)telefoon via een afstand te kunnen verwijderen;
- Het is raadzaam om een veilige opslagplek voor de back up te realiseren, bijvoorbeeld in de Cloud;

- Het is raadzaam om de medewerkers van KBS Advocaten te attenderen op het protocol bij telefoneren: Indien er wordt gebeld en er zitten mensen in de wachtkamer die het gesprek zouden kunnen horen, dan mag de naam van de bellende persoon niet worden genoemd (bij het doorverbinden).

Wellicht is de aanbeveling overbodig, aangezien het protocol al bestaat en door de vaste receptioniste wordt nageleefd. Echter, de oproepkrachten / secretaresses die de vaste receptioniste soms vervangen, weten vaak niet van het protocol af / houden zich niet aan het protocol.

Literatuur- en bronnenlijst

➤ Literatuur

ARTICLE 29 DATA PROTECTION WORKING PARTY, 2010

ARTICLE 29 DATA PROTECTION WORKING PARTY, "*Opinion 1/2010 on the concepts of "controller" and "processor"*", 16 februari 2010.

Van Balen & Nijveld, 2017

C. van Balen & O.S. Nijveld, '*De Algemene verordening gegevensbescherming: een introductie voor de zorgsector*', Tijdschrift voor Gezondheidsrecht 2017 (41), 2017.

College bescherming persoonsgegevens, 2016

College bescherming persoonsgegevens, "*Beleidsregels cameratoezicht*", 2 juni 2016

Comijs, 2017

D. Comijs, '*De bescherming van bijzondere persoonsgegevens in de Uitvoeringswet AVG*', NJB 2017/1281, 13 juni 2017

Groep Gegevensbescherming Artikel 29, 2017a

Groep Gegevensbescherming Artikel 29, "*Richtlijnen voor functionarissen voor gegevensbescherming (Data Protection Officer, DPO)*", 5 april 2017.

Groep Gegevensbescherming Artikel 29, 2017b

Groep Gegevensbescherming Artikel 29, "*gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking waarschijnlijk een hoog risico inhoudt in de zin van Verordening 2016/679*", 4 oktober 2017

Van der Jagt, 2013

F.C. van der Jagt, '*De nationale, Europese en internationale dimensie*', Arse Aqui, 15 juli 2013

Kursten, 2017

drs. J.C.E. Kursten, '*Vaststelling beleid huisartsenzorg en multidisciplinaire zorg 2018*', Nederlandse Zorgautoriteit, 13 juli 2017

Nederlandse Orde van Advocaten, 2004

Nederlandse Orde van Advocaten, "*Archivering op het advocatenkantoor*", februari 2004

Nederlandse Orde van Advocaten, 2018

Nederlandse Orde van Advocaten, "*Gedragsregels 2018*", 14 februari 2018.

Schermer, Hagenauw & Falot, 2018

B.W. Schermer, D. Hagenauw, N. Falot, '*Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming*', Ministerie van Justitie & Veiligheid, januari 2018.

Vermissen, Terstegge & Krijgsman, 2017

K. Vermissen, J. Terstegge, N. Krijgsman, "Grip op de AVG. De nieuwe privacywet voor niet-juristen", Wolters Kluwer, Deventer, 2017.

Zwenne & Mommers, 2016

G.J. Zwenne & I. Mommers, '*De tien belangrijkste veranderingen die de Algemene verordening gegevensbescherming gaat brengen (in minder dan vijfduizend woorden)*', Tijdschrift voor Compliance, 2016/4.

➤ Kamerstukken

Kamerstukken II 1997/98, 25892, nr. 3, (MvT)

Kamerstukken II 2017/18, 34 851, nr. 21

Kamerstukken I 2017/18, 34 851, nr. 144

➤ Elektronische bronnen

Autoriteit Persoonsgegevens, "Rechten van betrokkenen", bekeken op 25 februari 2018, <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/rechten-van-betrokkenen> (zoek op: AP rechten van betrokkenen)

Autoriteit Persoonsgegevens, "Mag u persoonsgegevens verwerken?", bekeken op 13 mei 2018, <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/mag-u-persoonsgegevens-verwerken#wanneer-mag-u-zich-baseren-op-de-grondslag-algemeen-belang-of-openbaar-gezag-6329> (zoek op: Voorbeeld algemeen belang AVG)

Autoriteit Persoonsgegevens, "AP geeft uitleg over grootschalige gegevensverwerking in de zorg", bekeken op 7 juni 2018, <https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-geeft-uitleg-over-grootschalige-gegevensverwerking-de-zorg> (zoek op: AP geeft uitleg over grootschalige verwerking)

Landelijke Huisartsenvereniging, "Analyse LHV: Functionaris Gegevensbescherming voor meeste praktijken niet noodzakelijk", bekeken op 13 mei 2018, <https://www.lhv.nl/actueel/nieuws/analyse-lhv-functionaris-gegevensbescherming-voor-meeste-praktijken-niet-noodzakelijk> (zoek op: LHV geen FG)

➤ Jurisprudentie

Gerechtshof Amsterdam, 13 september 2016, ECLI:NL:GHAMS:2016:3739

Hoge Raad, 16 maart 2018, ECLI:HR:2018:365

Hoge Raad, 23 maart 2010, ECLI:NL:HR:2010:BK6331

Hoge Raad, 21 december 2010, ECLI:NL:HR:2010:BL7688

HvJ EU, 13 mei 2014, C-131/12, ECLI:EU:C:2014:317 (*Google Spanje SL, Google Inc. / Agencia Espanola de Proteccion de Datos, Mario Costeja Gonzalez*)

Parquet bij de Hoge Raad, 12 januari 2018, ECLI:NL:PHR:2018:45

Parquet bij de Hoge Raad, 23 maart 2010, ECLI:NL:PHR:2010:BK6331

Parquet bij de Hoge Raad, 21 december 2010, ECLI:NL:PHR:2010:BL7688