



AVG vervangt de Wbp, wat betekent dit voor de werkwijze van de directie P&O van de organisatie met betrekking tot de verwerking van persoonsgegevens?

Onderzoeksrapport

Module RE441C: afstudeeronderzoek

Volledig anoniem – exclusief bijlagen

Hogeschool Leiden		Opleiding HBO-Rechten
Student	Onderzoeksdocent:	Anoniem
Sanoniem	Afstudeerbegeleider:	Anoniem
Klas: Anoniem	Opdrachtgever:	Anoniem
		Anoniem
		Anoniem
	Praktijkbegeleiders:	Anoniem
		Anoniem
	Inleverdatum:	19-01-2017 Collegejaar 2016-2017 Blok 13-14 Reguliere kans

Voorwoord

Beste lezer,

Met veel plezier en nieuwsgierigheid heb ik praktijkonderzoek uitgevoerd voor de directie P&O van de organisatie. In 2014 mocht ik de organisatie al mijn opdrachtgever noemen toen ik er, eveneens bij de directie P&O in het kader van mijn studie stage liep. Dit onderzoeksrapport is geschreven ter afsluiting van de opleiding HBO-Rechten.

Wanneer ik mijn studie succesvol afrond, is dit voor een groot deel te danken aan de medewerking van de organisatie. Een onderzoeksrapport schrijft zichzelf namelijk niet en daarom en grijp ik deze gelegenheid graag aan om de volgende mensen te bedanken voor hun hulp:

Tijdens het onderzoek stonden *anoniem* en de *anoniem* voor mij klaar. Zonder de scherpe blikken, het vertrouwen en de steun was ik niet geweest waar ik nu ben. *Anoniem*, bij deze erg bedankt voor alle mogelijkheden, jullie tijd, het meedenken en de altijd openstaande deur, mailbox en telefoon! *Anoniem*, ik vind het bijzonder fijn dat jij mij zowel bij mijn stage als afstuderen hebt willen begeleiden. Je hebt zoveel meer gedaan dan dat. Ook alle participanten die ik heb mogen interviewen wil ik hartelijk danken voor hun medewerking.

Tot slot wil ik graag *anoniem* en *anoniem* van Hogeschool Leiden bedanken voor het gedeelde enthousiasme over het onderwerp van onderzoek en de feedback die ik heb mogen ontvangen gedurende de afstudeerfase.

Sassenheim, januari 2017

SAMENVATTING

Aanleiding onderzoek

De Nederlandse Wet bescherming persoonsgegevens (Wbp) vervalt op 25 mei 2018. Deze wordt vervangen door een Europese Verordening: Algemene Verordening Gegevensbescherming (AVG). De AVG zal van toepassing zijn in alle Europese lidstaten. Er wordt een transitieperiode van twee jaar gehanteerd. Kort gezegd krijgt een lidstaat twee jaar de tijd om te voldoen aan de eisen van de AVG. De opdrachtgever voor dit onderzoek, de organisatie, is een *anoniem* organisatie met circa *anoniem* medewerkers, waaronder externen. Vanzelfsprekend heeft de directie Personeel en Organisatie (P&O) van de organisatie als werkgever een fors aantal persoonsgegevens te verwerken. Nu de implementatietermijn van de AVG loopt en ook de organisatie in mei 2018 een boete riskeert als zij niet voldoet aan de eisen van de AVG, wil de directie P&O van de organisatie weten wat zij moet aanpassen aan haar manier van werken met persoonsgegevens om te voldoen aan de AVG.

Doelstelling

Het doel van dit onderzoek is het schrijven van een advies voor de directie P&O van de organisatie over hoe te werken met de AVG. Het advies moet beschrijven wat de directie P&O van de organisatie moet aanpassen aan haar werkwijze in omgang met persoonsgegevens, om zo aan de eisen van de AVG te kunnen voldoen. Als wordt voldaan aan de AVG wordt de organisatie niet beboet.

Centrale vraag

Welk advies kan aan de directie P&O van de organisatie worden gegeven over het aanpassen van haar werkwijze met betrekking tot het verwerken van persoonsgegevens om te voldoen aan de eisen van de AVG aan de hand van afgenomen interviews, analyse van wet- en regelgeving en literatuuronderzoek?

Methoden van onderzoek

Ter beantwoording van de centrale vraag zijn vijf deelvragen gesteld.

Wat betreft het theoretisch-juridische onderzoeksgedeelte is ten eerste onderzocht hoe de huidige wetgeving rondom de bescherming van persoonsgegevens volgens de Wbp is vormgegeven. Ten tweede is gekeken wat de AVG inhoudt. Ten derde zijn verschillen tussen de Wbp en de AVG opgemerkt en uiteengezet. Hierbij is gebruik gemaakt van analyse van wet- en regelgeving en literatuuronderzoek. In het praktijkgericht onderzoeksgedeelte is door middel van interviews de huidige werkwijze van de directie P&O van de organisatie met betrekking tot verwerking van persoonsgegevens (in naleving van de Wbp) bij vier onderwerpen in kaart gebracht. De interviews zijn afgenomen onder experts op het gebied van gegevensverwerking binnen de directie P&O van de organisatie. Voor elk van de vier onderwerpen van gegevensverwerking is de functionaris (hierna participant) geïnterviewd die over het onderwerp gaat en met de systemen werkt. Daardoor was het mogelijk een volledig beeld van gegevensverwerking binnen de directie P&O van de organisatie te vormen. Dezelfde participanten zijn bevraagd over de impact van de verschillen tussen de Wbp en de AVG met als doel een beeld van de (toekomstige) werkwijze van de directie P&O van de organisatie aangaande persoonsgegevens in naleving van de AVG te vormen.

Om verbinding tussen het theoretisch-juridisch onderzoeksgedeelte en het praktijkgericht onderzoeksgedeelte te creëren, zijn drie verschillende 'tools' gebruikt:

1. Tabellen: De rollen binnen het proces van gegevensverwerking vanuit het theoretisch-juridisch onderzoeksgedeelte zijn voor elk van de vier onderwerpen ingevuld voor de directie P&O van de organisatie zodat er zicht is op wie welke rol uitoefent binnen het gegevensverwerkingsproces.
2. Formulering interviewvragen: De kennis over de Wbp die is verkregen via het theoretisch-juridisch onderzoeksgedeelte, is gebruikt bij de formulering van interviewvragen over de huidige werkwijze van de directie P&O van de organisatie. Over elk hoofdstuk uit de Wbp zijn vragen gesteld. Ook zijn vragen bij de verschillen tussen de Wbp en AVG uit het theoretisch-juridisch onderzoeksgedeelte bedacht en voorgelegd aan de participanten.
3. Tijdens afname van de interviews kwam naar voren dat door de participanten gebruik wordt gemaakt van intern beleid. Dit is beleid wat naast de Wbp een intern kader vormt voor gegevensverwerking binnen de directie P&O van de organisatie. Zodoende is het beleid gebruikt ter ondersteuning van de resultaten uit de interviews.

Onderzoeksresultaten

Uit het praktijkgericht onderzoeksgedeelte komt naar voren dat de directie P&O van de organisatie haar huidige werkwijze met betrekking tot het verwerken van persoonsgegevens in naleving van de Wbp op zo een manier heeft ingevuld dat voldaan wordt aan de Wbp. Alle onderdelen van de

Wbp zijn geïntegreerd in de werkwijze en worden nageleefd. Een voorbeeld hiervan is dat in de naleving algemene beginselen van gegevensverwerking, het doel van een verwerking van persoonsgegevens, maar ook de controle en de wijze van beveiliging worden vastgelegd in een intern document. De participanten hebben een positief beeld voor ogen over de hoeveelheid aanpassingen die de huidige werkwijze van de directie P&O van de organisatie nodig heeft om 'AVG-proof' te worden. Als naar het totaalbeeld van de elf verschillen waarover participanten zijn bevraagd gekeken wordt, vinden participanten dat de meeste verschillen geen of beperkte verandering met zich meebrengen. De verschillen zijn onderverdeeld in de categorieën: geen invloed, beperkte invloed en invloed op de werkwijze.

Conclusie

Voorop staat dat de organisatie *anoniem* een voorbeeldfunctie heeft met betrekking tot verwerking van persoonsgegevens en privacy. Dit omdat de organisatie *anoniem Anoniem*

De huidige werkwijze van de directie P&O van organisatie met betrekking tot verwerking van persoonsgegevens voldoet aan de eisen van de Wbp, de huidige wetgeving. Dit is vastgesteld op basis van de informatie die naar voren is gekomen uit de interviews met de functionarissen binnen de directie P&O van organisatie die zich bezig houden met gegevensverwerking.

De AVG verschilt op een aantal punten met de Wbp. Het gaat dan om -kort gezegd- de volgende verschillen:

- Toestemming betrokkene aantonen
- Controle van toestemming ouder bij verwerking gegevens kind
- Meer verplichtingen verwerkingsverantwoordelijke en verwerker
- Uitbreiding rechten van betrokkene
- Verandering uitgangspunt meldplicht datalekken
- Vaststellen bewaartermijn persoonsgegevens
- Toename instrumenten doorgifte gegevens naar derde landen
- Privacy by design & privacy by default
- Verplichting werken Data Privacy Impact Assessment (D)PIA
- Meldplicht wordt documentatieplicht
- Verplichting functionaris gegevensbescherming

De participanten zijn bevraagd over deze verschillen tussen de Wbp en de AVG.

Uit de interviews komt naar voren dat de werkprocessen bij de directie P&O van organisatie op een aantal onderdelen moeten worden aangepast. Voor wat betreft twee verschillen geldt dit niet. Het gaat dan om de verplichting om te werken met een (D)PIA. Dit gebeurt al bij de directie P&O van de organisatie. En verder om de verplichting een functionaris gegevensbescherming te benoemen. De organisatie heeft al een functionaris gegevensbescherming. De directie P&O van de organisatie zou om te voldoen aan de overige verschillen moeten nagaan hoe bestaande inrichting van processen kan worden aangepast en deze aanpassingen vervolgens moeten vastleggen en uitvoeren. Vanuit de AVG wordt zwaar aangestuurd op accountability, de manier van werken en afwegingen voor bepaalde keuzes moeten inzichtelijk zijn en vaststaan. De directie P&O van de organisatie moet om te voldoen aan de AVG aandacht besteden aan de verschillen 7.1 tot en met 7.8 en 7.10 (zie hoofdstuk 7).

Aanbevelingen

Voor elk van de verschillen is een aanbeveling opgenomen voor de directie P&O van de organisatie over hoe hier mee om te gaan (ook voor de twee punten waar de directie P&O van de organisatie al aan voldoet). De aanbevelingen zijn onderverdeeld in algemene en concrete aanbevelingen. In totaal is sprake van elf concrete aanbevelingen en vier algemene.

Een selectie van de aanbevelingen:

- Algemeen: Vervang de huidige interne Wbp-handenboeken in handboeken over de AVG en zorg daarin voor verwijzingen naar artikelen uit de AVG;
- Concreet, toestemming betrokkene: Neem een clause op in documenten/formulieren waarin de betrokkene toestemming geeft voor gegevensverwerking (aanstellingsformulier). Doe dit zodat helder is waarvoor de betrokkene precies zijn toestemming geeft;

Concreet, uitbreiding rechten van betrokkene: Licht betrokkene in over zijn nieuwe rechten: vergetelheid en dataportabiliteit. Kaart aan in welke gevallen vergetelheid gerechtvaardigd is en wat de betrokkene moet doen om dit recht te kunnen genieten. Geef aan dat het recht op dataportabiliteit geen verandering met zich meebrengt en dat persoonsgegevens reeds mobiel zijn via het *Anoniem*.

INHOUDSOPGAVE

Samenvatting	2
Inhoudsopgave	4
Afkortingen	7
Hoofdstuk 1: Inleiding	8
1.1 Aanleiding onderzoek en probleemanalyse	8
1.2 Doelstelling, centrale vraag en deelvragen	9
1.3 Operationaliseren van begrippen	10
1.4 Onderzoeksmethode + verantwoording per deelvraag	10
Hoofdstuk 2: Het juridisch kader - Wet bescherming persoonsgegevens	12
2.1 Voorgeschiedenis	12
2.2 Karakterisering	12
2.3 Toepassingsbereik	12
2.3.1 Persoonsgegevens, wat zijn dat precies?	12
2.3.2 Wanneer is er sprake van?	13
2.4 Werken met persoonsgegevens	13
2.4.1 Verwerking van bijzondere persoonsgegevens	14
2.4.2 Uitzondering toepassing Wbp op verwerking gegevens	14
2.5 Territoriale reikwijdte	14
2.6 Rollen in proces gegevensverwerking	15
2.7 Materiële voorschriften bij het werken met persoonsgegevens	16
2.8 meldings- en informatieverplichting	16
2.8.1 Meldingsverplichting	16
2.8.2 Informatieverplichting	16
2.9 De meldplicht datalekken	17
2.10 Rechten van de betrokkene	17
2.11 Bewaartermijn persoonsgegevens	17
2.12 Doorgifte persoonsgegevens	18
2.13 Toezicht naleving en sancties	18
2.13.1 Toezicht op de naleving van Wbp	18
2.13.2 Sancties	18
2.14 Conclusie	19
Hoofdstuk 3: Het juridisch kader - Algemene Verordening Gegevensbescherming	20
3.1 Voorgeschiedenis	20
3.2 Karakterisering	21
3.3 Toepassingsbereik	21
3.4 Werken met persoonsgegevens	21
3.5 Territoriale reikwijdte	21
3.6 Materiële voorschriften bij het werken met persoonsgegevens	22
3.6.1 Algemene beginselen van gegevensverwerking	22
3.6.2 Rechtmatige verwerking	22
3.7 Rollen in proces gegevensverwerking	24
3.8 Rechten van de betrokkene	25
3.9 Verplichtingen verwerkingsverantwoordelijke	26
3.10 Verplichtingen verwerker	26
3.11 Gezamenlijke verplichtingen verwerkingsverantwoordelijke en verwerker	26
3.11.1 Beveiliging gegevensverwerking	26
3.11.2 Functionaris voor gegevensbescherming	26
3.11.3 Privacy by design – privacy by default	27
3.12 De meldplicht datalekken	27
3.13 Toezicht naleving, handhaving en sancties	28
3.13.1 Toezicht	28
3.13.2 Handhaving	28
3.13.3 Sancties	28
3.14 Conclusie	29

Hoofdstuk 4: Het juridisch kader - Verschillen tussen de Wbp en AVG	30
4.1 Verschil tussen richtlijn en verordening – directe werking	30
4.2 Vergrote territoriale werkingssfeer	30
4.3 Vergrote materiële werkingssfeer	30
4.4 Meer verplichtingen voor verwerkingsverantwoordelijke en verwerker	31
4.5 Meldplicht wordt documentatieplicht	31
4.6 Uitbreiding rechten van betrokkene	31
4.7 Hogere boetes bij niet-naleving AVG dan bij niet-naleving Wbp	32
4.8 Verschillende uitgangspunten meldplicht datalekken	32
4.9 Toename instrumenten voor internationale doorgifte gegevens	32
4.10 Verplichting tot werken met (D)PIA	33
4.11 Aanstellen functionaris voor gegevensbescherming niet meer vrijwillig	33
4.12 Inkadering bewaartermijn persoonsgegevens	33
4.13 Oprichting Europees Comité voor gegevensbescherming	33
4.14 Mogelijkheid tot certificering organisaties	34
4.15 Aangescherpte check verwerking van persoonsgegevens van kinderen onder de 16	34
4.16 Verschil in rollen in proces gegevensverwerking tussen Wbp & AVG	34
4.17 Conclusie	36
Hoofdstuk 5: Totstandkoming resultaten	37
5.1 Methode	37
5.2 Participanten	37
5.3 Beknopte weergave onderwerp participant	37
5.4 Procedure interviews	38
5.5 Koppeling theorie naar praktijk	38
Hoofdstuk 6: Resultaten – Huidige werkwijze	39
6.1 Toepassing Wbp	39
6.2 Naleving algemene beginselen gegevensverwerking	40
6.3 Territoriale werking	40
6.4 Transparantie: meldings-en informatieverplichting	40
6.4.1 Meldingsverplichting	40
6.4.2 Informatieverplichting	40
6.5 Rechten van betrokkene: inzage, verzet en rectificatie	40
6.6 Meldplicht datalekken	41
6.7 Doorgifte persoonsgegevens naar derde landen	41
6.8 Verplichtingen verantwoordelijke en bewerker	42
6.9 Functionaris voor gegevensbescherming	42
6.10 Koppeling theorie naar praktijk: invulling tabellen rollen proces gegevensverwerking voor ANONIEM -P&O	42
6.11 Conclusie	43
Hoofdstuk 7: Resultaten - Beeld van toekomstige werkwijze	44
7.1 Toestemming betrokkene	44
7.2 Controle van toestemming ouder bij verwerking van gegevens kind & verbod	44
7.3 Meer verplichtingen verwerkingsverantwoordelijke en verwerker	45
7.3.1 Eigen register	45
7.3.2 Samen zorg voor beveiliging	45
7.4 Uitbreiding rechten van betrokkene	45
7.5 Verandering uitgangspunt meldplicht datalekken	46
7.6 Vaststellen bewaartermijn persoonsgegevens	46
7.7 Toename instrumenten doorgifte gegevens naar derde landen	46
7.8 Privacy by design & privacy by default	46
7.9 Verplichting werken (D)PIA	47
7.10 Meldplicht wordt documentatieplicht	47
7.11 Verplichting functionaris gegevensbescherming	47
7.12 Conclusie	48
Hoofdstuk 8: Conclusie en Aanbevelingen	49
8.1 Conclusie	49
8.2 Aanbevelingen	50
8.2.1 Bruikbaarheid	50

8.2.2 Doelstelling behaald	50
8.3 Verantwoording	51
Literatuurlijst	52
 Bijlagen	 55
<i>Anoniem</i>	

AFKORTINGEN

AMvB <i>Anoniem</i>	Algemene Maatregel van Bestuur
AP <i>Anoniem</i>	Autoriteit Persoonsgegevens
AVG Awb <i>Anoniem</i>	Algemene Verordening Gegevensbescherming Algemene wet bestuursrecht
BW <i>Anoniem</i>	Burgerlijk Wetboek
(D)PIA	(Data) Protection Impact Assessment
EC	Europese Commissie
EU	Europese Unie
EVRM	Europees verdrag inzake de rechten van de mens en de fundamentele vrijheden
FG	Functionaris voor de gegevensbescherming
GOR	Groepsondernemingsraad
Gw	Grondwet
MvT <i>Anoniem</i>	Memorie van Toelichting
VOG	Verklaring omtrent het gedrag
Wbp	Wet bescherming persoonsgegevens
WNT	Wet Normering Topinkomens
WPR <i>Anoniem</i>	Wet Persoonsregistraties
VWEU Stcrt.	Verdrag betreffende de Werking van de Europese Unie Staatscourant

HOOFDSTUK 1: INLEIDING

1.1. Aanleiding onderzoek en probleemanalyse

Situatieschets

Een ieder heeft recht op bescherming van zijn persoonsgegevens.¹ Dit recht is verankerd in de richtlijn Bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens. De richtlijn stamt uit 1995² en is in Nederland geïmplementeerd in de Wet bescherming persoonsgegevens (hierna Wbp) uit het jaar 2000. Privacy is aan verandering onderhevig. Dit is inherent aan de maatschappij, welke constant in beweging is. De Wbp beweegt ook mee. De laatste wijzigingen zijn doorgevoerd in januari 2016 en bestaan uit het instellen van de meldplicht datalekken en nieuwe boetebevoegdheden.³ Europa decentraal⁴, het kenniscentrum voor Europees recht en beleid voor (semi)overheidsorganisaties, erkent de ontwikkeling in digitalisering tussen 1995 en 2016 en de impact daarvan op privacy. Vanwege toename in dataverkeer en de ontwikkeling van de technologie, is de wetgeving op het gebied van privacy volgens het kenniscentrum toe aan vernieuwing.⁵

Om bescherming van persoonsgegevens anno 2016 te waarborgen, is vanuit de Europese Commissie en het Europees Parlement, de Algemene Verordening Gegevensbescherming (hierna AVG) tot stand gekomen.⁶ Dit totstandkomingsproces heeft zo'n vier jaar onderhandelen gekost.⁷ In de AVG staat (aanvullend) gemotiveerd waarom de huidige wetgeving niet meer afdoende is: "De mate waarin persoonsgegevens worden verzameld en gedeeld, is significant gestegen. Dankzij de technologie kunnen bedrijven en overheid bij het uitvoeren van hun activiteiten meer dan ooit tevoren gebruikmaken van persoonsgegevens (...). Die ontwikkelingen vereisen een krachtig en coherenter kader voor gegevensbescherming in de Unie, dat wordt gesteund door strenge handhaving, omdat zulks van belang is voor het vertrouwen dat nodig is om de digitale economie zich in de hele interne markt te laten ontwikkelen. Natuurlijke personen dienen controle over hun eigen persoonsgegevens te hebben. Er dient meer rechtszekerheid en praktische zekerheid te worden geboden aan natuurlijke personen, marktdeelnemers en overheidsinstanties."⁸

De AVG zal vanaf 25 mei 2018⁹ van toepassing zijn in alle Europese lidstaten. Vanaf deze datum geldt dan ook nog maar één privacywet in Europa, in plaats van nationale wetten op het gebied van privacy per lidstaat. In Nederland zal de Wbp worden ingetrokken.¹⁰ Er wordt een transitieperiode van twee jaar gehanteerd. Kort gezegd krijgt een lidstaat twee jaar de tijd om te voldoen aan de eisen van de AVG. Tijdens de transitieperiode geldt in Nederland onverkort de Wbp, na afloop van de periode vervalt deze.

De AVG heeft directe werking en hoeft niet meer in nationale wetgeving geïmplementeerd te worden¹¹, zoals bij de richtlijn uit 1995 het geval was. Uitvoeringswetgeving voor bepaalde onderdelen van de AVG volgt:

Op 9 december 2016 is de internetconsultatie gestart voor de Uitvoeringswet Algemene verordening gegevensbescherming. (Hierna: Uitvoeringswet). In deze wet wordt de intrekking van de Wbp geregeld. Verder bevat de wet bepalingen over de nationale toezichthouder, de Autoriteit persoonsgegevens. (Hierna: AP). Ook geeft de wet een nadere invulling van een aantal bepalingen van de AVG, bijvoorbeeld specifieke nationale regelgeving met betrekking tot genetische gegevens en specifieke uitzonderingen voor wetenschappelijk onderzoek. Tot en met 20 januari 2017¹² staat het een ieder vrij te reageren op het wetsvoorstel en bijbehorende toelichting.

Nadat de consultatieperiode verstreken is, worden alle reacties bekeken en wordt het wetsvoorstel eventueel aangepast. Het resultaat van de consultatie en de verwerking daarvan in het

¹ Art. 8 lid 1 Handvest van de grondrechten van de EU, art. 16 lid 1 VWEU.

² *Data Protection Directive* 95/46/EC.

³ Fennell e.a., 2016, p. 5.

⁴ Kenniscentrum voor Europees recht en beleid voor (semi)overheidsorganisaties. In 2002 mede opgericht door Ministerie van BZK.

⁵ Salverda, *Algemene Verordening Gegevensbescherming treedt in werking op 25 mei 2016*, Europa decentraal, 2016.

⁶ Vastgesteld op 27 april 2016.

⁷ Het eerste voorstel voor nieuwe privacywetgeving werd gepubliceerd door de Europese Commissie op 25-01-2012.

⁸ Europese Unie, PB L 119 van 4.5.2016, p. 2.

⁹ Art. 99 lid 2 AVG.

¹⁰ Art. 94 AVG.

¹¹ Kriens, *Algemene Verordening Gegevensbescherming*, VNG-ledenbrief, 12-07-2016.

¹² <https://www.internetconsultatie.nl/uitvoeringswetavg>.

conceptvoorstel, wordt in een verslag op hoofdlijnen vermeld en ook dit wordt openbaar gemaakt. Dat gebeurt nadat de Ministerraad (formeel de minister) het voorstel voor de Uitvoeringswet heeft goedgekeurd.¹³ Uiteindelijk zal de Uitvoeringswet worden ondertekend door de Minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK) samen met de Minister van Veiligheid en Justitie (VenJ). Net zoals bij dit bij de Wbp is gebeurd. Voorts zal er een invoeringswet tot stand moeten worden gebracht, waarmee alle verwijzingen in wetten naar de Wbp worden vervangen door een verwijzing naar de AVG of naar de Uitvoeringswet.¹⁴

Consequentie van de situatie

Als een organisatie/werkgever niet voldoet aan de AVG, kan een sanctie worden opgelegd. Deze sanctie kan bestaan uit een geldboete welke kan oplopen tot een bedrag van twintig miljoen euro of maximaal vier procent van de jaaromzet van een onderneming.¹⁵ De Nederlandse toezichthouder op naleving van de AVG is de AP.¹⁶

'Het probleem van de opdrachtgever'

De opdrachtgever is een *anoniem* organisatie met circa *anoniem* medewerkers, waaronder externen. Vanzelfsprekend heeft de directie P&O van de organisatie als werkgever een fors aantal persoonsgegevens te verwerken. De organisatieschets van de organisatie is opgenomen in bijlage 1. Nu de implementatietermijn van de AVG loopt en ook de organisatie in mei 2018 een boete riskeert als zij niet voldoet aan de eisen van de AVG, wil de directie P&O van de organisatie weten wat zij moet aanpassen aan haar manier van werken met persoonsgegevens om te voldoen aan de AVG.

In een intern memo van de organisatie over de uitvoering van de AVG;¹⁷ wordt aangegeven dat de AVG veel voorbereiding vergt van alle directies, zowel op het terrein van *anoniem*. In de memo wordt de verwachting uitgesproken dat zich waarschijnlijk knelpunten zullen voordoen bij de invoering en dat er vragen zullen komen over de uitleg van de AVG. Gelet op het belang van een rechtmatige verwerking van persoonsgegevens door de Rijksoverheid en door de organisatie, is het wenselijk om in een vroegtijdig stadium zicht op knelpunten en vragen te krijgen. Daarnaast wordt aangegeven dat met het vervallen van de Wbp voor alle *anoniem* het wettelijk kader waaronder voorheen gegevensverwerking plaatsvond, wijzigt. Er wordt benadrukt dat het van belang is dat de verschillende *anoniem* tijdig bekend raken zijn met de juridische kaders voor gegevensverwerking.

Concreet houdt dit in dat de directie P&O van de organisatie vragen heeft in aanloop naar werken met persoonsgegevens in naleving van de AVG:

Eerst is onderzocht hoe de huidige wetgeving rondom de bescherming van persoonsgegevens (Wbp) is vormgegeven. Daarna is gekeken wat de AVG inhoudt. Vervolgens zijn de verschillen tussen de Wbp en de AVG opgemerkt en uiteengezet. Hierna is door middel van interviews de huidige werkwijze van de directie P&O van de organisatie met betrekking tot het verwerken van persoonsgegevens (in naleving van de Wbp) in kaart gebracht. Tot slot zijn interviews afgenomen met als doel een beeld van de (toekomstige) werkwijze van de directie P&O van de organisatie met betrekking tot verwerking van persoonsgegevens in naleving van de AVG te vormen.

1.2 Doelstelling, centrale vraag en deelvragen

Doelstelling

Het doel van dit onderzoek is het schrijven van een advies voor de directie P&O van de organisatie over hoe te werken met de AVG. Het advies moet beschrijven wat de directie P&O van de organisatie moet aanpassen aan haar werkwijze in omgang met persoonsgegevens, om zo aan de eisen van de AVG te kunnen voldoen. Als wordt voldaan aan de AVG wordt de organisatie niet beboet. Dit advies zal tot stand komen door afname van interviews en analyse van relevante wet- en regelgeving en literatuur.

Centrale vraag

Welk advies kan aan de directie P&O van de organisatie worden gegeven over het aanpassen van haar werkwijze met betrekking tot het verwerken van persoonsgegevens om te voldoen aan de

¹³ <https://www.internetconsultatie.nl/veelgestelde vragen>.

¹⁴ Intern memo *ANONIEM* d.d. 6 september 2016.

¹⁵ Art. 83 lid 1 AVG.

¹⁶ *Toezicht en sancties*, Europa decentraal, 2016.

¹⁷ 6 september 2016.

eisen van de AVG aan de hand van afgenomen interviews, analyse van wet- en regelgeving en literatuuronderzoek?

Deelvragen

1. Hoe ziet de bescherming van persoonsgegevens volgens de Wbp, na analyse van wet- en regelgeving en literatuuronderzoek eruit?
2. Wat houdt de AVG in, aan de hand van analyse van wet- en regelgeving en literatuuronderzoek?
3. Wat zijn volgens wet- en regelgeving en literatuuranalyse de verschillen tussen de Wbp en AVG?
4. Wat is de huidige werkwijze van de directie P&O van de organisatie met betrekking tot het verwerken van persoonsgegevens in naleving van de Wbp na afname van interviews?
5. Wat is het beeld van de (toekomstige) werkwijze van de directie P&O van de organisatie met betrekking tot het verwerken van persoonsgegevens in naleving van de AVG na afname van interviews?

1.3 Operationaliseren van begrippen

Werkwijze

Manier waarop persoonsgegevens worden verwerkt
bij de directie P&O van de organisatie

1.4 Onderzoeksmethode + verantwoording per deelvraag

Samengevat: De deelvragen moeten worden gezien als stappen om uiteindelijk de centrale vraag te kunnen beantwoorden. Eerst is kennis van zowel de Wbp (deelvraag 1) als AVG (deelvraag 2) nodig. Als deze kennis verkregen is, worden verschillen tussen de Wbp en AVG zichtbaar (deelvraag 3). Het is van belang om de kennis over de Wbp uit deelvraag 1 te gebruiken om de huidige werkwijze van de directie P&O van de organisatie met betrekking tot het verwerken van persoonsgegevens in kaart te brengen. Een geselecteerde groep medewerkers (ook wel functionarissen) is geïnterviewd over topics uit deelvraag 1. Met de antwoorden op de interviewvragen is de huidige werkwijze van de directie P&O van de organisatie beschreven (deelvraag 4). Door beantwoording van deelvraag 3, zijn de verschillen tussen de Wbp en de AVG duidelijk. Om een beeld van de toekomstige werkwijze van de directie P&O van de organisatie in naleving van de AVG te kunnen schetsen, (deelvraag 5), zijn dezelfde participanten als bij deelvraag 4 geïnterviewd over de verschillen uit deelvraag 3. Er zijn open vragen gesteld, de verschillen zijn beschreven en er is gevraagd naar verwachtingen en knelpunten.

Hieronder volgt een uiteenzetting van methode en verantwoording per deelvraag:

Theoretisch-juridische onderzoeksgedeelte

Onder het theoretisch onderzoeksgedeelte vallen deelvraag 1 tot en met 3.

1. Hoe ziet de bescherming van persoonsgegevens volgens de Wbp, na analyse van wet- en regelgeving en literatuuronderzoek eruit? Onderzoeksmethode: Wetsanalyse aan hand van de MvT¹⁸ van de Wbp, de Wbp zelf en literatuuranalyse aan de hand van diverse handboeken en naslagwerken over de Wbp, welke zijn opgenomen in de literatuurlijst. De opbouw van de Wbp is aangehouden voor de structuur van de deelvraag. Zodat alle onderdelen van de wet zijn behandeld. Verantwoording onderzoeksmethode: Door globaal de opbouw van de Wbp aan te houden krijgt de deelvraag structuur. Het is van belang om een zo compleet mogelijk beeld van de Wbp te hebben om de bescherming van persoonsgegevens te kunnen duiden en daarmee deelvraag 1 te kunnen beantwoorden. Door niet alleen naar de Memorie van Toelichting (MvT) van de Wbp te hebben gekeken, maar ook naar relevante literatuur, is eenzijdigheid van bron voorkomen.

2. Wat houdt de AVG in, aan de hand van analyse van wet- en regelgeving en literatuuronderzoek? Onderzoeksmethode: Literatuuronderzoek aan de hand van parlementaire geschiedenis, de AVG zelf, diverse publicaties en literatuur over de AVG, welke is opgenomen in de literatuurlijst. Om een compleet beeld van de AVG te kunnen schetsen, is de opbouw van de AVG gevolgd. Verantwoording onderzoeksmethode: Met deze bronnen is een zo compleet mogelijk beeld van de AVG weergegeven: Wat de bedoeling van de AVG is, waaruit deze is opgebouwd en hoe deze werkt.

3. Wat zijn volgens wet- en regelgeving en literatuuranalyse de verschillen tussen de Wbp en AVG? Onderzoeksmethode: Door middel van deelvraag 1 en 2 zijn de Wbp en de AVG in kaart gebracht. Doordat de informatie is uitgezocht en volledig is, kunnen verschillen tussen de Wbp en de AVG worden geformuleerd met de kennis uit deelvraag 1 en 2. Verantwoording onderzoeksmethode: Doordat in deelvraag 1 en 2 is uitgezocht wat de Wbp en de AVG precies inhouden, kunnen zij als

¹⁸ Kamerstukken II 1997-1998, 25 892, nr. 3.

bron fungeren voor deelvraag 3. De verschillen tussen de Wbp en de AVG kunnen dus uit deelvraag 1 en 2 worden afgeleid. Samen met de literatuur, en diverse gepubliceerde teksten (zie literatuurlijst), zijn de bronnen voor deze deelvraag gevarieerd en is eenzijdigheid van bron voorkomen.

Praktijkgericht onderzoeksgedeelte

Onder het praktijk onderzoeksgedeelte vallen deelvraag 4 en 5. In hoofdstuk 5 wordt uitgebreid beschreven hoe de onderzoeksresultaten tot stand zijn gekomen.

4. Wat is de huidige werkwijze van **ANONIEM** P&O met betrekking tot het verwerken van persoonsgegevens in naleving van de Wbp na afname van interviews? Onderzoeksmethode: interviewen van een geselecteerd aantal participanten:

Hoofd P&O ondersteuning

Coördinator P-beheer

Coördinator Kwaliteitszorg, Administratieve Organisatie en Interne Controle (KAI)

Vervoerscoördinator (2 personen)

Verantwoording onderzoeksmethode¹⁹: Bij de directie P&O van de organisatie werken ongeveer **anoniem** mensen, maar niet iedere functionaris werkt met persoonsgegevens en ook niet in dezelfde mate of met dezelfde frequentie. Van belang is dat de groep functionarissen die geïnterviewd is, is geselecteerd op een aantal gronden. De functietitels die hierboven worden genoemd, worden bij de directie P&O van de organisatie bekleedt door de functionarissen die werken met de systemen waarmee gegevens worden verwerkt. Voor elk systeem is degene geïnterviewd die erover gaat (en ermee werkt). Door deze selectievorm is duidelijk wat voor persoonsgegevens er binnen de directie P&O van de organisatie worden verwerkt en hoe dit wordt gedaan.

Qua interviewvorm is gekozen voor het hanteren vaste vragen/onderwerpen, maar daarnaast ook bewust voor de mogelijkheid om door te kunnen vragen. Qua mate van gestructureerdheid in de interviews, is volgens de theorie van Baarda e.a. (2012) een half-gestructureerde vorm aangehouden²⁰ Deze interviewvorm past bij het doel van het interview, namelijk aan de hand van de antwoorden op de vragen, de werkwijze van de directie P&O van de organisatie aangaande persoonsgegevens kunnen duiden. Het type interview wat is afgenomen, heet volgens theorie van Baarda een 'elite- of expertinterview'²¹ omdat de geselecteerde functionarissen (de participanten) deskundig zijn op het gebied van persoonsgegevens/gegevensverwerking.

5. Wat is het beeld van de (toekomstige) werkwijze van de directie P&O van de organisatie met betrekking tot het verwerken van persoonsgegevens in naleving van de AVG na afname van interviews? Onderzoeksmethode: Interviewen van een geselecteerd aantal participanten: dezelfde functionarissen als de selectie die bij deelvraag 4 is genoemd. Informatie over de verschillen tussen de Wbp en AVG (zie bijlage 6) is voorafgaand aan het interview doorgegeven aan de participanten zodat deze niet blanco geïnterviewd werden. Tijdens het interview is verdere uitleg gegeven over wat de verschillen behelzen. Daarna zijn gerichte vragen gesteld over de verwachting in (toekomstige) omgang met de verschillen.

Verantwoording onderzoeksmethode: Eerst is een proefinterview²² afgenomen om te testen of door het stellen van de set vragen, de gewenste informatie werd verkregen: of deze concreet genoeg was en uitwerking ervan de beantwoording van de deelvraag mogelijk maakte. De vragen zijn na afname van het proefinterview deels herzien en verduidelijkt.

De resultaten van het praktijkonderzoek (deelvraag 4 en 5) zullen worden gepresenteerd tijdens de bedrijfspresentatie, de participanten zullen hiervoor worden uitgenodigd.

¹⁹ Zie ook *verantwoording onderzoeksmethode* deelvraag 5.

²⁰ Termen ontleend aan Baarda e.a., *Basisboek Interviewen*, 2012, p. 19, 20.

²¹ Term ontleend aan Baarda e.a., *Basisboek Interviewen*, 2012, p. 22.

²² Dit geldt ook voor deelvraag 4.

HOOFDSTUK 2: HET JURIDISCH KADER - WET BESCHERMING PERSOONSGEGEVENS

In dit hoofdstuk staat de Wet bescherming persoonsgegevens (Wbp) centraal. De opbouw van de wet wordt gevolgd en per onderdeel uiteengezet. Zo wordt onder andere toegelicht wanneer sprake is van persoonsgegevens in de zin van de Wbp en welke verschillende rollen er zijn bij het omgaan met persoonsgegevens. Verder komt de territoriale reikwijdte van de Wbp aan de orde en welke meldingsverplichtingen en informatieverplichtingen de wet oplegt. Ook de meldplicht bij datalekken, zoals die per 1 januari 2016 is ingevoerd, komt aan bod. Het doel hiervan is te kunnen aangeven hoe de huidige privacyregels eruitzien. De conclusie van dit hoofdstuk, is het antwoord op deelvraag 1.

2.1 Voorgeschiedenis

De Vries & Rutgers (2001) beschrijven dat in 1972 de maatschappelijke onrust rondom privacy in Nederland groeide. De voorgenomen volkstelling in datzelfde jaar, is de aanleiding geweest voor ontwikkeling van wetgeving op het gebied van privacy. Kranenborg & Verhey (2011) noemen de volkstelling zelfs de 'katalysator'.²³ Ondanks dat het jaar 1972 geldt als dé aanleiding, duurde het tot 1988 totdat er wetgeving was ontwikkeld.²⁴ In de Memorie van toelichting (MvT) van de Wbp wordt de herziening van de Nederlandse Grondwet beschreven als een ijkpunt: "Bij de herziening van de Grondwet in 1983 werd in artikel 10, eerste lid, de bescherming van de persoonlijke levenssfeer uitdrukkelijk als klassiek grondrecht geformuleerd. Daarnaast werd in het tweede en derde lid aan de formele wetgever de opdracht gegeven om regels te stellen omtrent de bescherming van persoonsgegevens. Artikel 10 sloot aan bij zich gelijktijdig ontwikkelende jurisprudentie van het Europese Hof voor de rechten van de mens over de omvang van het recht op respect voor het privéleven van het individu, neergelegd in artikel 8 van het EVRM, in relatie tot de opslag en het gebruik van persoonsgegevens."²⁵

Met de inwerkingtreding van Wet persoonsregistraties (WPR) in 1988, werd voldaan aan de opdracht van de wetgever om wetgeving ter bescherming van persoonsgegevens te ontwikkelen.²⁶ In 2001 is de WPR vervangen door de Wbp.²⁷ In de Wbp is de Europese richtlijn 95/46/EG geïmplementeerd. Deze richtlijn gaat over de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en het vrije verkeer van gegevens. Het doel van de richtlijn en daarmee ook het doel van de Wbp, is het vergroten van uniforme toepassing van het recht op gegevensbescherming binnen de EU.²⁸

2.2 Karakterisering

De Vries & Rutgers (2001) duiden de Wbp als een 'kaderwet met een ruime toepassing'.²⁹ Hooghiemstra & Nouwt (2007) vinden dat de Wbp niet in haar geheel kan worden ingedeeld in een rechtsgebied. De Wbp beslaat namelijk meer dan één rechtsgebied. Binnen het civiele recht, 'verleent zij rechten aan degenen van wie persoonsgegevens worden verwerkt'. (Zie 2.10 *Rechten van betrokkene*). Verder bevat zij bestuursrechtelijke componenten ter uitvoering van de wet, het toezicht op de naleving en de sanctionering.³⁰ Hooghiemstra & Nouwt (2007) benadrukken dat de Wbp gericht is op de waarborg van een grondrecht: het grondrecht op eerbiediging van de persoonlijke levenssfeer.³¹ De bescherming van persoonsgegevens vloeit hieruit voort.

2.3 Toepassingsbereik

2.3.1 Persoonsgegevens, wat zijn dat precies?

Vanuit de Wbp³² worden persoonsgegevens omschreven als elk gegeven, in zowel geschreven tekst als in beeld en geluid,³³ wat informatie kan verschaffen over een geïdentificeerde of identificeerbare natuurlijke persoon.³⁴ De begrippen 'geïdentificeerde' of 'identificeerbare persoon'

²³ Kranenborg & Verhey 2011, p. 1.

²⁴ De Vries & Rutgers 2001, p. 14.

²⁵ *Kamerstukken II* 1997-1998, 25 892, 3, p.7 (MvT).

²⁶ Art. 10 lid 2, 3 Gw.

²⁷ Art. 81 Wbp.

²⁸ Kranenborg & Verhey 2011, p. 11.

²⁹ De Vries & Rutgers 2001, p. 17.

³⁰ Hooghiemstra & Nouwt 2007, p. 19-20.

³¹ Art. 10 lid 1 Gw.

³² Art. 1 Wbp.

³³ *Kamerstukken II* 1997-1998, 25 892, 3, p. 50 (MvT).

³⁴ *Kamerstukken II* 1997-1998, 25 892, 3, p. 46 (MvT).

betekenen dat de identiteit van de persoon van wie de gegevens zijn bekend is, of dat deze te achterhalen valt 'zonder onevenredige inspanning'.³⁵ "Niet elk technisch of toevallig verband tussen een gegeven en een persoon is voldoende om een gegeven een persoonsgegeven te doen zijn [...]

2.3.2 Wanneer is er sprake van?

Er is sprake van een persoonsgegeven wanneer het gegeven voor een dergelijk op de persoon gericht doel, kan worden gebruikt."³⁶ De Vries & Rutgers (2001) geven aan dat een persoonsgegeven allerlei soorten informatie kan omvatten en noemt een aantal voorbeelden hiervan:³⁷

- Eigenschappen van een persoon;
- Gedragingen van een persoon;
- Opvattingen van een persoon.

De Vries & Rutgers (2001) nuanceren de bovenstaande voorbeelden door te benadrukken dat het gaat om gegevens die bepalend zijn voor de manier waarop iemand in het maatschappelijk verkeer wordt behandeld of beoordeeld. Hierbij valt bijvoorbeeld te denken aan een Verklaring omtrent het Gedrag (VOG). Er bestaat een subcategorie persoonsgegevens, welke worden geclassificeerd als bijzondere persoonsgegevens.³⁸ De categorie is limitatief. Het gaat om gegevens omtrent iemands:

Figuur 1: Bijzondere persoonsgegevens volgens de Wbp



De Hoge Raad heeft in 2010 beslist dat niet alleen gegevens die het ras van een persoon direct betreffen tot de bijzondere persoonsgegevens behoren maar ook gegevens waaruit informatie over het ras van een persoon kan worden afgeleid, zoals een foto.³⁹

2.4 Werken met persoonsgegevens

Persoonsgegevens kunnen zowel handmatig als (gedeeltelijk) geautomatiseerd verwerkt worden. De Wbp voorziet beide gevallen van een wettelijk kader, mits de niet-geautomatiseerde gegevens zijn opgenomen in een 'bestand' of bestemd zijn daarin te worden opgenomen.⁴⁰ Een bestand⁴¹ in de betekenisfeer van de Wbp wil zeggen dat het om een gestructureerde bundeling van persoonsgegevens van meerdere personen gaat. Het bestand kan zowel geautomatiseerde als niet-geautomatiseerde verwerkingen bevatten en is alleen middels bepaalde criteria toegankelijk.⁴² De Vries & Rutgers (2001) stellen dat bepalend is voor de reikwijdte van de Wbp, of sprake is van verwerking van persoonsgegevens.⁴³

De verwerking van persoonsgegevens staat in de Wbp omschreven als:

³⁵ Kranenborg & Verhey 2011, p. 61.

³⁶ Kamerstukken II 1997-1998, 25 892, 3, p. 47 (MvT).

³⁷ De Vries & Rutgers 2001, p. 18.

³⁸ Art. 16 t/m 22 Wbp.

³⁹ HR 23 maart 2010, ECLI:NL:PHR:2010:BK6331.

⁴⁰ Art. 2 lid 1 Wbp.

⁴¹ Art. 1 onder c Wbp.

⁴² Kamerstukken II 1997-1998, 25 892, 3, p. 53 (MvT).

⁴³ De Vries & Rutgers 2001, p. 18.

"Elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens."⁴⁴

Kranenborg & Verhey (2011) vatten al deze handelingen samen door de verwerking van persoonsgegevens te definiëren als: "het gehele proces dat een persoonsgegeven doormaakt vanaf het moment van verzamelen van een gegeven tot aan het moment van vernietiging."⁴⁵

2.4.1 Verwerking van bijzondere persoonsgegevens

Op de verwerking van bijzondere persoonsgegevens rust een verbod⁴⁶ Verwerking van dit type gegevens is slechts onder bepaalde voorwaarden toegestaan, tenzij uitdrukkelijke toestemming is verleend door betrokkene. Hooghiemstra & Nouwt (2007) geven aan dat drie punten essentieel zijn om te kunnen spreken van 'daadwerkelijke toestemming'.⁴⁷ Ten eerste gaat het erom dat de betrokkene in vrijheid zijn wil kan uiten. Ten tweede moet de wilsuiting van de betrokkene betrekking hebben op togespitste persoonsgegevens, er moet afbakening van gegevens hebben plaatsgevonden. Ten derde moet de betrokkene beschikken over 'noodzakelijke inlichtingen'. Dit wil zeggen dat de betrokkene moet weten welke gegevens verwerkt gaan worden en waarvoor dit nodig is.

2.4.2 Uitzonderingen toepassing Wbp op verwerking gegevens

In de wet zijn elke uitzonderingen opgenomen wanneer de Wbp niet van toepassing is op de verwerking van gegevens.⁴⁸ Verwerkingen ten behoeve van uitsluitend huishoudelijke of persoonlijke doeleinden zijn hier een voorbeeld van. Zo ook verwerkingen ten behoeve van inlichtingen- en veiligheidsdiensten (bedoeld in de Wet op de inlichtingen- en veiligheidsdiensten 2002). Alsmede verwerkingen ten behoeve van de uitvoering van de Kieswet en de Wet justitiële en strafvorderlijke gegevens. Ten slotte zijn ook verwerkingen ten behoeve van de uitvoering van de politietaak, bedoeld in de artikelen 3 en 4, eerste lid van de Politiewet 2012 en verwerking die is geregeld bij of krachtens de Wet basisregistratie personen niet van toepassing als het gaat om verwerking van persoonsgegevens volgens de Wbp.

2.5 Territoriale reikwijdte

De Wbp is van toepassing op de verwerking van persoonsgegevens in Nederland mits de verantwoordelijke voor de verwerking van de persoonsgegevens in Nederland gevestigd is.⁴⁹ De Wbp is eveneens van toepassing als de verantwoordelijke niet gevestigd is in de Europese Unie, maar dit geldt alleen als er gebruik wordt gemaakt van handmatige of geautomatiseerde verwerkingsmiddelen die zich in Nederland bevinden.⁵⁰

De verantwoordelijke buiten de EU moet dan een persoon of instantie in Nederland aanwijzen die namens hem handelt. In het kader van de Wbp is die persoon of instantie dan de verantwoordelijke.⁵¹

⁴⁴ Art. 1 sub b Wbp.

⁴⁵ Kranenborg & Verhey 2011, p. 65.

⁴⁶ Art. 16 Wbp.

⁴⁷ Hooghiemstra & Nouwt 2007, p. 42.

⁴⁸ Art. 2 sub a t/m f Wbp. jo. Art. 2 lid 3 Wbp.

⁴⁹ Art. 4 lid 1 Wbp.

⁵⁰ Art. 4 lid 2 Wbp.

⁵¹ Art. 4 lid 3 Wbp.

2.6 Rollen in proces gegevensverwerking

Gegevensverwerking is een proces waarbij diverse mensen zijn betrokken met ieder een eigen functie, positie en verantwoordelijkheden. Zie tabel 1 hieronder voor een weergave van de rollen vanuit de Wbp. In het resultaat hoofdstuk wordt een koppeling gemaakt naar invulling van de rollen voor de praktijk bij **ANONIEM** P&O, zie bijlage 2. Er wordt weergegeven welke rollen door wie worden ingevuld bij **ANONIEM** P&O als het gaat om gegevensverwerking.

Tabel 1: Rollen in proces van gegevensverwerking volgens Wbp

Rol	Functie/betekenis rol	Hiërarchie?	Herkomst rol
Verantwoordelijke: Natuurlijk persoon/rechtspersoon/bestuursorgaan/ieder ander.	Bevoegd om doel en middelen vast te leggen voor de verwerking van persoonsgegevens, belast met naleving materiële voorschriften gegevensverwerking + informatieplicht en meldplicht bij datalek	Eerste in de keten	Art. 1 sub d Wbp
Bewerker: Mogelijk binnen en buiten organisatie, maar vaker buiten. Als gesproken wordt over een functie binnen de organisatie dan wordt iemand eerder beheerder genoemd. ⁵²	Verwerking persoonsgegevens in opdracht van verantwoordelijke Mogelijk aansprakelijk bij niet naleving algemene beginselen gegevensverwerking ⁵³	Geen rechtstreeks gezag, niet ondergeschikt aan verantwoordelijke, maar wel in opdracht van en via overeenkomst ⁵⁴	Art. 1 sub e Wbp – MvT p. 64
Betrokkene	Degene op wie de persoonsgegevens betrekking hebben	Diverse rechten tegenover de verantwoordelijke	Art. 1 sub f Wbp – MvT p. 63
Derde: Een ieder, niet iemand in een van de rollen, doorgaans buiten de organisatie	Verwerking persoonsgegevens	Geen rechtstreeks gezag, geen overeenkomst	Art. 1 sub g Wbp
Ontvanger: Mogelijk binnen en buiten de organisatie	Degene aan wie persoonsgegevens worden verstrekt	Laatste in de keten	Art. 1 sub h Wbp – MvT p. 64
(Intern) beheerder Optionele rol	Verwerking persoonsgegevens	Onder rechtstreeks gezag verantwoordelijke	MvT p. 64
Toezichthouder: Autoriteit Persoonsgegevens (AP)	Toe zien of verwerking van persoonsgegevens overeenkomstig de Wbp wordt uitgevoerd Op verzoek uitbrengen van advies over voorstellen van wet en AMvB's.	Onafhankelijk	Art. 51 lid 1 Wbp
Functionaris voor gegevensbescherming Optionele rol. Het benoemen van een functionaris is niet verplicht.	Toezicht op de verwerking van persoonsgegevens door de verantwoordelijke die hem heeft benoemd	Zonder het ontvangen van aanwijzingen van verantwoordelijke of organisatie die hem heeft benoemd	Art. 62 Wbp

⁵² Kranenborg & Verhey 2011, p. 78.

⁵³ Art. 49 lid 3, lid 4 Wbp jo. *Materiële voorschriften bij het werken met persoonsgegevens.*

⁵⁴ Art. 14 lid 2 Wbp.

2.7 Materiële voorschriften bij het werken met persoonsgegevens

De Wbp bevat algemene beginselen van gegevensverwerking. De algemene beginselen gaan over de toelaatbaarheid en de kwaliteit van gegevensverwerking. De beginselen zijn voorschriften die samen een kader vormen over wanneer werken met bepaalde persoonsgegevens toelaatbaar is en hoe dit moet. Ook wordt middels de voorschriften invulling gegeven aan het begrip kwaliteit. De voorschriften zijn achtereenvolgens opgenomen in de artikelen 6 tot en met 24 Wbp.

Algemene beginselen van gegevensverwerking:

1. Gegevensverwerking moet in overeenstemming zijn met de Wbp en zorgvuldig en behoorlijk worden uitgevoerd.⁵⁵ Dit is gekoppeld aan art. 6:162 BW (onrechtmatige daad) en het zorgvuldigheidsbeginsel, wat één van de beginselen van behoorlijk bestuur is.
2. Gegevens mogen niet worden verzameld zonder dat daaraan voorafgaand een bepaald doel is gekoppeld.⁵⁶ Er moet melding van de verwerking worden gedaan bij de toezichthouder door de verantwoordelijke, behalve als het gaat om gegevens welke zijn opgenomen in een vrijstellingsbesluit.⁵⁷
3. Gegevens worden verkregen voor een 'gerechtvaardigd doel.' (Art. 8, onderdelen a tot en met f Wbp). De belangen van de verantwoordelijke en de betrokkene moeten tegen elkaar worden afgewogen; deze afweging dient controleerbaar te zijn.
4. Bij verdere verwerking van gegevens mag dit niet onverenigbaar zijn met het doel van verkrijging.⁵⁸ Gegevens mogen dus alleen verwerkt worden met het doel waarvoor zij zijn verzameld. Dit principe heet doelbinding.
5. De inhoudelijke kwaliteit van de gegevens moet toereikend, relevant, niet bovenmatig en nauwkeurig zijn.⁵⁹
6. Persoonsgegevens moeten worden beveiligd tegen verlies of enige vorm van onrechtmatige verkrijging. Beveiliging dient technisch en organisatorisch gewaarborgd te zijn.⁶⁰
7. Persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk voor de verwerking ervan.⁶¹ Zie 2.11 *Bewaartermijn persoonsgegevens*.

2.8 Meldings- en informatieverplichtingen

"Een geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, die voor de verwezenlijking van een doeleinde of van verscheidene samenhangende doeleinden bestemd is, wordt gemeld."⁶² Een melding wordt gedaan door de verantwoordelijke voorafgaand aan de verwerking van gegevens.

De melding is gericht aan de AP of (indien van een organisatie deze heeft aangesteld) de functionaris voor gegevensbescherming.⁶³ Wat er precies in de melding moet staan is opgenomen in art. 28 lid 1 sub a tot en met f Wbp.

2.8.1 Meldingsverplichting

De meldplicht is bedoeld ter bevordering van de transparantie van gegevensverwerking. Met de meldplicht wordt ook handelingsvrijheid van een ieder om voor op zichzelf gerechtvaardigde doeleinden gegevens te verwerken, ingeperkt. De wetgever heeft hiermee bedoeld de betrokkene niet onnodig aan verwerking van zijn persoonsgegevens bloot te stellen.⁶⁴

2.8.2 Informatieverplichting

De verantwoordelijke is verplicht om zijn identiteit en het doeleinde van de verwerking van persoonsgegevens kenbaar te maken aan de betrokkene. Aan deze informatieverplichting moet zijn voldaan voordat de gegevens van betrokkene in bezit van de verantwoordelijke komen.⁶⁵ Het is dus niet toegestaan om als verantwoordelijke eerst gegevens van de betrokkene te verzamelen, gegevens te 'verkrijgen' zogezegd en daarna aan te kondigen wat er met de gegevens wordt gedaan.

⁵⁵ Art. 6 Wbp.

⁵⁶ Art. 7 Wbp.

⁵⁷ Art. 7 Wbp.

⁵⁸ Art. 9 Wbp.

⁵⁹ Art. 11 Wbp.

⁶⁰ Art. 13 Wbp.

⁶¹ Art. 10 Wbp.

⁶² Art. 27 lid 1 Wbp.

⁶³ Art. 27 lid 3 Wbp.

⁶⁴ *Kamerstukken II 1997-1998, 25 892, 3, p. 132-133 (MvT).*

⁶⁵ Art. 33 lid 1, lid 2 Wbp.

2.9 De meldplicht datalekken

De meldplicht datalekken⁶⁶ is per 1 januari 2016 toegevoegd aan de Wbp. De verantwoordelijke is verplicht om het datalek te melden aan de AP en betrokkene. Ook wanneer een datalek slechts betrekking heeft op de gegevens van één persoon valt het datalek onder de meldplicht.⁶⁷ Bij verzaken van de meldplicht aangaande een datalek, riskeert de verantwoordelijke een dwangsom of een bestuurlijke boete, opgelegd door de AP. De boete kan oplopen tot maximaal 820.000 euro. Zie 2.13.2 *Sancties*. Een datalek wordt omschreven als "inbreuk op de beveiliging van persoonsgegevens: de persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking."⁶⁸ Europa decentraal (2015) noemt een aantal voorbeelden van beveiligingsproblemen waardoor een datalek kan ontstaan. Deze voorbeelden zijn niet-limitatief⁶⁹: verloren usb-stick, een gestolen laptop, inbraak in een databestand en brand in een datacentrum. Wanneer er inbreuk heeft plaatsgevonden, dient de verantwoordelijke zonder onredelijke vertraging (uiterlijk 72 uur na kennisname van het datalek), de inbreuk te melden aan de AP.⁷⁰ Wanneer de verantwoordelijke later dan 72 uur na het datalek melding maakt, moet de melding een motivering voor de vertraging bevatten.⁷¹ Melding door de verantwoordelijke aan de betrokkene is verplicht wanneer het datalek naar inschatting een hoog risico met zich meebrengt voor de persoonsgegevens van de betrokkene. Melding vindt 'onverwijld' dus direct, in duidelijke en eenvoudige taal plaats.⁷² Een datalek hoeft niet altijd door de verantwoordelijke aan de betrokkene te worden gemeld. Melding van een datalek is niet verplicht wanneer er passende technische en organisatorische beschermingsmaatregelen zijn genomen en deze zijn toegepast waardoor de persoonsgegevens onbegrijpelijk zijn voor onbevoegden. Of als er achteraf maatregelen genomen zijn waardoor het hoge risico voor de rechten en vrijheden van de betrokken zich waarschijnlijk niet meer zal voordoen. Melding is ook niet verplicht als het onevenredige inspanningen zou vergen. Een openbare mededeling voldoet dan ook.⁷³

2.10 Rechten van de betrokkene

De betrokkene kan aan de verantwoordelijke vragen om inzage als hij wenst te weten of zijn persoonsgegevens worden verwerkt.⁷⁴ Ook kan hij vragen om zijn gegevens te laten aanvullen, te verbeteren, verwijderen of af te schermen.⁷⁵ Ten kan de betrokkene zich verzetten: (de betrokkene wenst zijn gegevens niet te verlenen voor verwerking) als sprake is van bijzondere persoonlijke omstandigheden.⁷⁶

2.11 Bewaartermijn persoonsgegevens

De Wbp geeft geen termijn voor het bewaren van persoonsgegevens. De wet bepaalt dat persoonsgegevens niet langer mogen worden bewaard dan nodig is voor het doel waarvoor zij zijn verzameld.⁷⁷ Dit brengt met zich dat de verantwoordelijke zich dient af te vragen of er redenen zijn op grond waarvan (bijzondere) persoonsgegevens bewaard mogen blijven. Wel kan via bijzondere wetgeving een algemene termijn worden gefixeerd.⁷⁸

Bijzondere persoonsgegevens vormen een uitzondering qua bewaartermijn, bijvoorbeeld bij medische gegevens.⁷⁹ Een andere uitzondering waarbij volgens Hooghiemstra & Nouwt (2007) een 'soepeler norm' geldt⁸⁰ zijn gegevens bedoeld voor historische, statische of wetenschappelijke doeleinden.⁸¹ Een andere manier om toch met termijnen te werken kan middels een Algemene

⁶⁶ Art. 34A Wbp.

⁶⁷ Witteveen & Zondag, *Gepubliceerde regels meldplicht datalekken belangrijk voor decentrale overheden*, Europa decentraal, 14-12-2015.

⁶⁸ Salverda & Witteveen, *Richtsnoeren meldplicht datalek gepubliceerd*, Europa decentraal, 05-10 2015.

⁶⁹ Salverda & Witteveen, *Richtsnoeren meldplicht datalek gepubliceerd*, Europa decentraal, 05-10 2015.

⁷⁰ Art. 33 AVG.

⁷¹ *Meldplicht inbreuk persoonsgegevens*, Europa decentraal, 2016.

⁷² *Meldplicht inbreuk persoonsgegevens: meldplicht betrokkene*, Europa decentraal, 2016.

⁷³ *Meldplicht inbreuk persoonsgegevens*, Europa decentraal, 2016.

⁷⁴ Art. 35 Wbp.

⁷⁵ Art. 36 Wbp.

⁷⁶ Art. 40 lid 1 Wbp.

⁷⁷ Art. 10 Wbp.

⁷⁸ *Kamerstukken II 1997-1998*, 25 892, 3, p. 95 (MvT).

⁷⁹ Art. 7:454 lid 3 BW.

⁸⁰ Hooghiemstra & Nouwt 2007, p. 21.

⁸¹ Art. 10 Wbp.

Maatregel van Bestuur (AMvB). In de AMvB kunnen criteria en/of termijnen worden verbonden aan het bewaren van persoonsgegevens.⁸²

2.12 Doorgifte persoonsgegevens

Persoonsgegevens worden enkel doorgegeven aan een land buiten de EU (een derde land) als het desbetreffende land een 'passend beschermingsniveau' voor de gegevens hanteert.⁸³ De Wbp maakt onderscheid tussen doorgifte van persoonsgegevens naar een EU-lidstaat en doorgifte naar een derde land. Een beschermingsniveau wordt beoordeeld aan de hand van een aantal criteria.⁸⁴ Er wordt gekeken naar de aard van de gegevens en het doeleinde van de beoogde verwerking. Ook wordt gekeken naar het land waaruit de gegevens afkomstig zijn en het land waar de gegevens aan doorgegeven gaan worden. De sectoriële rechtsregels in het derde land worden nagegaan en ten slotte worden veiligheidsmaatregelen en de regels van het beroepsleven nagegaan. Indien een derde land geen passend beschermingsniveau heeft volgens de beoordeling, kunnen gegevens onder voorwaarden alsnog worden doorgegeven.⁸⁵ Als aan geen van voorwaarden kan worden voldaan, is een vergunning van de Minister van VenJ vereist voor doorgifte.⁸⁶

2.13 Toezicht naleving en sancties

2.13.1 Toezicht op de naleving van Wbp

Vanuit de Europese richtlijn 95/46/EC, welke geïmplementeerd is de Wbp, wordt voorgeschreven dat een lidstaat één of meer toezichthoudende autoriteiten dient in te stellen.⁸⁷ De autoriteit is belast met het toezicht op privacywetgeving in de lidstaat. In Nederland is de toezichthouder⁸⁸ de Autoriteit persoonsgegevens (hierna AP). Het is ook mogelijk om als verantwoordelijke een eigen interne 'toezichthouder' te benoemen.⁸⁹ Als een interne toezichthouder: een functionaris gegevensbescherming wordt benoemd, blijven de bevoegdheden van de AP onverminderd bestaan. Er is geen sprake van vervanging in toezicht.

2.13.2 Sancties

De AP mag een verantwoordelijke een bestuurlijke boete opleggen⁹⁰ of bestuursdwang⁹¹ toepassen. Bestuursdwang is een reparatoire sanctie, dit geeft aan dat de sanctie als doel heeft dat een fout binnen een termijn wordt gecorrigeerd zonder verder ingrijpen. Vindt er geen correctie plaats, dan voert de AP de correctie zelf uit en zijn kosten hiervan voor de verantwoordelijke.⁹² Een bestuurlijke boete wordt een repressieve sanctie genoemd. Dit wil zeggen dat de boete het doel heeft om af te schrikken. De hoogte van een bestuurlijke boete bij niet naleving van de Wbp kan oplopen tot €820.000,- bij specifieke overtredingen.⁹³ Verschillende factoren zijn bepalend voor de hoogte van de boete: de aard en omvang overtreding⁹⁴, duur van de overtreding⁹⁵, de impact van de overtreding op de bescherming van persoonsgegevens en van de persoonlijke levenssfeer voor) de betrokkenen en/of de maatschappij⁹⁶ Het maakt ook uit of er sprake is van opzet of ernstig verwijtbare nalatigheid.⁹⁷ Ten slotte worden ook de omstandigheden waaronder overtreding is gepleegd en financiële omstandigheden van de overtreder meegewogen.⁹⁸ In de algemene boetebeleidsregels van de Wbp (2016) staat aangegeven dat bij meerdere, samenhangende overtredingen de boete kan worden gematigd.⁹⁹ Van de bevoegdheid tot matigen is gebruik gemaakt in het volgende geval: een gemeente had geautomatiseerde verwerkingen van gegevens niet tijdig gemeld aan de AP. Het ging om acht overtredingen. De AP kon een boete opleggen van maximaal € 24.000 (€ 3.000 per overtreding) maar besloot deze te matigen tot

⁸² Art. 29 lid 2 onder e Wbp jo. *Kamerstukken II 1997-1998*, 25 892, 3, p. 95 (MvT).

⁸³ Art. 76 lid 1 Wbp.

⁸⁴ Art. 76 lid 3 Wbp.

⁸⁵ Art. 77 lid 1 sub a t/m 9 Wbp.

⁸⁶ Art. 77 lid 2 Wbp.

⁸⁷ Art 51 lid 1 Wbp.

⁸⁸ Art. 5:11 Awb.

⁸⁹ Art. 62 Wbp.

⁹⁰ Art. 66 Wbp

⁹¹ Art. 65 Wbp.

⁹² Art. 65, *Wbp naslag*, AP, 2016.

⁹³ Art. 66 lid 1 Wbp.

⁹⁴ Art. 6.1 sub a, *Boetebeleidsregels Autoriteit Persoonsgegevens 2016*.

⁹⁵ Art. 6.1 sub b, *Boetebeleidsregels Autoriteit Persoonsgegevens 2016*.

⁹⁶ Art. 6.1 sub c, *Boetebeleidsregels Autoriteit Persoonsgegevens 2016*.

⁹⁷ Art. 6.2, *Boetebeleidsregels Autoriteit Persoonsgegevens 2016*.

⁹⁸ Art. 6.3, *Boetebeleidsregels Autoriteit Persoonsgegevens 2016*.

⁹⁹ *Boetebeleidsregels Autoriteit Persoonsgegevens 2016*, Stcrt. 2016, 2043, p. 11.

€15.000.¹⁰⁰ Daarentegen kan ook voor iedere overtreding een aparte boete worden opgelegd of een gezamenlijke boete.¹⁰¹ Hierbij worden alle overtredingen in de boete meegenomen.¹⁰² Naast boetematiging kan ook boeteverhoging worden toegepast.¹⁰³

De AP mag een verantwoordelijke geen bestuurlijke boete opleggen voordat hij een bindende aanwijzing heeft gegeven.¹⁰⁴ Dit is zo omdat een verantwoordelijke eerst zelf de kans moet krijgen om zijn fout te herstellen, weliswaar binnen een door de AP gestelde termijn. Als de overtreding opzettelijk is gepleegd of het gevolg is van ernstig verwijtbare nalatigheid, mag de AP direct een bestuurlijke boete opleggen.¹⁰⁵ De bindende aanwijzingsverplichting vervalt.

2.14 Conclusie

Deelvraag 1: Hoe ziet de bescherming van persoonsgegevens volgens de Wbp, na analyse van wet- en regelgeving en literatuuronderzoek eruit?

Wbp van toepassing?

1. Allereerst moet blijken of gegevens *persoonsgegevens* zijn, als hier geen sprake van is, dan is de Wbp niet van toepassing. Persoonsgegevens worden omschreven als elk gegeven, in zowel geschreven tekst, beeld en geluid, welke informatie kunnen verschaffen over een natuurlijk persoon. Een persoonsgegeven kan dus vele vormen aannemen, maar een persoonsgegeven kan pas als zodanig worden aangemerkt wanneer het voor een dergelijk op de persoon gericht doel kan worden gebruikt.

2. Ten tweede moet blijken of is er sprake is van *verwerking van persoonsgegevens*. Verwerking is een ruim begrip en kan worden gedefinieerd als het gehele proces dat een persoonsgegeven doorloopt vanaf het moment van verzamelen tot aan het moment van vernietiging. Wil er sprake zijn van verwerking dan moeten er *handelingen* met de gegevens worden verricht.

Reikwijdte van bescherming persoonsgegevens

De Wbp is van toepassing op de verwerking van persoonsgegevens in Nederland mits de verantwoordelijke voor de verwerking van de persoonsgegevens in Nederland gevestigd is. De Wbp is eveneens van toepassing als de verantwoordelijke niet gevestigd is in de Europese Unie, maar dit geldt alleen als er gebruik wordt gemaakt van handmatige of geautomatiseerde verwerkingsmiddelen die zich in Nederland bevinden. Het bedrijf/de organisatie kan dus buiten de EU gevestigd zijn, maar de verwerking van de gegevens moet in Nederland plaatsvinden wil de Wbp van toepassing zijn.

Algemene beginselen gegevensverwerking

Is er sprake van een persoonsgegeven én van verwerking hiervan dan gelden de algemene beginselen van gegevensverwerking. De beginselen zijn voorschriften die samen een kader vormen over wanneer werken met bepaalde persoonsgegevens toelaatbaar is en hoe dit moet. Op de verwerking van bijzondere persoonsgegevens rust in beginsel een verbod. De Wbp erkent hiermee het verschil tussen 'gewone' en bijzondere persoonsgegevens. Bijzondere persoonsgegevens mogen niet worden verwerkt óf er moet uitdrukkelijke toestemming zijn van de betrokkene.

Rollen in proces van gegevensverwerking

De Wbp beschrijft acht rollen en functies binnen het proces van gegevensverwerking. Deze rollen kennen ieder hun eigen oorsprong, taken, positie en verantwoordelijkheid.

Rechten van betrokkene

De Wbp kent de betrokkene drie rechten toe welke hij kan inroepen tegenover de verantwoordelijke:

1. Recht op inzage. 2. Recht op verzet. 3. Recht op rectificatie.

Meldings- en informatieverplichtingen

De meldingsplicht zorgt voor meer transparantie rondom gegevensverwerking en zorgt voor beperking van gegevensverwerking doordat elk type verwerking (met uitzondering van gegevens die zijn opgenomen in een vrijstellingsbesluit) kenbaar moet worden gemaakt aan de AP.

Door middel van de informatieverplichting is de verantwoordelijke is verplicht om zijn identiteit en het doeleinde van de verwerking van persoonsgegevens kenbaar te maken aan de betrokkene. Deze weet dan waarom hij zijn gegevens afstaat en aan wie.

Meldplicht datalekken

Sinds januari 2016 is de meldplicht datalekken toegevoegd aan de Wbp. De verantwoordelijke is bij inbreuk op de beveiliging van persoonsgegevens (de persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking) verplicht dit binnen 72 uur te melden aan de AP. Als het

¹⁰⁰ Rb 9 augustus 2005, LJN: AU0980.

¹⁰¹ *Boetebeleidsregels Autoriteit Persoonsgegevens 2016*, Stcrt. 2016, 2043, p. 11.

¹⁰² Fennell e.a., 2016, p. 53.

¹⁰³ Art. 9.1 sub a, b, *Boetebeleidsregels Autoriteit Persoonsgegevens 2016*.

¹⁰⁴ Art. 66 lid 3 Wbp.

¹⁰⁵ Art. 66 lid 4 Wbp.

datalek naar inschatting een hoog risico met zich meebrengt wordt ook de betrokkene op de hoogte gebracht. Melding vindt 'onverwijld' dus direct, in duidelijke en eenvoudige taal plaats.

Toezicht & sancties

De AP heeft als toezichthouder op de naleving van de Wbp, de mogelijkheid om bestuursdwang toe te passen en eventueel een bestuurlijke boete van maximaal €820.000 op te leggen aan de verantwoordelijke bij niet naleving van de Wbp. Verschillende factoren spelen een rol bij het bepalen van het boetebedrag.

HOOFDSTUK 3: HET JURIDISCH KADER – ALGEMENE VERORDENING GEGEVENSBESCHERMING

In dit hoofdstuk staat de Algemene Verordening Gegevensbescherming (AVG) centraal. De opbouw van de Verordening wordt gevolgd en per onderdeel uiteengezet. Allereerst wordt ingegaan op de totstandkoming van de AVG. Vervolgens komen het materieel en het territoriaal toepassingsgebied van de AVG aan de orde. Ook wordt ingegaan op de verplichtingen van verantwoordelijke en van de verwerker en op de wijze van toezicht en handhaving in de AVG. Het doel hiervan is aan te geven hoe de nieuwe privacyregels er uit gaan zien. De conclusie van dit hoofdstuk, is het antwoord op deelvraag 2.

3.1 Voorgeschiedenis

Aan het feit dat de Nederlandse Wbp op 25 mei 2018 wordt ingetrokken¹⁰⁶ en de Algemene Verordening Gegevensbescherming (AVG) hiervoor in de plaats komt, gaan een aantal stappen vooraf. De Nederlandse Wbp is gebaseerd op richtlijn 95/46/EG. Volgens Kranenborg & Verhey (2011) de "belangrijkste en meest veelomvattende Europese richtlijn van de laatste vijftien jaar."¹⁰⁷ In de richtlijn is verankerd dat een ieder recht heeft op bescherming van zijn persoonsgegevens.¹⁰⁸ De richtlijn kwam tot stand nadat bleek dat de doelstellingen van het Verdrag van Straatsburg (1981) 'onvoldoende van de grond' kwamen, zo beschrijven Kranenborg & Verhey (2011)¹⁰⁹ In casu kwam het beoogde vrije verkeer van gegevens niet zo 'los' als was gehoopt. In de richtlijn zijn daarom de beginselen uit het Verdrag van Straatsburg duidelijker omschreven, geven Kranenborg & Verhey (2011) aan.¹¹⁰ Het doel van de richtlijn was om de bescherming en verwerking van persoonsgegevens te harmoniseren zodat een gelijkwaardig niveau ontstond binnen de lidstaten.¹¹¹

In mei 2003 presenteerde de Europese Commissie een eerste verslag over de toepassing van 95/46/EG.¹¹² Uit deze evaluatie is gebleken dat er 'aanzienlijke' verschillen bestaan tussen hoe lidstaten richtlijn 95/46/EG geïmplementeerd hebben in hun nationale wetgeving. Hierdoor wordt het doel van de richtlijn, een gelijk niveau van gegevensbescherming en vrij verkeer van gegevens binnen de lidstaten,¹¹³ niet of onvoldedig bereikt.

In 2009 werden twee rapporten gepubliceerd over de bescherming van persoonsgegevens in Europa. Het eerste rapport¹¹⁴ werd samengesteld door 'the future group'. The future group bestond onder meer uit de Ministers van Binnenlandse Zaken van verschillende lidstaten¹¹⁵. Het tweede rapport¹¹⁶ werd op verzoek van de Britse gegevensbeschermingsautoriteit opgesteld. In de rapporten stonden de sterke en zwakke punten van het Europese gegevensbeschermingsrechtelijk kader beschreven. De publicatie van deze rapporten viel samen met de inwerkingtreding¹¹⁷ van het verdrag van Lissabon. Het Verdrag van Lissabon bracht tot stand dat het Grondrechtenhandvest van de EU bindende werking kreeg. Door de verkregen bindende werking werd het belang van het recht op bescherming van persoonsgegevens erkend, aldus Kranenborg & Verhey (2011).¹¹⁸ De publicatie van de rapporten samen met de inwerkingtreding van het Verdrag van Lissabon, was reden voor Europese Commissie, welke tot dat moment een terughoudende houding had aangenomen, om te starten met de modernisatie en verdere uniformering van de Europese regelgeving over bescherming van persoonsgegevens.

Daarnaast speelt de modernisering van technologie een grote rol bij de bescherming en verwerking van persoonsgegevens. De AP geeft aan, dat ten tijde van de ontwikkeling van de richtlijn, het

¹⁰⁶ Art. 94 AVG.

¹⁰⁷ Kranenborg & Verhey 2011, p. 5.

¹⁰⁸ Art. 8 lid 1 Handvest van de grondrechten van de EU, art. 16 lid 1 VWEU jo. Art. 18 VWEU.

¹⁰⁹ Kranenborg & Verhey 2011, p. 30.

¹¹⁰ Kranenborg & Verhey 2011, p. 40.

¹¹¹ Art. 1 lid 1, 95/46/EG jo. Art. 1 lid 2, 95/46/EG.

¹¹² COM (2003) 265 def. 15 mei 2003.

¹¹³ Art. 1 lid 1 jo. Lid 2, Richtlijn 95/46/EG.

¹¹⁴ The future group, 2009, *Freedom, Security, Privacy – European home affairs in an open world*.

¹¹⁵ Kranenborg & Verhey 2011, p. 186.

¹¹⁶ Robinson e.a., 2009, *Review of the European Data Protection Directive*.

¹¹⁷ 01-12-2009.

¹¹⁸ Kranenborg & Verhey 2011, p. 36.

internet nog 'in de kinderschoenen' stond.¹¹⁹ Met kennis van nu kan geconcludeerd worden dat de richtlijn en daarmee de Wbp gedateerd is. De Eerste Kamer zegt over de huidige richtlijn dat zij op onderdelen tekortschiet om een niveau van gegevensbescherming te garanderen dat voldoende aansluit bij de behoeften van burgers en bedrijven om grensoverschrijdend zaken te kunnen doen in de hedendaagse informatiemaatschappij.¹²⁰

Kortom: de AVG vervangt de Wbp ondermeer om een ieder van bescherming van zijn persoonsgegevens anno nu te kunnen voorzien. Er is gedacht aan bepalingen rondom de hedendaagse technologie. Daarnaast is de AVG bedoeld om een gelijk(er) niveau van bescherming en verwerking van persoonsgegevens binnen de lidstaten van de EU te creëren.

3.2 Karakterisering

De AVG stelt regels vast betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van persoonsgegevens.¹²¹

3.3 Toepassingsbereik

Persoonsgegevens bestaan volgens de AVG uit: "alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Als identificeerbaar wordt beschouwd, een natuurlijk persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identicator zoals een naam, een identificatienummer, locatiegegevens, een online identicator (gebruikt bij internetbankieren) of één of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon."¹²²

3.4 Werken met persoonsgegevens

De AVG definieert verwerking van persoonsgegevens als "een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens."¹²³ Voorts wordt beschreven dat dit al dan niet kan worden uitgevoerd via geautomatiseerde procedures zoals: "Verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren¹²⁴ of combineren, afschermen, wissen of vernietigen van gegevens."¹²⁵ In de wettekst van art. 4 lid 2 AVG (zie hierboven) wordt gebruik gemaakt van de omschrijving 'al dan niet' als het gaat om uitvoering van verwerking van gegevens via automatische procedures. Deze omschrijving geeft naast automatische verwerking ruimte voor deels geautomatiseerde of handmatige verwerking. Als bij geautomatiseerde verwerking van persoonsgegevens bepaalde 'persoonlijke aspecten' worden geëvalueerd met het doel om voorspellingen te kunnen doen over deze persoon, heet dit profilering.¹²⁶ Bij persoonlijke aspecten moet worden gedacht aan beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag en locatie. Pseudonimisering¹²⁷ heeft net als profilering te maken met het verwerken van persoonsgegevens. Als persoonsgegevens gepseudonimiseerd worden, houdt dat in dat persoonsgegevens niet meer te koppelen zijn aan de betrokkene. De persoonsgegevens zijn dusdanig verwerkt dat deze niet meer herleidbaar zijn zonder er aanvullende gegevens van de betrokkene aan te moeten koppelen. Een gestructureerd geheel van persoonsgegevens wat volgens bepaalde criteria toegankelijk is, wordt een bestand genoemd. De kanttekening die bij dit gegeven moet worden geplaatst is dat niet uitmaakt of het geheel "gecentraliseerd of gedecentraliseerd is of op geografische wijze is verspreid."¹²⁸ Waar de gegevens zijn opgeslagen en eventuele verdeeldheid hierin, maakt dus geen verschil voor de naamgeving.

Een gestructureerd geheel van gegevens, wat volgens bepaalde criteria toegankelijk is, blijft een bestand. Ook als dit bijvoorbeeld gegevens zijn van een Nederlandse organisatie, maar deze bijvoorbeeld opgeslagen zijn op een server elders in de EU of een derde land.

3.5 Territoriale reikwijdte

¹¹⁹ Europese privacywetgeving, AP, 2016.

¹²⁰ Kamerstukken I 2011-2012, 2200 12, FI, p.7.

¹²¹ Art. 1 lid 1 AVG.

¹²² Art. 4 lid 1 AVG.

¹²³ Art. 4 lid 2 AVG.

¹²⁴ Als persoonsgegevens worden gealigneerd dan worden zij in de gewenste verhouding ten opzichte van elkaar geplaatst.

¹²⁵ Art. 4 lid 2 AVG.

¹²⁶ Art. 4 lid 4 AVG.

¹²⁷ Art. 4 lid 5 AVG.

¹²⁸ Art. 4 lid 6 AVG.

De AVG is van toepassing op de verwerking van persoonsgegevens in het kader van activiteiten van een vestiging van een verwerkingsverantwoordelijke of een verwerker in de EU. Het maakt niet uit of de verwerking binnen of buiten de EU plaatsvindt.¹²⁹ Concreet houdt dit in dat de AVG dus ook geldt voor bedrijven die buiten de EU gevestigd zijn, maar actief zijn op de Europese markt.

3.6 Materiële voorschriften bij het werken met persoonsgegevens

De AVG kent algemene beginselen van gegevensverwerking die moeten worden nageleefd als het gaat om de verwerking van persoonsgegevens. De algemene beginselen vormen een kader over hoe persoonsgegevens verwerkt moeten worden en hoe hieraan wordt voldaan. De beginselen zijn uitgewerkt in art. 6 AVG tot en met art. 11 AVG. Als vanuit tabel 2: *Rollen in proces van gegevensverwerking volgens AVG* wordt gekeken naar bij wiens functie de naleving van onderstaande beginselen past, is dit de taak van de verwerkingsverantwoordelijke. Hij is niet alleen verplicht de beginselen na te leven, maar moet dit ook kunnen aantonen.¹³⁰

3.6.1 Algemene beginselen van gegevensverwerking:

1. Persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is.¹³¹
2. Persoonsgegevens worden verzameld voor 'welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde' doeleinden en worden niet verder verwerkt dan dat nodig is voor dat specifieke doel.¹³²
3. Minimale gegevensverwerking: gegevens zijn toereikend, ter zake dienend en beperkt tot wat nodig is voor de doeleinden van de verwerking.¹³³ Lidstaten hebben de mogelijkheid¹³⁴ specifieke bepalingen in te voeren in naleving van de 'minimale gegevensverwerking' en de bewaartermijn van persoonsgegevens.
4. Persoonsgegevens moeten kloppend zijn (niet-foutief) en actueel.¹³⁵
5. Persoonsgegevens worden bewaard op een manier zodat de betrokkene niet meer te identificeren is behalve voor het doeleinde van de gegevensverwerking.¹³⁶
6. Passende technologische en organisatorische maatregelen, passende beveiliging. Beschermd tegen ongeoorloofde of onrechtmatige verwerking, tegen onopzettelijk verlies, vernietiging of beschadiging.¹³⁷

3.6.2 Rechtmatige verwerking

Verwerking van persoonsgegevens moet rechtmatig zijn. Art. 6 lid 1 geeft in sub a tot en met f AVG de voorwaarden voor rechtmatige verwerking van gegevens aan, zie figuur 2 hieronder. Let wel: de voorwaarden zijn niet cumulatief. Als aan één van de voorwaarden is voldaan is er al sprake van rechtmatige verwerking. Een voorbeeld hiervan is dat rechtmatige verwerking plaatsvindt als de betrokkene toestemming heeft gegeven voor de verwerking.¹³⁸

¹²⁹ Art. 3 lid 1 AVG.

¹³⁰ Art. 5 lid 2 AVG.

¹³¹ Art. 5 lid 1 sub a AVG.

¹³² Art. 5 lid 1 sub b AVG.

¹³³ Art. 5 lid 1 sub c AVG.

¹³⁴ Art. 6 lid 2 AVG.

¹³⁵ Art. 5 lid 1 sub d AVG.

¹³⁶ Art. 5 lid 1 sub e AVG.

¹³⁷ Art. 5 lid 1 sub f AVG.

¹³⁸ Art. 6 lid 1 sub a AVG.

Figuur 2: Voorwaarden voor rechtmatige verwerking van gegevens volgens de AVG



Toestemming

De verwerkingsverantwoordelijke moet kunnen aantonen dat de verwerking van persoonsgegevens berust op toestemming van de betrokkene.¹³⁹ Europa Decentraal (2016) benadrukt dat het verzoek om toestemming voor gegevensverwerking in begrijpelijke en gemakkelijke, toegankelijke vorm aangeboden moet worden aan de betrokkene.¹⁴⁰

Leeftijdsgrens

Als de betrokkene een kind is wat de leeftijd van zestien jaar nog niet heeft bereikt, is toestemming of machtiging van diegene die ouderlijke verantwoordelijkheid draagt over het kind, vereist. De verwerkingsverantwoordelijke levert 'redelijke inspanningen' om te controleren of wel of geen toestemming dan wel machtiging is verleend voor verwerking van de gegevens door de persoon die ouderlijke verantwoordelijkheid heeft over het kind.

Lidstaten mogen de eerdergenoemde leeftijd middels nationale wetgeving verlagen. De AVG stelt wel een ondergrens aan eventuele verlaging namelijk dertien jaar.

Verwerking van bijzondere persoonsgegevens

De AVG geeft aan dat er een verbod rust op het verwerken van bijzondere persoonsgegevens, tenzij er sprake is van een uitzondering. Een voorbeeld van een uitzondering is de betrokkene die toestemming heeft gegeven voor de verwerking van zijn persoonsgegevens. Bijzondere persoonsgegevens zijn in de AVG opgenomen als limitatieve gegevens.

Persoonsgegevens dragen het kenmerk bijzonder als zij betrekking hebben op:

- Ras of etnische afkomst;
- Politieke opvattingen, religieuze of levensbeschouwelijke overtuiging;
- Lidmaatschap van een vakbond;
- Genetische gegevens;
- Biometrische gegevens met het oog op de unieke identificatie van een persoon;
- Gegevens over gezondheid, seksueel gedrag of seksuele gerichtheid.

¹³⁹ Art. 7 lid 1 AVG.

¹⁴⁰ *Rechtmatigheid en transparantie*, Europa decentraal, 2016.

3.7 Rollen in proces gegevensverwerking

Gegevensverwerking is een proces waarbij diverse mensen zijn betrokken met ieder een eigen functie, positie en verantwoordelijkheden. Hieronder in tabel 2 zijn de rollen ingevuld zoals de AVG deze weergeeft. In het resultaat hoofdstuk wordt een koppeling gemaakt naar invulling van de rollen voor de praktijk, zie bijlage 2. Er wordt weergegeven welke rollen door wie worden ingevuld bij **ANONIEM** P&O als het gaat om gegevensverwerking.

Tabel 2: Rollen in proces van gegevensverwerking volgens AVG

Rol – Europese term	Rol – Nederlandse term	Functie/betekenis rol	Hiërarchie?	Herkomst rol
Controller	Verwerkingsverantwoordelijke	Natuurlijk persoon/rechtspersoon/overheidsinstantie, een dienst of een ander orgaan Alleen of samen het doel en de middelen voor de verwerking van persoonsgegevens vaststellen Passende technische en organisatorische maatregelen treffen om te waarborgen en kunnen aantonen dat verwerking in overeenstemming met de AVG gebeurt ¹⁴¹	Eerste in keten	Art 4 lid 7 AVG
Processor	Verwerker	Verwerking persoonsgegevens in opdracht van verwerkingsverantwoordelijke Mogelijk aansprakelijk bij niet naleving algemene beginselen gegevensverwerking ¹⁴² Aantal taken samen met verwerkingsverantwoordelijke ¹⁴³	Geen rechtstreeks gezag, niet ondergeschikt aan verantwoordelijke, maar wel in opdracht van en via overeenkomst ¹⁴⁴	Art. 4 lid 8 AVG
Data subject	Betrokkene	Degene op wie de persoonsgegevens betrekking hebben	Diverse rechten tegenover de verantwoordelijke	Art. 4 lid 11 AVG

¹⁴¹ Art. 24 lid 1 AVG.

¹⁴² Art. 49 lid 3, lid 4 Wbp jo. 3.6 Materiële voorschriften bij het werken met persoonsgegevens.

¹⁴³ Art. 32 lid 1 AVG.

¹⁴⁴ Art. 14 lid 2 Wbp.

Consent	Derde	Natuurlijk persoon of rechtspersoon, overheidsinstantie, dienst of ander orgaan, niet zijnde de betrokkene, Verwerkingsverantwoordelijke, verwerker, personen die onder rechtstreeks gezag van de Verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om persoonsgegevens te verwerken	Geen rechtstreeks gezag, geen overeenkomst	Art 4 lid 10 AVG
Recipient	Ontvanger	Degene aan wie persoonsgegevens worden verstrekt	Laatste in de keten	Art 4 lid 9 AVG
Supervisory authority	Toezicht houdende autoriteit	Een door een lidstaat onafhankelijke overheidsinstantie belast met het toezicht op de naleving van de AVG	Onafhankelijk ¹⁴⁵	Art. 4 lid 21 AVG
Data protection officer	Functionaris voor gegevensbescherming	Mogelijk een personeelslid van verwerkingsverantwoordelijke of verwerker of op grond van dienstverleningsovereenkomst Voorzien in informatie en advies aan verwerkingsverantwoordelijke, verwerker Houden van toezicht op naleving AVG	Ontvangt geen instructies m.b.t. uitvoer van zijn taken Wordt niet gestraft of ontslagen vanwege uitvoering van zijn taken	Art. 37 lid 6 AVG Art. 38 lid 3 AVG Art. 39 lid 1 sub a AVG Art. 39 lid 1 sub AVG

3.8 Rechten van betrokkene

De verwerkingsverantwoordelijke draagt zorg voor overdracht van bepaalde informatie over gegevensverwerking aan de betrokkene. Zo is de verwerkingsverantwoordelijke verplicht om de betrokkene binnen een gestelde termijn te informeren over onderstaande feiten zoals opgenomen in art. 13 lid 1 onder a tot en met e AVG:

- Identiteit + contactgegevens verwerkingsverantwoordelijke;
- Indien van toepassing, contactgegevens van functionaris gegevensbescherming;
- Verwerkingsdoeleinden en rechtsgrond verwerking;
- Gerechtigde belangen van de verwerkingsverantwoordelijke of van een derde als deze gebaseerd is op art. 6 lid 1 sub f AVG;
- De ontvangers of categorieën van ontvangers van de persoonsgegevens;
- Indien van toepassing: het voornemen van de verwerkingsverantwoordelijke om persoonsgegevens door te geven aan een derde land zoals omschreven in art. 46, 47 of 49 lid 1 AVG.

Dit is niet alle informatie die de verwerkingsverantwoordelijke verplicht is te verstrekken. In art. 13 lid 2 onder a tot en met f AVG is aanvullende informatie opgenomen die moet worden verstrekt om een behoorlijke en transparante verwerking van gegevens te waarborgen.

Verder heeft de betrokkene recht op inzage, als zijn gegevens ook daadwerkelijk zijn verwerkt.¹⁴⁶ Daarnaast heeft betrokkene recht op rectificatie¹⁴⁷ van zijn gegevens en kan hij onder voorwaarden zijn persoonsgegevens laten wissen.¹⁴⁸ Dit wordt ook wel het recht op vergetelheid genoemd. Aangaande rectificatie heeft betrokkene het recht een aanvullende verklaring te verstrekken om onvolledige persoonsgegevens compleet te maken. Recht op beperking van de verwerking¹⁴⁹ heeft de betrokkene als hij twijfelt aan de juistheid van de gegevens.¹⁵⁰ Of als zijn gegevens onrechtmatig zijn verwerkt en hij geen gebruik wenst te maken van het recht op vergetelheid.¹⁵¹ Ten slotte kan de betrokkene gebruik maken van dit recht als hij bezwaar heeft gemaakt en in afwachting van de uitkomst daarvan is.¹⁵² De AVG kent de betrokkene ook het recht om bezwaar te

¹⁴⁵ Art. 52 lid 1 AVG.

¹⁴⁶ Art. 15 AVG.

¹⁴⁷ Art. 16 AVG.

¹⁴⁸ Art. 17 AVG.

¹⁴⁹ Art. 18 AVG.

¹⁵⁰ Art. 18 lid 1 sub a AVG.

¹⁵¹ Art. 18 lid 1 sub b AVG.

¹⁵² Art. 18 lid 1 sub d AVG.

mogen maken toe.¹⁵³ Een betrokkene mag te allen tijde bezwaar maken tegen de verwerking van zijn persoonsgegevens op basis van art. 6 lid 1 sub e of f AVG (met inbegrip van profilering op basis van die bepalingen). Onder voorwaarden dat de verwerking verband houdt met zijn specifieke situatie. Wanneer gegevens geautomatiseerd verwerkt worden op basis van toestemming, dan heeft de betrokkene het recht om de gegevens mee te nemen.¹⁵⁴ Volgens Fennell e.a. (2016) heet dit principe het recht op dataportabiliteit.¹⁵⁵

Samengevat heeft de betrokkene het recht op:

- Informatie: bij verzameling van gegevens bij betrokkene recht op aanvullende informatie in samenhang met behoorlijke en transparante verwerking;
- Inzage: specifieke informatie wanneer persoonsgegevens daadwerkelijk zijn verwerkt;
- Rectificatie: betrokkene kan aanvullende verklaring verstrekken;
- Vergetelheid: persoonsgegevens kunnen onder voorwaarden worden gewist;
- Beperking van de gegevensverwerking;
- Dataportabiliteit: meenemen van informatie;
- Bezwaar: te allen tijde toegestaan, maar onder specifieke voorwaarden.
- Klachtrecht: betrokkene moet weten dat hij een klacht kan indienen bij de AP.

Om zijn rechten te effectueren kan de betrokkene zich wenden tot de functionaris voor gegevensbescherming.¹⁵⁶

In uitwerking van de rollen van het proces van gegevensbescherming worden hieronder de verplichtingen van de verwerkingsverantwoordelijke, verwerker en hun gezamenlijke verplichtingen beschreven. Een schematisch een volledig overzicht van de verplichtingen is opgenomen in bijlage 3.

3.9 Verplichtingen verwerkingsverantwoordelijke

De verwerkingsverantwoordelijke treft zowel bij de bepaling van de werkmiddelen als bij de verwerking zelf passende technische en organisatorische maatregelen.¹⁵⁷ Hij moet daarmee rekening houden met de aard van de verwerking, de omvang, context, het doel van de verwerking en de risico's voor de rechten en vrijheden van de betrokkene.

De verwerkingsverantwoordelijke is verplicht om bepaalde informatie (als betrokkene gebruik gemaakt heeft van het vergetelheidsrecht of rectificatierecht) te verstrekken aan de ontvanger van persoonsgegevens, tenzij dit onmogelijk is of onevenredig veel inspanning vergt.¹⁵⁸

De verwerkingsverantwoordelijke is verplicht¹⁵⁹ een register bij te houden van verwerkingsactiviteiten die onder zijn verantwoordelijkheid worden uitgevoerd. Art 30 lid 1 sub a tot en met 9 AVG beschrijft welke gegevens een register moet bevatten. Art. 42 lid 1 AVG uit dat bevordering van de invoering van een certificeringsmechanisme wenselijk is. Een dergelijk mechanisme op Europees niveau zou kunnen aantonen dat een verwerkingsverantwoordelijke en verwerkers bij het verwerken van persoonsgegevens overeenkomstig de AVG handelen.

3.10 Verplichtingen verwerker

De verwerker moet afdoende garanties kunnen geven aan de verwerkingsverantwoordelijke met betrekking tot het toepassen van passende technische en organisatorische maatregelen. Dit moet zodat duidelijk is dat aan de eisen van AVG wordt voldaan.¹⁶⁰ De verwerker mag geen andere verwerker in dienst nemen zonder voorgaande toestemming van de verwerkingsverantwoordelijke omdat deze werkt in opdracht van de verwerkingsverantwoordelijke. Toestemming moet schriftelijk plaatsvinden of specifiek duidelijk zijn gemaakt.¹⁶¹

De verwerker is verplicht¹⁶² een register bij te houden van alle categorieën van verwerkingsactiviteiten die hij uitvoert ten behoeve van de verwerkingsverantwoordelijke. Art. 30 lid 2 sub a tot en met d AVG geeft aan welke gegevens het register moet bevatten. In art. 28 lid 3 sub a tot en met h AVG zijn aanvullende bepalingen opgenomen waarin omschreven staat hoe verwerker zijn werk dient uit te voeren.

3.11 Gezamenlijke verplichtingen verwerkingsverantwoordelijke en verwerker

¹⁵³ Art. 21 AVG.

¹⁵⁴ Art. 20 AVG.

¹⁵⁵ Fennell e.a., 2016, p.95.

¹⁵⁶ Art. 38 lid 4 AVG.

¹⁵⁷ Art. 25 lid 1 AVG.

¹⁵⁸ Art. 19 AVG.

¹⁵⁹ Art. 30 lid 1 AVG.

¹⁶⁰ Art. 28 lid 1 AVG.

¹⁶¹ Art. 28 lid 2 AVG.

¹⁶² Art. 30 lid 2 AVG.

3.11.1 Beveiliging gegevensverwerking

De verwerkingsverantwoordelijke en de verwerker dragen samen zorg voor de beveiliging van de gegevensverwerking.¹⁶³ Zij houden hierbij rekening met de stand van de techniek en de uitvoeringskosten van de verwerking. Ook kijken zij naar de aard, omvang en de context van de gegevensverwerking. Zij brengen verwerkingsdoeleinden in kaart en kijken naar risico's voor de betrokkene die aan gegevensverwerking verbonden zijn. Wat een passend beveiligingsniveau onder meer hoort te bevatten, is verder uitgewerkt in art. 32 lid 1 sub a tot en met d AVG:

- Pseudonimisering en versleuteling van persoonsgegevens, indien mogelijk;
- Vermogen om vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
- Vermogen om bij een fysiek of technisch incident de beschikbaarheid van de toegang tot persoonsgegevens tijdig te herstellen;
- Procedure voor testen, evalueren, beoordelen van de doeltreffendheid van technische en organisatorische maatregelen die zijn genomen ter beveiliging van de verwerking.

3.11.2 Functionaris voor gegevensbescherming

De verwerkingsverantwoordelijke en de verwerker wijzen in een aantal gevallen een functionaris voor gegevensbescherming aan.¹⁶⁴ Een functionaris voor gegevensbescherming wordt door de verwerkingsverantwoordelijke en de verwerker tijdig betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. Ook ondersteunen zij hem bij zijn taken.¹⁶⁵ De verwerkingsverantwoordelijke kan bij de functionaris voor gegevensbescherming advies inwinnen over gegevensbeschermingseffectbeoordeling.¹⁶⁶

Gegevensbeschermingseffectbeoordeling wordt in Europese termen een Data Protection Impact Assessment (DPIA) genoemd en wordt gebruikt om de risico's van gegevensverwerking in kaart te brengen. Het uitvoeren van een beoordeling of een assessment is in een aantal gevallen verplicht. Art. 35 lid 3 AVG somt deze op. Verder geeft de AVG aan dat de toezichthouder (de rol van toezichthouder wordt beschreven in 3.13 *Toezicht naleving + handhaving, sancties*) een lijst opstelt met type van verwerking waarbij een beoordeling verplicht is en deze openbaar maakt.¹⁶⁷

3.11.3 Privacy by design – privacy by default

Onder privacy by design wordt kortgezegd verstaan gegevensbescherming door ontwerp. Onder privacy by default wordt kortgezegd verstaan gegevensbescherming door standaardinstellingen.¹⁶⁸ Zowel bij het ontwerpen van een informatiesysteem, als bij het verwerken van persoonsgegevens in een informatiesysteem, moet rekening gehouden worden met privacy. De AVG schrijft voor dat technische en organisatorische maatregelen genomen moeten worden gedurende het gehele proces van het verwerken van persoonsgegevens. Dus zowel op het tijdstip van de bepaling van het verwerkingsmiddel, als tijdens het verwerken zelf. Het doel van deze technische en organisatorische maatregelen is om de gegevensbeschermingsbeginselen, zoals minimale gegevensverwerking, op een doeltreffende manier uit te voeren. Daarnaast moeten er waarborgen in de verwerking ingebouwd worden ter naleving van de AVG en ter bescherming van de rechten van de betrokkenen. Een maatregel met betrekking tot transparantie van gegevensverwerking zou een kennisgeving aan de betrokkene kunnen zijn. In een dergelijke kennisgeving kan bijvoorbeeld staan of persoonsgegevens aan derden worden verstrekt en waarom. De betrokkene weet hierdoor waar hij aan toe is.”

3.12 De meldplicht datalekken

De meldplicht datalekken¹⁶⁹ is opgenomen in de Wbp en geldt sinds januari 2016. Bij intrekking van de Wbp en de officiële inwerkingtreding van de AVG, blijft deze van kracht. De verwerkingsverantwoordelijke is verplicht om een datalek te melden aan de AP. Een datalek in de betekenisfeer van de meldplicht datalekken is een “inbreuk op de beveiliging van persoonsgegevens: de persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking.”¹⁷⁰ Als sprake is van een ‘hoog risico’ met betrekking tot de gegevens van betrokkene dan moet deze ook worden ingelicht over het datalek.¹⁷¹ Of er sprake is van een hoog risico wordt beslist door de verwerkingsverantwoordelijke. De melding aan de AP moet een minimaal aantal

¹⁶³ Art. 32 lid 1 AVG.

¹⁶⁴ Art. 37 lid 1 sub a t/m c AVG.

¹⁶⁵ Art. 38 lid 2 AGV jo. Art 39 lid 1 AGV.

¹⁶⁶ Art 35 lid 2 AGV.

¹⁶⁷ Art. 35 lid 4 AVG.

¹⁶⁸ Art. 25 AVG.

¹⁶⁹ Art. 34A Wbp.

¹⁷⁰ Salverda & Witteveen, *Richtsnoeren meldplicht datalek gepubliceerd*, Europa decentraal, 05-10-2015.

¹⁷¹ Art. 34 lid 1 AVG.

mededelingen bevatten.¹⁷² Melding aan betrokkene moet worden gedaan in duidelijke en eenvoudige taal. De melding moet een beschrijving van de aard van de inbreuk bevatten en een aantal voorgeschreven gegevens en aanbevelingen uit art. 33 lid 3 sub a tot en met c AVG. Melden aan betrokkene is niet altijd verplicht, er zijn uitzonderingen.¹⁷³ Betrokkene hoeft niet te worden ingelicht over een datalek als: er passende technische en organisatorische beschermingsmaatregelen genomen zijn en deze zijn toegepast waardoor de persoonsgegevens onbegrijpelijk zijn voor onbevoegden. Of als er achteraf maatregelen genomen zijn waardoor het hoge risico voor de rechten en vrijheden van de betrokkene zich waarschijnlijk niet meer zal voordoen. Als de mededeling onevenredige inspanningen zou vergen, voldoet openbare melding ook.

Wanneer er inbreuk heeft plaatsgevonden, dient de verwerkingsverantwoordelijke zonder onredelijke vertraging (uiterlijk 72 uur) na kennisname van het datalek, de inbreuk te melden aan de AP, tenzij een risico onwaarschijnlijk is.¹⁷⁴ Wanneer de verwerkingsverantwoordelijke later dan 72 uur na het datalek melding maakt, moet de melding een motivering voor de vertraging bevatten.¹⁷⁵ Zelf is de verwerkingsverantwoordelijke verplicht om alle inbreuken in verband met persoonsgegevens te documenteren. Hij dient de gevolgen van de inbreuk en de getroffen maatregelen hiertegen te noteren.¹⁷⁶ Het doel van deze documentatie is dat de AP de naleving kan controleren.

3.13 Toezicht naleving en handhaving, sancties

3.13.1 Toezicht

De AVG verplicht iedere lidstaat om een onafhankelijke toezichthoudende autoriteit te benoemen (dit mogen er ook meerdere zijn¹⁷⁷), welke verantwoordelijk zijn voor het toezicht op toepassing van de AVG.¹⁷⁸ De onafhankelijkheid van de toezichthouder zit hem in het feit dat hij vrij blijft van 'rechtstreekse externe invloed' en geen instructies aanvaardt, ongeacht van wie deze afkomstig zijn.¹⁷⁹ De toezichthouder heeft een drietal bevoegdheden: onderzoeksbevoegdheden,¹⁸⁰ corrigerende maatregelen¹⁸¹ en autorisatie- en adviesbevoegdheden.¹⁸² In Nederland zal de toezichthouder de AP zijn, Europa decentraal (2016) geeft dit aan.¹⁸³ De toezichthouder is verplicht bij te dragen aan de consequente toepassing van de AVG in de gehele EU. Dit betekent onder andere dat de toezichthouder nauw samen dient te werken met andere toezichthoudende autoriteiten binnen de EU.¹⁸⁴

3.13.2 Handhaving

De AVG creëert een Europees Comité voor gegevensbescherming. Het Comité wordt een orgaan van de EU en krijgt rechtspersoonlijkheid.¹⁸⁵ Het Comité treedt bij de uitvoering van haar taken en bevoegdheden, welke zijn opgenomen in art. 70 en 71 AVG, onafhankelijk op.¹⁸⁶ Europa decentraal (2016) geeft kleur aan deze taken en bevoegdheden en noemt een paar voorbeelden zoals "het uitvaardigen van richtsnoeren, aanbevelingen en best practices inzake procedures voor het wissen van links, kopieën of reproducties van persoonsgegevens."¹⁸⁷

3.13.3 Sancties

¹⁷² Art. 33 lid 3 sub a t/m d AVG.

¹⁷³ Art. 34 lid 3 sub a t/m c AVG.

¹⁷⁴ Art. 33 lid 1 AVG.

¹⁷⁵ *Meldplicht inbreuk persoonsgegevens*, Europa decentraal, 2016.

¹⁷⁶ Art. 33 lid 5 AVG.

¹⁷⁷ Art 51 lid 1 AVG.

¹⁷⁸ Art. 51 lid 1 AVG.

¹⁷⁹ Art. 52 lid 2 AVG.

¹⁸⁰ Art. 58 lid 1 sub a t/m f AVG.

¹⁸¹ Art. 58 lid 2 sub a t/m j AVG

¹⁸² Art. 58 lid 3 sub a t/m j AVG

¹⁸³ *Toezicht en sancties*, Europa decentraal, 2016.

¹⁸⁴ Art. 57 lid 1 sub g AVG.

¹⁸⁵ Art. 68 lid 1 AVG.

¹⁸⁶ Art. 69 lid 1 AVG.

¹⁸⁷ *Toezicht en sancties*, Europa decentraal, 2016.

Nationale toezichthouders, zoals de AP zijn bevoegd om administratieve boetes op te leggen aan de verwerkingsverantwoordelijke.¹⁸⁸ De bedragen van deze boetes kunnen maximaal oplopen tot twintig miljoen euro of vier procent van de wereldwijde jaaromzet. Bij het opleggen van een administratieve boete wordt door de toezichthouder rekening gehouden met de omstandigheden van het geval. De boete wordt opgelegd naast of in plaats van¹⁸⁹ de corrigerende maatregelen. De boetes zijn in te delen in twee categorieën. Categorie één bestaat uit een boete die kan worden opgelegd bij inbreuken op de artikelen 8, 11 en 25 tot en met 43 AGV. Bij inbreuk op één van deze artikelen kan de boete oplopen tot een bedrag van tien miljoen euro. Categorie twee bestaat uit een boete die kan worden opgelegd bij een inbreuk op de beginselen inzake gegevensverwerking¹⁹⁰ (zoals beschreven in de gelijknamige alinea), bij een inbreuk op de rechten van de betrokkene¹⁹¹ of bij doorgifte van gegevens naar derde landen.¹⁹² De boete kan bij inbreuk op één van deze artikelen oplopen tot een bedrag van twintig miljoen euro of vier procent van de wereldwijde jaaromzet. Nota bene: als een verwerkingsverantwoordelijke of een verwerker opzettelijk of door nalatig gedrag inbreuk maakt op één of meerdere bepalingen van de AVG is de hoogte van de totale boete niet hoger dan de boete die de toezichthouder op kan leggen bij de zwaarste inbreuk.¹⁹³ Een administratieve boete kan ook worden opgelegd als een organisatie een corrigerende maatregel van de toezichthoudende autoriteit niet naleeft. Lidstaten moeten zelf regels vaststellen inzake 'andere sancties' die van toepassing zijn op inbreuken op de AVG.¹⁹⁴ Vanuit de AVG wordt aangegeven dat het in het bijzonder gaat om overtredingen waarbij het niet mogelijk is om een administratieve boete op te leggen.¹⁹⁵ Lidstaten zijn verplicht de nodige maatregelen treffen om ervoor te zorgen dat de zelf bedachte regels doeltreffend, evenredig en afschrikwekkend worden toegepast. De regels moeten in de vorm van een voorstel uiterlijk 25 mei 2018¹⁹⁶ aan de Europese Commissie worden medegedeeld.

3.14 Conclusie

Deelvraag 2: Wat houdt de AVG in, aan de hand van analyse van wet- en regelgeving en literatuuronderzoek?

De AVG is gericht op het **continueren en uniformeren** van de bescherming en verwerking van persoonsgegevens in Europa zoals Richtlijn 95/46/EG deze bewerkstelligde. **De AVG hoeft niet te worden geïmplementeerd** om directe werking te verkrijgen omdat het een Verordening is en geen Richtlijn. Dit heeft als uitwerking dat lidstaten de AVG op dezelfde manier toepassen en er geen verschillen in implementatiewijze tussen lidstaten zijn. De AVG is **van toepassing op persoonsgegevens**. Persoonsgegevens worden in de AVG aangemerkt als "alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Als identificeerbaar wordt beschouwd, een natuurlijk persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens of één of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon." De AVG is van toepassing op de **verwerking van persoonsgegevens** in het kader van activiteiten van een vestiging van een verwerkingsverantwoordelijke of een verwerker in de EU. Het maakt niet uit of de verwerking binnen of buiten de EU plaatsvindt. Concreet houdt dit in dat de AVG dus ook geldt voor bedrijven die buiten de EU gevestigd zijn, maar actief zijn op de Europese markt. Er is sprake van een **ruime reikwijdte**. Alle taken en verantwoordelijkheden in het **proces van gegevensverwerking** zijn verdeeld over **zeven rollen**. De rollen staan in hiërarchische verhouding tot elkaar. Een aantal taken zijn gezamenlijke taken. De AVG kent **algemene beginselen van gegevensverwerking** die moeten worden nageleefd door de verwerkingsverantwoordelijke (één van de rollen) als het gaat om de verwerking van persoonsgegevens. De algemene beginselen vormen een **kader** over hoe persoonsgegevens verwerkt moeten worden en hoe hieraan wordt voldaan. Het verwerken van persoonsgegevens mag alleen wanneer deze verwerking **rechtmatig** is, maar ook **behoorlijk** en **transparant**, de **betrokkene moet zijn toestemming voor de verwerking hebben verleend**. Daarnaast moet het transparant zijn dat de persoonsgegevens van de betrokkene worden verwerkt, en in hoeverre dit gebeurt. Een **certificeringsmechanisme** op Europees niveau zou kunnen aantonen dat een verwerkingsverantwoordelijke en verwerkers bij het verwerken van

¹⁸⁸ Art. 83 lid 1 AVG.

¹⁸⁹ Art. 83 lid 2 AVG.

¹⁹⁰ Art. 5 t/m 9 AVG.

¹⁹¹ Art. 12 t/m 22 AVG.

¹⁹² Art. 44 t/m 49 AVG

¹⁹³ Art. 83 lid 3 AVG.

¹⁹⁴ Art. 84 lid 1 AVG.

¹⁹⁵ Art. 84 lid 1 AVG.

¹⁹⁶ Art. 84 lid 2 AVG.

persoonsgegevens overeenkomstig de AVG handelen. **De betrokkene** is degene van wie de persoonsgegevens zijn, hij **heeft recht op**:

- Informatie: bij verzameling van gegevens bij betrokkene recht op aanvullende informatie in samenhang met behoorlijke en transparante verwerking;
- Inzage: specifieke informatie wanneer persoonsgegevens daadwerkelijk zijn verwerkt;
- Rectificatie: betrokkene kan aanvullende verklaring verstrekken;
- Vergetelheid: persoonsgegevens kunnen onder voorwaarden worden gewist;
- Beperking van de gegevensverwerking;
- Dataportabiliteit: meenemen van informatie;
- Bezwaar: te allen tijde toegestaan, maar onder specifieke voorwaarden.
- Klachtrecht: betrokkene moet weten dat hij een klacht kan indienen bij de AP.

Bovenstaande rechten kan hij inroepen tegen de verwerkingsverantwoordelijke. Een **datalek** is een inbreuk op de beveiliging van persoonsgegevens: de persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking. Een datalek **moet altijd gemeld worden** bij de AP. Er geldt een meldplicht. Melding aan betrokken wordt alleen gedaan als er sprake is van een hoog risico samenhangend met het lek. Of er sprake is van een hoog risico wordt bepaald door de verwerkingsverantwoordelijke. Hij maakt melding aan de AP en eventueel de betrokkene. Aanvullend is hij verplicht om alle inbreuken, dus alle datalekken te documenteren om naleving van de AVG te kunnen aantonen. De AVG **verplicht** iedere lidstaat een **toezichthouder te benoemen**, deze houdt onafhankelijk toezicht op de naleving van de AVG en werkt samen met toezichthouders in andere lidstaten. Daarnaast kent de AVG de toezichthouder, in Nederland is dit de AP, een **drietal bevoegdheden** toe: doen van onderzoek, opleggen van corrigerende maatregelen en autorisatie- en adviesbevoegdheden. De AP mag bij niet naleving een administratieve boete opleggen aan de verwerkingsverantwoordelijke. In de berekening van het boetebedrag wordt rekening gehouden met de omstandigheden van het geval. Ondanks deze afweging kan het **maximale boetebedrag** oplopen tot twintig 20 miljoen euro of vier procent van de wereldwijze jaaromzet van een bedrijf. Lidstaten worden door de AVG verplicht om een voorstel vorm te geven over sancties die zij opleggen in de gevallen waarin een administratieve boete niet mogelijk is. Dit voorstel moet uiterlijk 25 mei 2018 worden medegedeeld aan de Europese Commissie. Het is als organisatie verplicht om een functionaris gegevensbescherming, dit is een interne toezichthouder, in dienst te hebben als de organisatie een overheidsinstelling of overheidsorganisatie is. Met de inwerkingtreding van de AVG wordt het Europees **Comité voor gegevensbescherming** opgericht. Het Comité heeft diverse bevoegdheden tegenover de lidstaten.

HOOFDSTUK 4: HET JURIDISCH KADER - VERSCHILLEN TUSSEN DE WBP EN AVG

In dit hoofdstuk worden de verschillen tussen de Wbp en de AVG beschreven. Omdat de AVG de Wbp per 25 mei 2018¹⁹⁷ vervangt, is het van belang voor **ANONIEM** P&O om de verschillen tussen de huidige en de nieuwe privacyregels te kennen. Zo wordt het verschil tussen de juridische grondslag van Wbp en AVG uiteengezet. Verder wordt ingegaan op het verschil in territoriale en materiële werkingssfeer. Ook het verschil tussen het huidige sanctiebeleid en het nieuwe sanctiebeleid wordt toegelicht. De hoofdstukken twee en drie over de Wbp en de AVG zijn tevens gebruikt als bron om verschillen tussen de Wbp en AVG aan te kunnen onttrekken. De conclusie van dit hoofdstuk, is het antwoord op deelvraag 3.

4.1 Verschil tussen richtlijn en verordening – directe werking

De AVG is een Europese verordening en heeft automatisch directe werking, implementatie is niet nodig.¹⁹⁸ De toepassing van de AVG is daarmee hetzelfde voor iedere lidstaat. Waar lidstaten bij de implementatie van de richtlijn vrijheid kregen in de implementatiewijze, is dit bij de AVG niet het geval. Dit hangt samen met doel van de AVG: het vergroten van de uniformiteit in privacywetgeving binnen de EU.¹⁹⁹ Wel geeft de AVG lidstaten beperkt de mogelijkheid om wetgeving aan te passen aan eigen behoeftes. Met betrekking tot bepaalde onderwerpen is afwijken van de AVG mogelijk.²⁰⁰

De Wbp is gebaseerd op een Europese Richtlijn, Richtlijn 95/46/EG, deze moest worden geïmplementeerd in lokale wetten per Europees land (in Nederland was dit de Wbp) ter verkrijging van directe werking.²⁰¹

4.2 Vergrote territoriale werkingssfeer

De AVG is van toepassing op de verwerking van persoonsgegevens als de verwerkingsverantwoordelijke of de verwerker gevestigd is in de EU. Het maakt niet uit of de verwerking zelf binnen of buiten de EU wordt uitgevoerd.²⁰² De Wbp is enkel van toepassing op de verwerking van persoonsgegevens in Nederland, mits de verantwoordelijke voor de verwerking van de persoonsgegevens in Nederland gevestigd is.²⁰³ De Wbp is eveneens van toepassing als de verantwoordelijke niet gevestigd is in de Europese Unie, als er gebruik wordt gemaakt van handmatige of geautomatiseerde verwerkingsmiddelen die zich in Nederland bevinden.²⁰⁴ Voor de toepassing van de AVG maakt het geen verschil uit of de verwerking van persoonsgegevens binnen of buiten de EU wordt verricht.²⁰⁵

4.3 Vergrote materiële werkingssfeer

De AVG kent een grotere materiële werkingssfeer dan de Wbp. Dit wil zeggen dat er meer beginselen inzake verwerking persoonsgegevens moeten worden nageleefd. Europa decentraal (2016) geeft aan dat een aantal beginselen apart is opgenomen in de AVG.²⁰⁶ Het gaat om het transparantiebeginsel²⁰⁷, het toestemmingsbeginsel²⁰⁸ en het rechtmatigheidsbeginsel.²⁰⁹ In de Wbp zijn de beginselen niet apart opgenomen, maar verwerkt in andere artikelen. Toestemming voor gegevensverwerking volgens de AVG is als volgt te omschrijven: "Toestemming dient te worden gegeven door middel van een duidelijke actieve handeling, bijvoorbeeld een schriftelijke verklaring, ook met elektronische middelen, of een mondelinge verklaring (deze kan worden opgenomen), waaruit blijkt dat betrokkene vrijelijk, specifiek, geïnformeerd en ondubbelzinnig met de verwerking van zijn persoonsgegevens instemt."²¹⁰ De Wbp voorziet als het gaat om het begrip toestemming in de volgende definitie: "Elke vrije, specifieke en op informatie berustende wilsuiting waarmee betrokkene aanvaardt dat hem betreffende persoonsgegevens worden verwerkt."²¹¹ Het verschil tussen de AVG en de Wbp aangaande toestemming voor

¹⁹⁷ Art. 99 lid 2 AVG.

¹⁹⁸ Privacy: De Algemene Verordening Gegevensbescherming, Europa decentraal, 2016.

¹⁹⁹ Verordening (EU) 2016/679, 27-04-2016, overwegingen 1-13, nr. 10.

²⁰⁰ Verordening (EU) 2016/679, 27-04-2016, overwegingen 1-13, nr. 8.

²⁰¹ Factsheet: Rechtstreekse werking van bepalingen uit Europese richtlijnen: regels en risico's, Europa decentraal, 2009.

²⁰² Verordening (EU) 2016/679, 27-04-2016, overwegingen 22-25, nr. 22.

²⁰³ Art. 4 lid 1 Wbp.

²⁰⁴ Art. 4 lid 2 Wbp.

²⁰⁵ Art. 3 lid 1 AVG.

²⁰⁶ Rechtmatigheid en Transparantie, Europa decentraal, 2016.

²⁰⁷ Art. 5 lid 1 sub a AVG.

²⁰⁸ Art. 7 AVG.

²⁰⁹ Art. 5 lid 1 sub a AVG jo. Art. 6 lid 1 sub a t/m f AVG jo. Art. 7 AVG.

²¹⁰ Berkvens, Jakimowicz 2016, p. 215.

²¹¹ Art. 1 sub i Wbp.

gegevensverwerking van betrokkene is dat expliciete toestemming nodig is (middels een actieve handeling) in naleving van de AVG.

4.4 Meer verplichtingen voor verwerkingsverantwoordelijke en verwerker

Kranenborg & Verhey kaarten in 2011 al aan dat het 'lastig gevonden wordt' hoe verantwoordelijkheden tussen de verantwoordelijke en de bewerker zijn verdeeld.²¹² Aan de naamgeving van de rollen en het jaartal te zien, werd de verdeling dus als een moeilijk punt ervaren ten tijde van de Wbp. De AVG zorgt voor een toename in verplichtingen die de verwerkingsverantwoordelijke en de verwerker moeten naleven. Met meer verplichtingen om aan te voldoen, zou de verdeling van verantwoordelijkheden een struikelblok kunnen zijn, maar in AVG is hier iets op bedacht. In de overwegingen van de AVG staat beschreven dat "de verantwoordelijkheid en aansprakelijkheid van de verwerkingsverantwoordelijke moeten worden vastgelegd voor elke verwerking van persoonsgegevens die door of namens hem wordt uitgevoerd."²¹³ De AVG geeft de toezichthouder (zie 4.5 *Meldplicht wordt documentatieplicht*) de mogelijkheid om modelbepalingen²¹⁴ uit te vaardigen voor de relatie tussen verwerkingsverantwoordelijke en verwerker. Een overzicht van de verplichtingen van de verwerkingsverantwoordelijke, de verwerker en de verplichtingen die samenvallen is te raadplegen in bijlage 3.

4.5 Meldplicht wordt documentatieplicht

Met ingang van de AVG hoeven organisaties niet meer verplicht verwerkingen van persoonsgegevens aan te melden bij de nationale toezichthouders. In Nederland is de toezichthouder de Autoriteit Persoonsgegevens. In plaats van met de meldplicht uit de Wbp²¹⁵, gaan organisaties via de AVG met een documentatieplicht werken. Verwerkingsverantwoordelijken zijn verplicht een overzicht bij te houden van al hun verwerkingen van persoonsgegevens, niet alleen van de meldingsplichtige verwerkingen zoals zij waren aangegeven in de Wbp²¹⁶. Deze verandering brengt met zich mee dat met documenten moet kunnen worden aangetoond dat de juiste organisatorische en technische maatregelen zijn genomen om aan de AVG te voldoen. In hoofdstuk 3 over de AVG worden de begrippen privacy by default en privacy by design gedefinieerd. "Het doel van deze technische standaardinstellingen, (privacy by default) en organisatorische, ontworpen (privacy by design) maatregelen is om de algemene beginselen inzake verwerking persoonsgegevens²¹⁷ op een doeltreffende manier uit te voeren. Daarnaast moeten er waarborgen in de verwerking ingebouwd worden ter naleving van de AVG en in navolging daarvan ter bescherming van de rechten van de betrokkene."²¹⁸ Aanvullend moeten de standaardinstellingen (privacy by default) van een product of dienst, indien mogelijk, afgestemd zijn op de manier van gegevensverwerking. Gedurende het gehele ontwikkelingsproces van producten en diensten moet rekening worden gehouden met de privacy van betrokkene. Dit kan door technieken als pseudonimisering toe te passen (gegevens zijn dan niet meer te herleiden naar de betrokkene) en door zo min mogelijk persoonsgegevens te verwerken, namelijk door uitsluitend noodzakelijke persoonsgegevens te verwerken. (Minimale gegevensverwerking) Deze noodzakelijkheidseis geldt tevens voor de toegankelijkheid tot de gegevens en de bewaring ervan.²¹⁹ De gegevens moeten niet toegankelijk zijn voor personen zonder dat daar een reden voor is. Anders dan in naleving van de Wbp dienen organisaties straks actief beleid te voeren en maatregelen te implementeren waaruit blijkt dat de AVG wordt nageleefd. Dit betekent dat de verwerkingsverantwoordelijke verplicht is documentatie te hebben waarin alle aspecten van de verwerking van persoonsgegevens door de organisatie worden beschreven.²²⁰

4.6 Uitbreiding rechten van betrokkene

Het recht op vergetelheid²²¹ en dataportabiliteit²²² zijn nieuwe rechten voor de betrokkene, zij zijn opgenomen in de AVG en niet in de Wbp. Het recht op vergetelheid geeft de betrokkene de mogelijkheid zijn gegevens onder voorwaarden laten te wissen. Met het recht op dataportabiliteit heeft betrokkene de mogelijkheid om gegevens mee te nemen/aan een andere organisatie te geven. Aan gebruikmaken van dataportabiliteit zijn twee voorwaarden verbonden, art. 20 lid sub a

²¹² Kranenborg & Verhey 2011, p. 189.

²¹³ Verordening (EU) 2016/679, 27-04-2016, overwegingen 74-77, nr. 74.

²¹⁴ Art. 28 lid 6 AVG jo. Art. 28 lid 8 AVG.

²¹⁵ Art. 27 Wbp.

²¹⁶ Art. 34a Wbp.

²¹⁷ Art. art. 5 lid 1 sub a t/m f AVG.

²¹⁸ *Privacy by design and by default*, Europa decentraal, 2016.

²¹⁹ Art. 25 lid 2 AVG.

²²⁰ Art. 30 lid 1 sub a t/m g AVG.

²²¹ Art. 17 lid 1 sub a t/m f AVG.

²²² Art. 20 lid 1 sub a jo. Art. 20 lid 1 sub b AVG.

en b AVG geeft ze aan: 1. De verwerking berust op toestemming van betrokkene of op een overkomst; 2. De verwerking wordt via automatische procedure(s) verricht.

4.7 Hogere boetes bij niet-naleving AVG dan bij niet-naleving Wbp

Bij niet naleving van de AVG is de maximale boete die door de nationale toezichthouder (In Nederland de AP) kan worden opgelegd twintig miljoen euro of vier procent van de wereldwijde jaaromzet.²²³ Bij niet naleving van de Wbp is het maximale boetebedrag €820.000.²²⁴

In punt 4.1 (*Verskil tussen richtlijn en verordening – directe werking*) werd al aangegeven dat het in sommige gevallen mogelijk is om van de AVG af te wijken. In geval van boetes geeft de AVG lidstaten de vrijheid om zelf nationale regels vast te stellen over de vraag of en in hoeverre boetes kunnen worden opgelegd aan in de lidstaat gevestigde overheidsinstanties en overheidsorganen.²²⁵

4.8 Verschillende uitgangspunten meldplicht datalekken

Fennell e.a. (2016) geeft aan dat de meldplicht datalekken in januari 2016 is opgenomen in de Wbp.²²⁶ De AVG houdt de meldplicht in stand, maar hanteert andere uitgangspunten dan de Wbp. Zo zorgt de AVG voor 'drempelverlaging'. Onder de AVG moet elk datalek aan de toezichthouder worden gemeld, tenzij er geen risico is voor de vrijheden en rechten van betrokkene. De Wbp verplichtte slechts melding aan de toezichthouder bij een datalek met mogelijk 'ernstige nadelige gevolgen'.²²⁷ Ook de betrokkene werd vanuit een andere gedachtegang op de hoogte gebracht van het datalek. De Wbp verplichtte melding bij een vermoeden van 'ongunstige gevolgen' voor betrokkene.²²⁸ De AVG verplicht melding bij een hoog risico voor betrokkene.²²⁹ De beoordeling van het risico en melding van het datalek wordt respectievelijk verricht door de verwerkingsverantwoordelijke (AVG) of de verantwoordelijke (Wbp).

4.9 Toename instrumenten voor internationale doorgifte gegevens

De AGV kent drie manieren voor doorgifte van persoonsgegevens naar derde landen. (Landen buiten de EU). Dit zijn: 1. Doorgifte op basis van adequaatheidsbesluiten,²³⁰ 2. Doorgifte op basis van passende waarborgen,²³¹ 3. Doorgifte op basis van bindende bedrijfsvoorschriften.²³²

Bij 'adequacy finding' oftewel adequaatheidsbesluiten, heeft de Europese Commissie de waarborg van de bescherming van persoonsgegevens in het derde land van bestemming van de gegevens getoetst.²³³ Passende waarborgen kunnen worden ingezet als de Europese Commissie negatief oordeelt over het beschermingsniveau van een land. Doorgifte kan alsnog plaatsvinden als de verwerkingsverantwoordelijke en de verwerker passende waarborgen nemen en de betrokkene over 'afdwingbare rechten en doeltreffende rechtsmiddelen' beschikt.²³⁴

Een multinationale onderneming kan voor al haar onderdelen en vestigingen, ook de onderdelen die zich in derde landen bevinden, intern bindende privacyregels vaststellen.²³⁵ Na goedkeuring door de toezichthouder, mogen vanuit de Europese Unie (EU) zonder aanvullende eisen gegevens naar de vestiging in het derde land worden overgedragen.²³⁶

Doorgifte van gegevens naar een derde land in naleving van de Wbp is anders vormgegeven. Persoonsgegevens worden pas doorgegeven aan een derde land als het desbetreffende land een passend beschermingsniveau waarborgt.²³⁷ Een beschermingsniveau wordt beoordeeld aan de hand van een aantal criteria.²³⁸ In eerste instantie is de beoordeling van het niveau de taak van de verantwoordelijke, zo geeft de Wbp-naslag van de AP aan. Aanvullend kan de Europese Commissie vaststellen of een derde een passend beschermingsniveau heeft.²³⁹ Er wordt gekeken naar de aard van de gegevens en het doeleinde van de beoogde verwerking. Ook wordt gekeken naar het land waaruit de gegevens afkomstig zijn en het land waar de gegevens aan doorgegeven gaan worden. De sectoriële rechtsregels (de 'eigen regels' van het land aangaande gegevensbescherming) in het

²²³ Art. 83 lid 5 AVG.

²²⁴ Art. 66 lid 1 Wbp jo. Art 66 lid 2 Wbp.

²²⁵ Art. 83 lid 7 AVG jo. Art. 84 lid 1 AVG.

²²⁶ Fennell e.a. 2016, p. 5.

²²⁷ Art. 34a lid 1 Wbp.

²²⁸ Art. 34a lid 2 Wbp.

²²⁹ Art. 34 lid 1 AVG.

²³⁰ Art. 45 lid 1 AVG.

²³¹ Art. 46 lid 1 AVG.

²³² Art. 47 lid sub a t/m c AVG.

²³³ Art. 45 lid 2 AVG.

²³⁴ Art. 46 lid 1 AVG.

²³⁵ Art. 47 lid 1 sub a t/m c AVG.

²³⁶ De Jong, 'De Algemene verordening gegevensbescherming', *RegelMaat*, 2015.

²³⁷ Art. 76 lid 1 Wbp.

²³⁸ Art. 76 lid 3 Wbp.

²³⁹ Art. 76 lid 1 Wbp, *Wbp-naslag*, AP.

derde land worden nagegaan en ten slotte worden veiligheidsmaatregelen en de regels van het beroepsleven nagegaan.

4.10 Verplichting tot werken met (D)PIA

De AVG verplicht in bepaalde gevallen de uitvoering van een PIA (Privacy Impact Assessment) ook wel Data Protection Impact Assessment (DPIA) of een gegevensbeschermingseffectbeoordeling genoemd. Een gegevensbeschermingseffectbeoordeling is volgens de AVG van belang om risico's in beeld te brengen. 'In het bijzonder als bij verwerking van persoonsgegevens nieuwe technologieën worden gebruikt.'²⁴⁰ De AVG geeft aan dat een DPIA vereist is in de volgende gevallen. Dit is een niet-limitatieve opsomming: 1. Persoonlijke aspecten van natuurlijke personen worden systematisch en uitgebreid beoordeeld. De gegevens zijn gebaseerd op automatisch verwerking.²⁴¹ 2. Bijzondere persoonsgegevens worden op grote schaal verwerkt.²⁴² 3. Er wordt stelselmatig en op grote schaal gemonitord in openbaar toegankelijke ruimte.²⁴³ De AP stelt in samenspraak met andere Europese privacytoezichthouders (De evenbeelden van de Nederlandse AP) een aanvullende lijst op van alle soorten verwerkingen waarbij de uitvoering van een PIA verplicht is.²⁴⁴

4.11 Aanstellen functionaris voor gegevensbescherming niet meer vrijwillig

In de Wbp was het benoemen van een functionaris voor gegevensbescherming opgenomen als een kan-bepaling.²⁴⁵ Als sprake is van een kan-bepaling dan wil dat zeggen dat er keuzevrijheid is over de toepassing van een bepaling. De AVG verplicht sommige instellingen/bedrijven om een functionaris gegevensbescherming aan te stellen. Dit geldt voor overheidsorganisaties, organisaties met meer dan 250 werknemers en wanneer één van de hoofdtaken van een organisatie het verwerken van (bijzondere) persoonsgegevens is of de organisatie op grote schaal mensen volgt (bijvoorbeeld via profilering). Profilering is een evaluatie van bepaalde aspecten van een natuurlijk persoon met bedoeling om zaken te voorspellen of analyseren.²⁴⁶

Als een organisatie niet vanuit de AVG verplicht wordt (en dus buiten de categorieën valt) een functionaris gegevensbescherming aan te stellen, mag een organisatie dit alsnog vrijwillig doen. Een vrijwillige functionaris gegevens moet zich aan dezelfde regels houden als een functionaris gegevensbescherming die verplicht is aangesteld.²⁴⁷

4.12 Inkadering bewaartermijn persoonsgegevens

De AVG geeft aan dat de bewaartermijn van persoonsgegevens bekend moet zijn. Als een termijn aangeven niet mogelijk is, moeten criteria worden opgesteld aan de hand waarvan een termijn kan worden bepaald.²⁴⁸ De Wbp geeft in het kader van het bewaren van persoonsgegevens enkel aan dat gegevens niet langer mogen worden bewaard dan voor het doel van de verwerking noodzakelijk was.²⁴⁹

4.13 Oprichting Europees Comité voor gegevensbescherming

Met de inwerkingtreding van de AVG wordt het Europees Comité voor gegevensbescherming opgericht.²⁵⁰ Het Comité is onafhankelijk²⁵¹ en kan optreden door een bindend advies uit te brengen als sprake is van een situatie zoals gedefinieerd in art. 65 lid 1 sub a tot en met c AVG. Naast bindend advies kan het Comité ook 'regulier' advies uitbrengen in de situaties art. 64 lid 1 sub a tot en met f AVG. Ook kan het comité richtsnoeren en aanbevelingen uitvaardigen over de verwerking en bescherming van persoonsgegevens, zo geeft Europa decentraal (2016) aan.²⁵² Ook kan zij zelf, of op verzoek van een toezichthoudende autoriteit, de Europese Commissie of de voorzitter van het Europees Comité voor gegevensbescherming²⁵³ onderzoek uitvoeren met betrekking tot de AVG. Het comité stelt een jaarverslag²⁵⁴ op over de bescherming van natuurlijke personen met betrekking tot verwerking van persoonsgegevens in de EU en indien van toepassing over doorgifte naar derde landen. De taken en bevoegdheden van het Europees Comité voor

²⁴⁰ Art. 35 lid 1 AVG.

²⁴¹ Art. 35 lid 3 sub a AVG.

²⁴² Art. 35 lid 3 sub b AVG.

²⁴³ Art. 35 lid 3 sub c AVG.

²⁴⁴ Art. 35 lid 4 AVG.

²⁴⁵ Art. 62 Wbp.

²⁴⁶ Art. 4 lid 4 AVG.

²⁴⁷ *Functionaris voor gegevensbescherming*, Europa decentraal, 2016.

²⁴⁸ Art. 13 lid 2 sub a AVG.

²⁴⁹ Art. 10 Wbp.

²⁵⁰ Art. 68 lid 1 AVG.

²⁵¹ Art. 69 lid 1 AVG.

²⁵² *Toezicht en sancties*, Europa decentraal, 2016.

²⁵³ Art. 64 lid 2 AVG.

²⁵⁴ Art. 71 lid 1 AVG.

gegevensbescherming, zoals zojuist beschreven, is terug te vinden in de tabel: *Rollen in proces gegevensverwerking en bescherming - ontleend aan Wbp & AVG*. De weergave in de tabel is beperkt. Alle taken en bevoegdheden staan in de artikelen 64, 65, 70 en 71 AVG.

4.14 Mogelijkheid tot certificering organisaties

De AVG biedt organisaties de mogelijkheid om zich te laten certificeren. De Wbp kent deze mogelijkheid niet. Organisaties kunnen als zij gecertificeerd²⁵⁵ zijn, op Europees niveau aantonen dat hun verwerkingsverantwoordelijke en verwerkers bij het verwerken van persoonsgegevens overeenkomstig de AVG handelen en dat zij voldoende technische en organisatorische maatregelen hebben genomen. (Zie 3.11.3 *Privacy by design en default*).

4.15 Aangescherpte check verwerking van persoonsgegevens van kinderen onder de 16

Als persoonsgegevens van een kind in de leeftijdscategorie jonger dan zestien jaar worden verwerkt, is de AVG strikt. De enige uitzondering die lidstaten via nationale wetgeving kunnen toepassen, is de leeftijd waarop gegevens mogen worden verwerkt te verlagen tot dertien jaar. Dergelijke gegevens mogen alleen worden verwerkt met toestemming van de ouder(s) of wettelijke vertegenwoordiger(s) van het kind. De organisatie is verplicht zich 'redelijk' in te spannen om de gegeven toestemming te controleren. De AVG geeft geen definitie van 'redelijke inspanning.' Wat hier precies onder wordt verstaan zal moeten blijken uit de praktijk.

4.16 Verschil in rollen in proces gegevensverwerking tussen Wbp & AVG

In hoofdstuk 2 over de Wbp en hoofdstuk 3 over de AVG zijn tabel 1 en 2 opgenomen. In deze tabellen worden de rollen in het proces van gegevensverwerking en bescherming gedefinieerd voor zowel de Wbp als de AVG. In tabel 1 worden de rollen in het gegevensverwerkingsproces volgens de Wbp weergegeven. In tabel 2 worden de rollen in het gegevenswerkingsproces weergegeven voor de AVG. Als deze twee tabellen met elkaar worden vergeleken, wordt zichtbaar welke verschillen er zijn in de rollen tussen de Wbp en AVG. Behalve verschillen in naamgeving van rollen zijn er ook inhoudelijke verschillen in rollen tussen de Wbp en de AVG. In onderstaande tabel: tabel 3, worden alle verschillen weergegeven.

²⁵⁵ Art. 42 lid 1 AVG.

Tabel 3: Verschillen tussen de Wbp & AVG in proces gegevensverwerking

Naam rol volgens Wbp	Naam rol volgens AVG	Inhoud (wijziging) in rol
Verantwoordelijke	Verwerkingsverantwoordelijke	<u>Toename verplichtingen</u> : technische, organisatorische maatregelen uitgebreid. Moet kunnen worden aangetoond dat verwerking wordt uitgevoerd naar gelang de AVG ²⁵⁶ Bijhouden register verwerkingsactiviteiten
Bewerker	Verwerker	<u>Toename verplichtingen</u> : persoonsgegevens worden alleen verwerkt op basis van schriftelijke instructie ²⁵⁷ Mogelijk aansprakelijk bij niet naleving algemene beginselen gegevensverwerking ²⁵⁸ Aantal taken samen met verwerkingsverantwoordelijke ²⁵⁹
Betrokkene	Betrokkene	<u>Uitbreiding rechten</u> : recht op vergetelheid ²⁶⁰ en dataportabiliteit ²⁶¹
Derde	Derde	n.v.t.
Ontvanger	Ontvanger	n.v.t.
Toezichthouder	Toezichthouder	<u>Mogelijkheid tot opleggen hogere boetes</u> dan bij Wbp ²⁶² Maximaal €820.000 (Wbp) versus maximaal €20 miljoen of 4% wereldwijde jaaromzet (AVG) ²⁶³ <u>Bijdragen aan consequente toepassing AVG</u> -> meer samenwerking met andere nationale toezichthouders in EU ²⁶⁴
Functionaris voor gegevensbescherming	Functionaris voor gegevensbescherming	Bij AVG in sommige gevallen <u>verplichting tot aanstellen functionaris voor gegevensbescherming</u> ²⁶⁵ Wbp: benoeming functionaris voor gegevensbescherming is een kanbepaling ²⁶⁶ De functionaris stelt een lijst op van verwerkingen van persoonsgegevens waarbij een DPIA (gegevensbeschermingeffectbeoordeling) <u>verplicht</u> is. ²⁶⁷ De verwerkingsverantwoordelijke kan om advies verzoeken wanneer een DPIA nodig is.
n.v.t.	Europees comité voor gegevensbescherming	<u>Nieuw: Comité</u> : opgericht bij inwerkingtreding AVG – onafhankelijk – Taken en bevoegdheden als uitvaardigen van richtsnoeren, aanbevelingen en best practices ²⁶⁸ , onderzoek uitvoeren ²⁶⁹ , advies ²⁷⁰ , geschillenbeslechting ²⁷¹

²⁵⁶ Art. 24 lid 1 AVG.

²⁵⁷ Art. 28 lid 3 sub a AVG.

²⁵⁸ Art. 49 lid 3, lid 4 Wbp jo. *Materiële voorschriften bij het werken met persoonsgegevens.*

²⁵⁹ Art. 32 lid 1 AVG.

²⁶⁰ Art. 17 lid 1 sub a t/m f AVG.

²⁶¹ Art. 20 lid 1 sub a jo. Art. 20 lid 1 sub b AVG.

²⁶² Art. 66 lid 1 Wbp.

²⁶³ Art. 83 lid 5 sub a t/m e AVG.

²⁶⁴ Art. 57 lid 1 sub g AVG.

²⁶⁵ Art. 37 lid 1 sub a t/m c AVG.

²⁶⁶ Art. 62 Wbp.

²⁶⁷ Art. 35 lid 4 AVG.

²⁶⁸ *Toezicht en sancties*, Europa decentraal, 2016.

²⁶⁹ Art. 70 lid 1 sub e AVG.

²⁷⁰ Art. 64 lid 1 sub a t/m f AVG.

²⁷¹ Art. 65 lid 1 sub a t/m c AVG.

4.17 Conclusie

Deelvraag 3: Wat zijn volgens wet- en regelgeving en literatuuranalyse de verschillen tussen de Wbp en AVG?

De AVG heeft in tegenstelling tot de Wbp **directe werking** zonder dat hiervoor implementatie nodig is. Dit komt omdat de AVG een verordening is en de Wbp gebaseerd is op een Europese richtlijn. Daarnaast kent de AVG een **grotere materiële en territoriale werkingssfeer** dan de Wbp. Dit betekent dat er meer beginselen rondom het verwerken van persoonsgegevens moeten worden nageleefd (materieel). Een vergrote territoriale werkingssfeer wil in dit geval zeggen dat de AVG ook geldt voor organisaties die niet in de EU gevestigd zijn, zij moeten om onder het toepassingsbereik van de AVG te vallen wel persoonsgegevens laten verwerken in de EU.

Een aantal begrippen heeft een **nieuwe naam** gekregen, bijvoorbeeld een aantal rollen in het verwerkingsproces van gegevens. **Sommige bepalingen zijn 'helemaal' nieuw**, zij waren niet opgenomen in de Wbp. Zo biedt de AVG organisaties de mogelijkheid om zich te laten **certificeren**. Met een certificaat kunnen zij aantonen dat zij overeenkomstig de AVG maatregelen treffen op het gebied van **privacy by design** (organisatorische maatregelen) en **privacy by default** (technische maatregelen) gedurende het gehele proces van gegevensverwerking, zogezegd vanaf de verzameling van gegevens tot aan vernietiging ervan. Ook het **Europees comité voor gegevensbescherming** is nieuw en heeft een aantal bevoegdheden tegenover lidstaten.

Een aantal **bestaande rechten** vanuit de Wbp wordt met de inwerkingtreding van de AVG **uitgebreid**. Zo krijgen betrokkenen er twee rechten (vergetelheid en dataportabiliteit) bij en voorziet de AVG in meer instrumenten bij doorgifte van gegevens naar derde landen.

De **meldplicht datalekken** die al was opgenomen in de Wbp wordt **gecontinueerd** in de AVG, maar kent andere uitgangspunten over wanneer een datalek moet worden gemeld. Zo wordt een lek altijd gemeld aan de AP, tenzij een risico voor de rechten en vrijheden van natuurlijke personen onwaarschijnlijk is. Melden aan de betrokkene wordt slechts gedaan als er sprake is van een hoog risico aangaande zijn gegevens.

De AVG zorgt ook voor **meer kader** dan de Wbp: de bewaartermijnen van persoonsgegevens zijn niet meer zo 'vrijblijvend' zoals ten tijde van de Wbp. In principe moet een bewaartermijn helder zijn, is hier geen sprake van dan moeten er criteria worden opgesteld aan de hand waarvan een termijn kan worden bepaald. De AVG verplicht het werken met modelbepalingen en stelt een documentatieplicht in. Tegenover de documentatieverplichting staat wel dat niet ieder type verwerking van persoonsgegevens meer gemeld hoeft te worden aan de toezichthouder. De verwerkingsverantwoordelijke moet in plaats van de meldingen zelf een overzicht bijhouden van alle verwerkingen, niet alleen de meldingsplichtige verwerkingen zoals dit was vormgegeven in de Wbp.

Sommige bepalingen zijn strikter en zwaarder opgenomen in de AVG dan in de Wbp: De boetebedragen die kunnen worden opgelegd door de toezichthouder zijn hoger. Organisaties worden in bepaalde gevallen verplicht tot het uitvoeren van een DPIA om risico's voor gegevensverwerking in kaart te brengen. Het benoemen van een functionaris voor gegevensbescherming is niet langer vrijwillig, maar in bepaalde gevallen verplicht. Ook zijn voorwaarden voor de verwerking van persoonsgegevens van kinderen onder de zestien jaar opgenomen.

HOOFDSTUK 5: TOTSTANDKOMING RESULTATEN

De resultaten van het praktijkonderzoek worden beschreven in twee hoofdstukken. Hoofdstuk 6 ziet op deelvraag 4: *Wat is de huidige werkwijze van de directie P&O van de organisatie met betrekking tot het verwerken van persoonsgegevens in naleving van de Wbp na afname van interviews?* Hoofdstuk 7 ziet op deelvraag 5: *Wat is het beeld van de (toekomstige) werkwijze van de directie P&O van de organisatie met betrekking tot het verwerken van persoonsgegevens in naleving van de AVG na afname van interviews?*

5.1 Methode

Ter beantwoording van zowel deelvraag 4 als deelvraag 5, is de onderzoeksmethode interviewen gebruikt. In totaal zijn vier interviews afgenomen. Eén interview was een dubbelinterview (twee mensen werden tegelijk geïnterviewd). Eerst werden de participanten geïnterviewd ter beantwoording van deelvraag 4 en daarna ten behoeve van deelvraag 5. Dit gebeurde in één zitting. Elk interview duurde anderhalf uur. Transcripties van de interviews inclusief codering zijn opgenomen in bijlage 4.1 tot en met 4.4. Per paragraaf in hoofdstuk 6 en 7, is via een voetnoot aangegeven welke interviewvragen zijn gesteld voor totstandkoming van dat deel van de resultaten.

5.2 Participanten

De vijf geselecteerde participanten zijn deskundig op het gebied van persoonsgegevens/gegevensverwerking bij de directie P&O van de organisatie. Zij zijn geselecteerd voor een interview vanwege hun expertise. Het type interview dat van hen afgenomen is, is dan ook te classificeren als een 'elite- of expertinterview'.²⁷² De participanten werken met systemen waarmee gegevens worden verwerkt. Voor elk onderwerp is de functionaris geïnterviewd die over het onderwerp gaat en met de systemen werkt. Daardoor kan een volledig beeld van gegevensverwerking binnen de directie P&O van de organisatie worden gevormd.

Tabel 4: Participanten: functie, transcriptiecode, onderwerp en product/doel

Functie participant	Transcriptiecode participant ²⁷³	Onderwerp gegevensverwerking	Bijbehorend product/doel
Vervoerscoördinator (2 personen)	V1 V2	Vervoer	<i>Anoniem</i>
Hoofd P&O Ondersteuning	HPO	Personeels- en salarisadministratie	- Overzichten - Rapportage - Voortgangssysteem
Coördinator P-beheer	CP	<i>Anoniem</i>	Uitzending
Coördinator Kwaliteitszorg, Administratieve Organisatie en Interne Controle (KAI)	CK	Wet Normering Topinkomens (WNT)	Jaarverslag

5.3 Beknopte weergave onderwerp participant

Anoniem

Personeels- en salarisadministratie - Overzichten/rapportage

Periodiek worden diverse overzichten en rapportages opgemaakt. Deze overzichten dienen met name voor controletoepassing en zorgen ervoor dat gegevensverwerking kan worden verantwoord.

Anoniem

Wet Normering Topinkomens (WNT) – Jaarverslag

Het doel van de WNT is het tegengaan van bovenmatige beloningen en ontslagvergoedingen bij instellingen in de (semi) publieke sector. In de WNT worden inkomens en ontslagvergoedingen van topfunctionarissen bij instellingen met een publieke taak, genormeerd en openbaar gemaakt.

5.4 Procedure interviews

Qua type interview is gekozen voor halfgestructureerd interview.²⁷⁴ De vragen die zijn gesteld, waren ingedeeld per topic en dit gaf structuur. Aan alle vijf participanten zijn dezelfde vragen

²⁷² Term ontleend aan Baarda e.a., *Basisboek Interviewen*, 2012, p. 22.

²⁷³ Transcriptiecodes zijn gekoppeld aan de participanten zodat duidelijk is wie aan het woord is tijdens de interviews.

²⁷⁴ Termen ontleend aan Baarda e.a., *Basisboek Interviewen*, 2012, p. 19, 20.

gesteld. Doorvragen was vanwege de keuze voor een halfgestructureerd interview ook een mogelijkheid. Voorgaand aan het interview hebben de participanten informatie ontvangen over de opbouw van het interview en de wijze van terugkoppeling, deze informatie is opgenomen in bijlage 5. Daarnaast ontvingen zij een beknopte weergave van de verschillen tussen de Wbp en AVG (Zie bijlage 6). Zij ontvingen deze informatie over de verschillen zodat zij zich beperkt konden inlezen. De participanten hadden tijdens het interview de set interviewvragen tot hun beschikking zodat zij konden meelesen met de vragen en zicht hadden op het verloop van het interview. De set interviewvragen ontvingen de participanten ter plekke. Zij waren niet voorafgaand aan het interview bekend met de vragen. Tijdens afname van interviews werd elk topic kort toegelicht aan de participant zodat duidelijk werd waar de vragen op gericht waren. Na deze korte uitleg, werden de interviewvragen bij het specifieke topic gesteld.

5.5 Koppeling theorie naar praktijk

In het juridisch kader is de Wbp uiteengezet. Daarna is hetzelfde gedaan met AVG en tot slot zijn de verschillen tussen de Wbp en AVG weergegeven. Om verbinding tussen de conclusies uit de theorie en de resultaten van het praktijkonderzoek te creëren, zijn verschillende 'tools' gebruikt. Deze tools worden hieronder toegelicht:

Tabellen

Vanuit de theorie is een drietal tabellen geformuleerd over de rollen in het gegevensverwerkingsproces. Deze zijn opgenomen in deelvraag 1 tot en met 3. Voordat gestart werd met de afname van het interview, werd een tabel ingevuld voor de rollen in het gegevensverwerkingsproces van het onderwerp van de participant. Dit heeft geresulteerd in vier tabellen welke zijn opgenomen in bijlage 2.1 tot en met 2.4. Door middel van het invullen van deze tabellen, kan een koppeling gemaakt worden met de theorie: de tabellen vanuit de theorie zijn ingevuld voor **ANONIEM** P&O zodat er zicht is op wie welke rol uitoefent binnen het gegevensverwerkingsproces.

Formulering interviewvragen

De hoofdstukken uit het juridisch kader zijn gebruikt als topics voor de interviewvragen. Aan de hand van de hoofdstukken zijn vragen geformuleerd, zie bijlage 7 voor de volledige set interviewvragen.

Concreet: de hoofdstukken uit deelvraag 1, zijn de topics voor deelvraag 4, zie bijlage 8.1. De koppeling vanuit de theorie naar de directie P&O van de organisatie komt voort uit dat de Wbp zoals deze beschreven staat in het juridisch kader (deelvraag 1), de grondslag is voor de huidige werkwijze van de directie P&O van de organisatie (deelvraag 4). De kennis vanuit de Wbp is ingezet om gerichte vragen te formuleren over de toepassing van de Wbp bij **ANONIEM** P&O. Hierdoor kon deelvraag 4 worden beantwoord.

De hoofdstukken uit deelvraag 3 zijn de topics voor deelvraag 5, zoals opgenomen in bijlage 8.2. In het juridisch kader (deelvraag 3) zijn de verschillen tussen de Wbp en de AVG uiteengezet. Rondom deze verschillen (vanuit de theorie) zijn vragen geformuleerd. Op deze manier is ieder verschil stuk voor stuk voorgelegd aan de participanten en kon deelvraag 5 worden beantwoord.

Intern beleid ter ondersteuning interviewresultaten

Tijdens afname van de interviews kwam naar voren dat door de participanten veelvuldig gebruik wordt gemaakt van intern beleid. Dit is beleid wat naast de Wbp een intern kader vormt voor gegevensverwerking binnen de directie P&O van de organisatie. Zodoende is besloten dat het beleid wordt gebruikt ter ondersteuning van de resultaten uit de interviews. Een overzicht met de titels van het beleid dat is gebruikt ter ondersteuning, is opgenomen in bijlage 9.

HOOFDSTUK 6: RESULTATEN - HUIDIGE WERKWIJZE

De Wbp is opgebouwd uit verschillende hoofdstukken. In het juridisch kader zijn deze hoofdstukken uiteengezet.²⁷⁵ De directie P&O van de organisatie heeft zich aan de Wbp te houden bij de verwerking van persoonsgegevens omdat dit de geldende wet is. Over de hoofdstukken van de Wbp zijn vragen geformuleerd. Deze vragen zijn gesteld aan de participanten. Het doel van deze aanpak was de huidige werkwijze van de directie P&O van de organisatie met betrekking tot het verwerken van persoonsgegevens, in naleving van de Wbp na afname van interviews, te kunnen weergeven. *Deelvraag 4: Wat is de huidige werkwijze van de directie P&O van de organisatie met betrekking tot het verwerken van persoonsgegevens in naleving van de Wbp na afname van interviews?*

6.1 Toepassing Wbp²⁷⁶

In hoofdstuk 2: Het juridisch kader – Wet bescherming persoonsgegevens staat beschreven dat niet elk gegeven over iemand automatisch een persoonsgegeven is. Er is sprake van een persoonsgegeven wanneer het gegeven voor een dergelijk op de persoon gericht doel kan worden gebruikt.²⁷⁷ Bij alle vier de onderwerpen van gegevensverwerking bij de directie P&O van de organisatie, zijn de gegevens waarmee wordt gewerkt persoonsgegevens. De Wbp is daarom van toepassing. Een overzicht van deze gegevens is opgenomen bijlage 10. Er bestaat een subcategorie persoonsgegevens welke wordt geclassificeerd als bijzondere persoonsgegevens. In beginsel rust op de verwerking hiervan een verbod. Verwerking van bijzondere persoonsgegevens is slechts onder bepaalde voorwaarden toegestaan, tenzij uitdrukkelijke toestemming is verleend door betrokkene (degene van wie de persoonsgegevens zijn). Bij de directie P&O van de organisatie wordt gewerkt met volgende bijzondere persoonsgegevens (zie bijlage 11):

- Medische gegevens;
- BSN-nummer;
- Strafrechtelijk verleden;
- Lidmaatschap vakbond.

Persoonsgegevens mogen niet zomaar worden verwerkt, hier is toestemming van de betrokkene voor nodig. De Wbp definieert dat betrokkene middels elke vrije, specifieke en op informatie berustende wilsuiting, toestemming kan verlenen. Bij de directie P&O van de organisatie geeft de betrokkene op diverse manieren toestemming voor de verwerking van zijn gegevens. Bij het onderwerp vervoer is dit heel expliciet: betrokkene zet in het *Anoniem*²⁷⁸ een elektronisch vinkje. Met dit vinkje stemt hij in met doorgifte van zijn gegevens naar *Anoniem*²⁷⁹ en impliciet met de controle die de vervoerscoördinator van de directie P&O uitvoert op zijn reisgedrag. Naast expliciet, verleent de betrokkene ook impliciet toestemming. Als hij zijn ID-bewijst afstaat om er een kopie van te laten maken bijvoorbeeld. *Anoniem*

Voor de verwerking van gegevens van kinderen jonger dan zestien jaar, is toestemming of machtiging van diegene die ouderlijke verantwoordelijkheid draagt over het kind vereist vanuit de Wbp. Bij de directie P&O van de organisatie wordt beperkt gewerkt met gegevens van kinderen jonger dan zestien jaar. Het kan voorkomen dat een vijftien of zestienjarige stage komt lopen bij de directie P&O van de organisatie. Bij het onderwerp vervoer en WNT wordt er niet mee gewerkt. Bij *anoniem*) komt het voor dat medewerkers kinderen hebben en de directie P&O van de organisatie de kosten voor scholing op zich neemt. Als ouder moet je aantonen dat je kinderen hebt en over welke kind(eren) het gaat wil je aanspraak kunnen maken op de regeling. Hetzelfde geldt voor aanspraak maken op ouderschapsverlof, de leeftijd van het kind is doorslaggevend voor toekenning.

Wil er volgens de Wbp sprake zijn van verwerking van persoonsgegevens dan moeten 'handelingen' met de persoonsgegevens worden verricht. De Wbp geeft de definitie van handelingen²⁸⁰, de opsomming is niet-limitatief. Bij de directie P&O van de organisatie valt op dat de meeste van de handelingen die Wbp noemt, worden verricht. Echter worden er door de directie P&O van de organisatie geen gegevens gewist of vernietigd, dit is uitbesteed aan *Anoniem*. Zie voor een overzicht van de handelingen die worden verricht bijlage 12.

6.2 Naleving algemene beginselen gegevensverwerking (materiële werkingssfeer)²⁸¹

²⁷⁵ Hoofdstuk 2: Het juridisch kader – Wet bescherming persoonsgegevens.

²⁷⁶ Bijlage 4.1 – 4.4, deel 1, vraag 1a – 3b.

²⁷⁷ *Kamerstukken II 1997-1998, 25 892, 3, p. 47 (MvT).*

²⁷⁸

²⁷⁹

²⁸⁰ Art. 1 sub b Wbp: Elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorgifte, in verband brengen, afschermen, uitwissen, vernietigen van gegevens.

²⁸¹ Bijlage 4.1 – 4.4, deel 1, vraag 4 – 9c.

Gegevensverwerking moet behoorlijk en zorgvuldig worden uitgevoerd. In de Wbp zijn hiervoor zes algemene beginselen opgenomen. De directie P&O van de organisatie heeft voor elk van de zes beginselen naleving ingeregeld. Het overzicht hiervan is opgenomen in bijlage 13.

6.3 Territoriale werking²⁸²

De persoonsgegevens van betrokkenen worden doorgaans opgeslagen in Nederland. Reisdata van de *Anoniem*, curricula vitae en vacatures worden elders in Europa opgeslagen, de locatie van servers was niet altijd bekend bij de participanten.

6.4 Transparantie: meldings- en informatieverplichtingen²⁸³

6.4.1 Meldingsverplichting

Voorafgaand aan de daadwerkelijke verwerking van gegevens, moet melding worden gedaan door de verantwoordelijke aan de Functionaris voor gegevensbescherming (FG) of Autoriteit Persoonsgegevens (AP). (Als een organisatie geen FG heeft). Dit moet om onnodige verwerking van gegevens te voorkomen en risico's te beperken. Melding wordt door de directie P&O van de organisatie gedaan bij nieuwe verwerkingen.²⁸⁴ De basis voor de gegevensverwerking wordt voorgelegd aan de FG samen met het Interne Controle plan (IC-plan) en eventueel een Privacy Impact Assessment (PIA). Het komt voor dat een component in het proces van gegevensverwerking wijzigt. De verwerking is gemeld en gestart, maar gedurende het proces wordt opgemerkt dat aanpassing nodig is. In een dergelijke situatie wordt opnieuw melding gedaan de FG.²⁸⁵ Als de verwerking van gegevens onder het Vrijstellingsbesluit van de Wbp valt, vervalt de meldingsverplichting. Bij de directie P&O van de organisatie is sprake van vrijstelling van melding bij het verwerken van sollicitatiegegevens²⁸⁶ en de personeels- en salarisadministratie.²⁸⁷ *Anoniem*

6.4.2 Informatieverplichting

De betrokkene heeft het recht om te weten wie (welke organisatie/functionaris) zijn gegevens verwerkt en waarom (het doel). Het kenbaar maken van de identiteit van de verantwoordelijke en het doeleinde van de verwerking wordt door de directie P&O van de organisatie gedaan op verschillende manieren. Betrokkene wordt bijvoorbeeld verwezen naar het *Anoniem* waarop het IC-plan staat voor het onderwerp vervoer. Ook voor de andere onderwerpen is de betrokkene aangewezen op het *Anoniem*, informatie wordt digitaal aangeboden. Als het gaat om de personeels- en salarisadministratie, is algemeen bekend dat

Anoniem persoonsgegevens verwerkt. Ook bij verwerking van gegevens in uitvoering van de *ANONIEM* spreekt men van algemene bekendheid.

6.5 Rechten van betrokkene: inzage, verzet, rectificatie²⁸⁸

Voor alle drie de rechten zijn bij de directie P&O van de organisatie systemen ingericht.

Inzage: De betrokkene kan via het *Anoniem* zijn eigen personeelsdossier inzien. Dit gaat via *Anoniem*, een digitale tool. De betrokkenen die gebruik maken van een *Anoniem* hebben inloggegevens ontvangen voor de site van *Anoniem*, de verstrekker van de kaart. Zij kunnen op die manier hun eigen reisbewegingen inzien. *Anoniem*

Verzet: Bij *anoniem* en de personeel- en salarisadministratie kan de betrokkene verwerking van gegevens niet weigeren. Hij kan zich niet verzetten omdat hij anders geen salaris uitbetaald krijgt. Ook bij het onderwerp *ANONIEM* is verzet geen optie. *Anoniem* De betrokkene kan zich verzetten tegen gegevensverwerking als het doel van de verwerking verkrijging van een *Anoniem* is. Via het *Anoniem* kan de betrokkene bezwaar maken tegen verwerking van zijn gegevens. Als de betrokkene de *Anoniem* al in zijn bezit had op het moment van verzet, wordt door de directie P&O van de organisatie aan *Anoniem* gevraagd om zijn gegevens te wissen. Betrokkene kan dus een tijd gebruik maken van de *Anoniem*, maar zich later bedenken. Weigert de betrokkene op voorhand gegevensverwerking ten behoeve van de *Anoniem* (dus nog voordat hij er gebruik van heeft gemaakt) dan kan hij zelf een OV kaart aanschaffen den via OV-chipkaart.nl een lijst aanleveren

²⁸² Bijlage 4.1 – 4.4, deel 1, vraag 10.

²⁸³ Bijlage 4.1 – 4.4, deel 1, vraag 11a – 12b.

²⁸⁴ Verwerkingen welke nog niet eerder zijn verricht, waarvan de risico's van de verwerking nog niet geïnventariseerd zijn.

²⁸⁵

²⁸⁶ [redacted] verwerking te kunnen uitvoeren, moesten extra kolumnen in het systeem worden gebouwd.'

²⁸⁷

²⁸⁷ Art. 7 lid 1 jo. Art. 8 lid 1 Vrijstellingsbesluit Wbp.

²⁸⁸ Bijlage 4.1 – 4.4, deel 1, vraag 13a – 13c.

van zijn gemaakte reizen om voor een vergoeding in aanmerking te komen. De Groepsondernemingsraad (GOR) van de organisatie heeft deze alternatieve manier van gegevensaanlevering bedongen. Om verzet kan doorgaans digitaal worden verzocht. Als het een verwerking betreffende het P-dossier betreft dan kan een formulier worden ingevuld via het *Anoniem*. Wil het verzet slagen dan moet betrokkene gegronde redenen hebben en het gegeven waar het om gaat moet niet nadrukkelijk nodig zijn voor de verwerking.

Rectificatie: Met correctie of aanvulling van gegevens wordt verschillend omgegaan. De betrokkene kan door middel van zelf-service in het *Anoniem* eigenhandig correcties uitvoeren of contact opnemen met *Anoniem*. Op welke manier rectificatie kan worden uitgevoerd, hangt ervan af waar de fout zit of waar gegevens ontbreken. Een voorbeeld van correctie welke de betrokkene zelf kan uitvoeren, is naamvoering bij huwelijk/scheiding. Lukt het de betrokkene niet om via het *Anoniem* zelf rectificatie uit te voeren en helpt rechtstreeks contact met *Anoniem* de betrokkene ook niet verder? De betrokkene kan dan een e-mail²⁸⁹ sturen naar een contactpersoon.²⁹⁰

Anoniem

6.6 Meldplicht datalekken²⁹¹

De meldplicht datalekken is vanaf januari 2016 opgenomen in de Wbp. Een datalek wordt in de Wbp omschreven als "inbreuk op de beveiliging van persoonsgegevens: de persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking." Elk lek moet door de verantwoordelijke gemeld worden aan de FG of de AP (als een organisatie geen FG heeft). Een lek komt bij de directie P&O van de organisatie zeer weinig voor. De bepaling of sprake is van een datalek wordt per onderwerp van gegevensverwerking anders aangepakt, maar in principe wordt de interne procedure van de organisatie gevolgd. De beveiliging wordt opgeroepen middels een speciaal telefoonnummer. Als er sprake is van een incident kan de beveiliging een specialist inschakelen van de *Anoniem* en er wordt eventueel aangifte gedaan. De *Anoniem* en integriteitscoördinator worden ook altijd ingeschakeld.

Nazorg bij een datalek is bij de directie P&O van de organisatie primair de verantwoordelijkheid van de leidinggevende. Deze heeft zorgplicht tegenover de betrokkene. Een voorbeeld van toepassing van de zorgplicht is het verzenden van een e-mail naar de betrokkenen over het datalek, samen met instructies en/of tips om erger te voorkomen. Nazorg bij een datalek kan ook bestaan uit het aanpassen van processen zodat dat kans op een lek geminimaliseerd wordt.

6.7 Doorgifte persoonsgegevens derde landen²⁹²

Persoonsgegevens worden door de directie P&O van de organisatie zeer beperkt doorgegeven aan landen buiten de EU, de zogenaamde derde landen. *Anoniem* heeft met partijen onder zich privacyverklaringen gesloten zodat vaststaat dat doorgifte niet is toegestaan. Doorgifte naar een derde land komt enkel voor in de situatie wanneer betrokkene uitgezonden is middels *anoniem* en mogelijk buiten de EU werkzaamheden verricht, bijvoorbeeld op een *anoniem*

6.8 Verplichtingen verantwoordelijke en bewerker²⁹³

De verantwoordelijke is verplicht zorg te dragen voor behoorlijke en zorgvuldige verwerking, doeleinden, grondslagen voor verwerking, doelbinding, bewaren, data minimalisatie en kent geheimhoudingsplicht. Bij de directie P&O van de organisatie zijn de verplichtingen als volgt ingericht. De verplichtingen linken aan de algemene beginselen van gegevensverwerking: Geheimhoudingsplicht: *anoniem*. Data minimalisatie: alleen persoonsgegevens die nodig zijn voor het doel van de verwerking worden verwerkt. Grondslag verwerking: de grondslagen van de verwerkingen zijn terug te vinden in de wet en in diverse interne stukken van de directie P&O van de organisatie. Hoe doelbinding en bewaring van gegevens is ingericht, is opgenomen in het overzicht *Inregeling naleving algemene beginselen gegevensverwerking* (bijlage 13). De bewerker verricht zijn werkzaamheden via een bewerkersovereenkomst. Voor een bewerkersovereenkomst is een model.²⁹⁴ Ook is apart een dienstverleningsovereenkomst afgesloten. *Anoniem* is een bewerker van persoonsgegevens voor de directie P&O van de organisatie en wordt periodiek gecontroleerd door de *Anoniem* en de *Anoniem*. Tijdens die controles wordt nagegaan of de gegevensverwerkingen die worden uitgevoerd gerechtvaardigd zijn, onrechtmatige verwerking

²⁸⁹ Via de Awb is een e-mail namelijk aangemerkt als een besluit.

²⁹⁰ Zijn geboortedatum kan betrokkene zelf niet corrigeren, dit is situatie waarin een e-mail sturen de beste optie is.

²⁹¹ Bijlage 4.1 – 4.4, deel 1, vraag 14a - 14c.

²⁹² Bijlage 4.1 – 4.4, deel 1, vraag 15.

²⁹³ Bijlage 4.1 – 4.4, deel 1, vraag 16a, 16b.

²⁹⁴ [REDACTED]

moet worden uitgesloten. De kwaliteit en bescherming van gegevens is ook onderdeel van de controle. Mocht een controle een negatief resultaat tot gevolg hebben dan volgt het label 'onvolkomenheid.' *Anoniem* wordt ingelicht deze kan een waarschuwing of een berisping opleggen. Bij telefonisch contact met *Anoniem* wordt gevraagd een aantal beveiligingsvragen te beantwoorden zodat duidelijk is wie de beller is. Ook verificatie via het *Anoniem*²⁹⁵ wordt gebruikt.

6.9 Functionaris voor gegevensbescherming²⁹⁶

In de Wbp is de aanstelling van een FG opgenomen als een kan-bepaling. *Anoniem*²⁹⁷ De FG wordt benaderd als er sprake is van een nieuwe gegevensverwerking. Bij vervoer is bijvoorbeeld sprake geweest van het inschakelen van de FG omdat verschillend gedacht werd over of de privacy van de betrokkene in geding was bij gegevensverwerking ten behoeve van de *Anoniem*

6.10 Koppeling theorie naar praktijk: invulling tabellen rollen proces gegevensverwerking voor *ANONIEM* P&O

De rollen in het proces van gegevensverwerking zijn ingevuld voor de directie P&O van de organisatie. Uit de vier tabellen (zie bijlage 2.1 tot en met 2.4) zijn de volgende punten op te maken:

De verantwoordelijke is standaard de *Anoniem*. *Anoniem* De bevoegdheden van de *anoniem* zijn gemandateerd naar een intern beheerder. Een intern beheerder is bij de directie P&O van de organisatie vaak een functionaris belast met een specifieke portefeuille, bijvoorbeeld vervoer. De bewerkersrol wordt doorgaans ingevuld door *Anoniem*, maar er wordt ook samengewerkt met andere partijen, zoals *Anoniem*. De rol van de betrokkene wordt ingevuld door de medewerker binnen de organisatie. De rol van derde is niet bij alle vier de onderwerpen van gegevensverwerking ingevuld. Soms is sprake van dubbele rollen: een ontvanger kan ook bewerker zijn zoals bij *Anoniem*. Ook kan het zijn dat de beheerder en ontvanger dezelfde partij zijn.

***anoniem* 6.11 Conclusie**

Deelvraag 4: Wat is de huidige werkwijze van de directie P&O van de organisatie met betrekking tot het verwerken van persoonsgegevens in naleving van de Wbp na afname van interviews?

De gegevens waarmee wordt gewerkt, zijn **persoonsgegevens**. **Toestemming** voor gegevensverwerking geeft de betrokkene veelal via een eenzijdige rechtshandeling en impliciet. Soms wordt expliciet toestemming gegeven, dit kan bijvoorbeeld elektronisch. Voor de verwerking van gegevens van kinderen jonger dan zestien jaar gelden andere toestemmingsvoorwaarden. De directie P&O van de organisatie werkt op beperkte schaal met gegevens van deze doelgroep. Er worden **handelingen** met de gegevens verricht en daarmee wordt voldaan aan de voorwaarde van de Wbp om te kunnen spreken van verwerking van persoonsgegevens. Naast de Wbp is de verwerking gestoeld op **intern beleid** zoals controleprotocollen, handboeken, normenkaders en baselines voor de *Anoniem*. Voor elk van de zes materiële beginselen van gegevensverwerking **naleving ingeregeld**. Persoonsgegevens worden doorgaans **opgeslagen** in Nederland of elders binnen de EU. Wat betreft de **meldingsverplichting** geldt deze niet voor de personeel- en salarisadministratie, deze verwerkingen vallen onder het Vrijstellingsbesluit Wbp. Verwerkingen in het kader van de *ANONIEM* zijn ook uitgezonderd van melding. De **informatieverplichting** is zo ingericht dat betrokkene doorwezen wordt naar digitale informatie óf de informatie is algemeen bekend. Voor het drietal **rechten van betrokkene** zijn systemen ingericht. Betrokkene kan zelf digitaal zijn gegevens inzien, zich verzetten (onder voorwaarden) en gegevens beperkt (laten) rectificeren. Het hangt ervan af waar de fout zit of waar gegevens ontbreken. **Datalekken** komen zeer weinig voor. Het bepalen of er sprake is van een lek wordt per onderwerp van gegevensverwerking anders aangepakt. Wel is er een algemene procedure en zijn er verschillende

²⁹⁵ Persoonlijk identificatienummer.

²⁹⁶ Bijlage 4.1 – 4.4, deel 1, vraag 17.

²⁹⁷ [REDACTED]

vormen van nazorg. Van **doorgifte** van persoonsgegevens naar derde landen wordt enkel gebruik gemaakt door *anoniem*. De verplichtingen van de **verantwoordelijke en bewerker** zijn ingebed in de algemene beginselen van gegevensverwerking, *anoniem* en een model bewerkersovereenkomst. De organisatie heeft een **Functionaris voor gegevensbescherming** aangesteld. De door de Wbp gedefinieerde **rollen in het proces van gegevensverwerking** zijn door de directie P&O van de organisatie ingevuld. De rol van de verantwoordelijke wordt standaard ingevuld door de *anoniem*, maar wordt in de praktijk gemandateerd. *Anoniem* kan worden gezien als standaard bewerker. Daarnaast is niet ongewoon dat de invulling van bepaalde rollen dubbelingen bevat.

anoniem

HOOFDSTUK 7: RESULTATEN - BEELD VAN TOEKOMSTIGE WERKWIJZE

De AVG is opgebouwd uit verschillende hoofdstukken. In het juridisch kader zijn deze hoofdstukken uiteengezet.²⁹⁸ De Wbp wordt vervangen door de AVG. Voor de directie P&O van de organisatie houdt dit in dat het bestaande kader rondom gegevensverwerking moet worden aangepast aan de AVG. In het juridisch kader zijn de verschillen tussen de Wbp en AVG benoemd.²⁹⁹ De verschillen tussen de Wbp en de AVG zijn stuk voor stuk voorgelegd en toegelicht aan de participanten. Er is gevraagd naar de impact en de verwachtingen, knelpunten in omgang met de verschillen bij het verwerken van persoonsgegevens met betrekking tot de huidige werkwijze van de directie P&O van de organisatie. De verschillen zijn stuk voor stuk besproken en iedere participant heeft aangegeven hoe hij denkt over de toepassing van de verschillen op het onderwerp van gegevensverwerking waar hij mee werkt. Het doel van deze aanpak was een beeld van de (toekomstige) werkwijze van de directie P&O van de organisatie met betrekking tot het verwerken van persoonsgegevens, in naleving van de AVG, na afname van interviews te kunnen weergeven. *Deelvraag 5: Wat is het beeld van de (toekomstige) werkwijze van de directie P&O van de organisatie B met betrekking tot het verwerken van persoonsgegevens in naleving van de AVG na afname van interviews?*

7.1 Toestemming betrokkene³⁰⁰

De AVG verbindt voorwaarden aan de toestemming die betrokkene verleent voor de verwerking van zijn gegevens. De toestemming moet worden gegeven door middel van een duidelijke, actieve

²⁹⁸ Hoofdstuk 3: Het juridisch kader – Algemene Verordening Gegevensbescherming.

²⁹⁹ Hoofdstuk 4: Het juridisch kader – Verschillen tussen de Wbp en AVG.

³⁰⁰ Bijlage 4.1 – 4.4, deel 2, vraag 1a – 1c.

handeling. Dit kan schriftelijk, mondeling (via opname) of elektronisch. Uit de handeling moet blijken dat de betrokkene vrijelijk, specifiek, ondubbelzinnig en geïnformeerd instemt met de verwerking. De toestemming van betrokkene moet kunnen worden aangetoond.

Deze verandering is niet van toepassing op verwerking van persoonsgegevens ten behoeve van de *Anoniem*. Bij vervoer geeft de betrokkene toestemming via het *Anoniem*, dit is een duidelijke actieve (elektronische) handeling. Met de toekomstige normalisatie van arbeidsvoorwaarden zal ook de directie P&O van de organisatie te maken krijgen met een arbeidscontract. De toestemming van betrokkene komt dan tot stand via een tweezijdige rechtshandeling. In het huidige aanstellingsformulier zou bij het kopje 'ondertekening' kunnen worden opgenomen dat door middel van het ondertekenen van dit document de betrokkene toestemming geeft voor verwerking van zijn gegevens voor dit specifieke doel. (Het doel is ook opgenomen in het formulier). De toestemming van betrokkene is dan ook terug te vinden in zijn P-dossier. Hierdoor kan worden aangetoond dat betrokkene toestemming heeft verleend.

7.2 Controle van toestemming ouder bij verwerking gegevens kind & verbod³⁰¹

De AVG verplicht controle bij verwerking van persoonsgegevens van kinderen onder de zestien jaar.

Als gegevens worden verwerkt van een betrokkene die nog geen zestien jaar is, is toestemming of machtiging van degene die ouderlijke verantwoordelijkheid heeft vereist. Dit was ook al zo ten tijde van de Wbp. De verwerkingsverantwoordelijke is via de AVG verplicht om redelijke inspanning te leveren³⁰² om te kunnen controleren of toestemming daadwerkelijk is verleend.

Uit de huidige werkwijze van de directie P&O van de organisatie, is gebleken dat er beperkt met gegevens van kinderen onder de zestien jaar wordt gewerkt: bij ouderschapsverlof, scholing voor kinderen van uitgezonden ambtenaren en als er sprake is van een jonge stagiair. Wil de betrokkene geslaagd aanspraak kunnen maken op ouderschapsverlof of op een regeling voor zijn kind vanuit *anoniem*³⁰³ dan levert hij zelf specifieke persoonsgegevens van zijn kind(eren) aan. Doordat de betrokkene zelf de gegevens over zijn kind opgeeft, vinden de participanten dat controle en de bijbehorende redelijke inspanningsverplichting niet aan de orde is. Op de formulieren voor ouderschapsverlof wordt aangegeven om welk kind het gaat en hoe oud het kind is. Dit wordt gedaan omdat aanspraak op ouderschapsverlof mogelijk is totdat het kind acht jaar oud is. De formulieren worden ingevuld, maar niet apart geregistreerd. Bij *anoniem* wordt de geboortedatum van het kind gebruikt om ervan af te leiden of het kind leerplichtig is. Zo ja, dan kan het zijn dat de kosten voor scholing door de organisatie worden voldaan. Een stagiair jonger dan zestien jaar komt bijna nooit voor, maar in dat geval wordt toestemming gevraagd van de ouder. "Handtekening van de ouder is dus verplicht, zonder dat is het niet rechtsgeldig."³⁰⁴

Of de toestemming ook werkelijk is verleend door de ouder, kan worden gecontroleerd door middel van een kopie van het paspoort van de ouder. Vervolgens wordt de toestemming geregistreerd.

7.3 Meer verplichtingen verwerkingsverantwoordelijke en verwerker³⁰⁵

De naamgeving van de rollen verantwoordelijke en bewerker als bedoeld in de Wbp wordt door de AVG gewijzigd in verwerkingsverantwoordelijke en verwerker. Qua inhoud krijgen zij er een aantal taken en verantwoordelijkheden bij. Sommige verantwoordelijkheden worden gedeeld.

De verwerker en de verwerkingsverantwoordelijke moeten elk een eigen register bijhouden van alle verwerkingen. De verwerkingsverantwoordelijke tot welke hij opdracht geeft en de verwerker welke hij uitvoert.

7.3.1 Eigen register

Met betrekking tot *Anoniem* houdt iedere functionaris een lijstje bij welke opdrachten hij aan *Anoniem* heeft verstrekt. Dit wordt gedaan om te kunnen controleren wanneer bepaalde mutaties zijn verricht. De vraag rijst of het lijstje door kan gaan voor een register zoals de AVG deze heeft bedoeld. De personeels- en salarisadministratie werkt met logbestanden. Elke mutatie is via een logbestand te zien. De logbestanden zijn toegankelijk voor een geselecteerde groep functionarissen en worden ervaren als zijnde een register. Een register opzetten in uitvoering van de AVG zou dubbel werk zijn. Daarnaast is het haast onmogelijk salarismutaties bij te houden in een register omdat het om een zeer groot aantal mutaties gaat. Bij vervoer wordt geen register bijgehouden. *Anoniem*

³⁰¹ Bijlage 4.1 – 4.4, deel 2, vraag 2a – 2d.

³⁰² De AVG definieert het begrip niet, het zal in de praktijk ingevuld moeten worden.

³⁰³ [REDACTED]

³⁰⁴ Bijlage 4.2, deel 2, uitspraak van Hoofd P&O ondersteuning bij vraag 2b.

³⁰⁵ Bijlage 4.1 – 4.4, deel 2, vraag 3a – 3d.

7.3.2 Samen zorg voor beveiliging

Over gezamenlijk zorg dragen voor de beveiliging wordt verschillend gedacht door de participanten. Vanuit de personeels- en salarisadministratie kan namelijk geen toegang worden verschaft aan de verwerker. Het gaat immers om verschillende partijen en er wordt met verschillende systemen gewerkt. Afstemmen wordt eerder gezien als een optie in plaats van samen zorg dragen.

Alle participanten geven aan dat beveiliging al op verschillende manieren geïntegreerd is in de huidige werkwijze. *Anoniem*. Het *ANONIEM* schrijft voor dat op basis van een expliciete risicoafweging de betrouwbaarheidseisen voor informatiesystemen worden vastgesteld en dat de maatregelen die daarbij passen worden getroffen. Dit kan via het toepassen van het *Anoniem*. In een informatiebeveiligingsplan worden de analyse en de maatregelen vastgelegd.

Met een bewerker (*anoniem*) kunnen aanvullende afspraken worden gemaakt over beveiliging. Privacyverklaringen tussen partijen komen ook voor. Qua beveiliging moet rekening worden gehouden met richtsnoeren voor beveiliging van persoonsgegevens van de AP.³⁰⁶ De AP herzielt haar huidige richtsnoeren vanwege de invoering van de AVG.

7.4 Uitbreiding rechten van betrokkene³⁰⁷

De rechten van betrokkene zoals opgenomen in de Wbp worden uitgebreid met het recht op vergetelheid en dataportabiliteit. Vergetelheid: de betrokkene kan zijn gegevens laten wissen als: gegevens niet langer nodig zijn voor het doel van verwerking, hij zijn toestemming voor verwerking intrekt (dat kan op ieder moment), hij bezwaar maakt, zijn gegevens onrechtmatig zijn verwerkt.

In 2009 is bewaring van persoonsgegevens gedigitaliseerd en grotendeels uitbesteed aan *Anoniem*, *Anoniem*, en *Anoniem*: een *anoniem*.

Als informatie van vòòr de digitalisering nodig is, "of het nou over P-gegevens gaat, contracten of wat dan ook, alle dossiers zijn gecentraliseerd voor *anoniem* bij *Anoniem*."³⁰⁸ Tot een aantal jaar na het vijftienvestigste levensjaar van betrokkene, worden zijn aanstellingsbescheiden bewaard. Het doeleinde van de verwerking mag dan verlopen zijn, maar het is van belang dat de bescheiden kunnen worden gebruikt ter beantwoording van een vraag van bijvoorbeeld een nabestaande van de betrokkene.

Vergetelheid kan bij de directie P&O van de organisatie in bepaalde gevallen worden geëffectueerd, maar aan gebruik van het recht is een grens verbonden. Gegevens waaraan wettelijke bepaling gekoppeld is, denk aan uitvoering van de *ANONIEM* of het feit dat de fiscus registratie van een paspoortkopie van betrokkene verplicht, mogen niet worden 'vergeten.' Betrokkene kan bezwaar maken tegen de levering van zijn persoonsgegevens aan *Anoniem*. In dat geval wordt de levering gestopt, maar de reisdata (vanwege het kosten aspect) blijft daar nog beschikbaar.

De betrokkene heeft het recht gebruik te maken van dataportabiliteit: om zijn gegevens mee te nemen en door te geven. Dit kan als de verwerking berust op toestemming en de verwerking via automatische procedures wordt verricht. Bij de directie P&O van de organisatie is dit het geval. Via het *Anoniem* kan betrokkene bij zijn P-dossier. Op deze manier kan hij zijn eigen gegevens kopiëren of bijvoorbeeld naar zichzelf e-mailen. Gegevens zijn op deze manier mobiel.

7.5 Verandering uitgangspunt meldplicht datalekken³⁰⁹

De meldplicht zoals deze opgenomen was in de Wbp, wordt door de AVG gecontinueerd, maar kent andere uitgangspunten. Een datalek moet altijd gemeld worden aan de AP. Aan betrokkene hoeft het lek alleen gemeld te worden als sprake is van een hoog risico. De verwerkingsverantwoordelijke bepaalt dit. Ook moet een overzicht van datalekken worden bijgehouden.

De definitie van 'hoog risico' wordt door participanten als vaag ervaren. Het altijd moeten melden van een datalek wordt een goede ontwikkeling genoemd. In de huidige werkwijze wordt al geen onderscheid gemaakt in het aantal betrokkenen dat getroffen wordt door een datalek, melding wordt onverkort gedaan. (In principe intern omdat de organisatie een FG heeft). De *ANONIEM* en

³⁰⁶ [REDACTED]

³⁰⁷ Bijlage 4.1 – 4.4, deel 2, vraag 4, 5.

³⁰⁸ Bijlage 4.2, deel 2, uitspraak van Hoofd P&O ondersteuning bij vraag 9a.

³⁰⁹ Bijlage 4.1 – 4.4, deel 2, vraag 6a – 6c.

integriteitscoördinator en FG worden genoemd als personen om de uitgangspunten van de meldplicht te bewaken.

Een overzicht bijhouden van datalekken wordt niet gezien als een verplichting met veel invloed op het werkproces. Volgens de participanten komt een datalek zeer weinig voor. De organisatie is volledig in haar documentatie/accountability, door naast een overzicht van datalekken ook eventuele misstanden³¹⁰ binnen de organisatie te documenteren.

7.6 Vaststellen bewaartermijn persoonsgegevens³¹¹

De AVG verplicht dat een termijn moet zijn verbonden aan het bewaren van gegevens. Als dit niet mogelijk is, moeten er criteria worden opgesteld. Deze moeten zo zijn opgesteld, dat aan de hand daarvan alsnog een termijn kan worden gekoppeld aan bewaren van persoonsgegevens. Op archiveren bij de overheid is de Archiefwet van toepassing. Ten opzichte van de Wbp is de Archiefwet een *lex specialis* en hoger in rang. Dit wil zeggen dat de Archiefwet voorrang heeft op de Wbp. Het feit dat de Wbp geen termijn koppelt aan de bewaring van persoonsgegevens is dus ondergeschikt. De Archiefwet heeft betrekking op archiefbescheiden gedurende hun hele levensloop. De archiefbescheiden moeten ordentelijk moeten bewaard en daarvoor in aanmerking komende bescheiden moeten worden vernietigd.³¹²

Over het vaststellen en formuleren van criteria voor een bewaartermijn van persoonsgegevens wordt verschillend gedacht. Allereerst wordt een taak gezien voor *Anoniem* en *Anoniem* omdat dit opslaglocaties van persoonsgegevens zijn en zij fungeren als opslag van persoonsgegevens. Ook zijn er afspraken met *Anoniem* en *Anoniem* over termijnen die worden gehanteerd. *Anoniem*³¹³, fiscale wetgeving en diverse controleprotocollen zijn termijnen grotendeels afgebakend.

7.7 Toename instrumenten doorgifte gegevens naar derde landen³¹⁴

De AVG maakt doorgifte van persoonsgegevens naar derde landen mogelijk via een drietal opties (adequaateitsbesluiten, passende waarborgen, bindende bedrijfsvoorschriften). Vanuit de Wbp werd echter alleen een passend beschermingsniveau van het derde land vereist voor doorgifte. Alleen voor *anoniem* zou de toename aan instrumenten voor doorgifte naar derde landen relevant kunnen zijn. Bij de andere drie onderwerpen van gegevensverwerking worden geen persoonsgegevens doorgegeven aan derde landen.

7.8 Privacy by design & privacy by default³¹⁵

Organisatorische en technische maatregelen voor gegevensverwerking, noemt de AVG privacy by design (organisatorische maatregelen) en privacy by default (technische maatregelen). Vanaf het verzamelen tot aan de vernietiging van gegevens is de verwerkingsverantwoordelijke verplicht om maatregelen te nemen. Hij moet daarmee rekening houden met de aard, omvang, context, doel verwerking, risico's voor betrokkene van de gegevensverwerking. De AVG verplicht het voeren van actief beleid, zodat naleving kan worden aangetoond. Dit wordt accountability genoemd.

De participanten geven aan dat met alle bovenstaande componenten rekening wordt gehouden binnen het huidige gegevensverwerkingsproces. Hun verwachtingen over verandering die de AVG met zich meebrengt op dit onderdeel zijn niet hooggespannen. De tendens onder de participanten is dat aanpassing van maatregelen om aan te AVG te voldoen niet zo nodig is. Er wordt verwacht dat omgang met privacy by design de directie P&O van de organisatie niet raakt en dat het meer bij verwerker *Anoniem* een rol zal spelen.

Een sprekend voorbeeld van hoe de directie P&O van de organisatie met gegevensverwerking omgaat, is duidelijk geworden bij verwerking van persoonsgegevens om een *Anoniem* te kunnen verstrekken. *Anoniem* Omgang privacy by default

Technische maatregelen worden op verschillende manieren toegepast: via autorisatie kan een beperkt aantal functionarissen bij specifieke gegevens. De gegevens zelf zijn opgeslagen op een beveiligde opslaglocatie zoals de *Anoniem* of *Anoniem*. Voor toegang tot de opslaglocaties wordt met wachtwoorden gewerkt, als documenten worden verzonden wordt dit versleuteld gedaan.

³¹⁰ Bijvoorbeeld integriteitsschending.

³¹¹ Bijlage 4.1 – 4.4, deel 2, vraag 7a, 7b.

³¹²

³¹³

³¹⁴ Bijlage 4.1 – 4.4, deel 2, vraag 8.

³¹⁵ Bijlage 4.1 – 4.4, deel 2, vraag 9a, 9b.

7.9 Verplichting werken (D)PIA)³¹⁶

De AVG verplicht organisaties om met een (D)PIA (Data) Privacy Impact Assessment) te werken. Dit instrument wordt gebruikt om de risico's van gegevensverwerking in kaart te brengen.

De AVG geeft via een niet-limitatieve opsomming aan dat een DPIA vereist is in de volgende gevallen: 1. persoonlijke aspecten van natuurlijke personen worden systematisch en uitgebreid beoordeeld. De gegevens zijn gebaseerd op automatisch verwerking.³¹⁷ 2. Bijzondere persoonsgegevens worden op grote schaal verwerkt.³¹⁸ 3. Er wordt stelselmatig en op grote schaal gemonitord in openbaar toegankelijke ruimte.³¹⁹ Als gekeken wordt naar de situaties waarin een PIA vereist is volgens de AVG en deze wordt toegepast op de directie P&O van de organisatie dan verwerkt de directie P&O van de organisatie persoonsgegevens middels nummer één. De AP stelt in samenspraak met andere Europese privacytoezichthouders (De evenbeelden van de Nederlandse AP) een aanvullende lijst op van alle soorten verwerkingen waarbij de uitvoering van een PIA verplicht is.³²⁰

Anoniem. Binnen de directie P&O van de organisatie wordt de PIA ook gebruikt, maar niet bij alle vier de onderwerpen van gegevensverwerking. In uitvoering van de **anoniem** wordt er bijvoorbeeld niet mee gewerkt. De manier waarop met PIA's wordt gewerkt, is geen aanpak waar iedere participant over te spreken is. Dit komt omdat degene die de verantwoordelijkheid draagt over de verwerking, de PIA kan invullen. Objectiviteit van beoordeling van de risico's is daardoor discutabel.

7.10 Meldplicht wordt documentatieplicht³²¹

In naleving van de AVG hoeven verwerkingen van persoonsgegevens niet meer gemeld te worden bij de AP. In plaats daarvan zijn verwerkingsverantwoordelijke en verwerker verplicht een overzicht bij te houden van alle verwerkingen.

Uiteraard geldt de documentatieplicht niet voor verwerkingen die onder het Vrijstellingsbesluit Wbp vielen, deze verwerkingen hoefden al niet gemeld te worden. De meningen van de participanten over de documentatieplicht zijn verdeeld. Enerzijds wordt snelheidstoename in het proces genoemd als mogelijk positief gevolg van het komen te vervallen van de meldingsverplichting. Anderzijds wordt getwijfeld of de belangen van de betrokkene daardoor in het gedrang komen. Of er niet te snel aan de verwerking voorbij wordt gegaan omdat melden niet meer hoeft. Daarnaast wordt aangegeven dat de documentatieplicht voor de organisatie niet nieuw is. De werkwijze is al zo ingericht om waar nodig te documenteren.

7.11 Verplichting functionaris gegevensbescherming³²²

In de Wbp was het benoemen van een FG opgenomen als een kan-bepaling, het was niet verplicht. De AVG verplicht een FG bij overheidsorganisaties. Uit de interviews over de huidige werkwijze van de directie P&O van de organisatie, is gebleken dat de organisatie een FG heeft en deze is aangesteld om de organisatie en **anoniem** te bedienen. Dat het aanstellen van een FG niet langer een kan-bepaling is, vinden de participanten een goede ontwikkeling. Een FG wordt een must genoemd door de vervoerscoördinatoren. Van een organisatie zoals **ANONIEM** verwachten zij dat professioneel met gegevensverwerking omgegaan wordt en een FG kan daarom niet ontbreken. Belangenafweging bij het beoordelen van de risico's wordt erg belangrijk gevonden. De FG moet rekening houden met het belang van de medewerker, maar ook met de organisatie en de belangen van beide kanten afwegen.

anoniem 7.12 Conclusie

Deelvraag 5: Wat is het beeld van de (toekomstige) werkwijze van de directie P&O van de organisatie met betrekking tot het verwerken van persoonsgegevens in naleving van de AVG na afname van interviews?

De participanten zijn bevraagd over elf verschillen tussen de Wbp en de AVG.³²³

³¹⁶ Bijlage 4.1 – 4.4, deel 2, vraag 10a, 10b.

³¹⁷ Art. 35 lid 3 sub a AVG.

³¹⁸ Art. 35 lid 3 sub b AVG.

³¹⁹ Art. 35 lid 3 sub c AVG.

³²⁰ Art. 35 lid 4 AVG.

³²¹ Bijlage 4.1 – 4.4, deel 2, vraag 11a, 11b.

³²² Bijlage 4.1 – 4.4, deel 2, vraag 12.

³²³ Om een beeld te kunnen schetsen van (toekomstige) werkwijze is kennis van de huidige werkwijze vereist. (Deze is weergegeven via deelvraag 4).

Grosso modo is de verwachting van de participanten over impact van de elf verschillen op de werkwijze in te delen in drie categorieën: 1. Verschil heeft geen invloed op werkwijze; 2. Verschil heeft beperkt invloed; 3. Verschil heeft invloed.

De participanten zijn positief ingesteld over de hoeveelheid aanpassingen die de huidige werkwijze nodig heeft om 'AVG-proof' te worden. Als naar het beeld over de elf verschillen in zijn totaliteit gekeken wordt, vinden participanten dat de meeste verschillen vallen in categorie één of twee. Zie voor categorisatie van de verschillen tabel 5, welke hieronder is opgenomen.

Tabel 5: Elf verschillen tussen de Wbp en AVG ingedeeld in categorieën van mate van invloed op werkwijze

<i>Categorieën invloed van verschil op werkwijze ANONIEM-P&O</i>		
Categorie 1: Geen invloed	Categorie 2: Beperkt invloed	Categorie 3: Invloed
Vershil nummer 7.9	Vershil nummer 7.2	Vershil nummer 7.1
Vershil nummer 7.11	Vershil nummer 7.4	Vershil nummer 7.3
	Vershil nummer 7.5	
	Vershil nummer 7.6	
	Vershil nummer 7.7	
	Vershil nummer 7.8	
	Vershil nummer 7.10	

Voor toepassing van elk verschil wordt een aanbeveling gedaan. Deze zijn opgenomen in 8.2.2 *Concrete aanbevelingen bij de verschillen*.

HOOFDSTUK 8: CONCLUSIE EN AANBEVELINGEN

In dit hoofdstuk wordt de conclusie van dit onderzoek weergegeven door middel van beantwoording van de centrale vraag. Algemene en concrete aanbevelingen worden beschreven en ook wordt verantwoording afgelegd.

8.1 Conclusie

Ter beantwoording van de centrale vraag zijn vijf deelvragen gesteld. Drie hiervan maken deel uit van het theoretisch-juridische onderzoeksgedeelte. De andere twee vormen samen het praktijkgericht onderzoeksgedeelte.

Als centrale vraag is gesteld:

Welk advies kan aan de directie P&O van de organisatie worden gegeven over het aanpassen van haar werkwijze met betrekking tot het verwerken van persoonsgegevens om te voldoen aan de eisen van de AVG aan de hand van afgenomen interviews, analyse van wet- en regelgeving en literatuuronderzoek?

Voorop staat dat de organisatie als *anoniem* een voorbeeldfunctie heeft met betrekking tot verwerking van persoonsgegevens en privacy. Dit omdat de organisatie samen met *Anoniem anoniem*

De huidige werkwijze van de directie P&O van de organisatie met betrekking tot verwerking van persoonsgegevens voldoet aan de eisen van de Wbp, de huidige wetgeving. Dit is vastgesteld op basis van de informatie die naar voren is gekomen uit de interviews met de functionarissen binnen de directie P&O van de organisatie die zich bezig houden met gegevensverwerking.

De AVG verschilt op een aantal punten met de Wbp. Het gaat dan om -kort gezegd- de volgende verschillen:

- Toestemming betrokkene aantonen
- Controle van toestemming ouder bij verwerking gegevens kind
- Meer verplichtingen verwerkingsverantwoordelijke en verwerker
- Uitbreiding rechten van betrokkene
- Verandering uitgangspunt meldplicht datalekken
- Vaststellen bewaartermijn persoonsgegevens
- Toename instrumenten doorgifte gegevens naar derde landen
- Privacy by design & privacy by default
- Verplichting werken (D)PIA
- Meldplicht wordt documentatieplicht
- Verplichting functionaris gegevensbescherming

De participanten zijn bevraagd over deze verschillen tussen de Wbp en de AVG.

Uit de interviews komt naar voren dat de werkprocessen bij de directie P&O van de organisatie op een aantal onderdelen moeten worden aangepast. Voor wat betreft twee verschillen geldt dit niet. Het gaat dan om de verplichting om te werken met een (D)PIA. Dit gebeurt al bij de directie P&O van de organisatie. En verder om de verplichting een functionaris gegevensbescherming te benoemen. De organisatie heeft al een functionaris gegevensbescherming. De directie P&O van de organisatie zou om te voldoen aan de overige verschillen moeten nagaan hoe bestaande inrichting van processen kan worden aangepast en deze aanpassingen vervolgens moeten vastleggen en uitvoeren. Vanuit de AVG wordt zwaar aangestuurd op accountability, de manier van werken en afwegingen voor bepaalde keuzes moeten inzichtelijk zijn en vaststaan. De directie P&O van de organisatie moet om te voldoen aan de AVG aandacht besteden aan de verschillen 7.1 tot en met 7.8 en 7.10. Voor elk van de verschillen is een aanbeveling opgenomen hoe hier mee om te gaan (ook voor de twee punten waar *ANONIEM* P&O al aan voldoet)

8.2 Aanbevelingen

De aanbevelingen volgen uit het beeld van de toekomstige werkwijze (hoofdstuk 7) en gaan een stap verder dan de beantwoording van de centrale vraag. De aanbevelingen zijn onderverdeeld in algemeen en concrete aanbevelingen.

8.2.1 Algemene aanbevelingen

- Vervang de huidige interne Wbp-handenboeken in handboeken over de AVG en zorg daarin voor verwijzingen naar artikelen uit de AVG;
- Let in het bijzonder op het voeren van actief beleid: accountability. Zorg dat documentatie in orde is en dat afwegingen omtrent gegevensverwerking kunnen worden aangetoond. Pas daarvoor ook procesbeschrijvingen aan;
- Geef voorlichting over de AVG aan functionarissen die met persoonsgegevens werken.³²⁴

³²⁴ Deze algemene aanbeveling is niet af te leiden uit de resultaten, maar komt voort uit een gesprek met praktijkbegeleiders.

- Ga na in gevallen waarbij met een bewerkersovereenkomst wordt gewerkt, deze voldoet aan de eisen van de AVG.³²⁵

8.2.2 Concrete aanbevelingen bij de verschillen

Voor de aanbevelingen wordt de nummering van de verschillen gebruikt zoals in hoofdstuk 6. Aanbeveling 1 is een aanbeveling bij verschil 1 en zo verder.

1. Toestemming betrokkene Neem een clause op in documenten/formulieren waarin de betrokkene toestemming geeft voor gegevensverwerking (aanstellingsformulier). Doe dit zodat helder is waarvoor de betrokkene precies zijn toestemming geeft.

2. Controle van toestemming ouder bij verwerking gegevens kind Zorg ervoor dat wanneer er gewerkt wordt met gegevens van kinderen onder de zestien jaar, duidelijk is hoe controle van toestemming van de ouder tot stand komt en hoe zich dit verhoudt tot het leveren van 'redelijke inspanning' om deze na te gaan. Volgens participanten is controle dikwijls niet nodig omdat de betrokkene zelf de gegevens van zijn kind aanlevert. Zorg dat dit duidelijk is zodat geen twijfel bestaat over invulling van naleving van de verplichting.

3. Meer verplichtingen verwerkingsverantwoordelijke en verwerker Geef bij de AP aan dat bij de personeels- en salarisadministratie met logbestanden gewerkt wordt om mutaties bij te houden. Informeer naar een mogelijke vrijstelling voor het bijhouden van een register zodat geen dubbel werk wordt gedaan. De functionarissen binnen de directie P&O van de organisatie die zelf een lijstje bijhouden met welke opdrachten zij aan *Anoniem* hebben verstrekt, kunnen hun lijstje vergelijken met de eisen die de AVG stelt aan een register en het lijstje daarop aanpassen. (Zie 3.9 *Verplichtingen verwerkingsverantwoordelijke* en 3.10 *Verplichtingen verwerker*). Een register bijhouden in uitvoering van *anoniem*. Dit moet worden uitgezocht. Let op wanneer de AP nieuwe richtsnoeren uitvaardigt voor de beveiliging van persoonsgegevens en organiseer als deze eenmaal gepubliceerd zijn een check ten opzichte van de huidige beveiliging. Pas eventuele aanpassingen toe op eigen beveiliging. Verken in hoeverre het mogelijk is dat de verwerkingsverantwoordelijk en verwerker samen zorg dragen voor de beveiliging en stem waar mogelijk (verder) af.

4. Uitbreiding rechten van betrokkene Licht betrokkene in over zijn nieuwe rechten: vergetelheid en dataportabiliteit. Kaart aan in welke gevallen vergetelheid gerechtvaardigd is en wat de betrokkene moet doen om dit recht te kunnen genieten. Geef aan dat het recht op dataportabiliteit geen verandering met zich meebrengt en dat persoonsgegevens reeds mobiel zijn via het *Anoniem*.

5. Verandering uitgangspunt meldplicht datalekken Zorg dat afspraken worden gemaakt met de verwerkingsverantwoordelijke over wat een 'hoog risico' is voor de persoonsgegevens van betrokkene. Besteed aandacht aan de definitie van een datalek en formuleer hoe deze er voor de directie P&O van de organisatie uit kan zien zodat de kans op twijfel of wel of geen sprake is van datalek zo klein mogelijk is.

6. Vaststellen bewaartermijn persoonsgegevens Verken ondanks dat door de participanten verwacht wordt dat bewaartermijnen nagenoeg afgebakend zijn, of de bewaring van alle persoonsgegevens welke verwerkt zijn, gekoppeld is aan een termijn. Maak afspraken met *Anoniem*, *Anoniem* en *Anoniem* over het opstellen van criteria voor een termijn, mocht aan bepaalde persoonsgegevens geen termijn gekoppeld zijn.

7. Toename instrumenten doorgifte gegevens naar derde landen Verken of *anoniem*, in gevallen waar zij gegevens doorgeeft aan derde landen, baat heeft bij de nieuwe instrumenten voor de doorgifte die de AVG met zich meebrengt.

8. Privacy by design & privacy by default Loop na of het reëel is dat participanten aangeven dat privacy by design en default *Anoniem* raakt en de directie P&O van de organisatie voorbijgaat. Onderzoek of de aard, omvang, context, doel verwerking, en de risico's voor betrokkene van de gegevensverwerking net zo afgebakend is als dat wordt gedacht. Zorg dat geen twijfel kan bestaan over de invulling van de invulling van bovenstaande punten.

9. Verplichting werken (D)PIA Ga na, ondanks dat al sinds 2013 met PIA's wordt gewerkt of de directie P&O van de organisatie in alle gevallen dat de AVG een PIA vereist deze ook wordt toegepast. Houd de lijst die de AP zal uitvaardigen in de gaten. Stuur waar mogelijk op een objectieve invulling van de PIA zodat deze niet gekleurd kan worden ingevuld door verantwoordelijke van de verwerking.

10. Meldplicht wordt documentatieplicht Houd rekening met de mening van participanten over het vervallen van de meldplicht. Enerzijds wordt snelheidstoename in het proces genoemd als mogelijk positief gevolg van het komen te vervallen van de meldingsverplichting. Anderzijds wordt getwijfeld of de belangen van de betrokkene daardoor niet in het gedrang komen. Of er niet te snel aan voorbij wordt gegaan omdat melden niet meer hoeft.

³²⁵ Uit de resultaten is af te leiden dat met bewerkersovereenkomsten wordt gewerkt.

11. Verplichting functionaris gegevensbescherming Als samenwerking met de FG aan de orde is, let dan op de belangenafweging. De FG moet rekening houden met het belang van de medewerker, maar ook met de organisatie en de belangen van beide kanten even zwaar afwegen.

8.3 Verantwoording

8.3.1 Bruikbaarheid

De bruikbaarheid van het onderzoek zit in het toepassen van de verschillen tussen de Wbp en AVG uit het juridisch kader op de huidige werkwijze (praktijk) van de directie P&O van de organisatie met betrekking tot het verwerken van persoonsgegevens. Door middel van interviews met de functionarissen die in eigen persoon met de persoonsgegevens werken, is de theorie aan de praktijk gekoppeld. Uit de interviews zijn aandachtspunten naar voren gekomen. Punten die de directie P&O van de organisatie kunnen leiden naar concrete aanpassingen om te voldoen aan de eisen van de AVG.

8.3.2 Doelstelling behaald

Het doel van dit onderzoek was het schrijven van een advies voor de directie P&O van de organisatie over hoe te werken met de AVG. Het advies moet beschrijven wat de directie P&O van de organisatie moet aanpassen aan haar werkwijze in omgang met persoonsgegevens, om zo aan de eisen van de AVG te kunnen voldoen. Als wordt voldaan aan de AVG, wordt de directie P&O van de organisatie niet beboet.

De doelstelling van het onderzoek is globaal behaald en geeft richting (zie aanbevelingen) aan hoe de verschillen tussen de Wbp en de AVG kunnen worden toegepast in de praktijk bij de directie P&O van de organisatie.

LITERATUURLIJST

Literatuur

- B. Baarda e.a., *basisboek interviewen*, Groningen: Noordhoff Uitgevers, 2012
- J. Berkvens & C. Jakimowicz, *Tekstuitgave privacyverordening met geïntegreerde overwegingen, Wbp- en Richtlijn 95/46/EG-teksten en verwijstabellen*, Den Haag: Boom juridisch, 2016

- Factsheet: *Rechtstreekse werking van bepalingen uit Europese richtlijnen: Regels en risico's, Europa decentraal, 2009*
- S. Fennell e.a, *Privacy wetgeving*, Oisterwijk: Wolf Legal Publishers, 2016
- The future group, *Freedom, Security, Privacy – European home affairs in an open world: Report of the Informal High Level Advisory Group on the Future of European Home Affairs Policy*, juni 2008
- T.F.M. Hooghiemstra & S. Nouwt, *Tekst en toelichting Wet bescherming persoonsgegevens*, Den Haag: Sdu uitgevers, 2007
- J.P. de Jong, 'De Algemene verordening gegevensbescherming', *RegelMaat* 2015-1, p. 6-18
- H.R. Kranenburg & L.F.M. Verhey, *Wet bescherming persoonsgegevens in Europees perspectief*, Deventer: Wolters Kluwer, 2011
- J. Kriens, 'Algemene Verordening Gegevensbescherming', VNG-ledenbrief, 12-07-2016
- N. Robinson e.a, *Review of the European Data Protection Directive*, Cambridge: Rand Europe, 2009
- H.H. de Vries & D.J. Rutgers, *Wet bescherming persoonsgegevens toepassing in arbeidsverhoudingen*, Deventer: Wolters Kluwer, 2012

Parlementaire geschiedenis

- *Boetebeleidsregels Autoriteit Persoonsgegevens 2016*, Stcrt. 2016, 2043, p. 11.
- COM (2003) 265 def. 15 mei 2003
- Data Protection Directive 95/46/EC
- Europese Unie, PB L 119 van 4.5.2016, p. 2.
- Europese Unie, verordening 2016/679, Betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming), 27-04-2016, PB EU L119 van 4.5.2016
- *Kamerstukken II* 1997-1998, 25 892, 3 (MvT)
- *Kamerstukken I* 2011-2012, 22 112, FI, p.7
- Raad van de Europese Unie, Interinstitutioneel dossier: 2012/0011 (COD), 5419/1/16, REV 1, 08-04-2016
- Raad van de Europese Unie, Interinstitutioneel dossier: 2012/0011 (COD), 5853/12, 27-01-2012

Jurisprudentie

- HR 23 maart 2010, ECLI:NL:PHR:2010:BK6331
- Rb. 9 augustus 2005, LJN: AU0980

Overig – internetpublicaties

- *Europese privacywetgeving, 2016. Bekeken op 19-09-2016*, www.autoriteitpersoonsgegevens.nl (over privacy / wetten / lees meer over Europese privacywetgeving)
- *Functionaris voor gegevensbescherming, 2016. Bekeken op 10-10-2016*, www.europadecentraal.nl (onderwerp / informatiemaatschappij / Privacy: de Algemene

- *Meldplicht inbreuk persoonsgegevens*, 2016. Bekeken op 09-10-2016, www.europadecentraal.nl (onderwerp / informatiemaatschappij / Privacy: de Algemene Verordening Gegevensbescherming / Verplichtingen verantwoordelijke / Meldplicht inbreuk persoonsgegevens)
- *Privacy by design and by default*, 2016. Bekeken op 10-10-2016, www.europadecentraal.nl (onderwerp / informatiemaatschappij / Privacy: de Algemene Verordening Gegevensbescherming / Verplichtingen verantwoordelijke / Privacy by design and by default)
- *Privacy: de algemene verordening gegevensbescherming*, 2016. Bekeken op 10-10-2016, www.europadecentraal.nl (onderwerp / informatiemaatschappij / privacy: de algemene verordening gegevensbescherming)
- *Rechten van de betrokkene*, 2016. Bekeken op 09-10-2016, www.europadecentraal.nl (onderwerp / informatiemaatschappij / Privacy: de Algemene Verordening Gegevensbescherming / Rechten van de betrokkene)
- *Rechtmatigheid en transparantie*, 2016. Bekeken op 09-10-2016, www.europadecentraal.nl (onderwerp / informatiemaatschappij / Privacy: de Algemene Verordening Gegevensbescherming / Rechtmatigheid en transparantie)
- *Toezicht en sancties*, 2016. Bekeken op 19-09-2016, www.europadecentraal.nl (onderwerp / informatiemaatschappij / Privacy: de Algemene Verordening Gegevensbescherming / Toezicht en sancties)
- *Verplichtingen verantwoordelijke*, 2016. Bekeken op 09-10-2016, www.europadecentraal.nl (onderwerp / informatiemaatschappij / Privacy: de Algemene Verordening Gegevensbescherming / Verplichtingen verantwoordelijke)
- *Verwerken van persoonsgegevens*, 2016. Bekeken op 09-10-2016, www.europadecentraal.nl (onderwerp / informatiemaatschappij / Privacy: de Algemene Verordening Gegevensbescherming / Verwerken van persoonsgegevens)
- *Wat zijn persoonsgegevens?*, 2016. Bekeken op 18-09-2016, www.autoriteitpersoonsgegevens.nl (over privacy / persoonsgegevens / lees meer over Wat zijn persoonsgegevens?)
- *Wbp-naslag*, 2016. Bekeken op 18-09-2016, www.autoriteitpersoonsgegevens.nl (over privacy / wetten / lees meer over Wbp-naslag)

Met auteur:

- F. Salverda, '*Algemene Verordening Gegevensbescherming treedt in werking op 25 mei 2016*', 17-05-2016. Bekeken op 10-09-2016 www.europadecentraal.nl (nieuws / algemene verordening gegevensbescherming treedt in werking op 25 mei 2016)
- F. Salverda & R. Witteveen, '*Richtsnoeren meldplicht datalek gepubliceerd*', 05-10-2015. Bekeken op 09-10-2016, www.europadecentraal.nl (nieuws / Richtsnoeren meldplicht datalek gepubliceerd)
- R. Witteveen & P. Zondag, '*Gepubliceerde regels meldplicht datalekken belangrijk voor decentrale overheden*', 14-12-2015. Bekeken op 09-10-2016, www.europadecentraal.nl (nieuws / gepubliceerde regels meldplicht datalekken belangrijk voor decentrale overheden)