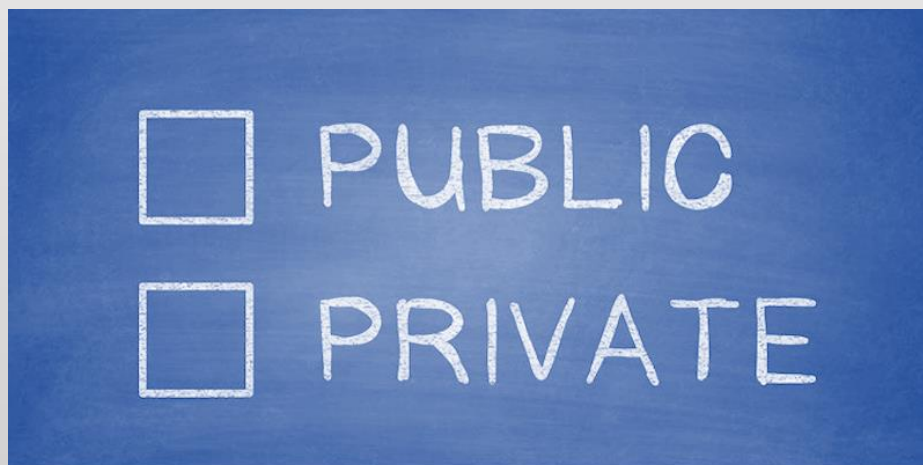


Gegevensverwerking volgens de privacywetgeving

Een onderzoek naar de verwerking
van persoonsgegevens van sw-
medewerkers binnen Baanbrekers



Leslie Pedro
Juridische Hogeschool Avans-Fontys te Tilburg
Baanbrekers

Waalwijk, 10 januari 2017

Gegevensverwerking volgens de privacywetgeving

Een onderzoek naar de verwerking van persoonsgegevens van
sw-medewerkers binnen Baanbrekers

Auteur: Leslie Pedro
Studentennummer: 2064231

Onderwijsinstelling: Juridische Hogeschool Avans-Fontys te Tilburg
1e docent: Mevr. mr. C.A.M. van der Voort
2e docent: Dhr. mr. B. Hooijdonk

Afstudeerorganisaties: Baanbrekers
Afstudeermentor: Mevr. L. Kruijthoff

Afstudeerperiode: September 2016 – Januari 2017

Waalwijk, 10 januari 2017

Voorwoord

Voor u ligt het onderzoeksrapport 'Verwerking van de persoonsgegevens volgens de privacywetgeving'. Het onderzoeksrapport is geschreven in het kader van mijn afstudeerscriptie. Dit onderzoek biedt aanbevelingen aan Baanbrekers, zodat de persoonsgegevens van de sw-medewerkers binnen Baanbrekers conform de wet worden verwerkt. In dit onderzoek zijn rechtsbronnen geanalyseerd en is in de praktijk onderzocht op welke wijze Baanbrekers de persoonsgegevens verwerkt. De uitkomsten van deze twee onderzoeken zijn vervolgens aan elkaar getoetst, op basis waarvan ik een conclusie heb getrokken en aanbevelingen heb geformuleerd.

Mijn dankwoord richt ik allereerst tot mijn stagedocente Caro van der Voort, voor haar ondersteuning, feedback en begeleiding bij de uitwerking van de scriptie. Daarnaast wil ik mijn stagementor Liesbeth Kruijthoff bedanken voor de begeleiding gedurende mijn stage. Zij heeft mij geholpen door het verschaffen van de nodige informatie, mij in contact te brengen met de juiste componenten en altijd beschikbaar te zijn om mijn vragen te beantwoorden. Tot slot bedank ik George Coret, Judith Daelmans, Angeline Grootswagers, Pieterneel Janssen, Conny Kleijssen, Jacqueline Loois, Dick Melissen en alle adviseurs van de afdeling Personeel en Organisatie voor het meewerken aan de interviews, het verschaffen van relevante informatie en de ondersteuning aan het uitwerken van het rapport.

Ik wens u veel leesplezier toe!

Leslie Pedro

Waalwijk, 10 januari 2017

Inhoudsopgave

Lijst van afkortingen

Lijst van begrippen

Samenvatting

Hoofdstuk 1: Inleiding.....	9
1.1 Probleembeschrijving.....	9
1.2 Doelstelling	10
1.3 Centrale vraag en deelvragen	10
1.4 Verantwoording van de onderzoeksstrategie	10
1.5 Verantwoording van de bronnen en methoden.....	11
Hoofdstuk 2 De achtergronden van de privacywetgeving	12
Hoofdstuk 3 De Wet bescherming persoonsgegevens	13
3.1 Wanneer is de Wbp van toepassing?.....	13
3.2 Welke eisen stelt de WBP aan het verwerken van persoonsgegevens?	15
3.3 De overige verplichtingen van de verantwoordelijke.....	19
3.4 De verwerking van bijzondere gegevens.....	20
3.5 Rechten van de betrokkene	21
3.6 Wat zijn de sancties bij het niet naleven van de Wbp?	22
Hoofdstuk 4 De Algemene Verordening Gegevensbescherming	24
4.1 Nieuwe begrippen	24
4.2 De werkingssfeer van de AVG	24
4.5 Privacymaatregelen	26
4.6 Rechten van betrokkenen	28
4.7 Sanctie: verhoogd boetemaximum.....	29
Hoofdstuk 5 Werkwijze van Baanbrekers getoetst aan de Wbp	30
Hoofdstuk 5 Werkwijze van Baanbrekers getoetst aan de Wbp	30
5.1 Welke persoonsgegevens worden verwerkt?	30
5.1.1 Bijzondere persoonsgegevens.....	31
5.2 Hoe werden en worden persoonsgegevens verzameld?	31
5.3 Op welke wijze worden de persoonsgegevens verwerkt?	32
5.4 De toepasselijkheid van de Wbp	34
5.5 Doeleinde en grondslag voor gegevensverwerking	34
5.6 Verdere verwerking van de persoonsgegevens.....	35
5.7 Beveiliging	35
5.8 Verplichtingen van de verantwoordelijke	37
5.9 De bewerkers en de bewerkersovereenkomst.....	39

5.10 Rechten van de betrokkene	40
5.11 Rechtmatigheidsbeginsel	40
5.12 Privacybeleid	40
Hoofdstuk 6 Werkwijze van Baanbrekers getoetst aan de AVG	41
6.1 De werkingssfeer van de AVG	41
6.2 Verplichtingen van de verantwoordelijke	41
6.3 Privacymaatregelen	42
6.4 Rechten van de betrokkene	43
Hoofdstuk 7 Conclusie en aanbevelingen.....	44
7.1 Conclusie en aanbevelingen over de eisen van verwerking van de Wbp.....	44
7.2 Conclusie en aanbevelingen over de overige verplichtingen van de verantwoordelijke uit de Wbp	46
7.3 Conclusie en aanbevelingen over het privacybeleid	47
7.4 Conclusies en aanbevelingen over de verplichtingen van de verantwoordelijke uit de AVG	47
7.5 Conclusies en aanbevelingen omtrent de privacymaatregelen uit de AVG.....	49
Bronnen- en literatuurlijst.....	50
Bijlagen	

Lijst van afkortingen

AMvB	Algemene Maatregel van Bestuur
AP	Autoriteit Persoonsgegevens
AVG	Algemene Verordening Gegevensbescherming
Awb	Algemeen wet bestuursrecht
BSN	Burgerservicenummer
College	College bescherming persoonsgegevens
Compas	Compassysteem
EVRM	Europees Verdrag tot bescherming van de Rechten van de Mens en de Fundamentele Vrijheden
FG	Functionaris van gegevensbescherming
GW	Grondwet
Meldplicht datalekken	Meldplicht datalekken en uitbreiding bestuurlijke Boetebevoegdheden Autoriteit Persoonsgegevens (Richtlijn 95/46/EG)
P&O	Personeel & Organisatie
Privacyrichtlijn	Richtlijn 95/46/EG van het Europees Parlement en de Raad van 4 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, PB L 281 van 23.11.1995.
Sw-klanten	Sociale werkvoorziening klanten
Sw-medewerkers	Sociale werkvoorziening medewerkers
UVRM	Universele Verklaring van de Rechten van de Mens
UWV	Uitvoeringsinstituut Werknemersverzekeringen
VN	Verenigde Naties
Wabb	Wet algemene bepalingen Burgerservicenummer
Wbp	Wet bescherming persoonsgegevens
Wet SAMEN	Wet Stimulering Evenredige Arbeidsdeelname Minderheden
Wpr	Wet persoonsregistratie
Wsw	Wet sociale werkvoorziening
WML	Dienst Werkbedrijf voor gesubsidieerde arbeid, activering en trajecten Midden-Langstraat

Lijst van begrippen

De definitie van enkele begrippen die regelmatig aan bod komen in het rapport worden hieronder op voorhand beschreven.

Arbeidsovereenkomst

De overeenkomst waarbij de ene partij, de werknemer, zich verbindt in dienst van de andere partij, de werkgever, om tegen loon gedurende zekere tijd arbeid te verrichten.¹

Autoriteit Persoonsgegevens

De toezichthouder op de naleving van de Wbp en andere wet- en regelgevingen omtrent de verwerking van persoonsgegevens.

Betrokkene

Degene op wie een persoonsgegeven betrekking heeft.²

Bewerker

De bewerker is diegene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreekse gezag te zijn onderworpen.³ De bewerker is een buiten de organisatie van de verantwoordelijke staande persoon of instelling en veelal zal het gaan om een persoon of instelling die niet in een hiërarchische relatie tot de verantwoordelijke staat.⁴

Bijzondere bestaanskosten

De kosten die niet behoren tot de algemeen noodzakelijke bestaanskosten, maar wel noodzakelijk zijn voor de belanghebbende. Deze kosten komen de draagkracht van de belanghebbende te boven.

Noodzakelijke bestaanskosten

De bestaanskosten die kunnen worden gerekend tot het op minimumniveau algemeen gangbare bestedingspatroon, zoals voeding, verwarming, gas, water, aanschaffing van kleren en vervanging en herstel van huisraad.⁵

Verantwoordelijke

De verantwoordelijke is de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.⁶ Verder draagt de verantwoordelijke zorg voor de naleving van de verplichtingen, waaraan voldaan moet worden voor een rechtmatige gegevensverwerking.⁷

¹ Artikel 7:610 lid 1 BW

² Artikel 1 lid 1 sub f Wbp

³ Artikel 1 sub e Wbp

⁴ 'Naslag artikel 14 Wbp', Autoriteit Persoonsgegevens, www.autoriteitpersoonsgegevens.nl (zoek op *artikel 14*).

⁵ 'Algemeen noodzakelijke kosten van het bestaan', Gemeente Krimpen aan den IJssel, www.krimpenaandenijssel.nl (zoek op *noodzakelijke bestaanskosten*).

⁶ Artikel 1 lid 1 sub d Wbp

⁷ Artikel 15 Wbp

Samenvatting

Baanbrekers is een uitvoeringsorganisatie die namens de gemeenten Heusden, Loon op Zand en Waalwijk de wettelijke verplichtingen uit de Participatiewet uitvoert. Eén van deze verplichtingen is werk creëren voor klanten uit de sociale werkvoorziening. Deze klanten zijn door middel van een indicatie, verkregen door het UWV, tewerkgesteld bij Baanbrekers. Voor de werkverhouding hebben de klanten een dienstverband gesloten met Baanbrekers, waarbij persoonsgegevens van de klanten zijn verwerkt. Een organisatie die persoonsgegevens verwerkt, dient dit conform de eisen van de privacywetgeving te doen. De privacywetgeving in Nederland met betrekking tot het verwerken van persoonsgegevens is momenteel neergelegd in de Wbp. In 2016 zijn wijzigingen doorgevoerd in deze wet. De wijzigingen zijn ten eerste de inwerkingtreding van de Wet Meldplicht datalekken en ten tweede de uitbreiding van de boetebevoegdheid van de toezichthoudende 'Autoriteit Persoonsgegevens'. Bovendien is de Wbp door de sterke toename van de digitalisering toe aan vernieuwing. Om deze reden wordt de Wbp in mei 2018 vervangen door de AVG. In de verordening zijn de bepalingen uit de Wbp overgenomen, gewijzigd of aangevuld en zijn nieuwe bepalingen toegevoegd. Al deze wijzigingen hebben gevolgen voor de wijze waarop binnen Baanbrekers persoonsgegevens worden verwerkt. In dit onderzoek is onderzocht in welke mate de werkwijze van Baanbrekers voldoet aan de Wbp inclusief de wijzigingen die zijn doorgevoerd in 2016 en de toekomstige wijzigingen in de AVG.

Om te beginnen is gekeken naar de achtergronden van de Wbp en de AVG, zodat duidelijk wordt waarom en sinds wanneer de bescherming van persoonsgegevens als belangrijk aspect wordt beschouwd van de privacy.

Ten tweede zijn de Wbp en de AVG inhoudelijk geanalyseerd. De eisen uit deze wetten zijn met nadere toelichting beschreven. Allereerst zijn de eisen uit de Wbp die relevant zijn voor Baanbrekers uitgewerkt. Daarna komen de eisen van de AVG aan bod. Voor de AVG zijn uitsluitend de bepalingen beschreven die ten opzichte van de Wbp zijn gewijzigd of toegevoegd.

Vervolgens is de wijze waarop Baanbrekers persoonsgegevens van sw-medewerkers verwerkt getoetst aan de eisen uit de privacywetgeving. Aan de hand van deze toetsing is beoordeeld aan welke eisen Baanbrekers wel en niet voldoet.

Concluderend voldoet Baanbrekers voor de Wbp niet aan de bewaartermijn, fysieke beveiliging, het sluiten van een bewerkersovereenkomst met de bewerkers waarmee de organisatie samenwerkt, de informatieplicht en het optimaal gebruiken van het privacybeleid. Voor de AVG kan geconcludeerd worden dat Baanbrekers niet voldoet aan de documentatieplicht, de aanvullende eisen van de informatieplicht en de bewerkersovereenkomst, het PIA, het privacybeleid en de rechten van de betrokkene.

De aanbevelingen zijn in het algemeen dat Baanbrekers ervoor kan kiezen om het huidige privacybeleid eerst te actualiseren of dit beleid meteen te vernieuwen voor de AVG. In beide gevallen is het van belang dat alle eisen die van toepassing zijn op Baanbrekers erin worden vastgesteld en dat binnen Baanbrekers wordt gewaarborgd dat het privacybeleid wordt nageleefd. Het toezicht hierop dient intern gehouden te worden door een mystery guest en de FG.

Hoofdstuk 1: Inleiding

In dit hoofdstuk wordt eerst de aanleiding en probleembeschrijving beschreven. Vervolgens komen de doelstelling, centrale vraag en deelvragen aan bod. Tot slot bevat dit hoofdstuk de verantwoording van de onderzoeksstrategie en de verantwoording van de methode van onderzoek.

1.1 Probleembeschrijving

Baanbrekers is een organisatie die namens de gemeenten Heusden, Loon op Zand en Waalwijk dienstverlening biedt aan werkgevers en aan mensen met een afstand tot de arbeidsmarkt.⁸ De organisatie is, als gevolg van de inwerkingtreding van de Participatiewet, ontstaan door de fusie van de Intergemeentelijke Sociale Dienst Midden-Langstraat en de Dienst Werkbedrijf voor gesubsidieerde arbeid, activering en trajecten Midden-Langstraat. De doelgroep van Baanbrekers bestaat uit mensen met een (combinatie van een) fysieke, verstandelijke of psychische beperking, maar ook uit vluchtelingen of mensen die (langdurig) aangewezen zijn op een bijstandsuitkering. Het doel van Baanbrekers is om deze mensen volwaardig te laten meedoen aan de maatschappij en aan werk.⁹ Baanbrekers is een uitvoeringsorganisatie van de hierboven genoemde gemeenten en zet zich daarom in voor inwoners die niet in hun eigen levensonderhoud kunnen voorzien of die te maken krijgen met hoge bijzondere bestaanskosten.¹⁰

Het personeel van Baanbrekers is verdeeld in twee categorieën. De eerste categorie bestaat uit reguliere medewerkers. Deze categorie telt circa 150 medewerkers. De tweede categorie wordt gevormd door sw-medewerkers. Deze categorie bestaat uit circa 650 medewerkers met beperkingen, die daardoor een afstand hebben tot de arbeidsmarkt. De medewerkers uit deze categorie zijn in dienstverband bij Baanbrekers, omdat zij een arbeidsovereenkomst in de zin van artikel 7:610 lid 1 BW hebben gesloten met Baanbrekers. Zij verdienen daardoor zelfstandig een eigen inkomen. Deze medewerkers kunnen ook individueel of in groepsverband gedetacheerd worden aan externe werkgevers. Niettemin blijft het dienstverband met Baanbrekers in stand. Naast de bovengenoemde categorieën zijn er ook ongeveer 1600 Participatiewet medewerkers, in het kader van een leer- en werktraject, werkzaam bij Baanbrekers. Deze medewerkers hebben een afstand tot de arbeidsmarkt, omdat zij (langdurig) aangewezen zijn op een bijstandsuitkering of omdat zij vluchtelingen zijn. De medewerkers uit deze groep hebben geen dienstverband met Baanbrekers, maar Baanbrekers bemiddelt deze medewerkers naar werk en biedt zo nodig de gelegenheid om arbeidsritme en werkervaring op te doen. Zij krijgen in ruil voor het werk dat zij verrichten een WWB-uitkering en eventueel een bijzondere bijstandsuitkering.¹¹

Het vervolg van dit rapport zal zich beperken tot de sw-medewerkers. Deze groep bestaat namelijk uit personeel dat werkzaam is bij Baanbrekers en personeel dat gedetacheerd is naar externe werkgevers, waardoor hun persoonsgegevens zowel intern als extern worden verwerkt en uitgewisseld.

Bij het sluiten van een arbeidsovereenkomst, beschikt de afdeling P&O van Baanbrekers over de persoonsgegevens van de circa 650 sw-medewerkers. Op het moment dat de reguliere medewerkers van Baanbrekers over deze persoonsgegevens beschikken, moeten zij conform de privacywetgeving met betrekking tot het verwerken van persoonsgegevens handelen. Binnen Baanbrekers is de afdeling P&O door de juriste op de hoogte gesteld van de wijzigingen die per 1 januari zijn ingevoerd in de Wbp. De wijzigingen die zijn ingevoerd in de Wbp zijn de meldplicht datalekken en de nieuwe boetebevoegdheden van de AP. De meldplicht houdt in dat organisaties een melding moeten doen bij de AP zodra zij een ernstig

⁸ 'Wie zijn wij', Baanbrekers, www.baanbrekers.org/ (zoek op *wie zijn wij?*).

⁹ 'Wie zijn wij', Baanbrekers, www.baanbrekers.org/ (zoek op *wie zijn wij?*).

¹⁰ 'Wat doen wij', Baanbrekers, www.baanbrekers.org/ (zoek op *wat doen wij?*).

¹¹ De genoemde uitkeringen zijn Wet werk en bijstandsuitkeringen.

datalek hebben.¹² Soms moeten zij een datalek ook melden aan de betrokkene.¹³ De boetebevoegdheid van de AP houdt in dat zij direct boetes op kan leggen als organisaties de Wbp overtreden.¹⁴ Tevens is de afdeling P&O op de hoogte gesteld van het feit dat de Wbp in 2018 vervangen zal worden door de AVG. De AVG is een Europese verordening, die veranderingen meebrengt in de geldende privacyregels. De regels in de geldende Wbp en toekomstige AVG zijn onder meer opgesteld om de optimale bescherming en beveiliging op de persoonsgegevens te kunnen bieden, door de gegevens zorgvuldig te verwerken.

De werkwijze van Baanbrekers bestaat uit het verwerken van persoonsgegevens voor het uitvoeren van hun diensten. Voor de gegevensverwerking is door de juriste van Baanbrekers in 2004 een privacybeleid opgesteld genaamd het 'Privacyreglement personeelsregistratie WML 2004'.¹⁵ Op de naleving van de regels die zijn opgenomen in het privacybeleid, wordt geen toezicht uitgeoefend. De Wbp, de wijzigingen die er zijn ingevoerd en de toekomstige AVG hebben gevolgen voor de werkwijze van Baanbrekers. Het is voor Baanbrekers dus van belang om te weten in hoeverre hun werkwijze voldoet aan de huidige en toekomstige privacywetgeving omtrent de bescherming van de persoonsgegevens, zodat zij rechtmatig handelen en geen boetes oplopen.

1.2 Doelstelling

Uiterlijk 10 januari 2017 wordt een onderzoeksrapport opgeleverd aan Baanbrekers waarin staat beschreven welke aanpassingen en verbeteringen op basis van de huidige Wbp en toekomstige AVG moeten worden doorgevoerd in de werkwijze, met betrekking tot de sw-medewerkers, die in dienst zijn bij Baanbrekers of via Baanbrekers werkzaam zijn bij externe werkgevers, zodat Baanbrekers de bescherming biedt conform de geldende en toekomstige regelgeving ten aanzien van het rechtmatig verwerken van persoonsgegevens.

1.3 Centrale vraag en deelvragen

In hoeverre dient Baanbrekers haar huidige werkwijze met betrekking tot het verwerken van persoonsgegevens van de sw-medewerkers, die in dienst zijn bij Baanbrekers of via Baanbrekers werkzaam zijn bij externe werkgevers, aan te passen en te verbeteren, zodat deze in overeenstemming is met de Wbp en AVG?

Met de volgende deelvragen zal een antwoord worden geformuleerd op de centrale vraag:

1. Welke eisen stelt de Wbp aan de verwerking van persoonsgegevens?
2. Welke wijzigingen zijn in de eisen van de AVG toegepast ten opzichte van de Wbp?
3. In hoeverre is de werkwijze en het privacybeleid van Baanbrekers omtrent de gegevensverwerking van sw-medewerkers in overeenstemming met de Wbp?
4. In hoeverre is de werkwijze en het privacybeleid van Baanbrekers omtrent de gegevensverwerking van sw-medewerkers in overeenstemming met de AVG?

1.4 Verantwoording van de onderzoeksstrategie

De onderzoeksstrategie die gebruikt is voor dit onderzoeksrapport is het onderzoek van het recht, literatuur en de praktijk. Voor de eerste en tweede deelvraag is onderzoek gedaan naar het recht en literatuur met betrekking tot de privacywetgeving. De eisen die zijn gesteld in de wet en de wijzigingen die zijn opgetreden en gaan optreden in de wet- en regelgeving zijn leidend geweest voor het vervolg van het rapport. De regelgeving is dus geanalyseerd en de literatuur waarbij nader toelichting werd gegeven op de wet is bestudeerd om de

¹² 'Meldplicht datalekken', Autoriteit Persoonsgegevens, www.autoriteitpersoonsgegevens.nl (zoek op *meldplicht datalekken*).

¹³ 'Meldplicht datalekken', Autoriteit Persoonsgegevens, www.autoriteitpersoonsgegevens.nl (zoek op *meldplicht datalekken*).

¹⁴ 'CBP krijgt boetebevoegdheid en wordt Autoriteit Persoonsgegevens', Autoriteit Persoonsgegevens, www.autoriteitpersoonsgegevens.nl (zoek op *boetebevoegdheid Autoriteit Persoonsgegevens*).

¹⁵ Bijlage 1 Privacyreglement personeelsregistratie

eerste en tweede deelvraag uit te werken. Voor de beantwoording van de derde en vierde deelvraag is het onderzoek naar de praktijk toegepast. Deze deelvragen gaan immers om de wijze waarop persoonsgegevens worden verwerkt binnen Baanbrekers.

1.5 Verantwoording van de bronnen en methoden

Na het bepalen van de onderzoeksstrategie is bepaald welke bronnen en methoden worden gebruikt voor de beantwoording van de centrale vraag. Voor dit onderzoeksrapport zijn de inhoudsanalyse, interview en observatiemethode toegepast. Hieronder wordt per deelvraag beschreven welke bronnen en methoden zijn toegepast.

*Deelvragen 1 en 2: Welke eisen stelt de Wbp aan de verwerking van persoonsgegevens en welke wijzigingen zijn in de AVG toegepast ten opzichte van de Wbp?*¹⁶

Om de eerste twee deelvragen te beantwoorden is gebruikt gemaakt van de inhoudsanalyse. De uitwerking van deze deelvragen is een beschrijving van de eisen die de wet stelt aan de verwerking van persoonsgegevens. Hiervoor is onderzoek gedaan naar wat in de wet is bepaald en is literatuur geanalyseerd voor nadere toelichting hierop. Boeken zoals “Sdu Commentaar Wet bescherming Persoonsgegevens” en “Wet bescherming persoonsgegevens in Europees perspectief” zijn geraadpleegd voor de deelvragen. Tevens zijn de memorie van toelichting en verschillende handleidingen en rapporten geraadpleegd om deze deelvragen te kunnen beantwoorden. Tot slot is jurisprudentie bestudeerd, om te zien hoe de privacywetgeving in de praktijk wordt toegepast.

*Deelvragen 3 en 4: In hoeverre is de werkwijze en het privacybeleid van Baanbrekers omtrent de gegevensverwerking van sw-medewerkers in overeenstemming met de Wbp en in hoeverre is de werkwijze en het privacybeleid van Baanbrekers omtrent de gegevensverwerking van sw-medewerkers in overeenstemming met de AVG?*¹⁷

Voor de uitwerking van deze twee deelvragen zijn meerdere interviews gehouden en is de observatiemethode toegepast. De interviews zijn gehouden met medewerkers van verschillende afdelingen, die voor de uitoefening van hun werkzaamheden persoonsgegevens verwerken. De privacywetgeving stelt veel eisen aan de gegevensverwerking. Om na te gaan hoe en of Baanbrekers deze toepast, was het effectief om daar naar te vragen aan degenen die er dagelijks mee bezig zijn. Daarnaast konden sommigen onderdelen van de werkwijze worden uitgewerkt aan de hand van observatie.

¹⁶ Deze deelvragen worden samen behandeld, omdat de gebruikte methode voor beiden hetzelfde is.

¹⁷ Deze deelvragen worden samen behandeld, omdat de gebruikte methode voor beiden hetzelfde is.

Hoofdstuk 2 De achtergronden van de privacywetgeving

In 1948 heeft de VN internationaal aandacht besteed aan de rechten van de mens door de UVRM aan te nemen. Het recht op bescherming van de persoonlijke levenssfeer komt tot uitdrukking in artikel 12 UVRM. Deze bepaling was echter niet juridisch bindend. Als gevolg hiervan werd het recht op bescherming van een persoonlijke levenssfeer door de VN verankerd in een Verdrag, namelijk in artikel 17 van het Internationaal Verdrag inzake burgerrechten en politieke rechten. Aan dit artikel kunnen wel juridische rechten ontleend worden, omdat het juridisch bindend is.

In 1950 is het EVRM tot stand gekomen. Dit verdrag heeft directe werking in Nederland, waardoor Nederlandse burgers zich op rechten voortvloeiende uit dit verdrag kunnen beroepen. De bescherming van het privacyrecht van de burger komt in dit verdrag uitdrukkelijk terug in artikel 8 EVRM. Lid 1 van dit artikel bepaalt dat eenieder recht heeft op respect van zijn persoonlijke levenssfeer. Dit recht strekt zich uit van het privéleven tot de correspondentie van de burger. Lid 2 bepaalt dat “geen enkele inmenging van openbaar gezag is toegestaan in de uitoefening van dit recht, voor zover dit niet in de wet is bepaald”. De basis voor de bescherming van persoonsgegevens wordt gevormd door de Europese Privacyrichtlijn 1995. De Privacyrichtlijn stelt met name beperkingen aan het verzamelen en het gebruiken van persoonsgegevens en verlangt van elke lidstaat dat een nationaal onafhankelijk orgaan wordt opgericht om toezicht te houden op de bescherming van de persoonsgegevens in die betreffende lidstaat. De toezichthouder in Nederland is de AP, die voorheen ‘College bescherming persoonsgegevens’ heette. De Wbp is de Nederlandse implementatie van de Privacyrichtlijn.

In het nationaal recht is de bescherming van privacy in 1983 verankerd in artikel 10 Gw. Dit artikel geeft iedereen het recht op eerbiediging van zijn persoonlijke levenssfeer. In 1989 werd uitvoering gegeven aan artikel 10 Gw door de totstandkoming van de Wpr. In november 1995 is door het Europees Parlement en de Raad van de Europese Unie een Privacyrichtlijn opgesteld. In 2001 is de Wpr vervangen door de Wbp, waarvan de Privacyrichtlijn voor een groot deel de basis was. De Wbp is daarnaast ook gebaseerd op artikel 8 EVRM en artikel 10 Gw.

Op 1 januari 2016 zijn enkele wijzigingen doorgevoerd in de Wbp. De wijzigingen bestaan uit de meldplicht datalekken en de bevoegdheid van de AP om sancties op te leggen aan een verantwoordelijke die onderworpen is aan een datalek. De sanctie bestaat uit het opleggen van een hoge bestuurlijke boete aan de betreffende verantwoordelijke. Bovendien zal de Wbp in mei 2018 vervangen worden door de AVG. In de AVG bestaan de wijzigingen, ten opzichte van de Wbp, uit aanpassingen van een aantal artikelen en artikelen die zijn toegevoegd.

Hoofdstuk 3 De Wet bescherming persoonsgegevens

De belangrijkste wet op het gebied van bescherming van privacy is de Wbp, ook wel 'privacywet' genoemd. Deze wet is op 1 september 2001 van kracht gegaan. In de Wbp worden kaders gegeven die verder worden uitgewerkt in bijzondere regelgevingen. Het doel van deze wet is het vormen van een grondslag voor de verwerking van persoonsgegevens, zodat deze gegevens op een behoorlijke en zorgvuldige wijze verwerkt worden. De Wbp beschermt enerzijds de burger tegen onrechtmatige gegevensverwerking en anderzijds geeft deze wet instanties de mogelijkheid om persoonsgegevens te verwerken, zodat de werkwijze effectief verloopt. Om die reden regelt de Wbp welke voorwaarden verbonden zijn aan het verwerken van persoonsgegevens en welke handelingen verricht mogen worden met de persoonsgegevens van een persoon. De AP houdt zich bezig met het toezicht op naleving van de Wbp en andere privacywetgevingen.

De deelvraag die wordt beantwoord in dit hoofdstuk is: “*Welke eisen stelt de Wbp aan de verwerking van persoonsgegevens?*” De uitkomst van deze deelvraag wordt, in relatie tot de centrale vraag, gebruikt als leidraad om verderop in het rapport te kunnen beoordelen of de werkwijze van Baanbrekers conform de Wbp is. In dit hoofdstuk wordt ten eerste beschreven wanneer de Wbp van toepassing is. Vervolgens wordt beschreven welke eisen aan de gegevensverwerking worden gesteld, wat de verplichtingen van de verantwoordelijke en de bewerker zijn, welke bijzondere persoonsgegevens verwerkt mogen worden, wat de rechten van de betrokkene zijn en welke sancties worden opgelegd bij het niet naleven van de Wbp. Tot slot wordt kort de bijzondere wetgeving weergegeven, waarop het doel en noodzaak van de gegevensverwerking van Baanbrekers is gegrond.

3.1 Wanneer is de Wbp van toepassing?

Artikel 2 lid 1 Wbp stelt dat “de Wbp van toepassing is op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede de niet geautomatiseerde persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen”. Verder is voor de toepasselijkheid van de Wbp van belang waar de activiteiten voor gegevensverwerking plaatsvinden. De Wbp is van toepassing op de verwerking van persoonsgegevens in het kader van activiteiten van een vestiging van een verantwoordelijke in Nederland.¹⁸ Om in de praktijk betekenis te kunnen geven aan de reikwijdte van deze artikelen, moeten verschillende begrippen nader gedefinieerd worden. Deze begrippen zijn onderstreept en worden hieronder nader toegelicht. Met de definities van deze begrippen wordt een toetsingskader opgesteld, waarmee kan worden bepaald of de Wbp van toepassing is. Daarna zullen de verwerkingen die genoemd zijn in artikel 2 lid 2 jo. lid 3 en artikel 3 Wbp, waarop de Wbp uitdrukkelijk niet van toepassing is verklaard, benoemd worden.

Geheel of gedeeltelijk geautomatiseerde gegevensverwerking

Van geautomatiseerde verwerking is sprake als gebruik wordt gemaakt van middelen en methoden van geautomatiseerde gegevensverwerking.¹⁹ Er is sprake van een gedeeltelijke geautomatiseerde verwerking als bij de verwerking ook gebruik wordt gemaakt van handmatige verwerking.

Niet geautomatiseerde verwerking in een bestand of bestemd voor een bestand

De Wbp is ook van toepassing op niet geautomatiseerde gegevensverwerking, bijvoorbeeld de verwerking in een gestructureerd dossier, mits deze gegevens in een bestand zijn opgenomen of bestemd zijn om daarin te worden opgenomen.

¹⁸ Artikel 4 lid 1 Wbp

¹⁹ P.J.J. van Buuren en L.F.M. Verhey, ‘*Wet bescherming persoonsgegevens in Europees perspectief*’, Deventer: Wolters Kluwer uitgevers 2011, pagina 59.

Bestand

Een bestand houdt volgens artikel 1 sub c Wbp in dat de gegevens onderlinge samenhang moeten vertonen en dat het systeem systematisch toegankelijk moet zijn.²⁰ De onderlinge samenhang kan blijken uit het gemeenschappelijk doel waarvoor de gegevens worden verwerkt of uit de omstandigheid dat de gegevens in de praktijk als een geheel worden beschouwd.²¹ De tweede voorwaarde heeft betrekking op de toegankelijkheid tot de structuur van verzameling. Het dient op een zodanige manier te zijn opgezet dat de gegevens gemakkelijk toegankelijk zijn.

Persoonsgegevens

De beschrijving van een persoonsgegeven is elk gegeven dat een natuurlijk persoon identificeert. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is.²² Naast de NAW-gegevens of het telefoonnummer van een persoon, komen ook diens medische gegevens of BSN in aanmerking voor het begrip 'persoonsgegeven'. De persoonsgegevens dienen van een natuurlijk persoon te zijn. Overleden personen vallen daar dus niet onder.²³

Verwerking van persoonsgegevens

De verwerking van persoonsgegevens bestaat uit een variatie van handelingen. Deze handelingen kunnen zelfstandig of tezamen worden verricht. Verwerken heeft betrekking op iedere handeling of geheel van handelingen die met de persoonsgegevens verricht kunnen worden, vanaf de verzameling tot aan het moment van vernietiging. De verwerking kan zowel op een geautomatiseerde wijze als op een handmatige wijze verricht worden. Artikel 1 sub b Wbp geeft een niet-limitatieve opsomming van handelingen die als een verwerking kunnen worden aangemerkt. Enkele handelingen die onder meer worden opgenoemd zijn: 'het verzamelen, vastleggen, bijwerken, wijzigen, opvragen, gebruiken, verstrekken, het afschermen, uitwissen of vernietigen van gegevens'.

Territoriale reikwijdte van de Wbp

Voor de toepasselijkheid van de Wbp is van belang waar de activiteiten voor gegevensverwerking plaatsvinden. Artikel 4 lid 1 Wbp bepaalt dat, in het kader van gegevensverwerking, de vestiging of meerdere vestigingen van de verantwoordelijke in Nederland gevestigd dienen te zijn. Artikel 4 lid 2 Wbp stelt dat de Wbp ook van toepassing is ingeval een gegevensverwerker niet in Nederland en ook niet in een andere lidstaat van de Europese Unie is gevestigd, maar wel gebruikmaakt van de middelen uit Nederland om persoonsgegevens te verwerken. Deze bepaling wordt verder niet uitgewerkt, omdat het niet van toepassing is op Baanbrekers.

Verwerkingen die zijn uitgesloten van de toepassing van de Wbp

Ondanks de toepassingsverklaring van de Wbp die hierboven is beschreven, is de Wbp op grond van artikel 2 lid 2 jo. lid 3 Wbp niet van toepassing verklaard op het verwerken van persoonsgegevens:²⁴

- indien dit uitsluitend voor persoonlijke of huishoudelijke doeleinden is;
- door of ten behoeve van de inlichtingen- en veiligheidsdiensten;
- ten behoeve van de uitvoering van de politietaak;
- door gemeenten in de gemeentelijke basisadministratie persoonsgegevens;

²⁰ Sauerwein & Linnemann 2001, pagina 15.

²¹ P.J.J. van Buuren en L.F.M. Verhey, 'Wet bescherming persoonsgegevens in Europees perspectief', Deventer: Wolters Kluwer uitgevers 2011, pagina 68.

²² 'Wat zijn persoonsgegevens', Autoriteit Persoonsgegevens, www.autoriteitpersoonsgegevens.nl (zoek op *Wet bescherming persoonsgegevens*).

²³ 'Wat zijn persoonsgegevens', Autoriteit Persoonsgegevens, www.autoriteitpersoonsgegevens.nl (zoek op *Wet bescherming persoonsgegevens*).

²⁴ E.Thole, F. van der Jagt en H. Roerdink, '50 vragen over privacy', Wolters Kluwer uitgevers 2010, pagina 22.

- ten behoeve van de uitvoering van de Wet justitiële en strafvorderlijke gegevens;
- ten behoeve van de uitvoering van de Kieswet;
- voor uitsluitend journalistieke, artistieke of literaire doeleinden.

3.2 Welke eisen stelt de WBP aan het verwerken van persoonsgegevens?

In de Wbp zijn voorwaarden opgesteld, die ook wel beginselen worden genoemd. De voorwaarden dienen in acht te worden genomen door een ieder die persoonsgegevens verwerkt, ongeacht in welke hoedanigheid men verwerkt. Het doel van deze voorwaarden is een rechtmatige verwerking van persoonsgegevens. Op grond van artikel 15 Wbp draagt de verantwoordelijke zorg voor de naleving van de voorwaarden, bedoeld in de artikelen 6 tot en met 12 en 14 lid 2 tot en met lid 5 Wbp. Indien er een schending van de beginselen plaatsvindt en de verantwoordelijke hiervan op de hoogte is, dan dient hij maatregelen te treffen. De betreffende voorwaarden en nadere uitleg hierover zijn hieronder beschreven.

Artikel 6 Wbp: Zorgvuldige en behoorlijke verwerking (rechtmatigheidsbeginsel)

Het algemene basisprincipe voor de verwerking van persoonsgegevens is artikel 6 Wbp. De verwerking van de persoonsgegevens dient te gebeuren in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze. Het woord 'wet' heeft mede betrekking op andere wetgevingen inzake de verwerking van persoonsgegevens.²⁵ Bij de interpretatie van de term 'behoorlijk' kan inspiratie worden geput uit de maatstaven die in het kader van de toepassing van de behoorlijkheidsnorm krachtens de Wet Nationale ombudsman zijn ontwikkeld.²⁶ Tot slot kan voor de invulling van het begrip 'zorgvuldig' in voorkomende gevallen worden aangesloten bij de zorgvuldigheidsnorm uit artikel 6:162 BW, evenals het zorgvuldigheidsbeginsel als algemeen beginsel van behoorlijk bestuur.²⁷ In de jurisprudentie is bepaald dat de uitwerking van deze norm is verwerkt in de overige eisen voor de gegevensverwerking in de Wbp.²⁸ Indien de verantwoordelijk dus aan alle voorschriften, die verbonden zijn aan de gegevensverwerking naleeft, is aan het rechtmatigheidsbeginsel van artikel 6 Wbp voldaan.

Artikel 7: Doelbindingsvereiste

Ten tweede moet voor het verwerken van de persoonsgegevens een concreet doel worden vastgelegd. Artikel 7 Wbp bepaalt dat de doeleinden voor de verwerking aan drie eisen moeten voldoen. De doeleinden dienen welbepaald, uitdrukkelijk omschreven en gerechtvaardigd te zijn. Welbepaald en uitdrukkelijk omschreven houdt in dat de doelstelling niet zo vaag of ruim mag zijn geformuleerd dat zij geen duidelijk kader kan bieden voor de vraag in hoeverre de verwerking in een concreet geval voor het omschreven doel nodig is.²⁹ Als er dus geen precieze doelomschrijving is, mogen persoonsgegevens niet verzameld worden. Bovendien dient het legitieme doel reeds bij het verzamelen van gegevens aanwezig te zijn. Het derde element van artikel 7, het 'rechtvaardigingsvereiste', wordt aan de hand van de gerechtvaardigde grondslagen in artikel 8 Wbp nader uitgewerkt.

Artikel 8 Wbp: Rechtvaardige grondslagen van verwerking

In artikel 8 Wbp zijn de rechtvaardigingsgrondslagen opgesomd, die volgens artikel 7 Wbp onder meer van toepassing zijn op een rechtmatige verwerking. Voor een gerechtvaardigd doel moet elke gegevensverwerking of categorie van gegevensverwerking gebaseerd zijn op

²⁵ 'Naslag artikel 6 Wbp', Autoriteit Persoonsgegevens, www.autoriteitpersoonsgegevens.nl (zoek op artikel 6).

²⁶ P.J.J. van Buuren en L.F.M. Verhey, 'Wet bescherming persoonsgegevens in Europees perspectief', Deventer: Wolters Kluwer uitgevers 2011, pagina 82.

²⁷ P.J.J. van Buuren en L.F.M. Verhey, 'Wet bescherming persoonsgegevens in Europees perspectief', Deventer: Wolters Kluwer uitgevers 2011, pagina 82.

²⁸ Rb 05 Maastricht december 2003, LJN AO0044.

²⁹ P.J.J. van Buuren en L.F.M. Verhey, 'Wet bescherming persoonsgegevens in Europees perspectief', Deventer: Wolters Kluwer uitgevers 2011, pagina 82.

ten minste één van de weergegeven gronden uit artikel 8 Wbp.³⁰ Grondslagen die relevant zijn voor dit onderzoek worden uiteengezet en de overige grondslagen worden uitsluitend opgenoemd.

Sub c: Voldoen aan een wettelijke verplichting

De eerste relevante grondslag stelt dat de verwerking noodzakelijk is voor de uitvoering van een wettelijke verplichting. Zonder verwerking van de gegevens moet het uitvoeren van de wettelijke verplichting redelijkerwijs niet goed mogelijk zijn.³¹ Het begrip noodzakelijk wijst erop dat er geen andere reële mogelijkheid is om de overeenkomst uit te voeren (subsidiariteit) en dat de gegevensverwerking niet verder gaat dan nodig (proportionaliteit).³²

Sub e: Vervulling van een publiekrechtelijke taak

Verder geldt de relevante grondslag dat gegevensverwerking noodzakelijk is voor het vervullen van een publiekrechtelijke taak. Een taak is publiekrechtelijk indien deze is gebaseerd op een speciaal voor het openbaar bestuur bij of krachtens de wet geschapen grondslag.³³

Tot slot zijn de resterende grondslagen dat de gegevensverwerking noodzakelijk is voor de uitvoering van een overeenkomst, noodzakelijk is voor een vitaal belang van de betrokkene en dat het noodzakelijk is voor een gerechtvaardigd belang van de verantwoordelijke of een derde. Ondubbelzinnige toestemming is nodig in specifieke gevallen of wanneer geen andere grond van toepassing is.

Noodzakelijkheidsnorm van artikel 8 Wbp

De noodzakelijkheidsnorm wordt in de wet ook geïdentificeerd als het subsidiariteitsbeginsel en het evenredigheidsbeginsel of proportionaliteitsbeginsel. Het subsidiariteitsbeginsel houdt in dat degene die persoonsgegevens wil verwerken hoort af te zien van de verwerking, indien hetzelfde doel ook langs een andere weg en met minder ingrijpende middelen kan worden gerealiseerd.³⁴ Het proportionaliteitsbeginsel of evenredigheidsbeginsel houdt in dat indien tot gegevensverwerking wordt overgegaan, het van belang is dat degene die gegevens wil verwerken in redelijkheid alle eventuele bestaande mogelijkheden benut om de inbreuk op de persoonlijke levenssfeer van betrokkenen te beperken.³⁵ Bij de verwerking van persoonsgegevens, mag de inbreuk op de belangen van betrokkene namelijk niet onevenredig zijn in verhouding tot het met de verwerking te dienen doel.³⁶ Het evenredigheidsbeginsel volgt uit het recht op eerbiediging van privé leven op grond van artikel 8 lid 1 EVRM. Uit jurisprudentie blijkt dat de verantwoordelijke steeds een belangenafweging moet maken tussen het eigen belang en dat van de betrokkene, om te beoordelen of de verwerking voldoet aan de beginselen van de noodzakelijkheidsnorm.³⁷

Artikel 9 Wbp: Verdere verwerking van persoonsgegevens

Artikel 9 Wbp bepaalt dat persoonsgegevens niet verder worden verwerkt op een wijze die onverenigbaar is met het hoofddoel waarvoor ze zijn verkregen. Ter nadere invulling van de verenigbaarheidseis zijn in lid 2 voorwaarden opgenomen, waarmee beoordeeld kan worden of een bepaalde wijze van gebruik onverenigbaar is.³⁸ De voorwaarden zijn:³⁹

³⁰ P.J.J. van Buuren en L.F.M. Verhey, 'Wet bescherming persoonsgegevens in Europees perspectief', Deventer: Wolters Kluwer uitgevers 2011, pagina 83.

³¹ Kamerstukken II 1997-1998, 25 892, nr. 3.

³² 'Wat is een verwerking als in de Wbp?', www.lexx-it.nl (zoek op *rechtvaardigingsgronden Wbp*).

³³ T.F.M. Hooghiemstra en S. Nouwt, 'Sdu Commentaar Wet bescherming persoonsgegevens', Sdu Uitgevers 2012, pagina 67.

³⁴ Kamerstukken II 1997-1998, 25 892, nr. 3.

³⁵ Kamerstukken II 1997-1998, 25 892, nr. 3.

³⁶ 'Naslag artikel 8 Wbp', Autoriteit Persoonsgegevens, www.autoriteitpersoonsgegevens.nl (zoek op *artikel 8*).

³⁷ HR 09 september 2011, LJN BQ8097

³⁸ T.F.M. Hooghiemstra en S. Nouwt, 'Sdu Commentaar Wet bescherming persoonsgegevens', Sdu Uitgevers 2012, pagina 56.

- de verwantschap tussen het doel van verwerking en het doel waarvoor de gegevens zijn verkregen;
- de aard van de betreffende gegevens;
- de gevolgen van de beoogde verwerking voor de betrokkene;
- de wijze waarop de gegevens zijn verkregen en
- de mate waarin jegens de betrokkene wordt voorzien in passende waarborgen.

Artikel 10: Bewaren

Persoonsgegevens worden niet langer bewaard in een vorm die het mogelijk maakt de betrokkene te identificeren, dan noodzakelijk is voor de verwerking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt.⁴⁰ Een termijn van bewaring kan worden gesteld indien daar voldoende redenen voor zijn. Zijn die termijnen verlopen dan mogen de gegevens niet meer verwerkt worden, tenzij voor een ander, daarmee verenigbaar doel.⁴¹ Indien persoonsgegevens niet meer noodzakelijk zijn voor de verwerking van de doeleinden waarvoor ze zijn verzameld, moeten de gegevens vernietigd worden.⁴² Op grond van lid 2 mogen persoonsgegevens echter langer worden bewaard voor historische, statische of wetenschappelijke doeleinden.

Artikel 11: Dataminimalisatie

Het doel waarvoor de gegevens zijn verzameld en verwerkt bepaalt welke gegevens verkregen mogen worden en de hoeveelheid daarvan. Dit is bepaald in artikel 11 lid 1 Wbp. In dit artikel zijn drie voorwaarden vastgesteld om de kwaliteit van de te verwerken persoonsgegevens te waarborgen. De voorwaarden zijn dat de persoonsgegevens die worden verwerkt, gezien het doel waarvoor het wordt verzameld, toereikend, ter zake dienend en niet bovenmatig dienen te zijn. Dit artikel bepaalt dat de verantwoordelijke erop moet toezien niet minder of meer persoonsgegevens te verzamelen dan nodig is. Daarbij stelt artikel 11 lid 2 Wbp dat de juistheid en nauwkeurigheid van gegevens in zekere zin moeten worden beoordeeld. De verantwoordelijke moet de nodige maatregelen treffen die in redelijkheid van hem kunnen worden gevergd om de nauwkeurigheid en juistheid te kunnen beoordelen.

Artikel 12: Geheimhoudingsplicht

In artikel 12 lid 1 Wbp staat dat een ieder die toegang heeft tot persoonsgegevens deze alleen mag verwerken in opdracht van de verantwoordelijke, behalve als de wet verplichtingen heeft geregeld die daarvan afwijken. In beginsel is de verantwoordelijke aansprakelijk voor de verwerking van de persoonsgegevens. Ieder die handelt onder het gezag van de verantwoordelijke dient te handelen overeenkomstig de door de verantwoordelijke gegeven aanwijzingen.⁴³ Beide partijen stellen het besluit stilzwijgend of uitdrukkelijk vast.

Lid 2 bepaalt dat zelfs indien gezien het beroep dat men uitoefent geen geheimhoudingsplicht geldt, men toch verplicht is tot geheimhouding van de persoonsgegevens waarvan kennis wordt genomen. Dit is op grond van lid 2 alleen uitgesloten op grond van een wettelijk voorschrift of als uit hun taak de noodzaak tot mededeling er is.

³⁹ Artikel 9 lid 2 sub a tot en met e Wbp

⁴⁰ Artikel 10 lid 1 Wbp

⁴¹ 'Naslag artikel 10 Wbp', Autoriteit Persoonsgegevens, www.autoriteitpersoonsgegevens.nl (zoek op *artikel 10*).

⁴² 'Bewaren van persoonsgegevens', Autoriteit Persoonsgegevens, www.autoriteitpersoonsgegevens.nl (zoek op *persoonsgegevens niet meer nodig*)

⁴³ T.F.M. Hooghiemstra en S. Nouwt, 'Sdu Commentaar Wet bescherming persoonsgegevens', Sdu Uitgevers 2012, pagina 66.

Artikel 13: Beveiliging

Artikel 13 bepaalt dat omtrent de beveiliging van persoonsgegevens passende technische en organisatorische maatregelen door de verantwoordelijke ten uitvoer gelegd moeten worden. Het doel van de beveiliging is te voorkomen dat persoonsgegevens verloren raken of dat ze niet overeenkomstig met de wet worden verwerkt. Onder onrechtmatige vormen van verwerking vallen de aantasting, wijziging, of verstrekking van de gegevens of onbevoegde kennisneming.⁴⁴

Passende technische en organisatorische maatregelen en passend beveiligingsniveau.

In artikel 13 Wbp wordt de nadruk gelegd op “passende technische en organisatorische maatregelen” en “passend beveiligingsniveau”. In het begrip ‘passend’ ligt besloten dat de beveiliging in overeenstemming moet zijn met de stand van de techniek.⁴⁵ Daarnaast impliceert het begrip ‘passend’ een proportionaliteitstoets: er moet evenredigheid bestaan tussen de

privacy risico's die de verwerking en de aard van de te beschermen gegevens met zich brengen enerzijds en de getroffen beveiligingsmaatregelen anderzijds.⁴⁶ Naarmate de gegevens een gevoeliger karakter dragen, dan wel de context waarin de gegevens worden gebruikt een grotere bedreiging vormen voor de persoonlijke levenssfeer, worden er zwaardere eisen gesteld aan het niveau van beveiliging.⁴⁷

Het is niet verplicht om de aller zwaarste beveiliging in te zetten, indien dat niet nodig is. Aan de hand van de omstandigheden van het geval moet worden bepaald wat een adequate maatregel voor beveiliging is. De te nemen maatregelen moeten worden afgestemd op de risico's van onrechtmatige verwerking die zich in de betrokken organisatie voordoen, waarbij tevens rekening dient te worden gehouden met de stand van de techniek en de kosten om de betrokken maatregelen ten uitvoer te brengen.⁴⁸ Periodieke toetsing is nodig om te bepalen of de genomen maatregelen voor beveiliging nog adequaat zijn gezien de omstandigheden van het geval.

Artikel 14: De bewerker

De verantwoordelijke kan er voor kiezen zijn verantwoordelijkheid te delegeren aan de bewerker. In artikel 14 Wbp zijn eisen vastgesteld waaraan de verantwoordelijke en bewerker moeten voldoen. De bewerker moet de verantwoordelijkheden van de verantwoordelijke opnemen als zijn eigen verantwoordelijkheden. Laat hij het naleven van de beginselen na, dan is de bewerker mede zelfstandig aansprakelijk.

Artikel 14 lid 1 Wbp geeft aan dat de bewerker zorg moet dragen voor een adequate beveiliging. Daarnaast dient de bewerker instructies van de verantwoordelijke op te volgen. Lid 2 bepaalt dat de bewerker en de verantwoordelijke een bewerkingsovereenkomst dienen te sluiten. Een bewerkersovereenkomst moet aan een aantal minimeisen voldoen:⁴⁹

- De overeenkomst moet specifiek gaan over de gegevensverwerking door de bewerker.
- De verplichtingen moeten over en weer duidelijk zijn vastgelegd in de overeenkomst. Welke persoonsgegevens worden verwerkt, de doeleinden van de verwerking, de duur van de opslag en beveiligingsmaatregelen moeten er bijvoorbeeld gedetailleerd in zijn opgenomen.

⁴⁴ ‘Naslag artikel 13 Wbp’, Autoriteit Persoonsgegevens, www.autoriteitpersoonsgegevens.nl (zoek op artikel 13).

⁴⁵ T.F.M. Hooghiemstra en S. Nouwt, ‘Sdu Commentaar Wet bescherming persoonsgegevens’, Sdu Uitgevers 2012, pagina 68.

⁴⁶ P.J.J. van Buuren en L.F.M. Verhey, ‘Wet bescherming persoonsgegevens in Europees perspectief’, Deventer: Wolters Kluwer uitgevers 2011, pagina 99.

⁴⁷ P.J.J. van Buuren en L.F.M. Verhey, ‘Wet bescherming persoonsgegevens in Europees perspectief’, Deventer: Wolters Kluwer uitgevers 2011, pagina 99.

⁴⁸ ‘Naslag artikel 13 Wbp’, Autoriteit Persoonsgegevens, www.autoriteitpersoonsgegevens.nl (zoek op artikel 13).

⁴⁹ ‘AP eist betere afspraken over digitaliseren patiëntdossiers’, Autoriteit Persoonsgegevens, www.autoriteitpersoonsgegevens.nl (zoek op eisen bewerkersovereenkomst).

- In de overeenkomst moet staan hoe de verantwoordelijke kan toezien op de naleving van de waarborgen.
- De overeenkomst moet een geheimhoudingsplicht bevatten voor de bewerker en zijn personeel.

3.3 De overige verplichtingen van de verantwoordelijke

Naast de eisen die hierboven zijn beschreven, dient de verantwoordelijke ook te voldoen aan de algemene meldingsplicht, de informatieplicht en de meldplicht voor datalekken. Deze eisen worden hieronder nader toegelicht.

Artikel 27 Wbp: Algemene meldingsplicht

Artikel 27 stelt dat een geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, die voor de verwezenlijking van een doeleinde of van verscheidene samenhangende doeleinden bestemd is, wordt gemeld. Dit artikel ziet op een verplichting tot melding alvorens met verwerking van gegevens wordt aangevangen.⁵⁰ De melding wordt volgens lid 3 gedaan bij de AP of de FG.⁵¹ Laat de verantwoordelijke deze plicht na, dan kan de AP een bestuurlijke boete opleggen ingevolge artikel 66 Wbp.

Lid 2 bepaalt dat voor niet geautomatiseerde verwerkingen alleen een melding wordt gedaan, als voorafgaand een onderzoek heeft plaatsgevonden. Handmatige verwerkingen zijn dus in beginsel vrijgesteld van de aanmeldingsprocedure. Indien de handmatige verwerking toch bedreigend blijkt te zijn voor de persoonlijke levenssfeer van de betrokkene, wordt na een voorafgaand onderzoek op grond van artikelen 31 jo. 32 Wbp een melding gedaan. Nadere regels omtrent de algemene meldingsplicht zijn opgenomen in bijlage 2.⁵²

Artikelen 33 jo. 34 Wbp: Informatieplicht

De betrokkene van wie de persoonsgegevens worden verwerkt, moet kunnen achterhalen wat er met die gegevens gebeurt. Organisaties moeten betrokkenen informeren welke gegevens zij gebruiken en met welk doel, de identiteit van de organisatie (naam en adres) en of zij de gegevens aan andere organisaties verstrekken.⁵³ De informatieplicht is in artikelen 33 jo. 34 Wbp geregeld en maakt deel uit van het transparantiebeginsel. In artikel 33 Wbp zijn regels gesteld in het geval dat de gegevens rechtstreeks van de betrokkene worden verkregen. In dit geval geldt de plicht tot informatieverstrekking voorafgaand aan de verkrijging van persoonsgegevens. De informatieverstrekking kan plaatsvinden door middel van overhandiging van een folder of formulier, een exemplaar van toepasselijke standaardvoorwaarden of het kan standaard in het invulformulier worden opgenomen. Artikel 34 Wbp regelt de gevallen waarbij de gegevens op een andere wijze worden verkregen, bijvoorbeeld door derde. Bij deze wijze van verkrijging van persoonsgegevens geldt de plicht tot informatieverstrekking op het moment dat de verantwoordelijke de gegevens vastlegt. Schending van de informatieplichten levert een verbintenis tot schadevergoeding op, en wel op grond van onrechtmatige daad.⁵⁴

In twee gevallen kan de verantwoordelijke ervan uitgaan dat de betrokkene op de hoogte is van de gegevensverwerking, waardoor geen informatieverstrekking nodig is. Dit is na toezending of uitreiking van bijvoorbeeld een folder en als uit een gedraging of een verklaring van de betrokkene naar objectieve maatstaven kan worden afgeleid dat de betrokkene op de hoogte is. Naar objectieve maatstaven houdt in dat een redelijk denkend mens uit de gedraging van de betrokkene zou kunnen opmaken dat deze op de hoogte is.

⁵⁰ T.F.M. Hooghiemstra en S. Nouwt, 'Sdu Commentaar Wet bescherming persoonsgegevens', Sdu Uitgevers 2012, pagina 116.

⁵¹ Artikel 62 Wbp

⁵² Bijlage 2 Nadere regels algemene meldplicht.

⁵³ 'Naslag artikel 33 en 34 Wbp', Autoriteit Persoonsgegevens, www.autoriteitpersoonsgegevens.nl (zoek op eisen informatieplicht).

⁵⁴ E.Thole, F. van der Jagt en H. Roerdink, '50 vragen over privacy', Wolters Kluwer uitgevers 2010, pagina 48.

Voor artikel 34 Wbp gelden als aanvullende uitzonderingen dat:⁵⁵

- mededeling van de informatie aan de betrokkene onmogelijk blijkt of een onevenredige inspanning kost;
- de vastlegging of de verstrekking bij of krachtens de wet is voorgeschreven.

Artikel 34a Wbp: Meldplicht datalekken

De meldplicht datalekken is vanaf 1 januari 2016 in werking getreden. Met de meldplicht wordt beoogd bij te dragen aan het behoud en herstel van vertrouwen in de omgang met persoonsgegevens.⁵⁶ Deze plicht stelt dat elke organisatie, respectievelijk de verantwoordelijke van de organisatie, die persoonsgegevens verwerkt direct een melding dient te doen bij de AP, zodra de organisatie een datalek heeft. In sommige gevallen wordt de melding ook gedaan aan de betrokkene, van wie de persoonsgegevens zijn gelekt. De verantwoordelijke die een datalek niet binnen de wettelijke termijn meldt, kan hoge boetes krijgen.⁵⁷ Nadere toelichting over wat een datalek is, wanneer en hoe een datalek wordt gemeld, door wie en aan wie een datalek wordt gemeld, de inhoud van de melding, de uitgebreide boetebevoegdheid en gevolgen van een onrechtmatig nalaten van de melding omtrent datalek zijn opgenomen in bijlage 3.⁵⁸

3.4 De verwerking van bijzondere gegevens

Naast de algemene persoonsgegevens zijn er ook bijzondere persoonsgegevens. Deze persoonsgegevens zijn bijzonder, omdat het gevoelige gegevens zijn die door de wetgever extra worden beschermd. Bijzondere persoonsgegevens zijn gegevens over iemands:⁵⁹

- Godsdienst of levensovertuiging;
- Ras;
- Politieke voorkeur;
- Gezondheid;
- Seksuele leven;
- Lidmaatschap van een vakbond;
- Strafrechtelijk verleden en
- BSN.

In beginsel is het op grond van artikel 16 Wbp verboden om bijzondere persoonsgegevens te verwerken. Er bestaat echter ontheffing op dit verbod als de verwerking haar grondslag vindt in de uitzonderingen die geregeld zijn in artikel 17 tot en met 22 Wbp. Voor dit onderzoek zijn de persoonsgegevens omtrent de gezondheid en BSN relevant. Hieronder is uitsluitend beschreven wat de verwerking van deze twee bijzondere persoonsgegevens inhouden, omdat de overige bijzondere gegevens geen toegevoegde waarde hebben voor dit onderzoek.

Artikel 21 Wbp: Uitzondering voor het verwerken van gegevens omtrent de gezondheid

In artikel 21 Wbp is vastgesteld in welke gevallen gegevens met betrekking tot de gezondheid van een persoon, ondanks de verbodsbepaling uit artikel 16 Wbp, verwerkt mogen worden. Het begrip 'gezondheid' omvat niet alleen de gegevens die in het kader van een medisch onderzoek of een medische behandeling door een arts worden verwerkt, maar alle gegevens die de geestelijke of lichamelijke gezondheid van een persoon betreffen.⁶⁰

⁵⁵ Artikel 34 lid 4 en 5 Wbp

⁵⁶ 'Meldplicht datalekken', Nederlands Juristen Blad, www.njb.nl (zoek op *nalaten meldplicht*)

⁵⁷ 'Bedrijven houden lekken vaak voor zich' 28 december 2016, NRC, www.nrc.nl (zoek op *Autoriteit Persoonsgegevens*).

⁵⁸ Bijlage 3 Nadere toelichting omtrent de meldplicht datalekken.

⁵⁹ 'Wat zijn persoonsgegevens', Autoriteit Persoonsgegevens, www.autoriteitpersoonsgegevens.nl (zoek op *Wet bescherming persoonsgegevens*).

⁶⁰ P.J.J. van Buuren en L.F.M. Verhey, 'Wet bescherming persoonsgegevens in Europees perspectief', Deventer: Wolters Kluwer uitgeverij 2011, pagina 109.

Artikel 21 lid 1 sub f Wbp bepaalt dat bestuursorganen of werkgevers of instellingen bijzondere gegevens omtrent de gezondheid mogen verwerken voor zover dat noodzakelijk is. De noodzakelijkheid geldt voor de verwerking die geschiedt voor de uitvoering van wettelijke voorschriften of collectieve arbeidsovereenkomsten en de re-integratie of begeleiding van werknemers of uitkeringsgerechtigden.⁶¹ In het kader van re-integratie dienen gegevens omtrent de gezondheid te worden verwerkt, om rekening te kunnen houden met het gezondheidsbelang van de werknemer.⁶²

Volgens lid 2 worden deze gegevens alleen verwerkt door een persoon uit hoofde van ambt, beroep of wettelijk voorschrift of door personen die krachtens een overeenkomst verplicht zijn tot geheimhouding. Bij het gebruiken en uitwisselen van medische gegevens dient de Wbp of een bijzondere wet de basis te bieden. Tenslotte is in lid 5 bepaald dat bij AMvB nadere regels kunnen worden gesteld voor onder andere artikel 21 lid 1 sub f Wbp.

Artikel 24 Wbp: Uitzondering voor het verwerken van de BSN

In artikel 24 lid 1 Wbp is bepaald dat: “een nummer dat ter identificatie van een persoon bij wet is voorgeschreven, wordt bij de verwerking van persoonsgegevens slechts gebruikt ter uitvoering van de betreffende wet dan wel voor doeleinden bij de wet bepaald.” Een BSN is een uniek nummer dat herleidt tot een persoon en valt dus onder een wettelijk voorgeschreven nummer als hier bedoeld. In lid 2 is bepaald dat bij AMvB andere dan in het eerste lid bedoelde gevallen kunnen worden aangewezen voor het gebruik van de BSN.

Naast de uitzonderingen die hierboven zijn opgenoemd en toegelicht, zijn in artikel 23 Wbp wederom algemene uitzonderingen vastgesteld op de verbodsbepaling van artikel 16 Wbp.

3.5 Rechten van de betrokkene

In de Wbp zijn rechten van de betrokkene vastgesteld, waarmee voldaan wordt aan het transparantiebeginsel en wordt gewaarborgd dat persoonsgegevens behoorlijk en zorgvuldig worden verwerkt. De rechten van de betrokkene zijn het recht van inzage in zijn gegevens, het recht van correctie van zijn gegevens en het recht van verzet tegen verwerking.

Artikel 35 Wbp: Recht van inzage (ook wel kennisneming)

De betrokkene heeft het recht zich, met redelijke tussenpozen, tot de verantwoordelijke te wenden met het verzoek hem mede te delen of zijn persoonsgegevens worden verwerkt. De verantwoordelijke moet dan een volledig overzicht van de betreffende gegevens overhandigen, tezamen met het doel van verwerking, de categorieën van gegevens waarop de verwerking betrekking heeft, (de categorieën van) ontvangers en de beschikbare informatie over de herkomst van de gegevens binnen vier weken schriftelijk delen aan de betrokkene.⁶³ Dit recht maakt naast de verplichting van informatieverstrekking van de verantwoordelijke, ook onderdeel uit van het transparantiebeginsel. Met het recht van inzage kan de betrokkene namelijk zien of de verantwoordelijke zijn verplichtingen nakomt, en als dat niet zo is, kan hij gebruik maken van zijn recht op correctie of verzet, naar de rechter gaan of door de AP een onderzoek laten instellen.⁶⁴ Nadere regels die van toepassing zijn op dit recht zijn geregeld in artikel 37 Wbp.

Artikel 36 Wbp: Recht van correctie

Op grond van artikel 36 Wbp kan de betrokkene, na de inzage van de verwerking van zijn persoonsgegevens, deze gegevens verbeteren, aanvullen, verwijderen of afschermen. Dit

⁶¹ Artikel 21 lid 1 sub f onder 1 jo. onder 2 Wbp

⁶² T.F.M. Hooghiemstra en S. Nouwt, ‘Sdu Commentaar Wet bescherming persoonsgegevens’, Sdu Uitgevers 2012, pagina 88.

⁶³ Mr. S.M. Huydecoper, ‘Wet bescherming en persoonsgegevens en ICT’, Sdu Uitgevers 2006, pagina 36.

⁶⁴ E.Thole, F. van der Jagt en H. Roerdink, ‘50 vragen over privacy’, Wolters Kluwer uitgevers 2010, pagina 149.

verzoekt de betrokkene aan de verantwoordelijke, waarbij de betrokkene uitdrukkelijk aangeeft welke correctie hij aangebracht wil zien. Dit recht kan uitsluitend worden uitgeoefend indien de persoonsgegevens feitelijk onjuist zijn of voor het doeleinde van de verwerking onvolledig, niet ter zake dienend of niet conform de wettelijke voorschriften zijn. De verantwoordelijke is op grond van artikel 38 lid 1 Wbp verplicht om in de situatie waarin hij op verzoek van de betrokkene een correctie doorvoert, derden aan wie de gegevens zijn verstrekt van die correctie op de hoogte te brengen.⁶⁵ De verantwoordelijke hoeft niet aan deze verplichting te voldoen als dit onmogelijk is of een onevenredige inspanning kost. Ook voor dit recht zijn nadere regels die van toepassing zijn, geregeld in artikel 37 Wbp.

Artikel 40 jo. 41 Wbp: Recht van verzet

Het recht van verzet kan op grond van artikelen 40 jo. 41 Wbp worden aangetekend. Artikel 41 Wbp is echter niet van toepassing voor dit onderzoek, omdat het gaat over verwerking in verband met de totstandbrenging of de instandhouding van een directe relatie tussen de verantwoordelijke of een derde en de betrokkene met het oog op werving voor commerciële of charitatieve doelen.⁶⁶ Dit artikel zal dus niet verder worden behandeld in dit rapport. Met het recht van verzet wordt bedoeld op het recht van de betrokkene om op zijn verzoek de verwerking van hem betreffende persoonsgegevens stop te zetten.⁶⁷ Op grond van artikel 40 lid 1 Wbp kan verzet worden aangetekend indien gegevens op grond van artikel 8 sub e jo. sub f Wbp worden verwerkt. Het verzet moet in verband zijn met de persoonlijke omstandigheden van de betrokkene. Artikel 8 sub e jo. sub f Wbp heeft betrekking op de gegronde grondslagen voor gegevensverwerking. In sub e gaat het over de noodzaak voor de goede vervulling van een publiekrechtelijke taak en in sub f over de noodzaak voor de behartiging van het gerechtvaardigde belang.

Als het verzet binnen vier weken na ontvangst gerechtvaardigd wordt verklaard door de verantwoordelijke, dan zal hij de verwerking van persoonsgegevens moeten beëindigen. Het verzet kan ook zien op alleen de verstrekking aan derden, zonder dat de verantwoordelijke de gegevensverwerking voor eigen doeleinden hoeft te beëindigen.⁶⁸

3.6 Wat zijn de sancties bij het niet naleven van de Wbp?

Op grond van artikel 51 lid 1 Wbp is de AP belast met het toezicht op een rechtmatige verwerking van persoonsgegevens. Wordt door de verwerker van de persoonsgegevens niet conform de wet gehandeld, dan is de AP bevoegd om sancties op te leggen. De sancties staan in hoofdstuk 10 van de Wbp. Paragraaf 1 van dat hoofdstuk behandelt de last onder bestuursdwang, paragraaf 2 behandelt de bestuurlijke boeten en tenslotte worden in paragraaf 3 strafrechtelijke sancties behandeld.

Last onder bestuursdwang

De AP is bevoegd om een last onder bestuursdwang en daarmee verwante bestuurlijke maatregelen toe te passen wanneer een overtreding is gepleegd. Een last onder bestuursdwang is geregeld in artikel 65 Wbp. De nadere regels omtrent de bestuursdwang zijn geregeld in de Awb. Voorafgaand aan het opleggen van bestuursdwang dient op grond van artikel 5:24 lid 2 Awb een termijn te worden gegund waarbinnen de organisatie de tenuitvoerlegging van de bestuursdwang-beschikking kan voorkomen door zelf maatregelen te nemen. In spoedeisende gevallen wordt geen termijn gegund.

Uit artikel 5:32 Awb volgt dat de AP in plaats van bestuursdwang ook een last onder dwangsom kan opleggen, behoudens als het belang dat beschermd wordt zich daartegen verzet.

⁶⁵ P.J.J. van Buuren en L.F.M. Verhey, *'Wet bescherming persoonsgegevens in Europees perspectief'*, Deventer: Wolters Kluwer uitgevers 2011, pagina 131.

⁶⁶ Artikel 41 lid 1 Wbp

⁶⁷ P.J.J. van Buuren en L.F.M. Verhey, *'Wet bescherming persoonsgegevens in Europees perspectief'*, Deventer: Wolters Kluwer uitgevers 2011, pagina 132.

⁶⁸ E.Thole, F. van der Jagt en H. Roerdink, *'50 vragen over privacy'*, Wolters Kluwer uitgevers 2010, pagina 53.

Bestuurlijke boete

De AP kan vanaf 1 januari 2016 organisaties een bestuurlijke boete opleggen als zij de Wbp overtreden.⁶⁹ Deze bevoegdheid krijgt de AP op grond van de 'Boetebeleidsregel Autoriteit Persoonsgegevens 2015'.⁷⁰ De gevallen waarin een bestuurlijke boete kan worden opgelegd, staan in artikel 66 leden 1 en 2 Wbp. Deze bevoegdheid kent wel enkele beperkingen die zijn geregeld in artikel 66 leden 2 en 3 en het beginsel dat bepaalt dat de AP geen boete oplegt indien er al een strafzaak is begonnen voor het geval of als het OM al een strafbeschikking heeft uitgevaardigd.

Strafrechtelijke sancties

In artikel 75 Wbp is de strafrechtelijke sanctie vastgesteld. In lid 1 is bepaald dat de strafrechtelijke sanctie wordt toegepast indien in strijd wordt gehandeld met hetgeen dat in artikel 4 lid 3 Wbp, 27, 28 of 78 lid 2 onder a Wbp of 79 lid 1 Wbp is bepaald.

⁶⁹ 'CBP krijgt boetebevoegdheid en wordt Autoriteit Persoonsgegevens', Autoriteit Persoonsgegevens, www.autoriteitpersoonsgegevens.nl (zoek op *bestuurlijke boete Wet bescherming persoonsgegevens*).

⁷⁰ Bijlage 4 Boetebeleidsregel Autoriteit Persoonsgegevens 2015.

Hoofdstuk 4 De Algemene Verordening Gegevensbescherming

De digitalisering van de samenleving en het feit dat de technologie zich steeds sneller ontwikkelt hebben als gevolg dat een enorme toename in dataverkeer is ontstaan. Tevens is een toename ontstaan in het verzamelen en delen van gegevens. Het gevolg hiervan is dat de risico's van datalekken en vragen van burgers omtrent wat er met de persoonsgegevens wordt gedaan ook zijn toegenomen. De wetgeving was daarom toe aan vernieuwing. Die vernieuwing is de AVG die in 2016 is aangenomen. De AVG heeft volgens artikel 1 lid 2 AVG de doelstelling om "de grondrechten en fundamentele vrijheden van natuurlijke personen, waaronder de persoonsgegevens, te beschermen". Vanaf de aanneming hebben decentrale overheden, op grond van artikel 99 AVG, twee jaar om hun werkwijze aan te passen aan de AVG. In 2018 zal de AVG directe werking hebben, omdat het een verordening is. De betrokken partijen moeten er dus meteen aan voldoen en belanghebbenden kunnen zich er meteen op beroepen. De Wbp zal dan niet meer gehanteerd worden in Nederland en zal vervallen.

De deelvraag die in dit hoofdstuk wordt uitgewerkt is: *'Welke wijzigingen zijn in de eisen van de AVG toegepast ten opzichte van de Wbp?'*. De wijzigingen die in dit hoofdstuk zijn beschreven hebben betrekking op de begrippen, de werkingssfeer van de AVG, de beginselen van gegevensverwerking, de verplichtingen van de verantwoordelijke, de privacymaatregelen, de rechten van de betrokkenen en welke sancties opgelegd kunnen worden bij het niet naleven van de AVG.

4.1 Nieuwe begrippen

In de AVG worden nieuwe begrippen geïntroduceerd.⁷¹ Enkele begrippen hebben een nieuwe benaming gekregen maar zijn inhoudelijk niet gewijzigd. Een voorbeeld hiervan zijn de begrippen "verantwoordelijke" en "bewerker" die in de AVG zijn opgenomen als "verwerkingsverantwoordelijke" en "verwerker". Daarnaast zijn er ook begrippen die niet eerder zijn gebruikt en dus geheel nieuw zijn in de privacywetgeving. Het gaat bijvoorbeeld om begrippen als "profilering", "pseudonimisering" en "inbreuk in verband met persoonsgegevens."

4.2 De werkingssfeer van de AVG⁷²

De AVG is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking. Ook is het van toepassing op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

De gevallen waarop de AVG niet van toepassing wordt verklaard en die zijn gewijzigd ten opzichte van de Wbp zijn:

- activiteiten die buiten de Unierecht vallen;
- de verwerking door lidstaten die activiteiten uitvoeren die vallen onder titel V, hoofdstuk 2 VEU en
- activiteiten van bevoegde autoriteiten met de intentie te voorkomen, het onderzoeken, de opsporing en het vervolgen in het kader van een strafbaar feit.

Ook zijn er wijzigingen opgetreden in de territoriale reikwijdte van de AVG vergeleken met de Wbp. Het begrip "Nederland" is vervangen door "de Unie", waardoor de werkingssfeer is vergroot. Bepalingen uit de overige leden van artikel 3 AVG worden verder niet behandeld, omdat deze niet relevant zijn voor dit onderzoek.

⁷¹ De omschrijving van de begrippen is terug te vinden in artikel 4 AVG.

⁷² De uitwerking van deze paragraaf is afgeleid uit artikel 2 en 3 AVG.

4.3 Beginselen inzake verwerking van de persoonsgegevens

De algemene beginselen voor de verwerking van persoonsgegevens staan in hoofdstuk 2 van

de AVG. Het basisprincipe bepaalt dat een rechtmatige gegevensverwerking bestaat uit een wijze van verwerking die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is.⁷³ Ten opzichte van het basisprincipe van de Wbp is de wijziging dat het begrip “transparant” het begrip “zorgvuldig” heeft vervangen. In de overige leden van het basisprincipe van de AVG zijn beginselen zoals rechtmatigheid, doelbinding, zorgvuldigheid en dataminimalisatie opgenomen, die ook in de Wbp onderdeel zijn van een rechtmatige verwerking. Er zijn echter twee beginselen toegevoegd: het gaat om het transparantie- en het verantwoordingsbeginsel.

Transparantiebeginsel

Het transparantiebeginsel, vastgelegd in artikel 12 AVG, houdt in dat de betrokkene in de gelegenheid moet worden gesteld om alle aspecten van de verwerking van zijn persoonsgegevens na te kunnen gaan.⁷⁴ Dit beginsel is niet opgenomen in de Wbp, maar wordt er wel in geïmpliceerd.

Verantwoordingsbeginsel

Het tweede beginsel is het verantwoordingsbeginsel, dat is geïmpliceerd in artikel 12 AVG. In de Wbp is de toezichthouder diegene voor wie de verantwoordingsplicht geldt. In de AVG geldt echter dat de betrokkene en de toezichthouder voor verantwoording terecht kunnen bij de verantwoordelijke.⁷⁵

4.4 Verplichtingen van de verantwoordelijke

De nieuwe verplichting van de verantwoordelijke die wordt geïntroduceerd in de AVG is de documentatieplicht. Daarnaast is in de AVG de informatieplicht van de verantwoordelijke versterkt. Deze twee begrippen zijn het verlengde van de twee geïntroduceerde beginselen, beschreven in paragraaf 4.3. Tot slot is de plicht tot het afsluiten van een bewerkersovereenkomst versterkt. Hieronder worden de drie verplichtingen beschreven.

Documentatieplicht

De documentatieplicht houdt in dat de verantwoordelijke alle processen inzake de gegevensverwerking dient te bewaren. Deze verplichting vervangt de meldplicht bij de AP. De documentatieplicht van de verantwoordelijke betreft de volgende informatie:⁷⁶

- De naam en de contactgegevens van de verantwoordelijke
- De naam en de contactgegevens van de FG
- Het doel van verwerking
- Beschrijving van de betrokkenen en de persoonsgegevens die worden verwerkt
- De ontvangers
- Informatie over doorgifte van persoonsgegevens aan derde landen, indien van toepassing
- Indien mogelijk de termijn waarbinnen de gegevens worden gewist
- Indien mogelijk een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

Informatieplicht

Zoals in paragraaf 3.3 omtrent de informatieplicht is vermeld, dient de verantwoordelijke diens contactgegevens te verstrekken aan de betrokkene. Daarbij informeert de verantwoordelijke ook over welke gegevens verwerkt worden, het doeleinde van verwerking

⁷³ Artikel 5 lid 1 sub a Algemene Verordening Gegevensbescherming

⁷⁴ Artikel 5 lid 1 sub a Algemene Verordening Gegevensbescherming

⁷⁵ Artikel 5 lid 2 Algemene Verordening Gegevensbescherming

⁷⁶ Artikel 30 lid 1 sub a tot en met g AVG

en eventuele verstrekking aan derde. In de AVG is bepaald dat de verantwoordelijke ook informatie dient te verstrekken over:⁷⁷

- De contactgegevens van de FG;
- De ontvangers van de persoonsgegevens;
- De termijn van opslag van de persoonsgegevens;
- De rechten van de betrokkene;
- Het recht van de betrokkene om een klacht in te dienen bij de AP;
- De noodzaak van de persoonsgegevens voor het uitvoeren van een wettelijke plicht.

Bewerkerovereenkomst

Nieuw opgenomen in de privacyverordening is de plicht dat de verantwoordelijke alleen van een dienst van een bewerker gebruik mag maken als de bewerker voldoende garanties biedt dat de verwerking wordt uitgevoerd volgens de regels van de verordening.⁷⁸ Zoals beschreven in paragraaf 3.2 zijn er verplichtingen die gebonden zijn aan een bewerkerovereenkomst. Deze worden in de AVG aangevuld met de volgende verplichtingen:⁷⁹

- Het vooraf toestemming vragen aan de verantwoordelijke bij het inschakelen van subbewerkers;
- Het meewerken met de verplichtingen rondom de beveiliging van persoonsgegevens en het melden van datalekken;
- Een plicht tot het verwijderen of teruggeven van persoonsgegevens na afloop van de dienstverlening;
- Een meewerkplicht tot audits en het ter beschikking stellen van informatie aan de verantwoordelijke;

De bewerker dient zich daarbij ook te houden aan de registratieplicht.

4.5 Privacymaatregelen

Privacy by design en privacy by default

Gedurende het gehele proces van gegevensverwerking moeten technische en organisatorische maatregelen genomen worden.⁸⁰ De AVG ziet er op toe dat gegevensbescherming wordt gewaarborgd door ontwerp en door standaardinstellingen. Dit dient zowel te gebeuren bij de bepaling van de verwerkingsmiddelen als bij het gehele proces van verwerking. Het doel hiervan is de gegevensbeschermingsbeginselen, zoals dataminimalisatie, op een doeltreffende manier uit te voeren. Daarnaast dienen de nodige waarborgen in de verwerking in te zijn gebouwd ter naleving van de voorschriften van deze verordening en ter bescherming van de rechten van de betrokkenen. In producten en diensten moet gestreefd worden naar het bieden van de hoogste mate van privacy.

Privacy by design gaat uit van het principe dat in een vroeg stadium wordt nagedacht over verschillende aspecten met betrekking tot de privacy. Privacy by default is het inbouwen van privacy, zodat het vanaf het begin van het proces in acht wordt genomen.

Privacy by design zorgt ervoor dat dataminimalisatie kan worden gewaarborgd, doordat vanaf het begin wordt beoogd stil te staan bij welke persoonsgegevens daadwerkelijk nodig zijn voor het doel van verwerking. Daarnaast beoogt privacy by design dat de persoonsgegevens die verwerkt worden zo veel mogelijk anoniem worden opgeslagen. Indien dit niet lukt dient gekozen te worden voor pseudonimisatie, waarbij de persoonsgegevens niet gekoppeld worden aan een specifiek persoon. Op deze manier wordt de identiteit van een betrokkene afgeschermd. Daarbij zorgt privacy by design er ook voor

⁷⁷ Artikel 13 lid 1 sub b en c jo. lid 2 sub a tot en met e AVG

⁷⁸ 'Functionaris van gegevensbescherming', Z. Bijron, www.privacycompany.eu (zoek op *functionaris van gegevensbescherming*).

⁷⁹ Artikel 28 lid 3 AVG

⁸⁰ Artikel 25 lid 1 AVG

dat wordt nagedacht over de bewaartermijn en de wijze waarop de betrokkene controle kan uitoefenen over zijn of haar persoonsgegevens.

Behalve het ontwerp dient volgens privacy by design ook aandacht besteed te worden aan een intern beleid. Deze dient zodanig goed te zijn dat werknemers daardoor geïnformeerd worden over het belang van de privacy en het privacybeleid wordt nageleefd.

Privacy impact assessment

Bij bijzonder risicovolle verwerkingen moet de verantwoordelijke een 'privacy impact assessment' vaststellen.⁸¹ De PIA, ook wel de privacyeffectbeoordeling, brengt de privacy risico's van een project in een vroeg stadium op een gestructureerde en heldere manier in beeld.⁸²

De grondbeginselen van de PIA geven weer wat het CBP verstond onder een PIA. De grondbeginselen zijn:⁸³

1. PIA is een instrument om privacyrisico's in een vroegtijdig stadium op een gestructureerde en heldere manier in beeld te kunnen brengen.
2. De PIA stimuleert organisaties om proactief na te denken over vragen als:
 - Wat is de impact van het beoogde project op de privacy van betrokkenen?
 - Wat zijn de risico's voor de betrokkenen en voor de organisatie?
 - Is een aanpak die minder gevolgen heeft voor de privacy ook mogelijk, gegeven de doelstellingen van het project?
3. Na het uitvoeren van de PIA kan de verantwoordelijke gerichte opdrachten geven aan degene die het product of dienst verder ontwikkelt opdat maatwerk kan worden geleverd en wordt voorkomen dat in een later stadium kostbare aanpassingen nodig zijn.
4. De PIA kan onderdeel worden van de privacy strategie en het kwaliteitssysteem van een organisatie of van de kwaliteitsbewaking van een project.
5. Door het gebruik van de PIA kan bescherming van persoonsgegevens op een gestructureerde manier onderdeel uitmaken van de belangenafweging en besluitvorming over een project.

De opdrachtgevers, opdrachtnemers en FG zijn degene die onder meer betrokken zijn bij de uitvoering van de PIA.⁸⁴

Functionaris van gegevensbescherming

De mogelijkheid om als privacymaatregel een FG aan te stellen is in de Wbp een discretionaire bevoegdheid, waardoor ieder organisatie zelfstandig kan bepalen of een dergelijk privacy instrument nodig is. De positie en takenpakket van de FG is in de AVG versterkt.⁸⁵

De verplichting om een FG aan te stellen in de privacyverordening geldt alleen voor publieke instanties en organisaties waarvan de aard van de verwerking hiertoe aanleiding geeft of in geval van grootschalige verwerking van bijzondere gegevens.⁸⁶ Een intern persoon aanstellen als FG is verstandig, omdat deze persoon al verstand heeft van de werkwijze van de organisatie. De FG moet onafhankelijk zijn van de instructies van de verantwoordelijke en

⁸¹ 'De Algemene verordening gegevensbescherming', www.openaccessadvocate.nl (zoek op *algemene verordening gegevensbescherming*).

⁸² 'Privacy impact assessment (PIA)', www.autoriteitpersoonsgegevens.nl (zoek op *privacy impact assessment*).

⁸³ Concept toetsmodel Privacy Impact Assessment, pagina 4.

⁸⁴ Handboek Privacy impact assessment (PIA), pagina 53.

⁸⁵ Artikel 17 tot en met 39 AVG

⁸⁶ 'Functionaris van gegevensbescherming', Z. Bijron, www.privacycompany.eu (zoek op *functionaris van gegevensbescherming*).

is gehouden aan de geheimhoudingsplicht. De FG rapporteert de omvang van zijn of haar takenpakket aan het managementteam.

De FG wordt betrokken bij alle zaken die betrekking hebben op de bescherming van persoonsgegevens en beheerst daardoor ook de privacyrisico's binnen de organisatie. Verder zorgt de FG voor het bewustzijn van privacy binnen de organisatie en ziet de FG erop toe dat de wetgeving en het privacybeleid van de organisatie wordt nageleefd. De FG wordt ook betrokken bij de uitvoering van de PIA. Tot slot is de FG de contactpersoon voor de toezichthouder en voor de betrokkenen.

Privacy beleid

De verplichting tot het uitvoeren van een privacybeleid is vastgelegd in artikel 24 lid 2 AVG. Het doel hiervan is de medewerkers die betrokken zijn bij de verwerking van persoonsgegevens bewust maken en opleiden over de privacy. Ook is een privacybeleid nuttig, omdat bij de audits die eventueel worden gehouden, kan worden aangetoond in hoeverre de organisatie bewust bezig is met de privacywetgeving.

4.6 Rechten van betrokkenen

In de AVG zijn ingrijpende wijzigingen gemaakt in de rechten van betrokkenen. Dit komt doordat de digitalisering is toegenomen, waardoor er meer mogelijkheden zijn om persoonsgegevens te verwerken op een ingrijpende manier. De rechten van betrokkenen zijn daarom uitgebreid in de AVG. De verwerkingsverantwoordelijke of verwerker moet daarom nog zorgvuldiger persoonsgegevens verwerken. De verwerkingsverantwoordelijke dient op de hoogte te zijn van de rechten die in 2018 zullen gelden, zodat deze rechten ten alle tijden in acht worden genomen bij de gegevensverwerking. De rechten die inhoudelijk in grote lijnen hetzelfde zijn gebleven zijn het recht op toegang, het recht op rectificatie en het recht op bezwaar of verzet. De AVG introduceert het recht van beperking van de verwerking en het recht op dataportabiliteit. Deze rechten worden hieronder geanalyseerd.

Recht op beperking van de verwerking

In artikel 18 AVG is bepaald dat de betrokkene het recht op beperking van verwerking kan uitoefenen indien:⁸⁷

- De betrokkene de juistheid van de persoonsgegevens betwist
- De verwerking onrechtmatig is en de betrokkene zich verzet tegen het wissen van de persoonsgegevens
- De verantwoordelijke de persoonsgegevens niet meer nodig heeft, maar de betrokkene wel voor de instelling, onderbouwing of uitoefening van een rechtsvordering
- De betrokkene bezwaar heeft gemaakt tegen de verwerking en in afwachting is van het antwoord op de vraag of de gerechtvaardigde gronden van verantwoordelijke zwaarder wegen dan die van de betrokkene.

Het recht op dataportabiliteit

Dataportabiliteit is kort gezegd de mogelijkheid om gegevens van het ene elektronische platform naar het andere over te kunnen dragen.⁸⁸ Dit recht wordt ook wel het recht van gegevensoverdraging genoemd. Het recht van gegevensoverdraging maakt het dus mogelijk om de gegevens die een betrokkene aan een verantwoordelijke heeft verstrekt, over te kunnen dragen aan een andere verantwoordelijke. Dit recht is geregeld in overweging 68, artikel 13 lid 2 en artikel 20 AVG, op voorwaarde dat de gegevens op grond van artikel 20 lid 1 sub b AVG op een geautomatiseerde wijze verwerkt zijn.

⁸⁷ Artikel 18 lid 1 AVG

⁸⁸ 'Recht op dataportabiliteit: een utopie?', www.ejure.nl (zoek op *dataportabiliteit* AVG)

4.7 Sanctie: verhoogd boetemaximum.

De verordening kent administratieve sancties, die bestuurlijke boetes betreffen. De hoogte van de boetes is door de commissie bepaald voor alle landen die tot de Europese Unie horen, zodat er geen onderlinge verschillen ontstaan tussen de landen.

Uit de verordening is af te leiden dat bij elke overtreding een sanctie moet worden opgelegd. Er is omtrent de boetes geen beleidsvrijheid mogelijk. Hoofdstuk 5 van de Awb vormt een volledig stelsel van waarborgen, dat nagenoeg in zijn geheel in acht moet worden genomen bij de boetes.

Hoofdstuk 5 Werkwijze van Baanbrekers getoetst aan de Wbp

In dit hoofdstuk wordt het privacybeleid en werkwijze van Baanbrekers getoetst aan de bepalingen uit de Wbp. Het gaat om de bepalingen die ongewijzigd blijven na de inwerkingtreding van de AVG. De deelvraag die in dit hoofdstuk wordt beantwoord is: *“In hoeverre is de werkwijze en het privacybeleid van Baanbrekers omtrent de gegevensverwerking van sw-medewerkers in overeenstemming met de Wbp?”*

Uit de uitwerking van deze deelvraag zal blijken waar de tekortkomingen zich bevinden in de huidige werkwijze en privacybeleid omtrent het verwerken van persoonsgegevens en op welke punten Baanbrekers ten opzichte van de Wbp actie moet ondernemen.

Voor de gegevensverwerking binnen Baanbrekers is, zoals eerder vermeld, een “Privacyreglement persoonsregistratie” opgesteld dat dateert uit 2004. Dit reglement dient als privacybeleid voor de medewerkers, die voor de functie die zij beoefenen persoonsgegevens verwerken. Om dit hoofdstuk uit te werken is het privacybeleid geanalyseerd en zijn er interviews afgenomen met medewerkers van verschillende afdelingen met betrekking tot de werkwijze binnen Baanbrekers. De relevante documenten en afgenomen interviews zijn opgenomen in de bijlagen. Indien de beschreven informatie rechtstreeks voortvloeit uit deze documenten en de uitgewerkte interviews, dan wordt dat uitdrukkelijk aangegeven.

5.1 Welke persoonsgegevens worden verwerkt?

Binnen Baanbrekers zijn gegevens van alle medewerkers die een dienstverband hebben opgenomen in een fysiek en digitaal dossier. Welke gegevens zijn verwerkt per sw-medewerker, hangt af van de omstandigheden van de persoon. Het gaat in ieder geval om zowel algemene als bijzondere persoonsgegevens. Uit het verrichtte onderzoek blijkt dat diverse gegevens worden verwerkt, zoals de naam, adres, woonplaats, werksituatie van de persoon, medische situatie, of de persoon in aanmerking komt voor een uitkering, thuissituatie en persoonlijke leven van de medewerker. In de tabel hieronder is een onderscheid gemaakt tussen de algemene en bijzondere persoonsgegevens die van de sw-medewerkers bij Baanbrekers worden verwerkt:⁸⁹

Algemene persoonsgegevens	Bijzondere persoonsgegevens
- Voorletters, voornaam, achternaam, meisjesnaam - Geboortedatum / leeftijd - Geboorteplaats - Nationaliteit - Burgerlijke staat - Geslacht - Adres - Woonplaats - Telefoonnummer vast en mobiel - E-mail adres - Bankrekeningnummer - Bruto-maandsalaris - Uitkeringsgerechtigd - Opleidingsgegevens - Werkervaringsgegevens - Nummer identiteitsbewijs en geldigheidsdatum - Kopie paspoort/identiteitskaart - Kopie rijbewijs - Verbliffsvergunning	- BSN - Gegevens omtrent de gezondheid

⁸⁹ Informatie omtrent de verwerkte persoonsgegevens is afgeleid uit het interview gehouden met de coördinator van de afdeling personeelsadministratie, opgenomen in bijlage 7.

- | | |
|--|--|
| <ul style="list-style-type: none"> - Foto betrokkene - Curriculum Vitae - Ziekmeldingen - Verzuimformulieren | |
|--|--|

5.1.1 Bijzondere persoonsgegevens

Bijzondere persoonsgegevens zijn gevoelige gegevens die door de wetgever extra worden beschermd. Uit paragraaf 5.1 blijkt dat het BSN en de gegevens omtrent de gezondheid de bijzondere persoonsgegevens zijn die binnen Baanbrekers worden verwerkt.⁹⁰

BSN

Baanbrekers verwerkt het BSN, omdat het een uniek gegeven is dat verbonden is aan een bepaald persoon. Hiermee zijn de sw-medewerkers snel te herkennen en kan efficiënt en op een snelle manier gehandeld worden met en voor de betrokkene. Het BSN wordt zowel in het fysieke als in het digitale dossier opgenomen.

Gegevens omtrent de gezondheid

Artikel 21 lid 1 sub f Wbp bepaalt dat bestuursorganen, werkgevers of instellingen bijzondere gegevens omtrent de gezondheid mogen verwerken voor zover dat noodzakelijk is voor de uitvoering van onder meer wettelijke voorschriften en de re-integratie of begeleiding van werknemers. Het is noodzakelijk voor Baanbrekers om persoonsgegevens te verwerken, omdat de organisatie de wettelijke verplichtingen van de Participatiewet uitvoert.

Binnen Baanbrekers bezit uitsluitend de bedrijfsarts over de medische gegevens van een sw-medewerker. De (her)indicatie die een sw-medewerker van het UWV heeft gekregen, wordt in het fysieke dossier gedaan. Verder wordt in het digitale cliëntdossier informatie omtrent de gezondheidstoestand ingevoerd. Alleen de mate waarin men arbeidsongeschikt is en de periode van arbeidsongeschiktheid wordt ingevoerd. Specifieke informatie gericht op de reden van de arbeidsongeschiktheid van een sw-medewerker wordt dus niet in het cliëntdossier vermeld.

5.2 Hoe werden en worden persoonsgegevens verzameld?

De wijze van verzameling bij Baanbrekers is van belang om te kunnen beoordelen of het verzamelen van persoonsgegevens conform de wet gebeurt.⁹¹ Hieronder worden verschillende wijzen beschreven waarop Baanbrekers persoonsgegevens van sw-medewerkers heeft verzameld. Indien de beschreven manier van persoonsgegevens verzamelen thans nog geldt binnen Baanbrekers, dan wordt dat erbij vermeld.

Gegevensoverdracht van het Uitvoeringsinstituut Werknemersverzekeringen

Sw-klanten moesten altijd naar het UWV voordat zij geholpen konden worden bij Baanbrekers. Bij het UWV werd de wsw-indicatie verkregen. De indicatie was van belang, omdat daarmee aan Baanbrekers kon worden aangegeven of de toestand van een klant licht, matig of ernstig was. Dit had namelijk invloed op de grootte van de afstand tot de arbeidsmarkt. Voor het verkrijgen van de wsw-indicatie werden persoonsgegevens verwerkt. Van de klanten die daarna werden doorverwezen naar Baanbrekers werden de persoonsgegevens digitaal of per post uitgewisseld met Baanbrekers.

Intake door beheerder wachtlijst

Bij Baanbrekers was een wachtlijstbeheerder in dienst die, nadat hij een melding ontving van

⁹⁰ Informatie omtrent de bijzondere persoonsgegevens is afgeleid uit het interview dat is gehouden met de coördinator van de afdeling personeelsadministratie, opgenomen in bijlage 7.

⁹¹ Informatie over de wijze van gegevensverzameling is afgeleid uit het interview met de coördinator van de afdeling personeelsadministratie (bijlage 7), en gesprekken gevoerd met de teamleider en adviseurs van de afdeling P&O.

het UWV, een intake hield met de sw-klanten. Bij de intake stelde hij aanvullende vragen aan de sw-klant. Het doel van het intakegesprek was om erachter te komen wat de gezondheidstoestand was van de klant. Hiermee werd namelijk beoordeeld wat voor werk een klant wel of niet kon verrichten. Hiervan werd een verslag gemaakt. Aan de hand van het verslag werd door de wachtlijstbeheerder en alle P&O adviseurs beoordeeld waar de klant het beste kon beginnen met werken.

Formulieren

Verder gaf de coördinator van de afdeling personeelsadministratie aan dat persoonsgegevens werden verzameld door middel van het invullen van formulieren. Op het moment dat een klant werd aangenomen als een sw-medewerker moest de medewerker, samen met de P&O adviseur, een aannameset aan formulieren volledig invullen met onder andere persoonsgegevens. De set werd daarna overgenomen door de afdeling personeelsadministratie. Deze afdeling zorgde ervoor dat persoonsgegevens werden ingevoerd in Compas. De formulieren werden daarna in het fysieke dossier gedaan. In het algemeen wordt deze wijze van verzamelen van persoonsgegevens nog steeds gebruikt bij de indiensttreding van het personeel.

Gegevensuitwisseling met externe organisaties

Tot slot werden persoonsgegevens verzameld door gegevensuitwisseling met externe organisaties. Op het moment dat een sw-medewerker van een soortgelijke organisatie als Baanbrekers werd overgenomen, bijvoorbeeld omdat de medewerker in gemeente Heusden, Waalwijk of Loon op Zand ging wonen, nam de afdeling P&O van die organisatie contact op met de afdeling P&O van Baanbrekers. De documenten over de betreffende sw-medewerker werden fysiek of digitaal opgestuurd. Deze documenten kwamen uiteindelijk, na eerst langs de afdeling P&O te zijn gegaan, terecht bij de afdeling personeelsadministratie. Ook deze wijze van verzameling komt nog steeds voor bij Baanbrekers.

5.3 Op welke wijze worden de persoonsgegevens verwerkt?

Baanbrekers verwerkt de persoonsgegevens van sw-medewerkers doormiddel van Compas en fysieke papieren dossiers. Beide wijzen van verwerking worden hieronder nader toegelicht.

Het Compassysteem

Compas is een standaard software voor bedrijven, instellingen en gemeenten die zich bezighouden met het uitvoeren van onder andere de Participatiewet en Wet Sociale Werkvoorziening.⁹² Binnen Baanbrekers wordt Compas gehanteerd om informatie, dat deel uitmaakt van een fysiek personeelsdossier, vast te leggen in een digitaal personeelsdossier.⁹³

Uit onderzoek blijkt dat begin jaren 90 binnen WML gebruik werd gemaakt van Compas. Bij de totstandkoming van Baanbrekers in 2013 is men Compas blijven gebruiken bij Baanbrekers. Compas wordt echter niet gebruikt door alle reguliere medewerkers van Baanbrekers. De autorisatie, waarmee toegang wordt verkregen tot Compas, is namelijk functiegericht. Als gevolg hiervan kunnen bijvoorbeeld de meeste medewerkers van de afdeling re-integratie en participatie en alle medewerkers van de afdeling inkomensondersteuning geen gebruik maken van Compas. De afdelingen die in ieder geval toegang hebben tot Compas, om persoonsgegevens van sw-medewerkers te verwerken, zijn de afdeling P&O en de afdeling personeelsadministratie.

⁹² 'Wat is compas', www.emergo-systems.nl (zoek op Compassysteem)

⁹³ De informatie met betrekking tot het Compassysteem is afgeleid uit het interview dat is gehouden met de systeembeheerder, opgenomen in bijlage 8.

Zoals eerder vermeld krijgt een reguliere medewerker toegang tot Compas door middel van een autorisatieformulier.⁹⁴ Met dit formulier is de autorisatie tot Compas zodanig ingericht dat de medewerkers verschillende autorisatie profielen hebben. De verschillende profielen geven de handelingen van verwerking aan die een medewerker kan uitvoeren. Medewerkers van de afdeling P&O kunnen bijvoorbeeld alleen persoonsgegevens van sw-medewerkers raadplegen en gebruiken in Compas. Medewerkers van de afdeling personeelsadministratie kunnen onder andere vastleggen, ordenen, bewaren, bijwerken, wijzigen, raadplegen, gebruiken enzovoorts. De coördinator is echter de enige die naast de opgenoemde handelingen persoonsgegevens kan verwijderen.

Naast het formulier dient een medewerker vooraf een geheimhoudingsverklaring te ondertekenen.⁹⁵ De beheerder controleert altijd in het digitale dossier of er een volledig ingevulde en ondertekende geheimhoudingsverklaring is.

Alhoewel de toegang tot Compas functiegericht is, kan een medewerker die normaliter geen toegang heeft tot Compas wel voor een bepaald project tijdelijk toegang krijgen, om persoonsgegevens te verwerken die betrekking hebben op het project.⁹⁶ Na het project wordt de medewerker weer uitgesloten van toegang.

De beheerder van Compas zorgt ervoor dat het systeem actueel blijft door de laatste bijwerkingen, die de leverancier voorstelt, door te voeren. De beheerder zorgt ook voor de inrichting van Compas. Hij houdt alles met betrekking tot het systeem bij en indien nodig zorgt hij, in overleg met de coördinator van personeelsadministratie en medewerkers van salarisadministratie voor de toevoeging van nieuwe afdelingen of organisatiestructuren. Hierdoor kunnen diverse gegevens ingevoerd worden. Bovendien houdt de beheerder zich bezig met zaken die betrekking hebben op de helpdesk. Het gaat dan bijvoorbeeld om medewerkers die problemen ervaren met een onderdeel van Compas of vragen hebben over het systeem.

Kortom houdt de beheerder zich bezig met zaken van systeemniveau die worden gebruikt door afdelingen of reguliere medewerkers die toegang hebben tot Compas. De teamleider van P&O houdt toezicht op de werkzaamheden van de beheerder.

Cliëntdossiers

Naast de digitale cliëntdossiers, maakt Baanbrekers gebruik van fysieke dossiers.⁹⁷ Deze dossiers worden bewaard in afsluitbare opbergkasten op de afdeling personeelsadministratie. De fysieke dossiers worden gebruikt, omdat niet alle stukken met betrekking tot een cliënt in Compas kunnen worden ingevoerd. Dit geldt bijvoorbeeld voor de (her)indicaties van sw-medewerkers of aangetekende brieven. Alhoewel niet alle stukken uit het fysieke cliëntdossier in Compas zijn ingevoerd geldt andersom wel dat alle stukken, waarin persoonsgegevens zijn verwerkt, in het fysieke cliëntdossier zijn terug te vinden.

De dossiers kunnen uitsluitend door de P&O adviseurs worden meegenomen. Elke andere medewerker kan de dossiers raadplegen op de afdeling personeelsadministratie of op de werkplek van een adviseur, in diens bijzijn. Medewerkers van andere afdelingen kunnen wel kopieën maken van bepaalde stukken. Aan het einde van het dienstverband of bij her- of overplaatsing naar een andere afdeling of organisatie dienen de kopieën echter weer te worden overgedragen aan de afdeling personeelsadministratie.⁹⁸

⁹⁴ Bijlage 13 Autorisatieformulier

⁹⁵ Bijlage 14 Geheimhoudingsverklaring

⁹⁶ De informatie met betrekking tot Compas is afgeleid uit het interview dat is gehouden met de systeembeheerder, opgenomen in bijlage 8.

⁹⁷ De informatie met betrekking tot de cliëntdossiers is afgeleid uit het interview dat is gehouden met de coördinator van de afdeling personeelsadministratie, opgenomen in bijlage 7.

⁹⁸ Checklist beveiliging persoonsgegevens van bijlage 1 Privacyreglement personeelsregistratie.

De dossiers van sw-medewerkers die uit dienst zijn, worden bewaard in de archiefruimte. De datum van de laatste brief, die Baanbrekers naar een sw-medewerker verstuurd, is bepalend voor de periode van bewaring. De dossiers worden op grond van de Archiefwet tien jaar bewaard. Vanaf dat moment kunnen alleen de medewerkers van de afdeling personeelsadministratie bij de dossiers.

5.4 De toepasselijkheid van de Wbp

De Wbp is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens en op de niet geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen. Verder is voor de toepasselijkheid van de Wbp van belang dat de verwerking van persoonsgegevens gebeurt in het kader van activiteiten die in een vestiging van een verantwoordelijke in Nederland worden uitgevoerd.

Zoals vermeld in paragraaf 5.1 verwerkt Baanbrekers zowel algemene als bijzondere persoonsgegevens. Deze gegevens voldoen aan de omschrijving van het begrip “persoonsgegevens” op grond van artikel 1 lid 1 sub a Wbp. Ze hebben namelijk betrekking op geïdentificeerde natuurlijke personen, de sw-medewerkers. Verder blijkt uit onderzoek dat het merendeel van de handelingen, die zijn opgenoemd in de omschrijving van het begrip “verwerken” op grond van artikel 1 lid 1 sub b Wbp, verspreid over verschillende afdelingen worden uitgevoerd binnen Baanbrekers. Dit is ook af te leiden uit paragraaf 4.2.

Daarnaast blijkt uit onderzoek dat de dossiers op alfabetische volgorde en op regeling bewaard worden in de afsluitbare opbergkasten. Hieruit kan worden geconcludeerd dat de dossiers worden bewaard volgens een bepaalde systematiek. Verder hebben de dossiers betrekking op personen. Er is binnen Baanbrekers dus ook sprake van een niet geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of daarvoor bestemd zijn.

Tot slot kan Baanbrekers worden aangemerkt als verantwoordelijke, omdat zij het doel en de middelen van verwerking bepaalt. Daarbij bevindt Baanbrekers zich in Nederland, waardoor de persoonsgegevens ook in Nederland worden verwerkt in het kader van onder meer het intern of extern aanbieden van werk aan de sw-medewerkers. Aan de territoriale reikwijdte wordt dus ook voldaan.

5.5 Doeleinde en grondslag voor gegevensverwerking

Artikel 7 Wbp bepaalt dat het doeleinde van gegevensverwerking welbepaald, uitdrukkelijk omschreven en gerechtvaardigd dient te zijn. Voor Baanbrekers is het doeleinde vastgelegd in het privacybeleid.⁹⁹ Artikel 2 van dit reglement bepaalt dat persoonsgegevens worden vastgelegd voor zover deze nodig zijn voor het voldoen aan de bijzondere wetgevingen. De letterlijke omschrijving van het doeleinde dateert uit 2004. Om die reden is in de omschrijving gebruik gemaakt van termen zoals “WML”, “Wet sociale werkvoorziening”, de “Wet inschakeling werkzoekenden”. Deze kunnen thans gewijzigd worden naar “Baanbrekers” en “de Participatiewet”. Het is dus noodzakelijk voor Baanbrekers om persoonsgegevens te verwerken, zodat Baanbrekers voldoet aan de wettelijke verplichtingen uit de Participatiewet. Naast het voldoen aan de wettelijke verplichting, vervult Baanbrekers dus ook een publiekrechtelijke taak. Baanbrekers voldoet aan de wettelijke verplichting, omdat het een uitvoeringsinstituut is voor de Gemeenten Heusden, Loon op Zand en Waalwijk. Hiermee vervult Baanbrekers een publiekrechtelijke taak.

Concluderend voldoet Baanbrekers aan de eisen van een welbepaald en uitdrukkelijk omschreven doel voor gegevensverwerking. Op grond van artikel 8 lid 1 sub c jo. sub e Wbp

⁹⁹ Artikel 2 van bijlage 1 Privacyreglement personeelsregistratie.

heeft Baanbrekers ook een gerechtvaardigde grondslag voor verwerking, waardoor Baanbrekers volledig voldoet aan artikel 7 Wbp.

5.6 Verdere verwerking van de persoonsgegevens

Persoonsgegevens mogen uitsluitend verder worden verwerkt op een wijze die verenigbaar is met het hoofddoel waarvoor de persoonsgegevens zijn verkregen. In het kader van individueel of groepsdetachering van sw-medewerkers, worden persoonsgegevens verder verwerkt naar derden.¹⁰⁰ Dit gebeurt door middel van gegevensuitwisseling naar verschillende organisaties die werk aanbieden in het kader van detachering. De gegevens die op het CV staan van een persoon worden uitgewisseld met organisaties vanwege de sollicitatie. Daarbij zorgt de werkmakelaar ervoor dat het BSN niet wordt meegestuurd. Verder wisselt de werkmakelaar gegevens uit die betrekking hebben op de beperkingen van de sw-medewerkers, waarbij de nadruk wordt gelegd op de competenties van de medewerker. De werkmakelaar geeft aan om welk soort beperking het gaat, welke kenmerken uit deze beperkingen voortvloeien en wat de medewerker daardoor niet kan doen binnen de organisatie. Voorafgaand aan het versturen van de persoonsgegevens worden de sw-medewerkers daarover geïnformeerd door de werkmakelaar tijdens overleg. De sw-medewerker wordt geïnformeerd over welke persoonsgegevens verstuurd worden en naar welke organisatie. Uitsluitend ingeval van herindicatie rapporten dient de sw-medewerker te tekenen voor akkoord, voordat het rapport verstuurd mag worden. In een dergelijk rapport wordt de evaluatie gegeven over een sw-medewerker met betrekking tot de voortgang van de medewerker. Uit onderzoek blijkt dat tot dusver niet is voorgekomen dat de sw-medewerker hier niet voor tekent. Dit zou namelijk betekenen dat de indicatie vervalst.

De persoonsgegevens worden zowel digitaal als per post verstuurd door de afdeling personeelsadministratie. Ingeval het om algemene persoonsgegevens gaat, voegt de werkmakelaar daar niets aan toe waaruit blijkt dat de bescherming en beveiliging van de persoonsgegevens gewaarborgd dient te worden. Van het tekenen van een geheimhoudingsverklaring is geen sprake. Uit onderzoek blijkt dat de werkmakelaars ervan uitgaan dat de externe organisatie de persoonsgegevens niet onrechtmatig verwerken. Uitsluitend bij herindicatie wordt de volgende tekst aan het einde van het rapport vermeld:

“Cliënt heeft een kopie ontvangen.

Werkgever heeft een kopie ontvangen.

Alle informatie inzake onze deelnemers aan een re-integratietraject wordt vertrouwelijk behandeld. Iedere medewerker die vanuit zijn/haar functie met vertrouwelijke informatie in aanraking komt, heeft een geheimhoudingsplicht.”

5.7 Beveiliging

De verantwoordelijke dient passende technische en organisatorische maatregelen ten uitvoer te leggen, om te voorkomen dat persoonsgegevens verloren raken of dat het niet overeenkomstig met de wet wordt verwerkt. Daarbij geldt dat zwaardere eisen worden gesteld aan het niveau van de beveiliging, naarmate de gegevens een gevoelige karakter hebben.

Technische beveiligingsmaatregelen

Binnen Baanbrekers zijn verschillende technische beveiligingsmaatregelen genomen om te voorkomen dat persoonsgegevens verloren raken of op een onrechtmatige wijze worden verwerkt. Allereerst wordt in de Privacyverklaring vermeldt dat binnen Baanbrekers continu wordt gecontroleerd of iemand niet illegaal toegang probeert te verschaffen tot de gebruikte systemen.¹⁰¹ Controle daarop wordt uitgevoerd door de systeembeheerder van Compas,

¹⁰⁰ Informatie omtrent de verdere verwerking is afgeleid uit het interview met de werkmakelaar, opgenomen in bijlage 9.

¹⁰¹ ‘Privacystatement’, Baanbrekers, www.baanbrekers.org/ (zoek op privacy).

maar ook door de afdeling automatisering die toegang heeft tot alle netwerken en systemen die gebruikt worden binnen Baanbrekers.

Ten tweede zijn in het privacybeleid ook bepalingen opgenomen omtrent de technische maatregelen die binnen Baanbrekers worden genomen. Deze staan in de 'Checklist beveiliging persoonsgegevens' die is opgenomen in bijlage 7 van het privacybeleid.¹⁰²

Eenieder dient een geheimhoudingsverklaring en autorisatieformulier te ondertekenen om autorisatie te krijgen tot het verwerken van persoonsgegevens in Compas. Compas is beveiligd met profielen. Elk medewerker krijgt een profiel, dat aangeeft welke rechten uit Compas aan de medewerker worden toegekend. In de profielen worden tot op tabblad niveau de bevoegdheden vastgelegd van een medewerker. De beheerder bepaalt dus welke handelingen van verwerking een medewerker kan plegen in Compas. Hierdoor kan een medewerker in feite toegang hebben tot Compas, maar alleen voor de functies waarvoor de beheerder het toestaat. Verder kan de beheerder de autorisatie bepalen per gegeven. Deze autorisatie bepaalt welke gegevens een medewerker kan raadplegen en welke gegevens toegevoegd, gewijzigd en verwijderd kunnen worden.

Tot slot is voor systemen en applicaties bepaald dat de beheerders daarvan zorg dragen voor het aanleggen van passende maatregelen om persoonsgegevens in het personeelsregistratiesysteem te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking onder andere door het gebruik en het jaarlijks wisselen van passwords, het beveiligd bewaren van elektronische informatiedragers, het uitvoeren van een back-up procedure ter voorkoming van het verlies van gegevens en het aanleggen van gebruikersprofielen voor gebruikers.¹⁰³ Bij deze maatregelen wordt rekening gehouden met een passende beveiliging, gelet op de risico's die de verwerking en de aard van de beschermende gegevens met zich meebrengen.

Organisatorische beveiligingsmaatregelen

In de 'Checklist beveiliging persoonsgegevens' zijn ook bepalingen opgenomen omtrent de organisatorische beveiligingsmaatregelen. Bij deze vorm van beveiliging gaat het om de maatregelen die in de organisatie worden genomen om persoonsgegevens van betrokkenen in bijvoorbeeld bepaalde ruimtes, werkplekken en kasten te beveiligen. Wat betreft de genomen maatregelen is allereerst ingevolge de checklist bepaald dat elk bevoegd persoon zorg dient te dragen voor de afsluitbaarheid en ontoegankelijkheid voor onbevoegden van kantoren, kasten, bureaulades, personeelsbakjes en overige ruimten en zaken binnen de organisatie waar zich persoonsgegevens bevinden. Indien de hierin aanwezige persoonsgegevens op een bepaald moment van de dag niet meer actief worden gebruikt, dienen genoemde zaken en/of ruimten afgesloten te zijn en dus niet toegankelijk te zijn voor onbevoegden.¹⁰⁴

Uit onderzoek is gebleken dat voorafgaand aan de fusie meerdere keren audits zijn gehouden om te controleren en te beoordelen of de medewerkers conform de Wbp handelden. Van elke audit is achteraf een verslag gemaakt met de constatering. Het verslag van de laatst gehouden audit voor de fusie, die dateert uit 2009, is opgenomen in bijlage 5.¹⁰⁵ Alhoewel dit een oude audit is, die waarschijnlijk niet langer het juiste beeld geeft van hoe wordt omgegaan met persoonsgegevens binnen Baanbrekers, is het wel van belang te bekijken wat daarin werd geconstateerd. Hieruit blijkt immers of de audits effectief zijn geweest.

¹⁰² 'Checklist beveiliging persoonsgegevens' van bijlage 1 Privacyreglement personeelsregistratie.

¹⁰³ 'Checklist beveiliging persoonsgegevens' van bijlage 1 Privacyreglement personeelsregistratie.

¹⁰⁴ 'Checklist beveiliging persoonsgegevens' van bijlage 1 Privacyreglement personeelsregistratie.

¹⁰⁵ Bijlage 5 Memo managementrapportage n.a.v. gehouden audit WBP d.d. 26.05.09

De audits werden gehouden door de toenmalige juristen van Baanbrekers. Steekproefsgewijs werden een aantal werkplekken in de organisatie onderzocht. De juristen controleerden of op de werkplekken persoonsgegevens “onbeveiligd” oftewel in een niet afgesloten kast, bureaulade of rolcontainer werden opgeborgen en daardoor toegankelijk voor een ieder waren.¹⁰⁶ De constatering werd per naam van diegene waarvan de werkplek werd bezocht, beschreven. Daarbij is achter elke naam aangegeven of het de eerste audit is die is gehouden op de werkplek of dat al (een aantal keren) eerder een audit is gehouden. Na de beschrijving per werkplek omtrent de constatering, is ook geconcludeerd of was voldaan aan de “clean desk policy”. De werkplekken zijn tot slot beoordeeld met een voldoende of (zware) onvoldoende.

Na 2009 is intern geen interne audit meer gehouden binnen WML. Ook na de fusie is binnen Baanbrekers tot dusver ook geen interne audit meer gehouden op de verwerking van persoonsgegevens. In het kader van projectgroep informatieveiligheid is in 2016 wel een audit gehouden door een externe mystery guest.¹⁰⁷ Uit deze audit bleek dat Baanbrekers faalde op het gebied van zorgvuldig omgaan met onder meer de persoonsgegevens van betrokkenen.

Naast de auditmaatregel is een andere maatregel dat in het privacybeleid is bepaald dat fysieke cliëntdossiers uitsluitend worden ingekeken bij de afdeling personeelsadministratie, waar de dossiers bewaard worden. De cliëntdossiers mogen uitsluitend worden meegenomen door de adviseurs van de afdeling P&O. Medewerkers van andere afdelingen mogen geen dossiers meenemen. Slechts indien toestemming is verkregen van een adviseur van de afdeling P&O mag een medewerker in diens aanwezigheid het dossier raadplegen.

Archiefruimten waar de non-actieve cliëntdossiers zich bevinden zijn afsluitbaar en uitsluitend toegankelijk voor medewerkers van de afdeling P&O, juridische zaken en personeelsadministratie.¹⁰⁸

5.8 Verplichtingen van de verantwoordelijke

*Bewaartermijn*¹⁰⁹

Persoonsgegevens worden niet langer bewaard dan noodzakelijk is voor de verwerking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt.¹¹⁰ Baanbrekers verklaart dit ook in het Privacystatement opgenomen op de website omtrent de verwerking van persoonsgegevens.¹¹¹ Daarnaast zijn over de bewaartermijn ook soortgelijke bepalingen opgenomen in het privacybeleid, met nadere toelichting daarop.

Persoonsgegevens van een sw-medewerker zullen niet meer noodzakelijk zijn voor Baanbrekers, wanneer dat wettelijk wordt bepaald of wanneer het dienstverband tussen de medewerker en Baanbrekers is beëindigd. Uit onderzoek blijkt dat wanneer een sw-medewerker uit dienst gaat de datum van de laatste brief die naar de sw-medewerker is gestuurd bepalend is voor de einddatum van het beheer van het dossier. Na de laatste correspondentie zal het dossier van de sw-medewerker en alle persoonsgegevens die erin zijn verwerkt in het archief worden gedaan. De periode van bewaring die Baanbrekers aanhoudt is zoals in de Archiefwet bepaald tien jaar. In het algemeen worden de fysieke cliëntdossiers tien jaar na het einde van het dienstverband bewaard. Het langer bewaren van persoonsgegevens kan nodig zijn vanwege de administratieve functie, financiële

¹⁰⁶ Bijlage 5 Memo managementrapportage n.a.v. gehouden audit WBP d.d. 26.05.09, pagina 1.

¹⁰⁷ Afgeleid uit gesprekken met teamleider van de afdeling P&O

¹⁰⁸ ‘Checklist beveiliging persoonsgegevens’ van bijlage 1 Privacyreglement personeelsregistratie.

¹⁰⁹ Informatie omtrent het bewaartermijn vloeit voort uit het interview dat is gehouden met de coördinator van de personeelsadministratie.

¹¹⁰ Artikel 10 lid 1 Wbp

¹¹¹ ‘Privacystatement’, Baanbrekers, www.baanbrekers.org/ (zoek op *privacy*).

verantwoording of bewijsvoering.¹¹² De digitale dossiers worden twee maanden na het dienstverband afgesloten voor mutatie. De medewerkers kunnen de dossiers dan uitsluitend raadplegen.

Artikel 16 lid 3 van het privacybeleid stelt dat de betrokkene een verzoek kan doen tot vernietiging van (delen van) het dossier. Dit verzoek wordt door Baanbrekers gehonoreerd, tenzij de gegevens vallen onder een wettelijke bewaarplicht of indien bewaring van de gegevens een aanmerkelijk belang is voor de beheerder.

Uit onderzoek blijkt dat Baanbrekers echter niet volledig voldoet aan de bewaartermijn. Een voorbeeld hiervan is dat in het verleden ook informatie omtrent de etnische achtergrond van de betrokkenen werden vastgelegd. Dit werd gedaan in het kader van Wet SAMEN, waarbij werkgevers hun allochtone medewerkers moesten registreren.¹¹³ Aan de hand van de registraties kon worden vastgesteld in hoeverre in de organisatie sprake was van evenredige arbeidsparticipatie van etnische minderheden. Wet SAMEN is vervallen, waardoor de gegeven omtrent de etnische achtergrond van een persoon niet meer wordt geregistreerd. Dit gegeven is echter niet uit het dossier van de betreffende sw-medewerkers gehaald. Uit onderzoek blijkt dat persoonsgegevens die niet meer noodzakelijk zijn voor verwerking, binnen Baanbrekers nooit uit de dossiers worden gehaald. Indien de betreffende gegevens niet worden bewaard voor historische, statische of wetenschappelijke doeleinden, is het bewaren van de gegevens in strijd met de bewaartermijn.

Dataminimalisatie

De persoonsgegevens die worden verwerkt dienen toereikend te zijn, ter zake dienend en niet bovenmatig te zijn voor de waarborging van de kwaliteit van de gegevens. Baanbrekers draagt er zorg voor niet meer of minder persoonsgegevens te gebruiken dan nodig is.¹¹⁴ Informatie die overbodig is wordt eruit gehaald. Dit blijkt bijvoorbeeld uit het feit dat persoonsgegevens die betrekking hebben op de etnische achtergrond van een sw-medewerker niet meer worden geregistreerd, omdat de Wet SAMEN is vervallen.

Algemene meldplicht

Een geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens dient door de verantwoordelijke voorafgaand aan het verwerken gemeld te worden bij de AP. Baanbrekers heeft een algemene melding gedaan bij de AP.¹¹⁵ In de melding heeft Baanbrekers aangegeven wat de doelen zijn van verwerking, welke soort gegevens per soort medewerker binnen de organisatie worden verwerkt en met welk doel. Voor de sw-medewerkers zijn de NAW-gegevens, indicatie- en herindicatiegegevens, gegevens voor eventuele aanspraken op een uitkering, arbeidsvoorwaardelijke gegevens, medische en psychologische gegevens, ziekteverzuimgegevens, ontslaggegevens, wettelijke gegevens, gegevens voor de behandeling personeelszaken, gegevens die betrokkene zelf aangeeft, ontwikkel- en begeleidingsgegevens en bijzondere persoonsgegevens betreffende de gezondheid van de sw-medewerker gemeld. Ook is in de melding vermeld naar welke interne en externe ontvangers de gegevens worden verstrekt.

Informatieplicht

Voor dat begonnen wordt met het verwerken van persoonsgegevens van een betrokkene, dient deze door de verwerker geïnformeerd te worden over welke gegevens verwerkt worden, voor welk doel en de verdere verwerkingen die verenigbaar zijn met het hoofddoel. Deze regel is ook opgenomen in het beleid.¹¹⁶

¹¹² Toelichting artikel 16, Bijlage 1 Privacyreglement personeelsregistratie.

¹¹³ *Kamerstukken II* 2003-2004, 29 275, nr. 3.

¹¹⁴ Informatie omtrent de toepassing van dataminimalisatie is afgeleid uit gesprekken met de teamleider van de afdeling P&O.

¹¹⁵ Bijlage 14 Gedetailleerde informatie algemene meldplicht Baanbrekers

¹¹⁶ Informatie omtrent de informatieplicht is afgeleid uit gesprekken met verschillende P&O adviseurs.

Uit onderzoek blijkt dat Baanbrekers ervan uitgaat dat de betrokkene op de hoogte is van de gegevensverwerking en het doel daarvan. Informatie over de gegevensverwerking wordt, zowel mondeling als schriftelijk, niet uit eigen initiatief gegeven. Een medewerker dient voor het dienstverband een aantal stukken te tekenen voordat hij officieel aangenomen kan worden. Hiermee wordt binnen Baanbrekers geacht duidelijk aan te hebben gegeven dat de persoonsgegevens van de betrokkene zullen worden verwerkt. De betrokkenen worden ook niet geïnformeerd over het feit dat gegevens worden uitgewisseld met bewerkers, zodat deze volgens de instructies van Baanbrekers diensten kunnen leveren. Betrokkenen worden alleen geïnformeerd in het kader van verdere verwerking voor detachering. In theorie is de informatieplicht dus wel vastgelegd, maar in de praktijk wordt hier niet voldoende invulling aan gegeven. Concluderend voldoet Baanbrekers niet aan de informatieplicht.

Meldplicht datalekken en uitbreiding boetebevoegdheid

Binnen Baanbrekers zijn regels opgesteld omtrent de interne procedure rondom de Meldplicht datalekken.¹¹⁷ De manager van onder andere de afdeling P&O is diegene die als verantwoordelijke wordt aangemerkt door de Wbp. Hij brengt verschillende afdelingen samen waaronder de afdeling Interne Controle en de juridische afdeling. Samen beoordelen zij volgens het stappenplan van meldplicht datalekken of er sprake is van een datalek. Indien dat het geval is, wordt de datalek binnen Baanbrekers geregistreerd en wordt daarna bepaald of het datalek zodanig ernstig is dat het gemeld dient te worden bij de AP. Sinds de inwerkingtreding van de Wet Meldplicht datalekken heeft geen datalek plaatsgevonden binnen Baanbrekers.

5.9 De bewerkers en de bewerkersovereenkomst

De bewerker en verantwoordelijke dienen een bewerkingsovereenkomst te sluiten waarin belangrijke bepalingen zijn vastgelegd met betrekking tot het verwerken van de gegevens. De bewerker volgt daarmee de instructies op van de verantwoordelijke. Baanbrekers werkt samen met de Arbodienst 'Zorg van de Zaak' en Dariuz met betrekking tot de gegevens van de sw-medewerkers.

De Arbodienst heeft professionals in dienst die Baanbrekers ondersteunen in het optimaal in hun kracht zetten van medewerkers. Dariuz maakt het door middel van hun systeem mogelijk om via een assessment inzicht te krijgen in werkcompetenties van de medewerkers. Hiermee kan bepaald worden of de werkprestatie van de werknemer achteruit is gegaan, stabiel is of vooruit is gegaan. Baanbrekers heeft een overeenkomst met deze organisatie gesloten, maar de overeenkomsten komen niet overeen met de inhoud van een bewerkersovereenkomst.

Binnen Baanbrekers is de bewerkersovereenkomst ter sprake gekomen in het kader van het projectgroep informatieveiligheid. Uit onderzoek is geconstateerd dat de bewerker en de bewerkersovereenkomst niet zijn geregeld in het privacybeleid. In de praktijk blijkt ook dat termen "bewerker" en "bewerkersovereenkomst" niet bekend waren bij de teamleider van de afdeling P&O, die verantwoordelijk is voor het sluiten van deze overeenkomst met de bewerkers. Binnen de organisatie is momenteel een standaard conceptbewerkersovereenkomst opgesteld, die bestemd is voor de bewerkers van de afdeling re-integratie en participatie en de afdeling inkomensondersteuning (voorheen: sociale dienst) van Baanbrekers.¹¹⁸ Deze overeenkomst gaat specifiek over de gegevensverwerking door de bewerker. Niet opgenomen is om welke persoonsgegevens het gaat, de doeleinden van de verwerking en de duur van de opslag, omdat dit een standaard concept bewerkersovereenkomst is. De beveiligingsmaatregelen zijn er overigens uitgebreid

¹¹⁷ Informatie omtrent de meldplicht datalekken en uitbreiding van de boetebevoegdheid is afgeleid uit het interview met de juriste, opgenomen in bijlage 10.

¹¹⁸ Bijlage 12 Concept bewerkersovereenkomst

wel in opgenomen. In de overeenkomst is ook opgenomen hoe de verantwoordelijke toeziet op de naleving van de waarborgen. Tot slot is een geheimhoudingsbepaling opgenomen in de overeenkomst en een geheimhoudingsverklaring.

Concluderend voldoet de conceptbewerkersovereenkomst binnen Baanbrekers in grote mate aan de eisen die eraan verbonden zijn. Wanneer Baanbrekers definitief een bewerkersovereenkomst sluit met de Arbodienst, Dariuz of andere bewerkers, dient de organisatie ook in de overeenkomst op te nemen om welk soort persoonsgegevens het gaat, het doeleinde van verwerking en de duur van de opslag, hetgeen momenteel niet gebeurt.

5.10 Rechten van de betrokkene

In artikel 11 van het privacybeleid is het recht op inzage vastgelegd en in artikel 14 het recht op correctie. Omtrent het recht van verzet is geen bepaling opgenomen in het beleid.

Recht op inzage

In het privacybeleid is bepaald dat betrokkene het recht heeft om inzage te verkrijgen en dat dit gebeurt onder begeleiding van de P&O adviseur. Indien de betrokkene niet voor zijn belangen kan opkomen, treedt een gemachtigde op voor de betrokkene. Indien de betrokkene het wenst, kunnen er kopieën van stukken uit de dossiers worden gemaakt.

Recht op correctie

Omtrent het recht op correctie is bepaald dat de betrokkene dit kan verzoeken na het uitoefenen van het recht op inzage. Dit kan door de betrokkene of diens wettelijke vertegenwoordiger worden verzocht bij de P&O adviseur. Dit kan uitsluitend als de betrokkene van mening is dat niet wordt voldaan aan de dataminimalisatie of dat er onrechtmatig wordt verwerkt.

5.11 Rechtmatigheidsbeginsel

Om te voldoen aan het rechtmatigheidsbeginsel dient de gegevensverwerking te gebeuren op een behoorlijke en zorgvuldige manier en in overeenstemming met de wet. Uit hetgeen wat in de bovengenoemde paragrafen van dit hoofdstuk is beschreven, kan geconcludeerd worden dat Baanbrekers niet voldoet aan de drie eisen en dat dus niet wordt voldaan aan het rechtmatigheidsbeginsel.

5.12 Privacybeleid

In het privacybeleid van Baanbrekers wordt beschreven wat van toepassing is op de organisatie, om welke reden het van toepassing is en op welke wijze de eisen van gegevensverwerking verwezenlijkt worden binnen Baanbrekers. Het privacybeleid is vanaf 2004 niet geactualiseerd, waardoor wijzigingen zoals de meldplicht datalekken of uitgebreide boetebevoegdheid van de AP niet in het privacybeleid zijn opgenomen. Een ander gevolg van het niet actualiseren van het privacybeleid is dat er nog oude termen in te vinden zijn, die thans gewijzigd zijn. Voorbeelden hiervan zijn de wetgevingen die in het privacybeleid zijn opgenoemd voor de grondslag van gegevensverwerking.¹¹⁹ Dit kan voor verwarring zorgen, terwijl het privacybeleid juist is bedoeld voor verduidelijking en kennistelling bij de medewerkers.

Tot slot blijkt uit onderzoek dat één van de belangrijkste afdelingen met betrekking tot de gegevensverwerking, niet op de hoogte was van het bestaan van het privacybeleid. Gezien het doel van het privacybeleid is dit geen gewenste situatie. Het privacybeleid wordt namelijk niet optimaal gebruikt voor wat het bedoeld is en kan dan ook niet effectief zijn.

¹¹⁹ Zie hiervoor paragraaf 5.5

Hoofdstuk 6 Werkwijze van Baanbrekers getoetst aan de AVG

In dit hoofdstuk wordt het privacybeleid en werkwijze van Baanbrekers getoetst aan de bepalingen uit de AVG. Uitsluitend de onderwerpen in de AVG die zijn gewijzigd ten opzichte van de Wbp worden getoetst. Hiermee wordt antwoord gegeven op de deelvraag: *“In hoeverre is de werkwijze en het privacybeleid van Baanbrekers omtrent de gegevensverwerking van sw-medewerkers in overeenstemming met de eisen uit de AVG?”* Met deze deelvraag worden de gebreken met betrekking tot de AVG weergegeven, waardoor een deel van de centrale vraag wordt beantwoord. De toetsing aan de AVG geeft ook actiepunten aan, waar Baanbrekers aandacht aan moet besteden. Ook in dit hoofdstuk wordt uitdrukkelijk aangegeven wanneer de beschreven informatie afkomstig is van de informatie opgenomen in de bijlagen.

6.1 De werkingssfeer van de AVG

De vergroting van de werkingssfeer van de AVG heeft geen invloed op de toepassing van de AVG op Baanbrekers. Er verandert namelijk niets aan de werkwijze van Baanbrekers als bedrijf dat zij buiten de werkingssfeer van de AVG zou vallen. De AVG zal dus van toepassing zijn op Baanbrekers, omdat de organisatie geheel of gedeeltelijk geautomatiseerd gegevens verwerkt. Daarnaast verwerkt Baanbrekers ook persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen. Tot slot bevindt Baanbrekers zich in de Europese Unie en verwerkt de organisatie persoonsgegevens in de Europese Unie.

6.2 Verplichtingen van de verantwoordelijke

In deze paragraaf wordt geanalyseerd in hoeverre Baanbrekers met de huidige werkwijze voldoet aan de documentatieplicht, de aanvullende eisen van de informatieplicht en bewerkersovereenkomst.

Documentatieplicht

In paragraaf 3.3 is vermeld dat Baanbrekers een algemene meldplicht heeft gedaan, waarin per soort medewerker is aangegeven welke persoonsgegevens worden verwerkt, voor welk doel en met welke interne en externe ontvangers de persoonsgegevens worden uitgewisseld.

De documentatieplicht eist vermelding van de naam en de contactgegevens van de organisatie. In de meldplicht zijn deze gegevens ook vrijgegeven. Verder is het doel van gegevensverwerking, de beschrijving van betrokkenen, de ontvangers en informatie over of doorgifte van persoonsgegevens aan derde landen indien dat van toepassing is, vermeld in de melding. Gezien de verdere eisen van de documentatieplicht, ontbreken in de algemene melding de naam en contactgegevens van de FG indien deze in dienst is in de organisatie, de termijn waarbinnen de gegevens worden gewist en indien mogelijk een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

De informatie die al wel vermeld is in de algemene melding vormt de basis voor het proces van gegevensverwerking die vastgelegd moet worden volgens de documentatieplicht. De basis kan geactualiseerd worden naar de tegenwoordige naam van de verantwoordelijke, welke persoonsgegevens worden verwerkt, soort medewerkers en ontvangers die thans voorkomen binnen Baanbrekers. Daarna kan de ontbrekende informatie worden aangevuld, zodat Baanbrekers voldoet aan de documentatieplicht van de AVG.

Informatieplicht

De informatieplicht komt thans voor in de Wbp. In de AVG wordt deze plicht versterkt door de aanvullende eisen die hieraan zijn verbonden. In paragraaf 5.8 is geconcludeerd dat Baanbrekers niet voldoet aan de informatieplicht ten opzichte van de Wbp. Uit eigen initiatief

geven de reguliere medewerkers namelijk geen informatie over welke persoonsgegevens worden verwerkt, voor welk doel en hoe ver de verwerking zich strekt.

Omtrent de eisen van de AVG heeft Baanbrekers nog geen FG in dienst, waardoor daar geen informatie over verstrekt kon worden. Verder informeert Baanbrekers ook niet over de ontvangers van de persoonsgegevens, de termijn van opslag van de persoonsgegevens, de rechten van de betrokkenen of het recht om een klacht in te dienen bij de AP en het belang van de persoonsgegevens om te voldoen aan de grondslagen van verwerkingen. Er kan dus geconcludeerd worden dat binnen Baanbrekers niet wordt voldaan aan de aanvullende eisen die in de AVG verbonden worden aan de informatieplicht.

Bewerkersovereenkomst

In paragraaf 5.9 is geconcludeerd dat het standaard concept bewerkersovereenkomst voldoet aan de eisen die de Wbp verbindt aan de overeenkomst. De AVG stelt aanvullende eisen aan deze overeenkomst. De bewerker dient vooraf toestemming te vragen aan de verantwoordelijke bij het inschakelen van subbewerkers. Daarnaast dient de bewerker mee te werken aan de verplichtingen omtrent de beveiliging en het melden van een datalek. Bovendien dient de bewerker persoonsgegevens na afloop van de dienstverlening te verwijderen of terug te geven. Tot slot moet de bewerker meewerken aan audits en houdt hij zich aan de registratieplicht.

In de standaard conceptovereenkomst is van deze aanvullende eisen alleen de verplichtingen met betrekking tot de beveiliging en het melden van een datalek opgenomen. De overige eisen zullen nog in de bewerkersovereenkomst moeten worden opgenomen om te voldoen aan de eisen van de AVG.

6.3 Privacymaatregelen

Privacy by design en privacy by default

Door middel van privacy by design en privacy by default wordt erop toegezien dat gegevensbescherming wordt gewaarborgd door ontwerp en door standaardinstellingen. Privacy by design zorgt ervoor dat dataminimalisatie kan worden gewaarborgd, doordat vanaf het begin wordt beoogd stil te staan bij welke persoonsgegevens daadwerkelijk nodig zijn voor het doel van verwerking.

In Compas komt privacy by default goed naar voren. In paragraaf 5.3 wordt beschreven hoe de privacy van persoonsgegevens wordt beschermd in Compas. Compas wordt door de beheerder zodanig ingericht dat de reguliere medewerkers alleen bij de persoonsgegevens terecht kunnen die daadwerkelijk nodig zijn voor het doel van verwerking. Van de overige cliëntdossiers of bevoegdheden wordt de medewerker uitgesloten. Hiermee wordt de dataminimalisatie gewaarborgd.

Naast Compas geeft de afdeling automatisering aan bij elk systeem de beveiliging te controleren. Ook zorgt deze afdeling met het instrument 'firewall' dat de middelen van het netwerk, systemen en de computers binnen Baanbrekers worden beschermd tegen misbruik.

Privacy impact assessment

De PIA is een instrument dat helpt de risico's te beheren van een project of bijzonder risicovolle verwerking van persoonsgegevens. Het is dus een instrument dat de privacy by design ondersteunt, zodat de privacyrisico's op een vroeg stadium worden herkend en vermeden.

Binnen Baanbrekers worden bijzondere persoonsgegevens verwerkt. Ongetwijfeld zullen deze gegevens deel uitmaken van sommige projecten die binnen de organisatie worden uitgevoerd. Dit valt dan onder een bijzonder risicovolle verwerking. De PIA zal dus moeten

worden gebruikt binnen Baanbrekers. In paragraaf 4.5 zijn de grondbeginselen opgenomen die gelden voor de PIA. Indien hier gebruik van wordt gemaakt zal de PIA het meest effectief zijn bij de uitvoering

van projecten. De risico's worden hiermee vroegtijdig herkend en kunnen dan ook op tijd worden aangepakt, zodat de risico's verminderd worden.

De opdrachtgevers, opdrachtnemers en FG zijn binnen Baanbrekers verantwoordelijk voor de uitvoering van de PIA. De AP kan een boete opleggen bij het niet uitvoeren van de PIA.

Functionaris van gegevensbescherming (ook wel privacyofficer)

De FG is een belangrijk persoon in een organisatie, omdat hij of zij betrokken wordt bij alle zaken die betrekking hebben op de bescherming van persoonsgegevens.¹²⁰ De FG is er voor de reguliere medewerkers, de betrokkene en de toezichthouder. Samenvattend bestaat het takenpakket van een FG uit het toezien op de naleving van de privacywetgeving en het privacybeleid dat geldt in de organisatie, waarvoor de FG werkzaam is.

Voor Baanbrekers is het verplicht om bij de inwerkingtreding van de AVG een FG in dienst te hebben, omdat Baanbrekers een publieke organisatie is. Daarnaast geeft de aard van de verwerking hiertoe aanleiding en wordt binnen Baanbrekers grootschalig bijzondere persoonsgegevens verwerkt. Binnen Baanbrekers is al bepaald dat de teamleider van de afdeling Interne Controle en de juriste de FG's zullen zijn. Binnen Baanbrekers wordt bewust een onderscheid gemaakt tussen privacy op beleidsmatig niveau en operationeel niveau. Privacy op beleidsmatig niveau is dat wat voor de interne organisatie gehanteerd wordt en is vastgelegd voor de kennisgeving en om bewustzijn te creëren bij de reguliere medewerkers. Operationeel niveau is dat wat ervoor zorgt dat wat is vastgelegd ook wordt toegepast. De teamleider van de afdeling interne controle gaat zich bezig houden met operationeel en de juriste op beleidsmatig niveau.

Privacybeleid

De AVG stelt in artikel 24 lid 2 AVG dat het uitvoeren van een privacybeleid verplicht is. Dit privacybeleid is een goed instrument om de privacy te kunnen waarborgen in een organisatie, omdat het voor kennisgeving en bewustzijn zorgt. De reguliere medewerkers van Baanbrekers zijn zich bewust van de noodzaak tot het opstellen van een intern beleid. Er wordt binnen Baanbrekers nog niet gewerkt aan dit beleid, maar uit onderzoek blijkt dat het voornemen om een privacybeleid op te stellen er wel is.¹²¹

6.4 Rechten van de betrokkene

Naast het recht van inzage, het recht van verzet en het recht van correctie introduceert de AVG het recht op beperking van de verwerking en het recht op dataportabiliteit. Deze rechten dienen, naast de rechten voortvloeiende uit de Wbp die ongewijzigd zijn in de AVG, opgenomen te worden in het nieuwe beleid. Daarnaast moeten er binnen Baanbrekers ook procedures zijn waarmee de betrokkene deze rechten zou kunnen uitoefenen. Baanbrekers moet het namelijk mogelijk maken voor de betrokkene om een verzoek, tot het uitoefenen van deze rechten, in te kunnen dienen.

¹²⁰ Informatie omtrent de FG is afgeleid uit het interview met de teamleider van de afdeling Interne Controle, opgenomen in bijlage 11.

¹²¹ Bijlage 10 Interview juriste

Hoofdstuk 7 Conclusie en aanbevelingen

Naar aanleiding van het onderzoek kunnen conclusies worden getrokken die in dit hoofdstuk zullen worden beschreven. De conclusies vloeien voort uit de toetsing van het privacybeleid en de wijze waarop Baanbrekers persoonsgegevens van sw-medewerkers verwerkt aan de eisen uit de Wbp en AVG. In dit hoofdstuk worden ook aanbevelingen gedaan, die gebaseerd zijn op de getrokken conclusies. De conclusies en aanbevelingen beantwoorden gezamenlijk de centrale vraag, die als volgt luidt: *“In hoeverre dient Baanbrekers hun huidige werkwijze met betrekking tot het verwerken van persoonsgegevens van de medewerkers uit de sociale werkvoorziening, die in dienst zijn bij Baanbrekers of via Baanbrekers werkzaam zijn bij externe werkgevers aan te passen, zodat deze in overeenstemming is met de Wet bescherming persoonsgegevens en Algemene Verordening Gegevensbescherming?”*

In het algemeen kan worden geconcludeerd dat Baanbrekers in haar huidige werkwijze op een aantal vlakken niet voldoet aan de eisen van de Wbp en AVG. Alhoewel de medewerkers van Baanbrekers zich bewust zijn van het belang van de privacywetgeving en dat er een privacybeleid is, zijn er toch onderdelen waarop Baanbrekers niet conform de wet handelt. Hierdoor voldoet Baanbrekers zowel voor de Wbp als de AVG niet aan het rechtmatigheidsbeginsel. Hieronder wordt in vijf paragrafen de conclusie nader uitgewerkt en worden aanbevelingen gedaan omtrent welke aanpassingen aan de huidige werkwijze moeten worden doorgevoerd om te kunnen voldoen aan de Wbp en AVG.

7.1 Conclusie en aanbevelingen over de eisen van verwerking van de Wbp

In dit onderzoek is geanalyseerd aan welke eisen Baanbrekers als verantwoordelijke nog moet voldoen voor een rechtmatige gegevensverwerking volgens de Wbp. De eisen van gegevensverwerking waar Baanbrekers nog niet aan voldoet zijn de bewaartermijn, fysieke beveiliging en het sluiten van een bewerkersovereenkomst met de bewerkers.

Bewaartermijn

De bepaling omtrent de bewaartermijn bepaalt dat persoonsgegevens niet langer worden bewaard dan noodzakelijk is voor de verwerkelijking van de doeleinden, tenzij de gegevens nodig zijn voor historische, statische of wetenschappelijke doeleinden.

Uit paragraaf 5.8 blijkt dat Baanbrekers persoonsgegevens die niet meer noodzakelijk zijn voor de doeleinden waarvoor de gegevens worden verzameld niet verwijderd. Indien de gegevens niet worden bewaard voor de historische, statische of wetenschappelijke doeleinden dient Baanbrekers de gegevens echter te verwijderen. De bepaling omtrent de bewaartermijn is opgenomen in het privacybeleid, maar deze wordt dus niet nageleefd. Aanbevolen wordt om medewerkers bewust te maken van deze bepaling en te waarborgen dat hier aan wordt voldaan. Het verwijderen dient zowel voor het fysieke als digitale dossier te gebeuren door de medewerkers van de afdeling personeelsadministratie. De teamleider van de afdeling P&O en de FG dienen toezicht te houden op de naleving van de bewaartermijn.

Beveiliging

In paragraaf 3.2 is vermeld dat de beveiliging bestaat uit de fysieke beveiliging en digitale beveiliging. Uit onderzoek blijkt dat Baanbrekers uitsluitend niet voldoet aan de eisen voor fysieke beveiliging. De fysieke beveiliging houdt in dat organisatorische beveiligingsmaatregelen genomen moeten worden, door de reguliere medewerkers die persoonsgegevens verwerken, voor de bescherming van deze gegevens.

Uit de audits die zijn vermeld in paragraaf 5.7 en het onderzoek dat is verricht voor dit rapport kan worden geconcludeerd dat in de praktijk niet voldoende maatregelen worden genomen om de beveiliging van persoonsgegevens te waarborgen. In het privacybeleid is, naast de bepalingen omtrent de beveiliging, een checklist opgenomen met voorbeelden van

de te nemen organisatorische beveiligingsmaatregelen om de privacybescherming te waarborgen.¹²² Het uitgangspunt van de checklist is dat de documenten waarin persoonsgegevens zijn verwerkt worden weggelegd in een afsluitbare en niet toegankelijke kast, lade of ruimte bij niet gebruik daarvan bij afwezigheid van degene die persoonsgegevens verwerkt. In de praktijk blijkt dat kantoren niet altijd op slot worden gedaan bij afwezigheid van de reguliere werknemers. Ook worden documenten niet altijd weggelegd in opbergruimtes die afsluitbaar zijn, waardoor deze eenvoudig toegankelijk zijn voor onbevoegden.

Een goede beveiliging is een onmisbaar aspect van de gegevensverwerking. Dit is niet alleen goed voor de naam van de organisatie, maar het geeft ook een gevoel van zekerheid en vertrouwen aan de betrokkenen. Het toont immers dat Baanbrekers het belangrijk vindt de persoonsgegevens van betrokkenen te beschermen. Het naleven van de fysieke beveiliging vraagt om bewustzijn, een actieve houding en discipline van de medewerkers.

Om aan de eis van een goede beveiliging te voldoen wordt ten eerste geadviseerd om de bevoegde medewerkers op de hoogte brengen over de eisen omtrent de beveiliging. Dit kan de manager of teamleider van de afdeling P&O doen door een kickoff meeting te organiseren waarbij het privacybeleid wordt toegelicht.

Ten tweede wordt aanbevolen een concrete procedure op te stellen met betrekking tot het toezicht op de naleving van de bepalingen omtrent de beveiliging. Het toezicht dient uitgevoerd te worden door de FG en een mystery guest. Uit onderzoek is gebleken dat Baanbrekers twee huidige medewerkers heeft aangewezen die bij de inwerkingtreding van de AVG in 2018 de functie van FG uit zullen oefenen.¹²³ De FG's zijn ingevolge hun takenpakket ook verantwoordelijk voor de toezicht op processen met betrekking tot de gegevensverwerking.¹²⁴ Zij moeten voorbereid worden op het houden van toezicht. De voorbereiding kan vormgegeven worden door in 2017 trainingen te volgen, zodat zij kennis op kunnen doen betreffende de beste wijze om toezicht uit te voeren. Verder dienen de FG's bij het daadwerkelijk uitvoeren van het toezicht de Plan Do Check Act cyclus toe te passen. Hiermee kunnen continu verbeteringen worden doorgevoerd in de werkwijze en leren de reguliere medewerkers op een snelle wijze de wet toe te passen.

Daarnaast dient een mystery guest in te worden geschakeld, zodat weer regelmatig audits worden gehouden. Een audit van een mystery geust zou door de aanwezigheid van de FG's, één keer in het jaar voldoende zijn. De audit zal het meest effectief zijn als het niet constant op een voorspelbaar moment wordt gehouden, maar elk jaar in een afwisselend periode. De resultaten dienen geëvalueerd te worden en door de manager meegedeeld te worden aan alle medewerkers die onder het onderzoek vallen. Daarnaast is het effectief om intern consequenties te verbinden aan de onrechtmatige verwerking van persoonsgegevens.

De bewerker en de bewerkersovereenkomst

Uit onderzoek blijkt dat Baanbrekers bewerkers heeft die voor het uitvoeren van hun diensten persoonsgegevens van de sw-medewerkers verwerken. Met deze partijen dient Baanbrekers een bewerkersovereenkomst te sluiten. Het inschakelen van een bewerker en het sluiten van een bewerkersovereenkomst met deze partij is echter niet geregeld in het privacybeleid. Uit onderzoek blijkt dat de reguliere medewerkers binnen Baanbrekers niet voldoende op de hoogte zijn van de omschrijving en functie van de bewerker en de eisen die de Wbp daaraan verbindt. Om die reden is er ook geen bewerkersovereenkomst gesloten met deze partijen. Baanbrekers heeft wel een overeenkomst gesloten met de bewerkers voor het leveren van diensten, maar de inhoud van deze overeenkomsten komt niet overeen met de eisen die de Wbp stelt aan de inhoud van een bewerkersovereenkomst. Uit de eisen die

¹²² Zie paragraaf 5.7

¹²³ Zie paragraaf 4.5 voor een nadere beschrijving hierover

¹²⁴ Hierover is meer te lezen in paragraaf 4.5

zijn opgenoemd in paragraaf 4.4 voldoen de huidige overeenkomsten nog niet aan de volgende voorwaarden:

- De verplichtingen moeten over en weer duidelijk zijn vastgelegd in de overeenkomst. Het soort gegevens, de doeleinden van de verwerking, de duur van de opslag en beveiligingsmaatregelen moeten gedetailleerd worden opgenomen.
- In de overeenkomst moet staan hoe de verantwoordelijke kan toezien op de naleving van de waarborgen.

Om te voldoen aan de eisen van de Wbp dient Baanbrekers allereerst in het privacybeleid vast te stellen wie een bewerker is en welke eisen de wet aan de verhouding tussen de verantwoordelijke en bewerker verbindt. Dit is van belang, omdat uit onderzoek blijkt dat de meeste medewerkers niet bekend waren met de termen “bewerker” en “bewerkerovereenkomst”. Daarnaast dient de teamleider van de afdeling P&O een bewerkersovereenkomst te sluiten met de bewerkers, waarbij alle eisen die verbonden zijn aan de inhoud van deze overeenkomst worden opgenomen. De teamleider kan er voor kiezen om een overeenkomst op te stellen waarbij alle eisen van de Wbp en de aanvullende eisen uit de toekomstige AVG worden opgenomen. Dit voorkomt dubbel werk en is meteen een goede voorbereiding op de inwerkingtreding van de AVG. Over de aanvullende eisen is meer te lezen in paragraaf 7.4.

7.2 Conclusie en aanbevelingen over de overige verplichtingen van de verantwoordelijke uit de Wbp

Naast de eisen die in paragraaf 7.1 zijn beschreven, voldoet Baanbrekers niet volledig aan de overige verplichtingen van de verantwoordelijke. Hieronder wordt toegelicht in welke onderdelen de tekortkomingen zich bevinden.

Informatieplicht

De informatieplicht houdt in dat Baanbrekers de sw-medewerkers moet informeren over:

- welke gegevens zij gebruiken en met welk doel;
- hun identiteit (naam en adres van de organisatie);
- of zij de gegevens aan andere organisaties verstrekken.

Uit onderzoek blijkt dat persoonsgegevens zowel verkregen worden van de betrokkene als van derden. De tekortkoming in de informatieplicht bevindt zich in het aangeven van het doel van verzameling van de gegevens en welk soort persoonsgegevens daarvoor nodig zijn. Men gaat er doorgaans van uit dat de betrokkene op de hoogte is van de informatie met betrekking tot de gegevensverwerking. Als dat niet het geval is, dan wordt binnen Baanbrekers verwacht dat de betrokkene uit zichzelf naar deze informatie vraagt. De informatieplicht stelt echter dat de verantwoordelijke op eigen initiatief vóór het moment van verkrijging volledig dient te voldoen aan de informatieplicht. Ingeval van gegevensverzameling via derden wordt bovendien niet aangegeven om welke persoonsgegevens het gaat en voor welk doel persoonsgegevens worden verzameld.

Het niet voldoen aan de informatieplicht heeft als gevolg dat ook niet voldaan wordt aan het transparantiebeginsel. Het transparantiebeginsel bestaat uit het recht van inzage van de betrokkene en de informatieplicht van de verantwoordelijke.

Voor de informatieplicht wordt aanbevolen de betreffende medewerkers allereerst bewust te maken van het belang om vooraf op eigen initiatief de volledige informatie te verstrekken aan de betrokkene. De verstrekking van informatie dient op een schriftelijke wijze te gebeuren, zodat aan de toezichthouder getoond kan worden dat aan de informatieplicht wordt voldaan.

Uit onderzoek blijkt dat de teamleider van de afdeling P&O van plan is om bij het aannemen van een nieuwe medewerker een usb-stick mee te geven, waarop alle belangrijke informatie met betrekking tot het dienstverband is opgeslagen. De medewerker kan de usb-stick

meenemen naar huis, om dit op gemak door te lezen. De reguliere medewerkers houden hiervoor een checklist bij om na te gaan of zij de medewerker hebben geïnformeerd over alle belangrijke zaken. Aan de teamleider wordt aanbevolen om de informatieplicht onderdeel te maken van de aannamesprocedure. Doordat de medewerker de informatie naar huis kan meenemen, stelt Baanbrekers op eigen initiatief de informatie ter beschikking van de medewerker. De medewerkers zullen voortaan een checklist gebruiken bij de aannamesprocedure. Op deze checklist dient de informatieplicht omtrent de gegevensverwerking opgenomen te worden. Met terugwerkende kracht dient aan het personeel dat al in dienst is een brief of folder te worden verstrekt waarin zij worden geïnformeerd over de wijze waarop Baanbrekers hun gegevens verwerkt.

7.3 Conclusie en aanbevelingen over het privacybeleid

Baanbrekers heeft een privacybeleid dat binnen de organisatie wordt aangeduid als het 'Privacyreglement personeelsregistratie'. Ondanks de aanwezigheid van het privacybeleid wordt deze niet optimaal gebruikt. Dit komt allereerst omdat blijkt dat niet alle medewerkers op de hoogte zijn gebracht van het beleid. Daarnaast zijn er ook medewerkers die wel van het bestaan afweten, maar er geen gebruik van maken. Het privacybeleid dateert uit 2004 en is nooit geactualiseerd, waardoor wijzigingen zoals de meldplicht datalekken, de uitgebreide boetebevoegdheid en nieuwe termen niet zijn opgenomen in het beleid.

Het privacybeleid dient tot het creëren van bewustzijn bij de reguliere medewerkers, zodat de privacy van gegevensverwerking wordt gewaarborgd. Naar aanleiding van de bevindingen heeft Baanbrekers twee opties met betrekking tot het wijzigen van het privacybeleid. Aangezien de Wbp nog anderhalf jaar geldt, voordat deze vervangen wordt door de AVG, kan de juriste het privacybeleid allereerst actualiseren. Hierdoor zal het privacybeleid de juiste informatie weergeven en wordt de rechtsgeldige informatie verstrekt. Daarna dient de juriste dit privacybeleid onder de aandacht te brengen van de reguliere medewerkers. Dit kan digitaal, maar dit heeft als nadeel dat mensen er mogelijk overheen zullen lezen of dat zij er niet voldoende aandacht aan zullen besteden. Een voorlichting in de vorm van een presentatie is dus een betere optie.

Bij het actualiseren van het privacybeleid gaat het echter niet om een grote hoeveelheid aan wijzigingen. Baanbrekers dient daarom te overwegen of het thans nut heeft om het privacybeleid te actualiseren aan de hand van de Wbp. Dit kan namelijk toch tijdrovend zijn, terwijl ook aandacht besteed dient te worden aan het opstellen van een geheel nieuw privacybeleid ten opzichte van de AVG. Een tweede optie is daarom om het privacybeleid direct te laten voldoen aan de eisen van de AVG. Zie hierover meer in paragraaf 7.5. Kiest Baanbrekers voor deze optie, dan dient de juriste allereerst te waarborgen dat de reguliere medewerkers van het bestaan van het huidige privacybeleid afweten. Daarna dient de juriste te toetsen in hoeverre de medewerkers daadwerkelijk op de hoogte zijn van de doorgevoerde wijzigingen, waarvan zij hen digitaal van op de hoogte heeft gesteld. Zij kan hiermee de medewerkers indien nodig bijscholen over de wijzigingen en nadere toelichting geven over het beleid.

7.4 Conclusies en aanbevelingen over de verplichtingen van de verantwoordelijke uit de AVG

Uit de toetsing aan de AVG is gebleken dat Baanbrekers allereerst niet voldoet aan de documentatieplicht en informatieplicht, waardoor de organisatie niet voldoet aan het transparantie- en verantwoordingsbeginsel ingevolge de uitwerking van de beginselen in paragraaf 4.3. Verder voldoet Baanbrekers ook niet aan eisen omtrent de bewerkersovereenkomst, de PIA, het privacybeleid en de rechten van de betrokkenen.

Documentatieplicht

De AVG bepaalt dat in de documentatieplicht informatie moet worden opgenomen met betrekking tot de naam en de contactgegevens van de organisatie en de FG, het doel van de gegevensverwerking, de beschrijving van de betrokkenen, de ontvangers, de termijn waarbinnen de gegevens worden gewist, indien mogelijk een beschrijving van de technische en organisatorische beveiligingsmaatregelen en tot slot informatie over of de gegevens worden verstrekt aan derde landen.

Uit onderzoek blijkt dat Baanbrekers nog geen documentatie heeft waarin het bovengenoemde is geregistreerd. Baanbrekers heeft in het kader van de eisen van de Wbp wel een algemene melding gedaan van de gegevensverwerking bij de AP. Deze melding vormt een basisdocument voor de documentatieplicht. In paragraaf 6.3 is vermeld dat een FG verplicht is voor Baanbrekers, omdat het een publieke organisatie is. De naam en contactgegevens van deze FG moeten dus worden vermeld in de documentatieplicht. Verder kan ingevolge paragraaf 4.3 vermeld worden dat de persoonsgegevens tien jaren na het einde van het dienstverband worden verwijderd. Tot slot dient de verantwoordelijke een algemene beschrijving te geven van de beveiligingsmaatregelen, zoals beschreven in paragraaf 4.7.

Informatieplicht

De informatieplicht van de Wbp wordt in de AVG overgenomen en versterkt door de volgende aanvullende eisen:

- De contactgegevens van de FG;
- De ontvangers van de persoonsgegevens;
- De termijn van opslag van de persoonsgegevens;
- De rechten van de betrokkene;
- Het belang van de persoonsgegevens voor het uitvoeren van een wettelijke plicht en het belang daarvan.

In paragraaf 7.2 is geconcludeerd dat binnen Baanbrekers niet wordt voldaan aan de informatieplicht van de Wbp. Dit houdt in dat ook nog niet wordt voldaan aan de aanvullende eisen die de AVG stelt. Deze eisen dienen allereerst in het nieuwe privacybeleid te worden verwerkt. In het privacybeleid moet nadruk worden gelegd op het feit dat de reguliere medewerkers op eigen initiatief dienen te voldoen aan de informatieverschaffing. Aanvullend op het advies dat omtrent de informatieplicht is gegeven in paragraaf 7.2, dient Baanbrekers de aanvullende eisen te verwerken in de informatie op de usb-stick en in de checklist, zodat de medewerkers niet weer het risico lopen niet te voldoen aan de informatieplicht. Tot slot dient de teamleider van de afdeling P&O samen met de FG's toezicht te houden op de volledige naleving van deze verplichting.

Bewerkersovereenkomst

De AVG stelt ook aanvullende eisen aan de bewerkersovereenkomst. In het standaard concept bewerkersovereenkomst van Baanbrekers zijn de volgende eisen van de AVG nog niet opgenomen:

- De bewerker dient vooraf toestemming te vragen aan de verantwoordelijke bij het inschakelen van subbewerkers;
- De bewerker dient na afloop van de dienstverlening de persoonsgegevens te verwijderen of terug te geven;
- De bewerker werkt mee aan audits en houdt hij of zij zich aan de registratieplicht.

De hierboven genoemde eisen dienen dus door de teamleider van de afdeling P&O opgenomen te worden in de bewerkersovereenkomst om te kunnen voldoen aan de AVG. Daarnaast dienen alle eisen die zijn opgenoemd in paragraaf 6.2, door de juriste opgenomen te worden in het privacybeleid. Door opname in het privacybeleid kan ten alle tijden worden gecontroleerd of aan alle eisen wordt voldaan.

7.5 Conclusies en aanbevelingen omtrent de privacymaatregelen uit de AVG

Privacy impact assessment

Het instrument PIA is bedoeld om privacy risico's in een vroege stadium in beeld te hebben bij het verwerken van bijzondere persoonsgegevens. Met dit instrument kunnen risico's die verbonden zijn aan projecten, waarbij gegevensverwerking plaatsvindt, vroegtijdig bekend worden gemaakt en vermeden worden.

Bij Baanbrekers komen projecten voor waarbij bijzondere persoonsgegevens verwerkt worden. Bij de inwerkingtreding van de AVG moet dus door middel van de PIA bij elk project worden geanalyseerd welke privacyrisico's kunnen voorkomen bij het uitvoeren van het project. Binnen Baanbrekers zijn onder meer de opdrachtgever(s), de verantwoordelijke van het project en de FG verantwoordelijk voor de PIA. Om er zeker van te zijn dat wordt voldaan aan de PIA, zijn in de bijlage van dit rapport principes opgenomen die bij een PIA in acht moeten worden genomen.¹²⁵ Deze kan in het privacybeleid worden toegevoegd bij de toelichting van de PIA.

Privacybeleid

In de AVG is de verantwoordelijke verplicht een intern privacybeleid op te stellen. In een privacybeleid worden de hoofdbeginselen uit de AVG, die ruim zijn geformuleerd, toegepast op concrete situaties die voorkomen in de organisatie. Hierdoor wordt duidelijk wanneer, voor wie en waarom de beginselen van de AVG van toepassing zijn.

Baanbrekers is van plan in 2017 een nieuw privacybeleid op te stellen voor de inwerkingtreding van de AVG. Aanbevolen wordt om aan het begin van 2017 aandacht te besteden aan het maken van een conceptprivacybeleid. Het gedeelte dat in dit rapport betrekking heeft op de AVG, kan dienen als leidraad bij het opstellen van het nieuwe privacybeleid. Als gevolg hiervan zou op een eenvoudige en minder tijdrovende wijze een nieuw privacybeleid kunnen worden opgesteld. Het privacybeleid dient op een zodanige manier te zijn opgesteld dat het duidelijk is, de medewerkers informeert en bewust maakt van het belang van de waarborging van de privacy.

Rechten van de betrokkenen

De nieuwe rechten die de AVG introduceert zijn het recht op beperking van de verwerking en het recht op dataportabiliteit. In het privacybeleid dient de juriste op te nemen wat deze rechten inhouden, wanneer het kan worden ingediend en door wie. Daarnaast dienen deze rechten op een begrijpelijke manier uitgelegd te worden aan de reguliere medewerkers. Tot slot moet in het privacybeleid worden opgenomen op welke manier Baanbrekers het mogelijk maakt voor de betrokkene om een verzoek tot gebruikmaking van deze rechten in te dienen.

¹²⁵ Bijlage 15 Principes PIA

Bronnen- en literatuurlijst

Artikelen

‘Bedrijven houden lekken vaak voor zich’ 28 december 2016, *NRC*, www.nrc.nl (zoek op *Autoriteit Persoonsgegevens*), laatst geraadpleegd op 6 januari 2017.

Boeken

Hooghiemstra & Nouwt 2012

T.F.M. Hooghiemstra & J. Nouwt, *Tekst en toelichting Wet bescherming persoonsgegevens*, Den Haag: Sdu 2012.

Huydecoper 2006

S.M. Huydecoper, *Wet bescherming en persoonsgegevens en ICT*, Sdu Uitgevers 2006.

Kranenborg & Verhey 2011

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

Thole, Van der Jagt & Roerdink 2010

E. Thole, F van der Jagt & H. Roerdink, *50 vragen over privacy*, Deventer: Kluwer 2010.

Van Schaaijk 2011

G.A.F.M. van Schaaijk, *Praktijkgericht juridisch onderzoek*, Den Haag: Boom Juridische uitgevers 2011.

Elektrische bronnen

‘Algemeen noodzakelijke kosten van het bestaan’, www.krimpenaandenijssel.nl (zoek op *noodzakelijke bestaanskosten*).

‘AP eist betere afspraken over digitaliseren patiëntdossiers’, www.autoriteitpersoonsgegevens.nl (zoek op *eisen bewerkersovereenkomst*).

‘Bewaren van persoonsgegevens’, Autoriteit Persoonsgegevens, www.autoriteitpersoonsgegevens.nl (zoek op *persoonsgegevens niet meer nodig*).

‘CBP krijgt boetebevoegdheid en wordt Autoriteit Persoonsgegevens’, www.autoriteitpersoonsgegevens.nl (zoek op *boetebevoegdheid Autoriteit Persoonsgegevens*).

‘De Algemene verordening gegevensbescherming’, www.openaccessadvocate.nl (zoek op *algemene verordening gegevensbescherming*).

‘Functionaris van gegevensbescherming’, www.privacycompany.eu (zoek op *functionaris van gegevensbescherming*).

‘Meldplicht datalekken’, www.autoriteitpersoonsgegevens.nl (zoek op *meldplicht datalekken*).

‘Naslag artikel 6 Wbp’, www.autoriteitpersoonsgegevens.nl (zoek op *artikel 6*).

‘Naslag artikel 8 Wbp’, www.autoriteitpersoonsgegevens.nl (zoek op *artikel 8*).

'Naslag artikel 10 Wbp', www.autoriteitpersoonsgegevens.nl (zoek op *artikel 10*).

'Naslag artikel 13 Wbp', www.autoriteitpersoonsgegevens.nl (zoek op *artikel 13*).

'Naslag artikel 14 Wbp', www.autoriteitpersoonsgegevens.nl (zoek op *artikel 14*).

'Naslag artikel 33 en 34 Wbp', www.autoriteitpersoonsgegevens.nl (zoek op *eisen informatieplicht*).

'Privacystatement', Baanbrekers, www.baanbrekers.org/ (zoek op *privacy*).

'Privacy impact assessment (PIA)', www.autoriteitpersoonsgegevens.nl (zoek op *privacy impact assessment*).

'Recht op dataportabiliteit: een utopie?', www.ejure.nl (zoek op *dataportabiliteit AVG*).

'Wat doen wij', Baanbrekers, www.baanbrekers.org/ (zoek op *wat doen wij?*).

'Wat is compas', www.emergo-systems.nl (zoek op *Compassysteem*).

'Wat is een verwerking als in de Wbp?', www.lexx-it.nl (zoek op *rechtvaardigingsgronden Wbp*).

'Wat zijn persoonsgegevens', www.autoriteitpersoonsgegevens.nl (zoek op *Wet bescherming persoonsgegevens*).

'Wie zijn wij', www.baanbrekers.org/ (zoek op *wie zijn wij?*).

www.rijksoverheid.nl

Handleiding en rapporten

Sauerwein & Linnemann 2002

L.B. Sauerwein & J.J. Linnemann, Handleiding voor verwerkers van persoonsgegevens, Den Haag: Ministerie van Justitie 2002.

König & Karssenberg 2015

drs. E. König & W. Karssenberg, Privacy Impact Assessment (PIA), Amsterdam: NOREA Kennisgroep Privacy 2015.

Jurisprudentie

Rechtbank Maastricht 05 december 2003, ECLI:NL:RBMAA:2003:AO0044.

Hoge Raad 09 september 2011, ECLI:NL:HR:2011:BQ8097.

Parlementaire stukken

Kamerstukken II 2003-2004, 29 275, nr. 3, Memorie van Toelichting verlenging Wet SAMEN

Kamerstukken II 1997-1998, 25 892, nr. 3, Memorie van Toelichting Wbp

Tijdschriften

Nederlands Juristenblad 2015

Stb. 2015, 230 Meldplicht datalekken, Nederlands Juristenblad 2015.

Rechtsbronnen

Algemene Verordening Gegevensbescherming

Algemeen wet bestuursrecht

Burgerlijk Wetboek
De Wet persoonsregistratie
Grondwet
Europees Verdrag tot bescherming van de Rechten van de Mens en de Fundamentele
Vrijheden
Internationaal Verdrag inzake burgerrechten en politieke rechten
Participatiewet
Universele Verklaring van de Rechten van de Mens
Wet algemene bepalingen burgerservicenummer
Wet bescherming persoonsgegevens