

Een schitterend privacybeleid

De ontwikkeling van een passend privacybeleid voor de
Diamant-groep



Annelies de Hullu

In opdracht van: De Diamant-groep

Tilburg, januari 2011

Een schitterend privacybeleid

De ontwikkeling van een passend privacybeleid voor de
Diamant-groep

Naam:	Annelies de Hullu
Studentnummer:	9962759
Opleiding:	Juridische Hogeschool Avans-Fontys
Locatie opleiding:	Tilburg
Stageverlener:	Diamant-groep Tilburg
Afstudeermentor:	Mr. C.J.M.M. de Beer
Eerste afstudeerdocent:	Mr. B. Kratsborn
Tweede afstudeerdocent:	Mr. M. Soysüren
Afstudeerperiode:	19 april 2010 tot 10 januari 2011

Tilburg, 10 januari 2011

Voorwoord

In het kader van mijn afstudeerstage van de opleiding HBO-Rechten aan de Juridische Hogeschool Avans-Fontys, heb ik stage gelopen op de afdeling juridische zaken van de Diamant-groep. Gedurende mijn afstudeerstage heb ik in opdracht van de Diamant-groep onderzoek gedaan op het gebied van de privacywetgeving. De doelstelling van het onderzoek is een nieuw privacyreglement op te stellen, dat binnen beide organisaties geïmplementeerd kan worden. Om uiteindelijk een passend privacyreglement op te kunnen stellen, was kennis omtrent de huidige wijze van gegevensverwerking noodzakelijk. Ik heb deze kennis verworven door het verspreiden van vragenlijsten onder de medewerkers en door de resultaten vervolgens te analyseren aan de hand van de normen uit de Wet bescherming persoonsgegevens (hierna: Wbp). Hierdoor is een duidelijk beeld van de organisatie ontstaan, dat bruikbare informatie opleverde voor de ontwikkeling van het nieuwe privacybeleid. Het onderzoek heeft plaatsgevonden in de periode van 19 april 2010 tot 10 januari 2011.

Hierbij wil ik ook een aantal mensen bedanken voor hun inbreng, kritische blik en ondersteuning tijdens het gehele proces. In de eerste plaats mijn begeleider binnen de Diamant-groep, mr. Cees de Beer. Een woord van dank gaat ook uit naar mijn andere collega's op de afdeling juridische zaken, te weten mw. Pauline Scheffers en dhr. Hans Palmen. Ook zij hebben een belangrijke bijdrage aan mijn scriptie geleverd. Mw. Anouk Snoeren, collega en personeelsadviseur binnen 18k, wil ik bedanken voor haar kritische blik en eerlijkheid met betrekking tot de vragenlijsten. Door haar feedback is de vragenlijst aanzienlijk gewijzigd voordat deze verspreid werd onder de medewerkers.

Tevens wil ik mijn eerste scriptiebegeleider, mr. Bram Kratsborn, vanuit de Juridische Hogeschool graag bedanken. Hij heeft met een positief kritische blik naar mijn scriptie gekeken en indien noodzakelijk, daarbij kanttekeningen geplaatst. Daarnaast diende hij regelmatig als sparringpartner met betrekking tot inhoudelijke vraagstukken.

Tot slot bedank ik mijn ouders voor hun geloof in mij en mijn kunnen. Zij zijn mijn stimulans om elke dag het beste uit mezelf te halen en daar helemaal voor te gaan.

Om misverstanden te voorkomen dient overal in dit rapport waar gesproken wordt over de Diamant-groep, ook 18k gelezen te worden. Als een bepaling slechts van toepassing is op één van beide organisaties, wordt dit specifiek aangegeven. Overal waar gesproken wordt over 'hij' en 'medewerker', wordt tevens 'zij' en 'medewerkster' bedoeld.

Annelies de Hullu

Tilburg, januari 2011

Inhoudsopgave

VOORWOORD

LIJST VAN AFKORTINGEN

BEGRIPPENLIJST

SAMENVATTING

1. INLEIDING	9
§ 1.1 PROBLEEMBESCHRIJVING	10
§ 1.2 DOEL- EN VRAAGSTELLING.....	11
§ 1.3 BEPERKINGEN	11
§ 1.4 ONDERZOEKSMETHODIEK	12
§ 1.4.1 <i>Literatuur- en empirisch onderzoek</i>	12
§ 1.4.2 <i>Betrouwbaarheid en validiteit</i>	12
§ 1.5 OPBOUW VAN HET RAPPORT	13
2. ORGANISATIEBESCHRIJVINGEN.....	14
§ 2.1 DE DIAMANT-GROEP	14
§ 2.2 18K	14
§ 2.3 DE RELATIE TUSSEN DE DIAMANT-GROEP EN 18K	15
3. DE WET BESCHERMING PERSOONSGEGEVENS	16
§ 3.1 BREED WETTELIJK KADER OP INTERNATIONAAL NIVEAU	16
§ 3.2 WETTELIJK KADER OP NATIONAAL NIVEAU	16
§ 3.3 DE REIKWIJDTE VAN DE WBP	17
§ 3.4 VOORWAARDEN VOOR DE VERWERKING VAN PERSOONSGEGEVENS	17
§ 3.4.1 <i>Algemene beginselen betreffende de gegevensverwerking</i>	18
§ 3.4.2 <i>Gronden voor gegevensverwerking</i>	19
§ 3.5 DE VERWERKING VAN BIJZONDERE PERSOONSGEGEVENS	20
§ 3.5.1 <i>Ontheffing van het verbod om bijzondere persoonsgegevens te verwerken</i>	20
§ 3.5.2 <i>Algemene uitzonderingen om persoonsgegevens te verwerken</i>	21
§ 3.5.3 <i>Het burgerservicenummer</i>	22
§ 3.6 DE VERPLICHTINGEN VAN DE VERANTWOORDELIJKE.....	23
§ 3.6.1 <i>Geheimhoudingsplicht</i>	23
§ 3.6.2 <i>Beveiliging</i>	23
§ 3.6.3 <i>Bewaring</i>	24
§ 3.6.4 <i>Meldingsplicht</i>	24
§ 3.6.5 <i>Informatieplicht</i>	24
§ 3.7 RECHTEN VAN DE BETROKKENE	26
§ 3.7.1 <i>Inzage</i>	26
§ 3.7.2 <i>Correctie</i>	26
§ 3.7.3 <i>Verzet</i>	26
§ 3.8 RECHTSBESCHERMING	27
§ 3.8.1 <i>Bezwaar</i>	27
§ 3.8.2 <i>Schadevergoeding</i>	27
§ 3.8.3 <i>Verbod</i>	27
4. HET COLLEGE BESCHERMING PERSOONSGEGEVENS	28
§ 4.1 HET CBP EN DE TAKEN VAN DIT ORGAAN	28
§ 4.2 MELDINGSPROCEDURE.....	28
§ 4.2.1 <i>De melding en vrijstelling van melding</i>	28
§ 4.2.2 <i>Voorafgaand onderzoek</i>	29
§ 4.3 DE FUNCTIONARIS VOOR DE GEGEVENS BESCHERMING	29
§ 4.4 DE PRIVACY OFFICER	30

§ 4.5 SANCTIES.....	30
§ 4.5.1 Bestuursdwang en last onder dwangsom.....	30
§ 4.5.2 Bestuurlijke boete	31
§ 4.5.3 Strafrechtelijke sancties.....	31
5. PRIVACY BINNEN DE DIAMANT-GROEP	32
5.1 PERSOONSDOSSIER EN COMPAS	32
§ 5.1.1 Persoonsdossiers	32
§ 5.1.2 Compas.....	33
§ 5.2 DE BEKENDHEID MET DE WBP	34
§ 5.3 WELKE PERSOONSgegevens WORDEN VERWERKT EN IS DIT WETTELIJK TOEGESTAAN?	35
§ 5.3.1 De verwerking van algemene persoonsgegevens	35
§ 5.3.2 De verwerking van bijzondere persoonsgegevens	36
§ 5.3.2.1 Gezondheidsgegevens	36
§ 5.3.2.2 Strafrechtelijke gegevens.....	39
§ 5.3.2.3 Gegevens omtrent ras of etniciteit.....	40
§ 5.3.2.4 Overige bijzondere persoonsgegevens.....	42
§ 5.3.3 De toereikendheid van de huidige autorisaties	42
§ 5.3.4 De verwerkingshandelingen.....	43
§ 5.4 DE GRONDSLAG OM GEGEVENS TE VERWERKEN	43
§ 5.5 VAN WIE WORDEN ER PERSOONSgegevens VERWERKT?.....	44
§ 5.6 INTERNE EN EXTERNE VERSTREKKING VAN PERSOONSgegevens	45
§ 5.7 DE WIJZE WAAROP DE PERSOONSgegevens WORDEN VERWERKT	46
§ 5.8 DE DOELEINDEN VAN DE VERWERKING	46
§ 5.9 DE TOEREIKENDHEID VAN DE HUIDIGE BESCHERMINGSMAATREGELEN	47
§ 5.9.1 Beveiliging.....	47
§ 5.9.2 Bewaring	49
§ 5.9.3 Informatieverstrekking aan nieuwe medewerkers.....	49
§ 5.10 DE VERPLICHTINGEN VAN DE VERANTWOORDELIJKE.....	50
§ 5.11 DE RECHTEN VAN BETROKKENEN	50
§ 5.12 HET MELDEN VAN GEGEVENSVERWERKINGEN BIJ HET CBP EN HET VOORAFGAAND ONDERZOEK	51
§ 5.13 HET BELANG VAN EEN PRIVACYREGLEMENT.....	52
CONCLUSIE	53
AANBEVELINGEN	57
EVALUATIE	
LITERATUURLIJST	

Lijst van afkortingen

18k	De B.V. 18k
art.	Artikel
Awb	Algemene wet bestuursrecht
BSN	burgerservicenummer
CBP	College bescherming persoonsgegevens
EHRM	Europees Hof voor de Rechten van de Mens
EU	Europese Unie
EVRM	Europees Verdrag tot Bescherming van de Rechten van de Mens en de Fundamentele Vrijheden
FG	Functionaris voor de gegevensbescherming
Gw	Grondwet
IOP	Individueel Ontwikkelingsplan
IVBP	Internationaal Verdraag inzake Burgerrechten en Politieke rechten
NAW	naam, adres, woonplaats
OR	Ondernemingsraad
Sw	Sociale Werkvoorziening
UVRM	Universele Verklaring van de Rechten van de Mens
UWV	Uitvoeringsinstituut Werknemersverzekeringen
Vb	Vrijstellingsbesluit
VN	Verenigde Naties
Wabb	Wet algemene bepalingen burgerservicenummer
Wbp	Wet bescherming persoonsgegevens
WOR	Wet op de Ondernemingsraden
WPR	Wet persoonsregistraties
Wsw	Wet sociale werkvoorziening
WVP	Wet verbetering Poortwachter
WWB	Wet Werk en Bijstand

Begrippenlijst Wbp

Persoonsgegevens - In artikel (hierna: art.) 1 sub a Wbp wordt een persoonsgegeven gedefinieerd als elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Wil er sprake zijn van een persoonsgegeven, dient de identiteit van de persoon aan de hand van het gegeven redelijkerwijs, zonder onevenredige inspanning vastgesteld te kunnen worden. Gegevens over rechtspersonen vallen in principe niet onder de Wbp, met uitzondering van de gegevens over contactpersonen binnen deze ondernemingen.

Een gegeven verschaft informatie over een natuurlijk persoon indien het:

- feitelijke informatie over een persoon geeft. Bijvoorbeeld naam, geboortedatum of geslacht;
- een waardering over een bepaalde persoon geeft. Bijvoorbeeld het IQ;
- medebepalend is voor de wijze waarop de betrokken persoon wordt beoordeeld of behandeld in het maatschappelijke verkeer;
- een neerslag vormt van een beslissing die over een bepaalde persoon is genomen;
- betrekking heeft op een product of proces, maar indirect informatie verschaft over een bepaald persoon. Bijvoorbeeld als met de gegevens de arbeidsproductiviteit van een werknemer in kaart kan worden gebracht;
- uitsluitend voorwerpen aanduidt, die personen in hun maatschappelijke positie kunnen raken.¹

Er is sprake van identificeerbaarheid als de gegevens alleen of in combinatie met andere gegevens, zo kenmerkend zijn voor een bepaalde persoon dat deze direct of indirect kan worden geïdentificeerd. Met direct identificerende gegevens wordt bijvoorbeeld de combinatie van naam, adres, woonplaats (hierna: NAW) en geboortedatum bedoeld. Deze combinatie is dermate uniek en kenmerkend dat identificatie eenvoudig kan plaatsvinden. Indirect identificerende gegevens zijn gegevens die zijn ontdaan van de naam, maar door een combinatie met andere gegevens weer kunnen worden teruggebracht tot een bepaalde persoon, die op deze wijze kan worden geïdentificeerd. Dit zijn bijvoorbeeld gegevens als leeftijd, woonplaats, beroep en burgerservicenummer (hierna: BSN). Ook een telefoonnummer, het kenteken en inkomen zijn persoonsgegevens.

Verwerken - Art. 1 sub b Wbp omschrijft verwerken als elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens. Het begrip 'verwerken' omvat dus iedere technische verwerkings- of gebruikshandeling met betrekking tot persoonsgegevens. Wil er echter sprake zijn van een verwerking, dan dient degene die de verwerkingshandeling uitvoert enige feitelijk macht over de persoonsgegevens te kunnen uitoefenen. Of dit ook daadwerkelijk gebeurt is niet relevant.²

Bestand - Een bestand is op grond van art. 1 sub c Wbp elk gestructureerd geheel van persoonsgegevens dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen. Kort gezegd betekent dit dat de gegevens onderlinge samenhang moeten vertonen en dat het systeem systematisch toegankelijk moet zijn. Het begrip 'bestand' is van belang als criterium voor de afbakening van de reikwijdte van de Wbp (zoals bepaald in art. 2 lid 1 Wbp). Een bestand kan zowel geautomatiseerde als handmatige verwerkingen bevatten. Wat betreft de handmatige verwerkingen vallen alleen **bestanden** onder het toepassingsbereik van de Wbp.³

¹ Hooghiemstra & Nouwt 2007, p. 34-35; Sauerwein & Linnemann 2002, p. 12-13.

² Berkvens & Prins 2007, p. 30-31.

³ Hooghiemstra & Nouwt 2007, p. 37.

Een ongestructureerd personeelsdossier valt dus niet onder de reikwijdte van de Wbp, maar een op enigerlei wijze gesystematiseerde verzameling van personeelsdossier in een dossierkast wel.⁴

Verantwoordelijke - Conform art. 1 sub d Wbp is de verantwoordelijke degene die het doel en de middelen van de verwerking vaststelt. De verantwoordelijke kan een natuurlijke persoon, rechtspersoon, bestuursorgaan, of ieder ander zijn. De feitelijke uitvoering kan gedelegeerd of gemandateerd worden aan anderen.⁵

Bewerker - De bewerker wordt in art. 1 sub e Wbp geduid als degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen. De bewerker is een buiten de organisatie van de verantwoordelijke staande persoon.⁶ De dienstverlening van de bewerker moet gericht zijn op het uitvoeren van een bepaalde verwerking van persoonsgegevens ten behoeve van de opdrachtgever. De bewerker heeft geen zeggenschap over de gegevensverwerking, maar handelt naar de instructies en onder verantwoordelijkheid van de verantwoordelijke.⁷

Betrokkene - De betrokkene is volgens art. 1 sub f Wbp degene van wie de persoonsgegevens worden verwerkt.

Derde - Conform art. 1 sub g Wbp is de derde iedereen die gemachtigd is om persoonsgegevens te verwerken, niet zijnde de betrokkene, de verantwoordelijke, de bewerker of een persoon die rechtstreeks onder het gezag van de verantwoordelijke of de bewerker valt. Een derde heeft geen gezagsverhouding of contractuele relatie met de betrokkene.⁸

Ontvanger - De ontvanger is conform art. 1 sub h Wbp degene aan wie de persoonsgegevens worden verstrekt. Dit kan zowel een intern als extern persoon zijn. Een intern persoon is bijvoorbeeld een andere medewerker binnen de Diamant-groep of 18k, waaraan gegevens worden verstrekt. Een extern persoon is bijvoorbeeld het Uitvoeringsinstituut Werknemersverzekeringen (hierna: UWV), hulpverlenende instanties of de gemeente.

Overige begrippen

Payrolling - Bij payrolling worden medewerkers door 18k ter beschikking gesteld aan een opdrachtgever om arbeid te verrichten. De opdracht is gesloten tussen 18k en de opdrachtgever. De werkzaamheden worden onder het toezicht en leiding van de opdrachtgever uitgevoerd. Detachering is in belangrijke mate te vergelijken met payrolling.

⁴ De Vries & Rutgers 2007, p.18.

⁵ Sauerwein & Linnemann 2002, p. 17.

⁶ Hooghiemstra & Nouwt 2007, p. 40.

⁷ Sauerwein & Linnemann 2002, p. 17-18.

⁸ Hooghiemstra & Nouwt 2007, p. 42.

Samenvatting

Binnen de Diamant-groep is er op dit moment geen deugdelijk privacybeleid. In verband met het behalen van het 'Blik op Werk Keurmerk', het ethisch perspectief gezien de diverse doelgroep en het voorkomen van klachten, is een nieuw privacybeleid noodzakelijk. De doelstelling van dit rapport luidt daarom: *'op 10 januari 2011 is er, op grond van de vereisten in de Wbp, een privacyreglement voor de Diamant-groep opgesteld, dat gebaseerd is op duidelijke aanbevelingen ten aanzien van het huidige privacybeleid binnen de organisatie. De onderlinge relatie tussen de organisaties en de privacy van verschillende groepen medewerkers wordt gewaarborgd, door de unieke bedrijfsstructuur als uitgangspunt te nemen bij het opstellen van het privacyreglement en het doen van aanbevelingen.'* Om deze doelstelling te kunnen bereiken is de volgende vraagstelling geformuleerd: *'aan welke wettelijke vereisten uit de Wbp moet het nieuwe privacyreglement voldoen en op welke wijze kan er aan het privacybeleid binnen de Diamant-groep vorm worden gegeven, zodat in de onderlinge relatie tussen beide organisaties de privacy van verschillende groepen medewerkers gewaarborgd wordt?'* De deelvragen waren met name gericht op het in kaart brengen van de huidige wijze van gegevensverwerking binnen de Diamant-groep.

Tijdens dit onderzoek is gebruik gemaakt van desk- en fieldresearch. De fieldresearch bestond uit het houden van interviews en het verspreiden van vragenlijsten onder medewerkers van de Diamant-groep. De deskresearch bestond uit een uitgebreide literatuurstudie.

Het is gebleken dat de normen in de Wbp erg vaag zijn. In de memorie van toelichting op de Wbp en de literatuur wordt getracht invulling te geven aan deze normen. Er bestaat echter veelal geen pasklaar antwoord op concrete interne situaties. Om uiteindelijk de resultaten van de vragenlijsten op een juiste manier te interpreteren zijn eerst de organisaties omschreven. Vervolgens zijn de belangrijkste begrippen uit de Wbp uiteengezet. Tot slot worden de resultaten van de vragenlijsten uitgebreid uitgewerkt en toegelicht.

Wat met name opvalt is dat de medewerkers onvoldoende kennis van de Wbp hebben. Ze zijn dan ook veelal niet in staat hun eigen handelen te toetsen aan de Wbp. Deze lijn loopt als een rode draad door het gehele onderzoek. Medewerkers zijn zich vaak niet bewust van de mogelijke gevaren die hierdoor kunnen ontstaan. Het gebrek aan kennis is enerzijds te wijten aan het onvoldoende informeren van nieuwe medewerkers, anderzijds investeert de organisatie onvoldoende in het op peil brengen en houden van kennis. Opgemerkt wordt dat het onderwerp 'privacy' niet leeft binnen de organisatie. Met het informatiesysteem Compas bestaan veel privacygerelateerde problemen, met name als het gaat om beveiliging. Dit is enerzijds te wijten aan het programma, anderzijds aan de medewerkers die met het programma werken. Daarnaast worden te veel bijzondere persoonsgegevens verwerkt, met name gezondheidsgegevens. De kans op privacyinbreuk is, gezien de omvangrijke gegevensstromen en vele bijzondere persoonsgegevens die verwerkt worden, tamelijk groot. Daarbij worden praktische maatregelen ter beveiliging van de persoonsgegevens (zoals de clean-desk methode en (automatische) vergrendeling van de computer) te weinig getroffen.

De belangrijkste aanbeveling is dan ook om structureel te investeren in kennis op het gebied van privacyrecht bij de medewerkers. De bewustwording dient bij medewerkers vergroot te worden, onder andere door het betrekken van medewerkers bij het onderwerp, het invoeren van een privacyreglement, het opstellen van werkinstructies en betere informatievoorziening bij indiensttreding. Uiteindelijk dient een gedragsverandering op te treden bij de medewerkers. Door deze maatregelen gaan de medewerkers bewuster om met de gegevens die zij verwerken (onder andere in Compas). Daarnaast dient gekeken te worden naar de beveiligingsopties van Compas en dient er een beveiligingsplan en autorisatiebesluit vastgesteld worden. Een privacyofficer kan aan het hierboven geschetste proces een positieve bijdrage leveren, daarom wordt geadviseerd een dergelijke persoon aan te stellen.

1. Inleiding

De probleembeschrijving wordt geschetst in paragraaf 1.1, door het uitwerken van de achtergronden en de concrete aanleiding van dit onderzoek. In paragraaf 1.2 staan de doel- en vraagstelling en deelvragen centraal. De beperkingen worden besproken in paragraaf 1.3 en tot slot komt in paragraaf 1.4 de onderzoeksmethodiek aan de orde.

§ 1.1 Probleembeschrijving

Een medewerker is herstellende van een operatie. Nadat deze medewerker is teruggekeerd op het werk komt hij erachter dat zijn leidinggevende in zijn personeelsdossier heeft gelezen welke operatie hij heeft ondergaan, terwijl hij deze informatie niet nodig had voor de uitoefening van zijn functie. Deze informatie blijkt tevens te zijn verspreid onder andere collega's. De medewerker heeft hiervoor geen toestemming gegeven en besluit een klacht in te dienen over deze gang van zaken. Welke criteria en bepalingen uit de privacywetgeving zijn van belang om deze klacht te kunnen beoordelen? Hoe kan de Diamant-groep dergelijke klachten voorkomen? Dit soort problemen speelt binnen de Diamant-groep als het gaat over privacy.

De Diamant-groep is in Tilburg en omstreken het leerwerkbedrijf dat mensen met een afstand tot de arbeidsmarkt passend werk en ontwikkeling biedt. De Diamant-groep is nauw verbonden met de BV 18k (hierna: 18k). 18k is een privaatrechtelijke organisatie en heeft als doelstelling de Diamant-groep te ondersteunen in haar opdrachten middels het leveren van personeelsdiensten en arbeidsontwikkeling. Een uitgebreidere beschrijving van beide organisaties en hun onderlinge relatie is opgenomen in hoofdstuk 2.

De Diamant-groep voert voor een aantal gemeenten de Wet Sociale Werkvoorziening (hierna: Wsw) uit. De problematiek van de Wsw-doelgroep is over het algemeen erg divers. De Diamant-groep wil haar wettelijke verplichting, zoals deze is vastgelegd in de Wsw, zorgvuldig en goed uitvoeren. Hierdoor is het onvermijdelijk dat allerlei (persoons)gegevens van verschillende groepen medewerkers verwerkt worden. Gezien het karakter van de Diamant-groep is het mogelijk gerechtvaardigd dat zij meer en andere gegevens verwerken dan een reguliere organisatie. Volstrekt helder is dat beide organisaties ook zorg dienen te dragen voor een goede bescherming en afscherming van deze gegevens. Gezien de problematiek van de doelgroep waarmee de Diamant-groep te maken heeft, wordt het belang van een goed privacyreglement nogmaals onderstreept.

Een goed privacybeleid ontbreekt echter binnen de organisatie. De bestaande reglementen zijn vastgesteld in de periode 2004/2005 en zijn zodoende behoorlijk verouderd. Tevens zijn de werkzaamheden van beide organisaties sindsdien sterk veranderd, aangezien er nu ook opdrachten voor derden worden uitgevoerd en er dus persoonsgegevens van derden worden verwerkt. Nu de organisatie in zijn geheel het 'Blik op Werk Keurmerk' wil behalen, is een gedegen privacyreglement dat voldoet aan alle wettelijke vereisten noodzakelijk.

De Diamant-groep heeft behoefte aan informatie omtrent de Wbp en de mogelijkheden tot implementatie van de vereisten die uit deze wet volgen binnen de organisaties. Er is onvoldoende duidelijk aan welke wettelijke verplichtingen een nieuw privacyreglement moet voldoen. De opdracht luidt dan ook om aanbevelingen te doen ten aanzien van het pakket van vereisten dat volgt uit de Wbp waaraan voldaan moet worden. Zoals al aangegeven dient hiervoor de huidige wijze van gegevensverwerking binnen de organisatie in kaart te worden gebracht. Ook dient gekeken te worden naar de onderlinge relatie tussen de Diamant-groep en 18k en de verschillende groepen medewerkers die binnen de organisaties werkzaam zijn. Naar aanleiding van dit onderzoek wordt een privacyreglement opgesteld, dat binnen beide organisaties geïmplementeerd kan worden.

§ 1.2 Doel- en vraagstelling

De doelstelling van het onderzoeksrapport 'Een schitterend privacybeleid. De ontwikkeling van een passend privacybeleid voor de Diamant-groep' luidt:

op 10 januari 2011 moet er, op grond van de vereisten in de Wbp, een privacyreglement voor de Diamant-groep opgesteld zijn, dat gebaseerd is op duidelijke aanbevelingen ten aanzien van het huidige privacybeleid binnen de organisatie. De onderlinge relatie tussen de organisaties en de privacy van verschillende groepen medewerkers worden gewaarborgd, door de unieke bedrijfsstructuur als uitgangspunt te nemen bij het opstellen van het privacyreglement en het doen van aanbevelingen.

Naar aanleiding van deze doelstelling is de volgende vraagstelling geformuleerd:
aan welke wettelijke vereisten uit de Wbp moet het nieuwe privacyreglement voldoen en op welke wijze kan er aan het privacybeleid binnen de Diamant-groep vorm worden gegeven, zodat in de onderlinge relatie tussen beide organisaties de privacy van verschillende groepen medewerkers gewaarborgd wordt?

Onderstaande deelvragen dienen beantwoord te worden om de vraagstelling te kunnen beantwoorden en de doelstelling te behalen.

1. Hoe zien de organisaties van de Diamant-groep en 18k eruit en welke verhouding bestaat er tussen beide organisaties en hun werkzaamheden?
2. Welke verplichtingen vloeien voort uit de Wbp?
3. Wat is de huidige wijze van verwerken van persoonsgegevens binnen de Diamant-groep?
 - a. In welke mate zijn de medewerkers van de organisaties met de Wbp bekend?
 - b. Welke middelen worden ingezet om persoonsgegevens te registreren?
 - c. Welke persoonsgegevens worden verwerkt en is dit wettelijk gezien toegestaan?
 - d. Op welke grondslag worden persoonsgegevens verwerkt?
 - e. Van wie en door wie worden persoonsgegevens verwerkt?
 - f. Hoe worden de persoonsgegevens verwerkt en wat gebeurt ermee?
 - g. Voor welke doeleinden worden de persoonsgegevens verwerkt?
 - h. Welke beschermingsmaatregelen zijn er op dit moment getroffen en zijn deze toereikend?
 - i. In welke mate speelt de onderlinge relatie tussen de Diamant-groep en 18k een rol in de huidige wijze van het verwerken van persoonsgegevens?
4. Welke leemten bestaan er op dit moment tussen het huidige privacybeleid en de wettelijke vereisten uit de Wbp en welke oplossingen bestaan er voor deze hiaten?

De beoogde doelgroep van dit rapport is het hogere management binnen de Diamant-groep. Het management dient namelijk actie te ondernemen naar aanleiding van de conclusies en aanbevelingen. Aangezien het rapport, en het daaruit voortvloeiende privacyreglement, van belang is voor alle lagen in de organisatie, is er naar gestreefd om het rapport leesbaar te maken voor iedere geïnteresseerde medewerker.

§ 1.3 Beperkingen

In het kader van het inzien en uitlenen van persoonsdossiers is een aantal praktische problemen in de uitvoering ontstaan. Bijna ieder persoonsdossier bestaat uit een a- en b-dossier. Het a-dossier bevat documenten betreffende de indicatie van een medewerker, de arbeidsovereenkomst(en) en diverse andere documenten betreffende de loopbaan van de medewerker. Het b-dossier bevat alleen vertrouwelijke informatie. Hierbij dient gedacht te worden aan brieven en verslagen in verband met een hoorzitting of een disciplinair traject, maar ook brieven over corrigerende gesprekken en brieven in verband met een ontslagprocedure komen in dit b-dossier terecht.

De Diamant-groep heeft meerdere bedrijfsonderdelen op verschillende locaties, maar slechts één archief in het hoofdgebouw. De regel is dat het a-dossier alleen persoonlijk kan worden opgehaald bij het archief en b-dossiers het archief niet mogen verlaten om meegenomen te worden naar een ander bedrijfsonderdeel. Wel mogen de b-dossiers ingezien worden in het archief en is het toegestaan kopieën van de stukken in het b-dossier te maken. Dit is met het oog op de privacy een bijzonder onwenselijke situatie, aangezien juist de vertrouwelijke stukken vermenigvuldigd kunnen worden. Verder is er geen enkele controle op wat daarna met deze kopieën gebeurt. Deze handelwijze leidt tot een inbreuk op de privacy van betrokkenen. Tevens kan deze situatie leiden tot het ontstaan van schaduw dossiers (hierdoor ontstaan meerdere dossiers over één zaak). Dergelijke dossiers bevatten vaak niet alle relevante stukken en daarnaast is de kans groot dat stukken verloren gaan. In paragraaf 5.1.1 wordt hier nader op in gegaan.

De regels rondom het inzien en uitlenen van persoonsdossiers worden streng nageleefd, dit kan echter leiden tot tijdsverlies en inefficiënt werken. Er bestaat behoefte aan een nieuwe praktische handleiding omtrent het inzien en uitlenen van persoonsdossiers. Hoewel dit onderwerp te maken heeft met de privacy, valt het maken van deze handleiding buiten het bereik van dit onderzoek, gezien de reikwijdte van en de beperkte tijd voor dit onderzoek.

§ 1.4 Onderzoeksmethodiek

Het onderzoek bestaat uit twee onderzoekstypen, te weten literatuur- en empirisch onderzoek. Daarnaast is het van belang om te bepalen hoe een onderzoek betrouwbaar en valide blijft.

§ 1.4.1 Literatuur- en empirisch onderzoek

Het literatuuronderzoek heeft voornamelijk voor het empirisch onderzoek plaatsgevonden, met als doel het vormen van het theoretisch kader. Ook in een later stadium is het literatuuronderzoek van belang geweest, om resultaten uit het empirisch onderzoek juist te kunnen kwalificeren. Middels onderstaande empirische (kwalitatieve) methoden, is genuanceerde informatie uit de praktijk verzameld.

Surveyonderzoek - Middels het surveyonderzoek is de huidige situatie ten aanzien van de verwerking van persoonsgegevens in kaart gebracht binnen beide organisaties. Uit de resultaten zijn de aspecten naar voren komen die niet voldoen aan de normen in de Wbp.

Interviews - Als aanvulling op het surveyonderzoek is een aantal mensen geïnterviewd, met als doel de organisaties en hun onderlinge samenhang te leren kennen. De interviews hebben plaatsgevonden met de heer Van der Linden (bestuurssecretaris Diamant-groep, voorheen hoofd juridische zaken), de heer Den Brok (technisch Compas-beheerder), de heer Wijn (hoofd informatie en automatisering) en de heer De Beer (senior juridische zaken). Deze medewerkers hebben informatie verschaft over de huidige wijze van gegevensverwerking en de bescherming van deze gegevens binnen de Diamant-groep. Vanuit het verleden kent de Diamant-groep een nauwe verwantschap met de Gemeente Tilburg. Daarom is ook een medewerker juridische zaken van de Gemeente Tilburg geïnterviewd, te weten de heer De Gier.

§ 1.4.2 Betrouwbaarheid en validiteit

De betrouwbaarheid van het onderzoeksrapport is gewaarborgd door:

- Een heldere onderzoeksopzet.
- Het nastreven van een respons zo dicht mogelijk bij 100% op het surveyonderzoek en hiervoor de nodige acties ondernemen.

- Het voornamelijk gebruik maken van betrouwbare bronnen, zoals Europese Richtlijnen, wet- en regelgeving (zoals de Wbp en de Wsw), de bijbehorende Memorie van Toelichting, interne regelgeving (zoals de bestaande reglementen en werkinstructies) en besluiten.
- Het gebruik van betrouwbare boeken en rapporten. De auteurs van deze werken publiceren vaker boeken, rapporten of artikelen op het gebied van het privacyrecht.

De validiteit van dit onderzoek is middels onderstaande punten gewaarborgd:

- De centrale vraagstelling is voldoende afgebakend, zodat er geen niet-relevante informatie wordt verzameld en er geen belangrijke vragen worden overgeslagen.
- De centrale vraagstelling is opgedeeld in deelvragen, dit maakt het mogelijk om gedurende het onderzoek te controleren of er antwoord wordt gegeven op de vraagstelling. Hierdoor wordt in de gaten gehouden of het onderzoek valide is en blijft.
- Elke stap in het onderzoek heeft plaatsgevonden vanuit de doelstelling. Hierdoor wordt de kans dat er uiteindelijk geen antwoord wordt gegeven op de vraagstelling kleiner.
- De onderzoeksresultaten worden regelmatig voorgelegd aan de begeleiders. Op deze wijze blijft er controle over het onderzoeksproces en over de vooraf bepaalde metingen.

§ 1.5 Opbouw van het rapport

Om de resultaten van de vragenlijsten op een juiste wijze te kunnen interpreteren en te verklaren is een helder beeld van de structuur, werkzaamheden en de onderlinge relatie tussen de Diamant-groep en 18k noodzakelijk. In hoofdstuk 2 wordt dit nader uitgewerkt. Hetzelfde geldt voor het theoretisch kader. Zonder theoretisch kader is het niet mogelijk onderbouwde conclusies te trekken uit de resultaten van de vragenlijsten. In hoofdstuk 3 worden de hoofdlijnen uit de Wbp besproken en worden de belangrijkste artikelen kort uitgewerkt en nader verklaard. Aangezien de Diamant-groep onvermijdelijk krijgt te maken met het College Bescherming Persoonsgegevens (hierna: CBP), is een korte beschrijving van de taken waarbij het CBP een rol speelt of die binnen zijn bevoegdheden liggen wenselijk. In hoofdstuk 4 wordt daarom kort aandacht besteed aan het CBP. Hoofdstuk 5 is het kernhoofdstuk van dit onderzoek. In dit hoofdstuk staat de verwerking van de resultaten van de vragenlijsten centraal en wordt een beeld gevormd van de gegevensverwerkingen binnen de Diamant-groep. Ook wordt getoetst of de huidige verwerkingen aan de normen in de Wbp voldoen. Om het hoofdstuk overzichtelijk te houden, is in de tekst een aantal grafieken ingevoegd. De totale uitwerking van alle vragenlijsten is toegevoegd in een aparte bijlage. Tot slot worden conclusies getrokken op basis van de toets die in dit hoofdstuk wordt uitgevoerd en worden aanbevelingen gedaan over hoe de aandachtspunten verbeterd kunnen worden en hoe het nieuwe privacyreglement het best binnen de organisatie geïmplementeerd kan worden. Naar aanleiding van bovenstaande wordt een nieuw privacyreglement opgesteld dat voldoet aan de normen in de Wbp en tevens zorgt voor een werkbare situatie voor de medewerkers.

Dit rapport bevat een aantal bijlagen. Dit zijn documenten die niet te raadplegen zijn door derden, aangezien het hier gaat om interne regelgeving, die alleen te raadplegen is door medewerkers van de Diamant-groep via de beveiligde intranetomgeving.

In de voetnoten wordt slechts een verkort verwijssysteem gehanteerd; een uitgebreide literatuurlijst is achteraan opgenomen.

2. Organisatiebeschrijvingen

Om uiteindelijk een goed beeld te kunnen vormen van de vele gegevensverwerkingen die binnen de Diamant-groep plaats hebben en daar onderbouwde uitspraken over te kunnen doen, wordt in dit hoofdstuk een korte beschrijving gegeven van beide organisaties. In paragraaf 2.1 wordt de Diamant-groep afzonderlijk kort weergegeven, hierna zal in paragraaf 2.2 18k kort beschreven worden. Vervolgens zal in paragraaf 2.3 de relatie tussen de Diamant-groep en 18k aan de orde komen. Voor een totaaloverzicht van beide organisaties zijn in bijlage I de organogrammen van respectievelijk de Diamant-groep en 18k opgenomen.

§ 2.1 De Diamant-groep

De Diamant-groep, sinds 1 januari 1976 gevestigd in de gemeente Tilburg, is een organisatie die door subsidiëring werkgelegenheid creëert voor mensen met een afstand tot de arbeidsmarkt. Mensen ontwikkelingsmogelijkheden bieden is dan ook de primaire opdracht voor de Diamant-groep. De Diamant-groep werkt met allerlei verschillende groepen, zoals mensen met een psychische, geestelijke en/of lichamelijke beperking. Daarnaast werkt zij bijvoorbeeld ook met langdurig werklozen, herintreders of schoolverlaters met een achterstand.

In opdracht van zes gemeenten voert de Diamant-groep de Wsw uit. Hiertoe hebben deze gemeenten en de Diamant-groep afspraken met elkaar gemaakt in de Gemeenschappelijke regeling Werkvoorzieningschap Diamant-groep. De Diamant-groep wordt bestuurd door deze gemeenten, te weten: Tilburg, Dongen, Gilze-Rijen, Hilvarenbeek, Alphen-Chaam en Goirle.

In het strategisch plan heeft de Diamant-groep de keuze gemaakt passende voorzieningen aan te bieden aan alle medewerkers. Het streven is medewerkers een werkplek te bieden buiten de muren van de Diamant-groep. Dit betekent dat er passende werkplekken gecreëerd moeten worden, zodat medewerkers zich op hun werkplek maximaal kunnen ontwikkelen en waar mogelijk doorstromen van werkplekken met een intensieve begeleiding naar steeds meer zelfstandige werkplekken en uiteindelijk naar helemaal zelfstandige werkplekken.

Inmiddels heeft de Diamant-groep zich ontwikkeld tot een leerwerkbedrijf met meer dan 3000 medewerkers. Zoals gezegd biedt de Diamant-groep veel mensen aan de onderkant van de arbeidsmarkt vormen van arbeidsontwikkeling aan die passen bij hun vermogens, capaciteiten en beperkingen. Een groot aantal van deze mensen werkt op basis van individuele detachering, groepsdetachering of begeleid werken buiten de muren van de Diamant-groep. Binnen de Diamant-groep zijn veel werkzaamheden gericht op het bieden van individueel maatwerk aan medewerkers. Gezien dit bijzondere karakter worden binnen de organisatie, meer bijzondere gegevens verwerkt om een werktraject tot een succes te maken dan gebruikelijk is bij een 'normaal' arbeidscontract.

§ 2.2 18k

18k werd in 2005 opgericht als zelfstandig opererende organisatie naast de Diamant-groep. Het primaire doel voor de oprichting van 18k was gelegen in het feit dat de Diamant-groep hiermee sneller kon reageren op veranderende regelgeving en ontwikkelingen op de arbeidsmarkt.

18k heeft zich om deze reden gespecialiseerd op de thema's arbeidsontwikkeling en personeelsdiensten en houdt zich dagelijks bezig met de vele aspecten die spelen rondom arbeidsontwikkeling en het leveren van personeelsdiensten in de breedste zin van het woord.

Producten die 18k daarbij aanbiedt zijn onder meer arbeidsontwikkeling, personeelsdiensten (zoals salaris- en personeelsadministratie en juridische zaken), bestandsanalyse, payrolling en alfacheques.

Hoewel 18k feitelijk losstaat van de Diamant-groep, is de Diamant-groep wel de grootste opdrachtgever van 18k. Dit maakt dat 18k te beschouwen is als een privaatrechtelijke zusteronderneming van de Diamant-groep. 18k heeft als primaire doelstelling de Diamant-groep te ondersteunen in haar opdrachten. Daartoe worden twee belangrijke diensten geleverd, te weten personeelsdiensten en arbeidsontwikkeling. Daarnaast analyseert en diagnosticeert 18k dossiers van externe opdrachtgevers, adviseren zij over dossiers en worden payrollactiviteiten uitgevoerd. Hiervoor heeft 18k een veelheid aan mensen, mogelijkheden en middelen ter beschikking. Momenteel werken er bij 18k 178 medewerkers die gezamenlijk het kaderpersoneel vormen.

§ 2.3 De relatie tussen de Diamant-groep en 18k

Zoals eerder aangegeven, hebben de Diamant-groep en 18k zeer nauwe banden met elkaar. De aandelen van 18k zijn voor 100% in handen van de BV Bepro (onderdeel van de Diamant-groep).

Zoals reeds eerder aangegeven levert 18k op het gebied van personele ondersteuning en arbeidsontwikkeling instrumenten aan de Diamant-groep. Binnen de bedrijfsonderdelen van de Diamant-groep zijn door 18k personeelsteams ingericht. Deze leveren ondersteuning bij personele activiteiten zoals op het gebied van verzuimbegeleiding, opstellen van Individuele Ontwikkelingsplannen (hierna: IOP), beoordelings- en functioneringsgesprekken en het verder ontwikkelen van een innovatief en hedendaags personeelsbeleid. Daarnaast verzorgt 18k ook de totale personeels- en salarisadministratie voor de Diamant-groep.

De bijzondere onderlinge relatie tussen de Diamant-groep en 18k, de verschillende doelgroepen en het leveren van personeelsdiensten, maakt dat er binnen de organisaties veel en vaak vertrouwelijke gegevensverwerkingen plaatshebben. Dit laatste maakt het noodzakelijk het huidige privacybeleid nader te onderzoeken om te komen tot aanbevelingen voor de ontwikkeling van een nieuw privacybeleid.

Om later in dit onderzoeksrapport de term ‘verantwoordelijke’ goed te kunnen plaatsen, is een verklaring van dit begrip in de onderlinge verhouding tussen de Diamant-groep en 18k noodzakelijk. In de begrippenlijst is het begrip ‘verantwoordelijke’ reeds kort toegelicht. In aanvulling daarop wordt opgemerkt dat binnen de Diamant-groep en 18k sprake is van een afzonderlijke verantwoordelijkheid per (deel)verwerking. Verschillende verwerkingen zijn min of meer geïntegreerd zonder dat een gemeenschappelijke verantwoordelijke aanwezig is. De Diamant-groep is aansprakelijk voor de privacy van zijn medewerkers (zoals de Sw-medewerkers en ambtenaren). Daarnaast is 18k verantwoordelijk voor de waarborging van de privacy van zijn medewerkers (zoals het 18k kaderpersoneel, Alfacheque-medewerkers, gedetacheerden et cetera). In beginsel is iedere verantwoordelijke aansprakelijk voor zijn deel. De betrokkene kan slechts één van de verantwoordelijken aanspreken.⁹

Het archief van de Diamant-groep is zowel het archief van de Diamant-groep als van 18k. Afgesproken is dat de Diamant-groep verantwoordelijk is voor de zaken die rondom het archief spelen.

⁹ Hooghiemstra & Nouwt 2007, p. 38-39.

3. De wet bescherming persoonsgegevens

In onderstaande paragrafen wordt kort het wettelijk kader inzake het privacyrecht op internationaal en nationaal niveau geschetst. Ook zullen de relevante bepalingen uit de Wbp in dit hoofdstuk kort uiteengezet worden.

§ 3.1 Breed wettelijk kader op internationaal niveau

Op internationaal niveau is vooral binnen de Verenigde Naties (hierna: VN) aandacht besteed aan mensenrechten, waaronder ook het recht op bescherming van privacy valt. Op 10 december 1948 is door de Algemene Vergadering van de VN de Universele Verklaring van de Rechten van de Mens (hierna: UVRM) aangenomen. Art. 12 van de UVRM vormt het eerste internationale artikel waarin het recht op bescherming van de persoonlijke levenssfeer is vastgelegd. Dit artikel richt zich tegen willekeurige inmenging van de overheid in persoonlijke aangelegenheden en vormt het fundament voor de internationale ontwikkeling van het recht op privacy. Aangezien het slechts gaat om een aanbeveling, is de Universele verklaring juridisch niet bindend. Om dit probleem tegen te gaan heeft de VN in 1969 onder andere het Internationaal Verdrag inzake Burgerrechten en Politieke rechten (hierna: IVBP) uitgevaardigd, dat wel juridische binding heeft.¹⁰ In dit kader is art. 17 IVBP van belang. De tekst van dit artikel is nagenoeg identiek aan de tekst uit art. 12 UVRM. Gezien de juridische binding die er aan ontleend kan worden, is art. 17 IVBP echter van grotere waarde.

Ook art. 8 van het in 1950 door de Raad van Europa opgestelde Europees Verdrag tot Bescherming van de Rechten van de Mens en de Fundamentele Vrijheden (hierna: EVRM) is in belangrijke mate een afgeleide van art. 12 UVRM. Art. 8 EVRM regelt het recht op respect voor het privé-, familie- en gezinsleven, de woning en correspondentie. In de Nederlandse samenleving speelt art. 8 EVRM een veel grotere rol dan art. 17 IVBP. Dit kan met name verklaard worden vanuit het verschil in sanctiesystematiek. Het valt buiten de reikwijdte van dit rapport om deze verschillen te behandelen.¹¹

§ 3.2 Wettelijk kader op nationaal niveau

Binnen Nederland wordt in art. 10 van de Grondwet (hierna: Gw) ingegaan op de bescherming van de persoonlijke levenssfeer. Bij de herziening van de Gw in 1983 werd in art. 10 lid 1 de bescherming van de persoonlijke levenssfeer uitdrukkelijk als klassiek grondrecht¹² geformuleerd. Tevens wordt in het tweede en derde lid aan de formele wetgever de opdracht gegeven regels te stellen omtrent de bescherming van persoonsgegevens.¹³ Zowel de Wet Persoonsregistraties (hierna: WPR) als de Wbp zijn voortgevloeid uit deze verplichting. In de internationale en Europese verdragen wordt gesproken over de term 'privéleven', terwijl in art. 10 Gw wordt gesproken over 'persoonlijke levenssfeer'. Dit is slechts een verschil in terminologie, geen verschil in betekenis.

In 1976 verscheen het eindrapport van de Staatscommissie-Koopmans, dat reeds een uitgebreid voorontwerp van de WPR bevatte. In 1981 is het 'Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens'¹⁴ van de Raad van Europa tot stand gekomen. In art. 4 lid 1 en lid 2 van dit verdrag is vastgelegd dat partijen bij het verdrag wetgeving tot stand zouden brengen op basis van bepaalde grondbeginselen van gegevensbescherming. Naar aanleiding hiervan is uiteindelijk pas op 1 januari 1989 de WPR in werking getreden.¹⁵

¹⁰ Berkvens & Prins 2007, p. 9.

¹¹ Zie in dit verband art. 28 en 42 IVBP en art. 29 t/m 35 EVRM.

¹² Klassieke grondrechten beschermen de burger tegen bemoeienis of inmenging van de overheid.

¹³ Hooghiemstra & Nouwt 2007, p. 16.

¹⁴ Trb. 1988, 7.

¹⁵ De Vries & Rutgers 2001, p. 13-15.

In 1995 is de 'Europese richtlijn betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens'¹⁶ vastgesteld. In deze richtlijn wordt bepaald dat alle betrokkenen voor 24 oktober 1998 implementatiewetgeving tot stand moesten brengen. Deze harmonisatierichtlijn vormde in Nederland de aanzet tot het wijzigen van de WPR.¹⁷

Uiteindelijk is de Wbp op 1 september 2001 in werking getreden en is het in Nederland op dit moment de meest specifieke privacywetgeving. De Wbp stelt diverse voorwaarden voor een (zorgvuldige) omgang met persoonsgegevens, doordat de wet enkele procedureregels en een algemeen toetsingskader voor de afweging van de rechtmatigheid van verwerkingen in concrete situaties biedt. De Wbp schrijft in feite een afweging van belangen voor.¹⁸

§ 3.3 De reikwijdte van de Wbp

De reikwijdte van de Wbp wordt bepaald door het begrip 'verwerken van persoonsgegevens'. Op grond van art. 1 sub b Wbp omvat het verwerken van persoonsgegevens het gehele proces dat een persoonsgegeven doormaakt vanaf de verzameling tot het moment van vernietiging.¹⁹ Een omschrijving van het begrip 'verwerken' en 'persoonsgegeven' is opgenomen in de begrippenlijst. Art. 2 lid 1 Wbp bepaalt dat de Wbp van toepassing is op de (gedeeltelijk) geautomatiseerde verwerking van persoonsgegevens. Dus als er met behulp van computers persoonsgegevens worden opgeslagen of er in een kast persoonsgegevens bewaard worden die met behulp van een computer te raadplegen zijn.²⁰ Ook op de handmatige verwerking van persoonsgegevens is de Wbp van toepassing, mits de gegevens zijn opgenomen in een bestand of bestemd zijn om daarin te worden opgenomen. Er is sprake van een bestand als de gegevens onderlinge samenhang vertonen en het systeem systematisch toegankelijk is. In de begrippenlijst wordt het begrip 'bestand' nader omschreven.²¹

Indien er sprake is van verwerking van persoonsgegevens in het kader van één of meerdere van de hieronder genoemde doeleinden, is de Wbp niet van toepassing conform art. 2 lid 2 jo art. 3 lid 1 Wbp. Het gaat om de verwerking van gegevens:

- voor uitsluitend persoonlijke of huishoudelijke doeleinden. Het gaat dan om persoonlijke werkaantekeningen of eigen lijstjes van medewerkers met adresgegevens van personen met wie zij regelmatig contact onderhouden. Indien een verwerking beoogd is voor gebruik door meerdere personen, is de Wbp wel van toepassing²²;
- door of ten behoeve van de inlichtingen- en veiligheidsdiensten;
- ten behoeve van de uitvoering van de politietaak;
- die is geregeld krachtens de Wet gemeentelijke basisadministratie persoonsgegevens;
- ten behoeve van de uitvoering van de Kieswet;
- ten behoeve van de uitvoering van de Wet justitiële en strafvorderlijke gegevens;
- voor uitsluitend journalistieke, artistieke of literaire doeleinden.

Deze uitzonderingen zijn niet van toepassing op de Diamant-groep.

§ 3.4 Voorwaarden voor de verwerking van persoonsgegevens

In de Wbp is een aantal algemene beginselen geformuleerd, die van toepassing zijn op iedere gegevensverwerking. Deze beginselen vormen een uitwerking van de in Richtlijn 95/46/EG neergelegde voorschriften en worden besproken in paragraaf 3.4.1. De wettelijke gronden die een gegevensverwerking rechtvaardigen, staan centraal in paragraaf 3.4.2.

¹⁶ Richtlijn 95/46/EG (PbEG 1995, L 281/31)

¹⁷ Kamerstukken II 1997/1998, 25892, nr. 3, p. 3-5 (MvT).

¹⁸ Berkvens & Prins 2007, p. 25.

¹⁹ De Vries & Rutgers 2001, p. 17-18.

²⁰ Sauerwein & Linnemann 2002, p. 16.

²¹ De Vries & Rutgers 2001, p. 18.

²² Hooghiemstra & Nouwt 2007, p. 57.

§ 3.4.1 Algemene beginselen betreffende de gegevensverwerking

Het rechtmatigheidbeginsel - De verwerking van persoonsgegevens dient conform art. 6 Wbp in overeenstemming met de wet, behoorlijk en zorgvuldig te gebeuren. Als de verantwoordelijke hier niet aan voldoet, handelt hij onrechtmatig jegens de betrokkene. Gebeurt dit in het kader van een overheidstaak, dan handelt hij in strijd met de algemene beginselen van behoorlijk bestuur.²³ Het rechtmatigheidbeginsel kan gezien worden als het basisartikel van de Wbp en vormt een kapstok voor andere relevante wetten.²⁴

Het beginsel van doelbinding - Persoonsgegevens mogen op grond van art. 7 Wbp slechts verzameld worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Dit houdt in dat er geen gegevens verzameld mogen worden zonder dat er vooraf een precies doel is vastgesteld door de verantwoordelijke. 'Welbepaald' houdt in dat de doelomschrijving duidelijk, dus niet te vaag en niet te ruim, moet zijn. Het is belangrijk dat de doelomschrijving dermate afgebakend is dat deze tijdens het verzamelingsproces als toetsingskader kan dienen om te bepalen of gegevens wel noodzakelijk zijn voor de bepaalde doelen. De verantwoordelijke dient te beoordelen of hij ook met minder gegevens de doelen kan bereiken. 'Uitdrukkelijk omschreven' betekent dat de verantwoordelijke het doel waarvoor hij gegevens verwerkt vooraf moet hebben omschreven.²⁵ Er is sprake van 'gerechtvaardigde doeleinden' als de gegevensverwerking gebaseerd kan worden op één van de gronden uit art. 8 Wbp. Deze gronden worden besproken in paragraaf 3.4.2.

Het beginsel van niet-onverenigbaarheid - Verzamelde gegevens mogen vanzelfsprekend gebruikt worden voor de doeleinden waarvoor ze zijn verzameld. Gegevens mogen, zoals bepaald is in art. 9 Wbp, ook verder verwerkt worden, mits het doel voor de verdere verwerking verenigbaar is met het doel waarvoor de gegevens oorspronkelijk zijn verzameld. Dit beginsel vormt het sluitstuk van het doelbindingsvereiste. Art. 9 lid 2 Wbp somt een aantal niet limitatieve factoren op die bij de afweging of sprake is van verenigbaar gebruik in ieder geval een rol spelen. In ieder geval spelen een rol: de aard van de gegevens, de gevolgen van de beoogde verwerking voor de betrokkene, de wijze waarop de gegevens zijn verkregen en de mate waarin jegens de betrokkene is voorzien in passende waarborgen.²⁶

Het kwaliteitsbeginsel - De gegevens dienen conform art. 11 Wbp, met het oog op het doel waarvoor zij verzameld zijn, toereikend, ter zake dienend en niet bovenmatig te zijn. 'Ter zake dienend' houdt in dat de verantwoordelijke enkel gegevens mag verwerken die noodzakelijk zijn voor het doel. Overbodige gegevens mogen dus niet verwerkt worden. 'Toereikend' wil zeggen dat een verantwoordelijke alle gegevens dient te verwerken die voor het doel noodzakelijk zijn. Indien er te weinig gegevens worden verzameld, kan er namelijk een onvolledig en onjuist beeld van de betrokkene ontstaan. De gegevens mogen bovendien niet 'bovenmatig' zijn. Dit houdt in dat de verantwoordelijke niet te gedetailleerde gegevens mag verwerken als dat voor het doel niet noodzakelijk is.²⁷ Uitgangspunt is dat de verantwoordelijke er zorg voor dient te dragen dat hij voldoende en adequate gegevens verwerkt voor het vooraf vastgestelde doel. Verder dienen de persoonsgegevens volgens art. 11 lid 2 Wbp juist en nauwkeurig te zijn. Deze norm legt een continue verplichting tot toetsing op de verantwoordelijke. Het betreft echter geen absolute verplichting, al volgt er wel een zekere inspanningsverplichting uit. De verantwoordelijke dient de nodige maatregelen te treffen om een juiste en nauwkeurige verwerking te waarborgen, mits dit in redelijkheid van hem gevergd kan worden.²⁸

²³ Sauerwein & Linnemann 2002, p. 19.

²⁴ De Vries & Rutgers 2001, p. 22.

²⁵ Hooghiemstra & Nouwt 2007, p. 65; Sauerwein & Linnemann 2002, p. 20.

²⁶ De Vries & Rutgers 2001, p. 28.

²⁷ Sauerwein & Linnemann 2002, p. 27-28.

²⁸ Kamerstukken II 1997/1998, 25892, nr. 3, p. 99 (MvT).

Proportionaliteit en subsidiariteit - In het kader van de Wbp spelen zowel het proportionaliteits- als het subsidiariteitsbeginsel een belangrijke rol. Op grond van art. 8 EVRM geldt het proportionaliteitsbeginsel rechtstreeks. Dit beginsel houdt in dat de inbreuk op de belangen van de betrokkene niet onevenredig mag zijn in verhouding tot het beoogde doel. In deze evenredigheidsstoets speelt het subsidiariteitsbeginsel mede een rol. Dit houdt in dat het doel waarvoor de persoonsgegevens worden verwerkt in redelijkheid niet op een andere, voor de betrokkene minder nadelige wijze, kan worden bereikt. In dat geval dient er afgezien te worden van de verwerking. Worden er toch gegevens verwerkt dan rust op degene die persoonsgegevens verwerkt de plicht om binnen redelijke grenzen een inbreuk op de persoonlijke levenssfeer van anderen te vermijden dan wel zo beperkt mogelijk te houden.²⁹ Een afweging van belangen is dan noodzakelijk. Of er inbreuk wordt gemaakt is afhankelijk van de aard van de gegevens en de wijze waarop deze worden gebruikt.³⁰

§ 3.4.2 Gronden voor gegevensverwerking

In art. 8 sub a tot en met f Wbp zijn zes wettelijke grondslagen geformuleerd, op basis waarvan gegevensverwerking is toegestaan. Slechts in het geval de verwerking gebaseerd kan worden op ten minste één van deze grondslagen, is sprake van een rechtmatige verwerking.

Ondubbelzinnige toestemming van de betrokkene - Art. 1 sub i Wbp bepaalt dat toestemming van de betrokkene elke vrije, specifieke en op informatie berustende wilsuiting is, waarmee de betrokkene aanvaardt dat zijn persoonsgegevens worden verwerkt. 'Ondubbelzinnig' duidt op het feit dat bij de verantwoordelijke geen enkele twijfel mag bestaan over de gegeven toestemming. Er dient aan drie criteria voldaan te worden: het is in de eerste plaats van belang dat de betrokkene zijn wil in vrijheid heeft geuit. Zo is er van vrije wil geen sprake als de betrokkene onder druk van de omstandigheden heeft ingestemd, of hij in een erg afhankelijke positie staat tot de verantwoordelijke, bijvoorbeeld in de verhouding tussen werkgever en werknemer. Ten tweede moet de wilsuiting betrekking hebben op een bepaalde gegevensverwerking of een bepaalde categorie van verwerkingen. Dit betekent dat een onbepaalde machtiging om persoonsgegevens te verwerken niet valt onder rechtsgeldige toestemming. Tot slot dient de betrokkene zo goed mogelijk te zijn ingelicht over de gegevensverwerking, zodat hij bewust zijn toestemming kan geven. De betrokkene dient dus altijd op de hoogte te worden gesteld door de verantwoordelijke. De toestemming hoeft niet schriftelijk te worden gegeven, maar kan dus bijvoorbeeld blijken uit een gedraging van de betrokkene.³¹

De uitvoering of voorbereiding van een overeenkomst - Een verwerking kan op deze grondslag gebaseerd worden indien het niet mogelijk is de overeenkomst uit te voeren zonder de verwerking van persoonsgegevens. De betrokkene dient partij te zijn bij de overeenkomst, voor de verantwoordelijke is dat geen noodzakelijkheid.³² De overeenkomst zelf is vaak niet gericht op het verwerken van persoonsgegevens, maar een noodzakelijk uitvloeisel daarvan. Verwerking is verder geoorloofd indien dit noodzakelijk is in de precontractuele fase. Het moet dan gaan om handelingen die op verzoek van de betrokkene worden verricht teneinde een overeenkomst te kunnen sluiten.³³

Het nakomen van een wettelijke verplichting - Er kunnen enkel gegevens verwerkt worden op basis van deze grondslag, indien de uitvoering van de wettelijke verplichting zonder de gegevensverwerking redelijkerwijs niet mogelijk is. De verplichting dient op de verantwoordelijke zelf te rusten.

²⁹ Hooghiemstra & Nouwt 2007, p. 17.

³⁰ *Kamerstukken II* 1997/1998, 25892, nr. 3, p. 7 (MvT).

³¹ De Vries & Rutgers 2001, p. 23-24; Sauerwein & Linnemann 2002, p. 21-22.

³² Sauerwein & Linnemann 2002, p. 22-23.

³³ De Vries & Rutgers 2001, p. 24-25.

Met 'wet' wordt in dit verband een 'algemeen verbindend voorschrift' bedoeld. Zodoende kan een verwerking bijvoorbeeld ook plaatsvinden op basis van een gemeentelijke verordening.³⁴

Bestrijding van een ernstig gevaar voor de gezondheid van betrokkene - In dit geval moet er sprake zijn van een dringende medische noodzaak.

Er is bijvoorbeeld toestemming nodig voor een medische behandeling, echter de betrokkene zelf is buiten bewustzijn geraakt als gevolg van een ongeval.³⁵

Een goede vervulling van een publiekrechtelijke taak - Met een publiekrechtelijke taak wordt een taak bedoeld die bij of krachtens de wet is opgedragen aan een bestuursorgaan. Het dient dus te gaan om taken die specifiek bij een bestuursorgaan zijn neergelegd.³⁶ Indien het gaat om taken die ook door particulieren worden verricht, zoals het sluiten van een arbeidsovereenkomst, kan de verwerking niet gebaseerd worden op deze grondslag.

Een gerechtvaardigd belang - Een gerechtvaardigd belang is aanwezig als de betreffende verwerking noodzakelijk is voor het verrichten van reguliere bedrijfsactiviteiten. Bij iedere verwerking zal de verantwoordelijke een afweging moeten maken tussen zijn belang en het individuele belang van de betrokkene om gevrijwaard te blijven van inbreuken op zijn privacy. De verantwoordelijke heeft in dit kader een motiveringsplicht.³⁷ De verantwoordelijke zal inzichtelijk moeten kunnen maken dat hij daadwerkelijk een gerechtvaardigd belang heeft, dat de gegevensverwerking niet achterwege kan blijven, dat het doel dat met de verwerking wordt nagestreefd niet via een andere weg kan worden bereikt en dat de verwerking evenredig is aan het nagestreefde doel.³⁸

§ 3.5 De verwerking van bijzondere persoonsgegevens

De wet maakt een onderscheid tussen algemene en bijzondere persoonsgegevens. Algemene persoonsgegevens zijn bijvoorbeeld NAW-gegevens, geboortedatum, telefoonnummer, leeftijd, BSN et cetera. De bijzondere persoonsgegevens worden in art. 16 Wbp limitatief opgesomd en worden hieronder in paragraaf 3.5.1 besproken. In paragraaf 3.5.2 wordt de restbepaling besproken die het mogelijk maakt om bijzondere persoonsgegevens te verwerken.

§ 3.5.1 Ontheffing van het verbod om bijzondere persoonsgegevens te verwerken

Verwerking van bijzondere persoonsgegevens is in beginsel niet toegestaan, aangezien het risico op inbreuk op privacy van betrokkenen bij de verwerking van dergelijke gegevens aanzienlijk groter is. Van het verbod kan slechts ontheffing worden verleend indien de verwerking zijn grondslag vindt in art. 17 tot en met art. 22 Wbp.³⁹

Godsdienst of levensovertuiging (art. 17 Wbp) - Verwerking kan slechts geschieden door (kerk)genootschappen op geestelijke grondslag of instellingen op godsdienstige of levensbeschouwelijke grondslag. Andere instellingen mogen deze gegevens verwerken, voor zover dit noodzakelijk is met het oog op de geestelijke verzorging van de betrokkene, tenzij deze daartegen schriftelijk bezwaar maakt.⁴⁰

Ras of etniciteit (art. 18 Wbp) - Persoonsgegevens betreffende iemands ras of etniciteit mogen verwerkt worden met het oog op identificatie van de betrokkene en slechts voor zover dit voor dit doel onvermijdelijk is.

³⁴ Sauerwein & Linnemann 2002, p. 23.

³⁵ De Vries & Rutgers 2001, p. 25.

³⁶ De Vries & Rutgers 2001, p. 26.

³⁷ Sauerwein & Linnemann 2002, p. 26.

³⁸ De Vries & Rutgers 2001, p. 26.

³⁹ Hooghiemstra & Nouwt 2007, p. 98.

⁴⁰ Hooghiemstra & Nouwt 2007, p. 99.

Het begrip ras dient ruim te worden opgevat en omvat ook huidskleur, afkomst en nationale of etnische afstamming.⁴¹ Persoonsgegevens betreffende iemands ras mogen ook verwerkt worden voor het voeren van een voorkeursbeleid voor bepaalde minderheidsgroeperingen.

Politieke gezindheid (art. 19 Wbp) - Instellingen met een politieke grondslag mogen dergelijke gegevens verwerken betreffende hun leden of werknemers, dan wel andere tot de instelling behorende personen. Daarnaast mogen deze gegevens verwerkt worden indien de verwerking geschiedt met het oog op de eisen die met betrekking tot iemands politieke gezindheid redelijkerwijs kunnen worden gesteld in verband met de vervulling van functies in bestuursorganen en adviescolleges.

Vakbondslidmaatschap (art. 20 Wbp) - Verwerking van deze gegevens is enkel toegestaan door een vakbond of vakcentrale, voor zover dat noodzakelijk is.

Gezondheid (art. 21 Wbp) - Gezondheidsgegevens mogen enkel worden verwerkt op een wijze die de persoonlijke levenssfeer van de werknemer niet aantast. Onder gezondheidsgegevens vallen niet alleen gegevens waarop het medisch beroepsgeheim rust, maar alle gegevens die de geestelijke of lichamelijke gezondheid van een persoon betreffen.⁴² Een bestuursorgaan of werkgever mag conform art. 21 lid 1 sub f Wbp gezondheidsgegevens verwerken in twee situaties. In de eerste plaats betreft het verwerkingen die noodzakelijk zijn voor de uitvoering van een wettelijk voorschrift, pensioenregelingen of een collectieve arbeidsovereenkomst die samenhangt met de gezondheidstoestand van de werknemer of de uitkeringsgerechtigde. In de tweede plaats is verwerking toegestaan als dat noodzakelijk is voor de re-integratie of begeleiding van uitkeringsgerechtigden of medewerkers in verband met ziekte of arbeidsongeschiktheid. Beide onderdelen uit art. 21 lid 1 sub f Wbp worden begrensd door de noodzakelijkheidseis.⁴³ Deze gegevens mogen dus niet onbeperkt verwerkt worden. In paragraaf 5.3.2.1 wordt nader op het verwerken van gezondheidsgegevens ingegaan.

Strafrechtelijke persoonsgegevens (art. 22 Wbp) - Strafrechtelijke persoonsgegevens zien zowel toe op veroordelingen als op min of meer gegronde verdenkingen. Strafrechtelijke gegevens mogen worden gebruikt naar aanleiding van een verzoek van betrokkene, met het oog op een beslissing omtrent of een maatregel met betrekking tot hem. Tevens is de verwerking toegestaan ter bescherming van de belangen van de verantwoordelijke of personen in zijn dienst, voor zover deze slachtoffer zijn geweest of dreigen te worden van een strafbaar feit. De verantwoordelijke is dan gemachtigd om binnen zijn organisatie gegevens vast te leggen en te gebruiken. Indien deze gegevens verwerkt worden over personeel dat in dienst is van de verantwoordelijke, dient dit te gebeuren overeenkomstig de procedure in de Wet op de ondernemingsraden (hierna: WOR). Op basis van art. 22 lid 6 Wbp is dit artikel van overeenkomstige toepassing op persoonsgegevens betreffende een door de rechter opgelegd verbod naar aanleiding van onrechtmatig of hinderlijk gedrag.⁴⁴

Seksuele leven - Het bijzondere persoonsgegeven betreffende iemands seksuele leven is niet opgenomen in een specifiek artikel in de Wbp. Verwerking van dergelijke persoonsgegevens is enkel toegestaan als er sprake is van een ontheffing uit art. 23 Wbp. Dit artikel wordt hieronder in paragraaf 3.5.2 uitgewerkt.

§ 3.5.2 Algemene uitzonderingen om persoonsgegevens te verwerken

In art. 23 Wbp is een aantal algemene uitzonderingen op het verbod om bijzondere persoonsgegevens te verwerken geformuleerd.

⁴¹ Hooghiemstra & Nouwt 2007, p. 101.

⁴² Lioen & Van Munster-Frederiks/Van de Velde & Terhorst 2008, p. 75.

⁴³ Hooghiemstra & Nouwt 2007, p. 109-110.

⁴⁴ Hooghiemstra & Nouwt 2007, p. 117-118.

Deze bepaling is een restbepaling, die enkel van toepassing is indien de verwerking van bijzondere gegevens niet op art. 17 tot en met art. 22 Wbp gebaseerd kan worden.

Uitdrukkelijke toestemming - Indien 'uitdrukkelijke toestemming' is vereist, dient er sprake te zijn van een expliciete wilsuiting. Dat kan in woord, geschrift of gedrag. Voor de overige criteria wordt verwezen naar paragraaf 3.4.2. Een eenmaal gegeven toestemming kan op ieder willekeurig moment worden ingetrokken. Dit heeft echter geen gevolgen voor de gegevensverwerking die voor het moment van intrekking heeft plaatsgevonden.⁴⁵

De gegevens zijn door betrokkene duidelijk openbaar gemaakt - Het dient hier te gaan om een spontane gedraging van de betrokkene, waar niet door enig ander persoon met het oog op een eventuele gegevensverwerking om is gevraagd. Dat de gegevens openbaar zijn, moet volgen uit het gedrag van de betrokkene waaruit de intentie om openbaar te maken uitdrukkelijk blijkt.⁴⁶

Noodzakelijk in verband met een gerechtelijke procedure - Het kan voorkomen dat particulieren hun rechten in een gerechtelijke procedure niet kunnen uitoefenen, omdat zij niet beschikken over bepaalde gegevens van hun wederpartij. Deze gegevens kunnen noodzakelijk zijn voor de vaststelling, uitoefening of verdediging van een recht. In deze situatie zal er altijd een afweging van belangen moeten plaatsvinden van het recht van de betrokkene om bepaalde privacygevoelige gegevens geheim te houden en het recht van de wederpartij op een eerlijk proces.⁴⁷

Noodzakelijk ter voldoening aan een volkenrechtelijke verplichting - Het verbod om bijzondere gegevens te verwerken is alleen dan niet van toepassing indien er sprake is van een 'zwaarwegend algemeen belang'.⁴⁸

Noodzakelijk vanwege een zwaarwegend belang - In dit geval dient de verwerking noodzakelijk te zijn met het oog op een zwaarwegend algemeen belang en dienen er in het belang van de persoonlijke levenssfeer passende waarborgen te worden gecreëerd. Als de verwerking van bijzondere persoonsgegevens niet gebaseerd kan worden op één van de bepalingen uit art. 23 Wbp, is het mogelijk dat een verwerking zijn grondslag vindt in een bijzondere wet (de Wbp of een andere formele wet) of in een ontheffing van het CBP.⁴⁹

§ 3.5.3 Het burgerservicenummer

Art. 24 Wbp gaat in op de verwerking van identificatienummers. Het meest bekende identificatienummer is het BSN, voorheen het sofinummer. Gezien de plaats van deze bepaling in de wet, zou gedacht kunnen worden dat de identificatienummers behoren tot de bijzondere persoonsgegevens. Art. 16 Wbp somt de bijzondere persoonsgegevens echter limitatief op, dit betekent dat een identificatienummer geen bijzonder persoonsgegeven is. Gezien de aparte regeling van art. 24 Wbp, nemen deze nummers toch een bijzondere positie in de Wbp in.

Identificatienummers mogen op grond van art. 24 lid 1 Wbp enkel gebruikt worden indien dat bij wet is voorgeschreven, het gebruik noodzakelijk is voor de uitvoering van de betreffende wet of voor doeleinden zoals die bij de wet zijn bepaald. Het voorstaande betekent dat voor het gebruik van een identificatienummer een wettelijke grondslag noodzakelijk is. In art. 1 onderdeel d van de Wet algemene bepalingen burgerservicenummer (hierna: Wabb) wordt bepaald wie gebruikers kunnen zijn.

⁴⁵ *Kamerstukken II 1997/1998, 25892, nr. 3, p. 65-68 (MvT).*

⁴⁶ Hooghiemstra & Nouwt 2007, p. 125.

⁴⁷ Hooghiemstra & Nouwt 2007, p. 125.

⁴⁸ Hooghiemstra & Nouwt 2007, p. 126.

⁴⁹ Hooghiemstra & Nouwt 2007, p. 126.

Een gebruiker kan een overheidsorgaan zijn, of ieder ander dan een overheidsorgaan of degene aan wie het BSN is toegekend, voor zover deze werkzaamheden verricht waarbij het gebruik van het BSN bij of krachtens wet is voorgeschreven.⁵⁰

Krachtens art. 10 Wabb kan een overheidsorgaan bij het verwerken van persoonsgegevens in het kader van de uitvoering van zijn taak gebruik maken van het BSN. Voor een overheidsorgaan wordt in de Wabb een algemene wettelijke grondslag gecreëerd voor het gebruik van het BSN. Art. 1 onderdeel c Wabb bepaalt dat een overheidsorgaan een orgaan van een rechtspersoon is dat krachtens publiekrecht is ingesteld of een ander persoon of college is dat met enig openbaar gezag is bekleed. Conform deze definitie is de Diamantgroep als een overheidsorgaan aan te merken, dat krachtens de Wabb gerechtigd is om het BSN te gebruiken, mits dat noodzakelijk is voor de uitvoering van haar taak. De Wabb is een bijzondere wet ten opzichte van de Wbp en daarom gaat art. 10 Wabb voor op art. 24 Wbp.

18k is geen overheidsorgaan in het kader van de Wabb. Dergelijke instanties mogen het BSN slechts gebruiken voor zover daarvoor een (andere) wettelijke grondslag in een specifieke wet bestaat. Een werkgever moet bijvoorbeeld het BSN van zijn medewerkers verwerken in verband met de uitwisseling van gegevens met de Belastingdienst. Deze verplichting is geregeld in de belastingwetgeving⁵¹. Andere werkzaamheden blijven vallen onder het verbod van art. 24 Wbp.⁵² In de Wsw is niet bepaald dat een privaatrechtelijke organisatie, zoals 18k, het BSN mag gebruiken. Afhankelijk van het doel waarvoor het BSN wordt verwerkt, is verwerking dus wel of niet toegestaan.

§ 3.6 De verplichtingen van de verantwoordelijke

De verantwoordelijke die gegevens verwerkt moet voldoen aan een aantal verplichtingen. Respectievelijk worden in de paragrafen 3.6.1 tot en met 3.6.5 de geheimhoudingsplicht, de zorgplicht voor een deugdelijke beveiliging en bewaring, de meldingsplicht en de informatieplicht uitgewerkt.

§ 3.6.1 Geheimhoudingsplicht

Op de personen die gegevens verwerken, rust conform art. 12 lid 2 jo art. 15 Wbp een geheimhoudingsverplichting ten aanzien van de gegevens die zij verwerken. Art. 12 lid 2 Wbp geldt slechts voor zover deze personen niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift gebonden zijn aan een geheimhoudingsplicht.

§ 3.6.2 Beveiliging

Op grond van art. 13 Wbp dient de verantwoordelijke zorg te dragen voor passende technische en organisatorische maatregelen om de persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. Deze maatregelen dienen een passend beveiligingsniveau te garanderen, gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich mee kunnen brengen. De maatregelen dienen mede gericht te zijn op voorkoming van onnodige verzameling en verdere verwerking van persoonsgegevens. Het begrip 'passend' verwijst in de eerste plaats naar de technische middelen en de kosten die de beveiliging met zich meebrengt. Tevens dienen de beveiligingsmaatregelen conform het proportionaliteitsbeginsel in verhouding te staan tot de aard van de te beschermen gegevens. Hoe gevoeliger de gegevens zijn of hoe groter de bedreiging voor de persoonlijke levenssfeer is, des te zwaarder de beveiligingseisen wegen.

⁵⁰ Handleiding voor de gebruiker van het burgerservicenummer (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties) 2007, p. 12-13

⁵¹ Zie art. 53 Algemene Wet Inzake Rijksbelasting

⁵² Handleiding voor de gebruiker van het burgerservicenummer (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties) 2007, p. 5.

Onder het begrip 'onrechtmatige verwerking' valt aantasting van de persoonsgegevens, onbevoegde kennisname, wijziging of verstrekking daarvan. Ook moet de verantwoordelijke er zorg voor dragen dat de door hem ingeschakelde bewerker voldoende beveiligingsmaatregelen treft. Art. 14 lid 1 Wbp voorkomt dat de verantwoordelijke en de bewerker zich wat betreft hun verantwoordelijkheden achter elkaar verschuilen bij eventuele tekortkomingen in de gegevensverwerking.⁵³

§ 3.6.3 Bewaring

Persoonsgegevens mogen op basis van art. 10 Wbp niet langer bewaard worden dan noodzakelijk is voor de doeleinden waarvoor zij zijn verzameld of worden gebruikt. De Wbp voorziet dus niet in concrete bewaartermijnen voor bepaalde persoonsgegevens. Dit brengt met zich mee dat de verantwoordelijke zich dient af te vragen of er redenen zijn op grond waarvan gegevens vastgelegd kunnen blijven. Indien er voldoende redenen zijn, dan kan hij bepalen welke termijnen gelden om die gegevens te bewaren. Zijn deze termijnen verlopen, dan mogen de persoonsgegevens niet meer verwerkt worden, tenzij voor een ander verenigbaar doel, zoals statische archivering.⁵⁴

In bijzondere wetten, zoals de Archiefwet, kunnen nadere regels worden gesteld ten aanzien van de bewaartermijnen. In de Archiefwet gaat het enkel om archiefbescheiden van de Nederlandse overheid. Gezien zijn publiekrechtelijke karakter, is de Diamant-groep aan deze bepalingen gebonden. De Archiefwet kent geen algemene bewaartermijn, maar schrijft voor dat elk overheidsorgaan over een selectielijst moet beschikken, waarin staat welke stukken op termijn vernietigd moeten worden en welke stukken voor altijd bewaard moeten blijven.⁵⁵

Tot slot geeft het Vrijstellingsbesluit (hierna: Vb) voor bepaalde persoonsgegevens een indicatie van wat redelijke bewaartermijnen zijn. De genoemde bewaartermijnen dienen slechts als richtsnoer, aangezien het Vb alleen van toepassing is op de meldingsplicht. Op het moment dat de gegevens langer bewaard worden dan de genoemde termijn in het Vb, dient de gegevensverwerking doorgaans gemeld te worden bij het CBP, tenzij de bewaartermijn langer is vanwege een wettelijke bewaarplicht.⁵⁶

§ 3.6.4 Meldingsplicht

Op de verantwoordelijke rust de verplichting om in beginsel iedere gedeeltelijk of geheel geautomatiseerde verwerking van persoonsgegevens te melden bij het CBP, alvorens hij met de verwerking aanvangt. Paragraaf 4.2 gaat nader op deze plicht in.

§ 3.6.5 Informatieplicht

Het transparantiebeginsel – De verstrekking van informatie aan betrokkenen hangt nauw samen met het transparantiebeginsel. Het transparantiebeginsel is een rode draad door de Wbp en vindt zijn uitwerking in de informatieplicht, zoals deze is opgenomen in art. 33 en 34 Wbp. De informatieplicht is een uitwerking van het rechtmatigheidsbeginsel, neergelegd in art. 6 Wbp. Behoudens uitzonderingen is de gegevensverwerking slechts 'behoorlijk' in de zin van art. 6 Wbp, indien de betrokkene daarvan op de hoogte wordt gebracht. Op de verantwoordelijke rust de verplichting om op zijn eigen initiatief de betrokkene op de hoogte te stellen van het bestaan van de gegevensverwerking. Dit is een belangrijk instrument om de gegevensverwerking transparant te maken. Op de betrokkene rust geen onderzoeksplicht ten aanzien van de informatie die over hem wordt verzameld.⁵⁷

⁵³ Hooghiemstra & Nouwt 2007, p. 97.

⁵⁴ Kamerstukken II 1997/1998, 25892, nr. 3, p. 95 (MvT).

⁵⁵ *Bewaartermijnen van uw persoonsgegevens* (Informatieblad CBP).

⁵⁶ *Bewaartermijnen van uw persoonsgegevens* (Informatieblad CBP).

⁵⁷ Kamerstukken II 1997/1998, 25892, nr. 3, p. 149 (MvT).

De informatieplicht is ten opzichte van de WPR aangescherpt, aangezien de bepaling onder de WPR wel ruimte liet voor een beperkte onderzoeksplicht van de betrokkene.

De omvang - Op basis van art. 33 lid 2 Wbp deelt de verantwoordelijke in beginsel zijn identiteit en de doeleinden van de verwerking aan de betrokkene mee. In de praktijk zal de verantwoordelijke echter vaak nadere informatie dienen te verstrekken (conform art. 33 lid 3 jo art. 34 lid 3 Wbp), alvorens de gegevensverwerking als rechtmatig aangemerkt wordt. De omvang van de informatieplicht is tevens afhankelijk van de wijze waarop het contact tot stand komt. Op de verantwoordelijke rust een extra verantwoordelijkheid tot informeren als hij zelf het initiatief neemt tot het contact met de betrokkene. De betrokkene die de verantwoordelijke benadert, zal veelal op de hoogte zijn van diens identiteit en doeleinden.⁵⁸

De wijze - Indien de gegevens bij de betrokkene zelf worden verzameld, dient de verantwoordelijke de betrokkene conform art. 33 Wbp voorafgaand aan het moment van verkrijging op de hoogte te brengen. De informatie kan bijvoorbeeld opgenomen worden op het formulier waarop de betrokkene zijn gegevens invult. Als de betrokkene via een website zijn persoonsgegevens invult, volstaat een duidelijke verwijzing naar het privacystatement of -reglement. Indien de gegevens buiten de betrokkene om worden verkregen, geldt art. 34 Wbp. De informatie dient dan verstrekt te worden op het moment van vastlegging dan wel uiterlijk op het moment van de eerste verstrekking aan een derde.⁵⁹ De informatie moet op zodanige wijze worden verstrekt dat de betrokkene er daadwerkelijk de beschikking over krijgt. Een algemene verwijzing naar elders verkrijgbare informatie voldoet dus niet.⁶⁰ Indien het gaat om een beperkt aantal personen, dienen de betrokkenen persoonlijk geïnformeerd te worden. Als het om een grotere groep gaat mag de informatie verstrekt worden via bijvoorbeeld een blad of tijdschrift. Het is van belang dat iedere betrokkene wordt bereikt, een advertentie in een landelijk dag- of huis-aan-huisblad is dus niet altijd voldoende.⁶¹

Uitzonderingen - Er kan geen verdergaande actie van de verantwoordelijke ten aanzien van zijn informatieplicht worden geleverd, indien:

- de betrokkene niet te achterhalen is of de vereiste inspanning om de betrokkene op de hoogte te stellen niet in verhouding staat tot het doel dat daarmee wordt gediend. In dat geval dient de verantwoordelijke conform art. 34 lid 4 Wbp, als compenserende waarborg de herkomst van de gegevens vast te leggen, zodat de betrokkene altijd achteraf op zijn verzoek de informatie kan verkrijgen (zie paragraaf 3.7.1).
- de betrokkene in een situatie kan weten of weet dat, door wie en hoe de gegevens worden verwerkt. Dat is het geval als:
 - o een gedraging of verklaring van de verantwoordelijke aanleiding geeft tot het gerechtvaardigde vermoeden dat de betrokkene reeds op de hoogte is.⁶²
 - o dit uit een gedraging of verklaring van de betrokkene naar objectieve maatstaven kan worden afgeleid. Naar 'objectieve maatstaven' houdt in dat ieder ander dan de verantwoordelijke dit ook uit de gedragingen zou afleiden.
- de betrokkene de informatie toegezonden of uitgereikt heeft gekregen. Het is niet aan de verantwoordelijke om te controleren of de betrokkene de informatie ook daadwerkelijk gelezen heeft.⁶³

Conclusie - Indien aan de informatieplicht is voldaan, kan er geen sprake meer zijn van een onrechtmatige verkrijging. Nadere informatieverstrekking kan dan alleen nog aan de orde zijn, als er latere ontwikkelingen zijn, die aan de betrokkene hadden moeten worden meegedeeld, als zij op dat tijdstip bekend waren geweest.⁶⁴

⁵⁸ Kamerstukken II 1997/1998, 25892, nr. 3, p. 151-154 (MvT).

⁵⁹ Berkvens & Prins 2007, p. 39.

⁶⁰ Sauerwein & Linnemann 2002, p. 36.

⁶¹ Informatieplicht (Informatieblad CBP).

⁶² Kamerstukken II 1997/1998, 25892, nr.3 p. 151 en 155-156 (MvT).

⁶³ Sauerwein & Linnemann 2002, p. 33-34.

⁶⁴ Kamerstukken II 1997/1998, 25892, nr.3 p. 154-155 (MvT).

§ 3.7 Rechten van de betrokkene

Betrokkenen hebben een aantal rechten te weten: inzage, correctie en verzet. In paragraaf 3.7.1 tot en met 3.7.3 zullen deze rechten kort worden besproken.

§ 3.7.1 Inzage

Een belangrijk onderdeel van het transparantiebeginsel is dat iedereen in de gelegenheid moet zijn om na te kunnen gaan of en waar zijn persoonsgegevens worden verwerkt.⁶⁵ De betrokkene die gebruik wil maken van zijn inzage-recht kan conform art. 35 Wbp een verzoek richten aan de verantwoordelijke. Deze dient binnen vier weken een duidelijk en begrijpelijk schriftelijk overzicht van ten minste de volgende gegevens te verstrekken:

- de doeleinden van de verwerking;
- de categorieën van gegevens waarop de verwerking betrekking heeft;
- de ontvangers of categorieën van ontvangers;
- indien beschikbaar, informatie over de herkomst van de gegevens.

De verantwoordelijke kan slechts in uitzonderlijke gevallen een verzoek om inzage weigeren. Bijvoorbeeld ter bescherming van rechten en vrijheden van anderen of zichzelf.⁶⁶ Om de belangen van een derde te waarborgen is het noodzakelijk dat deze op de hoogte wordt gesteld van een voornemen tot honorering van een inzageverzoek en de gelegenheid krijgt om zijn zienswijze kenbaar te maken (mits hij daartoe een gerechtvaardigd belang heeft). De verantwoordelijke dient voordat hij aan het verzoek voldoet, op grond van art. 37 lid 2 Wbp, de identiteit van de betrokkene vast te stellen.⁶⁷

§ 3.7.2 Correctie

De betrokkene kan conform art. 36 Wbp de verantwoordelijke verzoeken zijn persoonsgegevens te corrigeren, wanneer deze feitelijk onjuist zijn, voor de doeleinden onvolledig of niet ter zake dienend zijn, dan wel in strijd zijn met een wettelijk voorschrift. Dit recht is echter niet bedoeld gegevens, bestaande uit indrukken, meningen en conclusies, waarmee de betrokkene zich niet kan verenigen, te corrigeren of te verwijderen.⁶⁸ Het correctierecht omvat:

- het verbeteren van persoonsgegevens;
- het aanvullen van persoonsgegevens;
- het verwijderen van persoonsgegevens;
- het afschermen van persoonsgegevens.

De verantwoordelijke beslist binnen vier weken na ontvangst van het verzoek schriftelijk in hoeverre hij aan het verzoek voldoet. Een weigering om aan het verzoek te voldoen dient gemotiveerd te worden. De verantwoordelijke dient de correctie zo spoedig mogelijk na de beslissing uit te voeren. Het correctierecht hangt niet samen met de vraag of de verantwoordelijke tekort is geschoten in zijn zorgplicht voor de juistheid van de gegevens.⁶⁹

§ 3.7.3 Verzet

De betrokkene kan op grond van art. 40 lid 1 Wbp het recht van verzet hebben. Dit recht bestaat alleen indien de verwerking plaatsvindt op grond van een publiekrechtelijke taak of een gerechtvaardigd belang van de verantwoordelijke of een derde (art. 8 sub e of sub f Wbp).

⁶⁵ Hooghiemstra & Nouwt 2007, p. 164.

⁶⁶ *Het geven van inzage in persoonsgegevens* (Informatieblad CBP).

⁶⁷ CBP 4 februari 2003, z2002-1511; Hooghiemstra & Nouwt 2007, p. 165 en 175-176.

⁶⁸ ABRvS 16 maart 2005, LJN AT0510.

⁶⁹ Hooghiemstra & Nouwt 2007, p. 174.

De gegevensverwerking is in beginsel rechtmatig, maar wordt pas onrechtmatig nadat de betrokkene op grond van een bijzondere situatie verzet aantekent en dit verzet gerechtvaardigd wordt geacht. Het aantekenen van verzet is vormvrij. De verantwoordelijke beoordeelt binnen vier weken of het verzet gerechtvaardigd is. Dit zal hij doen door de bij de verwerking spelende belangen opnieuw tegen elkaar af te wegen, daarbij rekening houdend met de door de betrokkene aangevoerde bijzondere omstandigheden.⁷⁰ Indien het verzet gerechtvaardigd is, dient de verantwoordelijke de verwerking onmiddellijk te beëindigen.

§ 3.8 Rechtsbescherming

In de paragrafen 3.8.1, 3.8.2 en 3.8.3 worden respectievelijk de mogelijkheden van een betrokkene besproken om bezwaar te maken, schadevergoeding te eisen of bij de rechter een verbod te eisen tegen de verwerking.

§ 3.8.1 Bezwaar

Een beslissing van een bestuursorgaan op verzoek van een betrokkene is conform art. 45 Wbp een besluit in de zin van de Algemene wet bestuursrecht (hierna: Awb). Het dient dan wel te gaan om verzoeken als bedoeld in art. 35 Wbp (recht op inzage), art. 36 Wbp (recht op correctie) en art. 40 Wbp (recht op verzet). Dit houdt in dat voor betrokkene bezwaar en beroep openstaat op grond van art. 7:1 lid 1 jo art. 8:1 lid 1 Awb. Zowel een toewijzing als een afwijzing is vatbaar voor bezwaar en beroep. Indien de betrokkene een dringend belang heeft bij het onmiddellijk staken van de verwerking, kan hij bij de bestuursrechter een voorlopige voorziening aanvragen op basis van art. 8:81 lid 1 Awb.⁷¹ De aan de betrokkene toegekende rechten hebben in beginsel alleen betrekking op de betrokkene zelf, al is het niet altijd te vermijden dat honorering van een verzoek ook enig inzicht kan geven in gegevens die op anderen betrekking hebben, waar de betrokkene ook belang bij heeft.

§ 3.8.2 Schadevergoeding

De verantwoordelijke kan op basis van art. 49 lid 3 Wbp aansprakelijk worden gesteld voor geleden schade, voor zover hij in strijd heeft gehandeld met de wettelijke voorschriften in de Wbp. De betrokkene kan besluiten zich hiervoor tot de rechtbank te wenden. Als de verantwoordelijke kan bewijzen dat de schade hem niet kan worden toegerekend, kan hij geheel of gedeeltelijk ontheven worden van deze aansprakelijkheid. Een bewerker is zelfstandig aansprakelijk voor zijn aandeel in de schade, maar ook de verantwoordelijke is voor deze schade aansprakelijk, aangezien de verwerking altijd onder zijn verantwoordelijkheid plaatsvindt.⁷² De schade kan bestaan uit materiële en/of immateriële schade. Materiële schade is schade aan het bezit of vermogen van iemand, die direct in geld is uit te drukken. Immateriële schade is bijvoorbeeld aantasting van iemands goede naam.⁷³

§ 3.8.3 Verbod

Indien een betrokkene schade lijdt, of dreigt te lijden, doordat een verantwoordelijke in strijd met de Wbp handelt, kan de rechter hem op grond van art. 51 Wbp dergelijk gedrag verbieden en hem verplichten maatregelen te treffen tot herstel van de gevolgen van dat gedrag. De betrokkene dient hiertoe een verzoekschrift in bij de rechter.

⁷⁰ Hooghiemstra & Nouwt 2007, p. 179-180.

⁷¹ Hooghiemstra & Nouwt 2007, p. 190.

⁷² Hooghiemstra & Nouwt 2007, p. 194.

⁷³ 'Openbaar Ministerie', <www.om.nl/u_en_het_om/juridisch_jargon/>; zoektermen: materiële schade en immateriële schade.

4. Het College bescherming persoonsgegevens

Het CBP is een belangrijk orgaan als het gaat om de verwerking van persoonsgegevens. Aangezien de Diamant-groep niet om het CBP heen kan als zij overeenkomstig de Wbp wenst te handelen, wordt in dit hoofdstuk respectievelijk ingegaan op de taken van het CBP, de meldingsprocedure, de functionaris voor de gegevensbescherming (hierna: FG) en de sanctiemogelijkheden van het CBP.

§ 4.1 Het CBP en de taken van dit orgaan

Om te bevorderen dat de privacy van de burgers voldoende gewaarborgd wordt en de wetten die het gebruik van persoonsgegevens regelen worden nageleefd, is in 2001 het CBP ingesteld. Het CBP is primair opgericht om toezicht te houden. Het functioneren van het CBP wordt in art. 51 tot en met art. 61 Wbp geregeld.

Opgesomd heeft het CBP onder andere de volgende taken en bevoegdheden:

- toetsing van gedragscodes en reglementen aan de normen in de Wbp;
- kosteloze bemiddeling bij geschillen over de uitoefening van rechten;
- uitvoeren van (ambtshalve) onderzoek naar bepaalde gegevensverwerkingen;
- bijhouden van een meldingenregister;
- ontheffing verlenen van het verbod om bijzondere gegevens te verwerken;
- behandeling van klachten;
- uitvoeren van voorafgaand onderzoek;
- opleggen van sancties aan verantwoordelijken.⁷⁴

§ 4.2 Meldingsprocedure

In verband met de meldingsprocedure is een tweetal zaken van belang, te weten: de melding en de vrijstelling van melding en het voorafgaand onderzoek. Deze onderwerpen worden respectievelijk besproken in paragraaf 4.2.1 en 4.2.2.

§ 4.2.1 De melding en vrijstelling van melding

In paragraaf 3.6.4 is reeds kort ingegaan op de meldingsplicht. Op iedere verantwoordelijke rust in beginsel de verplichting om elke gedeeltelijk of geheel geautomatiseerde verwerking van persoonsgegevens te melden bij het CBP. De verantwoordelijke dient de melding te doen voordat hij met de verwerking aanvangt. De meldingsplicht is geregeld in art. 27 lid 1 Wbp. Handmatige verwerkingen hoeven in beginsel niet te worden gemeld, tenzij de verwerking onderworpen is aan een voorafgaand onderzoek (zie paragraaf 4.2.2). Art. 28 lid 1 Wbp bepaalt waaruit de melding dient te bestaan. De verantwoordelijkheid voor de beslissing om te melden en om dit juist en volledig te doen, ligt bij de organisatie zelf.

Het melden van gegevensverwerkingen zorgt voor openheid en daarmee controleerbaarheid voor de betrokkenen. Zij worden in staat gesteld om kennis te nemen van de gegevens die over hen worden verwerkt en op basis van welke doelen dat gebeurt. Zodoende worden de betrokkenen in staat gesteld hun rechten uit te oefenen (zie paragraaf 3.7).

Het melden bevordert dus de transparantie. Daarnaast kan het CBP via de melding controleren of de verantwoordelijke de gegevens verwerkt overeenkomstig de vooraf geformuleerde doelen. Op deze wijze wordt effectiever toezicht mogelijk. De melding wordt opgenomen in een openbaar meldingsregister en is te raadplegen op de site van het CBP.

⁷⁴ De Wet Bescherming Persoonsgegevens. Over de bescherming van uw persoonlijke gegevens, CBP 2001, p. 8-11; 'Overzicht van de taken en bevoegdheden van het CBP', <www.cbpreb.nl/Pages/ind_cbp.aspx>.

Indien de verantwoordelijke een verwerking heeft gemeld, wil dit niet zeggen dat de betreffende verwerking ook goedgekeurd is door het CBP. Het CBP volstaat met een formele toets of de melding compleet is.⁷⁵ De verantwoordelijke blijft zelf verantwoordelijk voor de beoordeling of een bepaalde gegevensverwerking al dan niet rechtmatig is.

Het niet melden kan leiden tot een boete van het CBP op grond van art. 66 Wbp. Vanaf 2003 zijn er 29 boetes opgelegd variërend van € 3.000 tot € 15.000. Per overtreding kan een boete van maximaal € 4.500 worden opgelegd. De afgelopen jaren zijn een aantal zaken voorgelegd aan de rechter.⁷⁶

Een aantal verwerkingen is vrijgesteld van melding. Dit geldt voor de verwerkingen die zijn opgenomen in het Vb. Deze vrijstellingen hebben betrekking op verwerkingen die veel voorkomen en standaard zijn, die met waarborgen omkleed zijn en waarvan algemeen bekend is dat zij plaatsvinden. Indien sprake is van een vrijstelling blijven de overige regels uit de Wbp gelden. Verwerkingen zijn niet vrijgesteld als er meer dan één verantwoordelijke is, er gegevens naar landen buiten de Europese Unie (hierna: EU) worden doorgegeven of een gegevensverwerking specifieke risico's met zich meedraagt en is onderworpen aan een voorafgaand onderzoek.⁷⁷

§ 4.2.2 Voorafgaand onderzoek

Bij bepaalde gegevensverwerkingen is het risico van een inbreuk op fundamentele rechten en vrijheden van betrokkenen groot. Voor deze verwerkingen is een voorafgaand onderzoek conform art. 31 en art. 32 Wbp verplicht. Dit onderzoek vormt een extra controlemiddel voor het CBP.⁷⁸ Indien de verantwoordelijke voornemens is gegevens te verwerken waarin een voorafgaand onderzoek noodzakelijk is, is hij verplicht dit bij de melding aan het CBP expliciet aan te geven. Het CBP stelt vervolgens een vooronderzoek in van maximaal vier weken. Na deze periode ontvangt de verantwoordelijke een besluit van het CBP om al dan niet tot nader onderzoek over te gaan. De verantwoordelijke dient de verwerking uit te stellen, totdat het onderzoek is afgerond of hij een bericht heeft ontvangen dat niet tot nader onderzoek wordt overgegaan. Indien het CBP besluit tot nader onderzoek, mag dit maximaal twintig weken duren.⁷⁹ Naar aanleiding van dit onderzoek geeft het CBP een niet-bindende verklaring af over de rechtmatigheid van de voorgenomen gegevensverwerking. Deze verklaring is een besluit in de zin van de Awb. Dit betekent dat bezwaar (bij het CBP) en beroep bij de rechtbank openstaat conform art. 7:1 lid 1 jo art. 8:1 lid 1 Awb.⁸⁰

§ 4.3 De functionaris voor de gegevensbescherming

De FG is een door de verantwoordelijke aangestelde toezichthouder binnen het eigen bedrijf, die er op toeziet dat verwerking van persoonsgegevens overeenkomstig de Wbp plaatsvindt. Art. 62 tot en met art. 64 Wbp gaan over de FG. De FG dient als aanspreekpunt voor betrokkenen en draagt bij aan het vergroten van het privacybewustzijn binnen de organisatie.⁸¹ Alleen een persoon, die voldoende betrouwbaar wordt geacht, kan benoemd worden tot FG. Het CBP moet op de hoogte worden gebracht van de aanstelling van een FG. De Diamant-groep heeft op dit moment geen FG aangesteld.

Hieronder staan de belangrijkste taken van een FG opgenoemd. Een FG dient:

- te beschikken over toereikende kennis van de organisatie, de gegevensverwerkingen binnen de organisatie, de betrokken belangen en privacywetgeving;

⁷⁵ Melden en vrijstellingen (Informatieblad CBP).

⁷⁶ Rechtbank 's-Hertogenbosch 18 januari 2005, LJN AT0462

⁷⁷ Melden en vrijstellingen (Informatieblad CBP).

⁷⁸ De Vries & Rutgers 2001, p. 37-38.

⁷⁹ Voorafgaand Onderzoek (Informatieblad CBP).

⁸⁰ Hooghiemstra & Nouwt 2007, p. 481-482.

⁸¹ De functionaris voor de gegevensbescherming (Informatieblad CBP).

- een volledig onafhankelijke positie te hebben (aanwijzingen zijn dus niet toegestaan) en toegang te hebben tot alle systemen waarmee gegevens worden verwerkt;
- zich te houden aan zijn geheimhoudingsplicht;
- verslag uit te brengen over onregelmatigheden aan de verantwoordelijke;
- niet-bindende adviezen en aanbevelingen uit te brengen richting de verantwoordelijke;
- een register bij te houden van de bij hem aangemelde gegevensverwerkingen;
- klachten te behandelen;
- voorlichting te geven;
- interne regelingen te ontwikkelen.⁸²

§ 4.4 De privacy officer

Zoals blijkt uit hetgeen hierboven omschreven is, is de FG een officieel persoon met taken en bevoegdheden die vastgelegd zijn in de Wbp. In plaats van het aanstellen van een FG, kan een organisatie ook besluiten een privacy officer aan te stellen.⁸³ Het grootste onderscheid is dat een privacy officer minder 'officieel' is. Een organisatie kan zelf beslissen een privacy officer aan te stellen en hoeft deze aanstelling, in tegenstelling tot de FG, niet bij het CBP te melden. Vanzelfsprekend is het van belang dat de privacy officer kennis heeft van de relevante wetgeving op privacygebied en daarnaast gedurende langere tijd aandacht vraagt voor het onderwerp privacy. De belangrijkste taak van de privacy officer is gelegen in zijn toetsende functie. De privacy officer dient de gegevensverwerkingen in kaart te brengen en (steekproefsgewijs) te kijken of medewerkers de Wbp naleven. Verder kan de privacy officer een belangrijke rol spelen in het bijwerken van de meldingen aan het CBP en in het naleven van beveiligingsvoorschriften. De overige taken en bevoegdheden zijn door een organisatie zelf te bepalen, echter veelal te vergelijken met die van een FG.

§ 4.5 Sancties

Het CBP heeft verschillende sanctiemogelijkheden indien een verantwoordelijke zich niet aan de regels in de Wbp houdt. In onderstaande paragrafen worden respectievelijk de bestuursdwang, de last onder dwangsom, de bestuurlijke boete en de strafrechtelijke mogelijkheden besproken.

§ 4.5.1 Bestuursdwang en last onder dwangsom

In art. 65 Wbp wordt aan het CBP de bevoegdheid toegekend om bestuursdwang⁸⁴ toe te passen, indien een verantwoordelijke naar oordeel van het CBP in strijd handelt met de Wbp. Het CBP kan tot dit oordeel komen naar aanleiding van een voorafgaand onderzoek, een ambtshalve onderzoek of op verzoek van de betrokkene. Voordat het CBP overgaat tot het daadwerkelijk toepassen van bestuursdwang, krijgt de verantwoordelijke nog één mogelijkheid de overtreding zelf ongedaan te maken. Doet de verantwoordelijke dit niet, dan zal het CBP de overtreding ongedaan maken op kosten van de verantwoordelijke.⁸⁵

In plaats van het toepassen van een bestuursdwang, kan het CBP ook een last onder dwangsom⁸⁶ opleggen. Ook in deze situatie krijgt de verantwoordelijke nog een termijn om de overtreding ongedaan te maken. Nadat de gestelde termijn verlopen is, mag het CBP de vastgestelde dwangsom (tot een vastgesteld maximum, afhankelijk van de zaak) innen, totdat de verantwoordelijke de overtreding ongedaan maakt.

⁸² Hooghiemstra & Nouwt 2007, p. 203-205; De Vries & Rutgers 2007, p. 43-44; *De functionaris voor de gegevensbescherming* (Informatieblad CBP).

⁸³ De informatie in deze paragraaf is afkomstig van de heer Onno de Gier, medewerker van de afdeling juridische zaken van de gemeente Tilburg. Een volledige weergave van het gesprek is bijgevoegd in bijlage II.

⁸⁴ De uitvoering van bestuursdwang volgt de regels in de Awb, te weten art. 5:21 tot en met art. 5:31 Awb.

⁸⁵ De Vries & Rutgers 2001, p. 45.

⁸⁶ Het opleggen van een last onder dwangsom is geregeld in art. 5:32 tot en met art. 5:36 Awb.

Dat dit maximum erg hoog kan liggen blijkt uit de dwangsom die het CBP oplegde aan een handelsbureau: € 600 per overtreding, met een maximum van €120.000. Deze uitspraak is overeind gebleven bij de rechter.⁸⁷

Het besluit tot toepassen van bestuursdwang of het opleggen van een last onder dwangsom, zijn beschikkingen waartegen bezwaar (bij het CBP) en beroep bij de rechtbank openstaat conform art. 7:1 lid 1 jo art. 8:1 lid 1 Awb.

§ 4.5.2 Bestuurlijke boete

Op grond van art. 66 Wbp heeft het CBP de bevoegdheid om een bestuurlijke boete van ten hoogste € 4.500,- op te leggen, indien de verantwoordelijke art. 27, 28 of 79 lid 1 Wbp overtreedt. Het CBP kan een bestuurlijke boete opleggen indien de verantwoordelijke:

- niet of te laat meldt terwijl dit wel verplicht was;
- melding van een niet-geautomatiseerde verwerking achterwege laat, voor zover deze onderworpen is aan een voorafgaand onderzoek;
- start met de verwerking alvorens melding heeft plaatsgevonden;
- onvolledig of onjuist heeft gemeld;
- nalaat de doeleinden van de gegevensverwerking te melden;
- wijzigingen in de opgave van de melding te laat of niet heeft doorgegeven;
- de gegevensverwerkingen die reeds plaatsvonden, niet binnen een jaar na de inwerkingtreding van de Wbp, in overeenstemming met de wet heeft gebracht door deze alsnog te melden bij het CBP.
- een specifieke categorie van verwerkingen niet bewaart of vastlegt.

Het CBP mag geen boete opleggen, als de verantwoordelijke aannemelijk kan maken dat de overtreding hem niet kan worden toegerekend. Het CBP dient bij de vaststelling van de hoogte van de boete in ieder geval rekening te houden met de ernst en de duur van de overtreding. Ook andere factoren, zoals recidive en de bereidwilligheid van de verantwoordelijke, kunnen een rol spelen. Art. 70 lid 1 Wbp bepaalt dat een boete wordt opgelegd bij beschikking van het CBP. Dit betekent dat bezwaar bij het CBP en beroep bij de rechtbank op grond van art. 7:1 lid 1 Awb jo art. 8:1 lid 1 Awb openstaat.⁸⁸

§ 4.5.3 Strafrechtelijke sancties

Conform art. 75 lid 1 en lid 2 Wbp kan het Openbaar Ministerie tegen de hieronder genoemde overtredingen van de Wbp strafvervolgung instellen:

- op basis van dezelfde gronden die ook een bestuurlijke boete rechtvaardigen (zie paragraaf 4.5.2), dus op basis van art. 27, 28 en 79 lid 1 Wbp;
- bij overtreding van het verbod gericht tot een verantwoordelijke die buiten de EU is gevestigd, om in Nederland gegevens te verwerken zonder een vertegenwoordiger aan te wijzen, art. 4 lid 3 Wbp;
- bij doorgifte van gegevens naar landen buiten de EU waarvan op Europees niveau is bepaald dat er geen passend beschermingsniveau aanwezig is, art. 78 lid 1 onder a Wbp.⁸⁹

Overtredingen van deze bepalingen zijn op grond van art. 75 lid 1 Wbp overtredingen met als maximale straf een geldboete van de tweede categorie (maximaal € 3.700). Indien de verantwoordelijke de bepalingen uit art. 75 lid 1 Wbp opzettelijk overtreedt, is er sprake van een misdrijf blijkens art. 75 lid 3 Wbp. De maximale straf is dan een gevangenisstraf van zes maanden of een geldboete van de derde categorie (maximaal € 7.400,-).

⁸⁷ Vزر. Rb. 's-Gravenhange 31 maart 2004, nr. AWB04/166 BESLU

⁸⁸ Hooghiemstra & Nouwt 2007, p. 207-208 en 210.

⁸⁹ Hooghiemstra & Nouwt 2007, p. 212.

5. Privacy binnen de Diamant-groep

In dit hoofdstuk wordt ingegaan op de verwerking van gegevens binnen de Diamant-groep. Om onderbouwde uitspraken te kunnen doen over privacygerelateerde onderwerpen binnen de Diamant-groep is een vragenlijst uitgezet onder verschillende personen binnen de organisatie. Het doel van de vragenlijst was om aan de hand van de resultaten een beeld te krijgen van de huidige stand van zaken ten aanzien van gegevensverwerking. De vragenlijsten zijn verspreid onder geselecteerde medewerkers, werkzaam in verschillende functies en op verscheidene niveaus, om zo een compleet mogelijk beeld te krijgen. In bijlage III is de gebruikte vragenlijst en de bijbehorende toelichting toegevoegd.

In onderstaande paragrafen zullen de belangrijkste resultaten en conclusies naar aanleiding van de vragenlijsten worden besproken. Van de resultaten is een totaaloverzicht gemaakt, dat bijgevoegd is in bijlage IV. In totaal zijn er 68 vragenlijsten verspreid, waarvan er 56 terug zijn ontvangen. Door de hoge respons van ruim 82%, is het gerechtvaardigd om onderbouwde uitspraken te doen met betrekking tot de huidige stand van zaken ten aanzien van privacy en deze resultaten te vertalen naar de gehele organisatie.

Paragraaf 5.1 gaat over het gebruik van analoge persoonsdossiers en het informatiesysteem Compas. De bekendheid van de Wbp onder medewerkers staat centraal in paragraaf 5.2. In paragraaf 5.3 tot en met paragraaf 5.8 wordt respectievelijk ingezoomd op welke gegevens worden verwerkt, op welke wettelijke grondslag dat gebeurt, wie persoonsgegevens verwerken, de betrokkenen, interne en externe verstrekking, de wijze waarop de persoonsgegevens worden verwerkt en voor welke doeleinden. De huidige beschermingsmaatregelen en de toereikendheid van deze maatregelen worden besproken in paragraaf 5.9. In paragraaf 5.10 worden de verplichtingen van de verantwoordelijke besproken en in paragraaf 5.11 de rechten van betrokkenen. Het melden van de gegevensverwerkingen bij het CBP staat in paragraaf 5.12 centraal en het belang van een privacyreglement in paragraaf 5.13.

Binnen de Diamant-groep zijn op dit moment twee reglementen op het gebied van privacy van kracht. Enerzijds bestaat de 'Regeling persoonsdossiers 2004', anderzijds het 'Reglement kantoorfaciliteiten 2005'. Deze reglementen zijn inmiddels behoorlijk verouderd, gezien de vaststellingsdata. In bijlage V en bijlage VI zijn beide reglementen bijgevoegd. De Diamant-groep is recentelijk bezig geweest met het opstellen van het 'Reglement cameratoezicht'. Dit reglement is bijgevoegd in bijlage VII. Een omschrijving van de bestaande knelpunten van deze reglementen is opgenomen in bijlage VIII, aangezien dit onderzoek niet tot doel heeft de knelpunten in de huidige reglementen te onderzoeken, maar juist gericht is op het opstellen van een nieuw privacyreglement dat de toets van de Wbp kan doorstaan.

5.1 Persoonsdossiers en Compas

De Diamant-groep maakt gebruik van analoge persoonsdossiers. Daarnaast wordt gebruik gemaakt van een digitaal informatiesysteem om persoonsgegevens te verwerken.

§ 5.1.1 Persoonsdossiers

Analoge persoonsdossiers - Binnen de organisatie is bepaald dat de analoge persoonsdossiers op dit moment leidend zijn en blijven ten opzichte van de digitale dossiers in Compas. In paragraaf 1.3 is reeds een en ander uitgewerkt met betrekking tot de opbouw van de analoge persoonsdossiers en het onderscheid tussen de a- en b-dossiers. Inmiddels worden diverse stukken uit de analoge dossiers gedigitaliseerd en verwerkt in Compas. Alle persoonsdossiers worden opgeborgen in het persoons- en beleidsarchief.

Schaduwdoossiers - Binnen de organisatie is bekend dat medewerkers in bepaalde functies vanuit praktische overwegingen schaduwdoossiers bijhouden. Zij hoeven dan niet naar het archief om bepaalde doossiers in te zien. Het voorstaande maakt dat het oorspronkelijke dossier vaak incompleet is en de kans dat stukken kwijtraken groot is. Om deze reden is het bijhouden van schaduwdoossiers verboden. Het bestaan van dergelijke doossiers is uit de vragenlijsten niet duidelijk naar voren gekomen. Gezien het bestaande verbod, viel dit echter ook niet te verwachten. Het bijhouden van schaduwdoossiers is in strijd met de Wbp. Op de eerste plaats wordt niet gehandeld conform het rechtmatigheidsbeginsel. Daarbij zijn de doeleinden voor het aanleggen van een schaduwdoossier onverenigbaar met de doeleinden van de oorspronkelijke verwerking. Tot slot kan de verwerking niet gebaseerd worden op één van de wettelijke grondslagen uit de Wbp. Het bijhouden van schaduwdoossiers vormt dus een inbreuk op het recht van privacy van betrokkenen.

§ 5.1.2 Compas

Compas verschaft geautoriseerde medewerkers toegang tot informatie over medewerkers in dienst van de Diamant-groep.⁹⁰ Geautoriseerde medewerkers kunnen informatie toevoegen, wijzigen en/of verwijderen. Toegang tot bepaalde informatie en een goed informatiesysteem zijn noodzakelijk om de wettelijke verplichtingen in de Wsw goed uit te kunnen voeren.

Voordat medewerkers toegang kunnen krijgen tot Compas, vraagt het programma om een gebruikersnaam en wachtwoord. In het systeem wordt een onderscheid gemaakt tussen het personeels- en cliëntdossier. In het personeelsdossier staan de volgende gegevens: NAW, geboortedatum, BSN, opleiding, arbeidsverleden, soort dienstverband, werktijden, plaatsing (intern of extern), leidinggevende, gegevens omtrent het functioneren, salaris, (reden van) ziekte, notities en alle verstuurd brieven. In het cliëntdossier staan gegevens als: NAW, historie qua opleiding, werk en uitkering, Wsw-indicatie, de plaatsing op de wachtlijst en de gestarte trajecten. Gezien de grote hoeveelheid informatie in Compas, is dit systeem voor de goede uitvoering van de opdrachten voor de Diamant-groep van groot belang.

Enig inzicht in de opbouw van Compas is van belang om de problemen met het programma te kunnen plaatsen. Binnen de Diamant-groep zijn medewerkers werkzaam op basis van verschillende regelingen, zoals de Wsw of de Wet Werk en Bijstand (hierna: WWB). Elk dossier van een medewerker is binnen Compas geplaatst bij een afdeling. Een gebruiker kan een dossier pas zien wanneer hij een rechtenprofiel heeft waarbinnen hij is gemachtigd voor de betreffende regeling én afdeling. Alle gegevens zijn slechts te benaderen via een menu. Als de gebruiker niet via enig profiel voor een menu is gemachtigd, kan hij die gegevens niet zien. In elk menu staan meerdere tabbladen. Een gebruiker krijgt alleen iets te zien op een tabblad als hij daartoe via een profiel is gemachtigd. Op een tabblad zijn de gegevens ingedeeld in groepen. Per (sub)groep (bijvoorbeeld 'adresgegevens') kan worden bepaald of de gebruiker die gegevens mag lezen, wijzigen, toevoegen en/of verwijderen.

Hieronder volgt een niet limitatieve lijst van veel voorkomende problemen met Compas en de medewerkers die met het systeem werken.

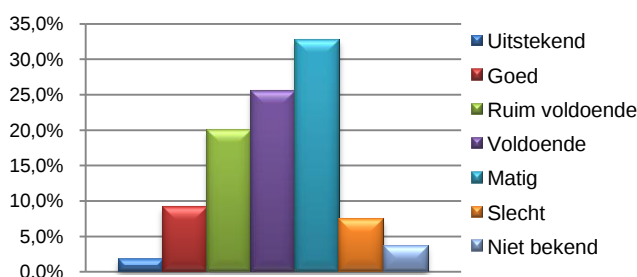
- Gegevens van Sw-medewerkers kunnen gemiddeld gezien worden door 120 gebruikers.
- Er is een aantal klachten bekend van medewerkers van wie privacygevoelige informatie werd verspreid binnen de organisatie, door medewerkers die in Compas bepaalde informatie konden raadplegen.
- Als medewerkers intern van functie veranderen, wordt dit door de leidinggevende niet of niet tijdig doorgegeven. Hierdoor behoudt de medewerker zijn oude rechtenprofiel, terwijl hij ook een nieuw rechtenprofiel, behorende bij zijn nieuwe functie, toegekend krijgt. Op deze wijze stapelen de rechtenprofielen van deze medewerker zich op.

⁹⁰ De informatie in deze paragraaf is voor een belangrijk deel afkomstig van Jan den Brok, technisch Compas-beheerder werkzaam op de afdeling Informatie & Automatiseringen van de Diamant-groep. Een volledig verslag van het interview is bijgevoegd in bijlage IX.

- Enige tijd geleden bleek dat onlangs gestart was met het plaatsen van kopieën van het legitimatiebewijs en de bankpas in Compas, zonder de betreffende medewerkers hier vooraf over te informeren. Deze informatie kan door een grote groep gebruikers worden geraadpleegd. Hoewel de medewerkers geacht worden integer te zijn, dient de Diamant-groep af te wege van deze verwerking wel noodzakelijkheid is. Daarbij is de werkgever verplicht zorg te dragen voor passende beveiligingsmaatregelen, hetgeen nu niet het geval is. Na een klacht van een medewerker worden voorlopig geen nieuwe kopieën in Compas geplaatst.
- Medewerkers plaatsen regelmatig gevoelige informatie met betrekking tot verzuim, functioneren of medische gegevens in Compas. Doordat de gebruikers Compas vaak niet op een juiste manier gebruiken, worden deze gegevens niet altijd op de goede wijze, met het juiste beveiligingsniveau, verwerkt. Subjectieve informatie (zonder onderliggende feiten), zoals conclusies of gevoelens van medewerkers zelf, wordt vaak in Compas geplaatst. Dit probleem hangt samen met het feit dat medewerkers onvoldoende worden ingelicht over het gebruik van Compas. In paragraaf 5.9.3 wordt hier nader op ingegaan.
- Als een gebruiker notities mag lezen, geldt dat altijd minstens voor de notitiesoort 'algemeen'. In 2009 bleek, naar aanleiding van een klacht, dat onder deze notitiesoort allerlei opmerkingen staan genoteerd, die (zeer) privacygevoelige informatie bevatten.
- Vergelijkbare problemen spelen rondom geïmporteerde documenten. Gebruikers zijn verplicht daarvoor een documentsoort te kiezen met bijbehorende rechtenconsequenties. Veel gebruikers kiezen gemakshalve 'algemeen', daarmee maken ze het document leesbaar voor iedereen die documenten kan lezen. Onder de op deze wijze geïmporteerde documenten bevinden zich onder andere medische verslagen.
- In Compas is het op dit moment zo geregeld dat een medewerker die documenten kan aanmaken, tevens alle documenten (zoals brieven en rapportages) kan lezen en wijzigen.
- Een autorisatiebesluit, waarin wordt bepaald welke autorisaties voor welke functiegroepen bestaan en wie beslist over het aanmaken van nieuwe autorisaties en deze toekent, ontbreekt. Op dit moment vraagt de leidinggevende van een nieuwe medewerker diens rechten aan. Meestal gebeurt dit door de opgave van de naam van een collega waarvan de rechten mogen worden overgenomen.
- Sinds kort doet Compas aan 'logging'. Dit betekent dat van een groot aantal gegevens valt na te gaan wie ze wanneer heeft voorzien van welke waarde.

§ 5.2 De bekendheid met de Wbp

Uit een recentelijk gepubliceerd onderzoek van NPS-Nipo in samenwerking met KPMG⁹¹ blijkt dat er vaak geen eenduidig beeld bestaat van het begrip 'privacy' binnen organisaties. Hierdoor zal de waarborging van de privacy nooit sluitend kunnen zijn. Aan de medewerkers van de Diamant-groep is gevraagd hoe goed zij naar hun mening op de hoogte zijn van de hoofdlijnen in de Wbp. In onderstaande tabel zijn de resultaten in percentages weergegeven.



Figuur 1: Resultaten kennis hoofdlijnen Wbp

Uit gesprekken met diverse mensen binnen de Diamant-groep is gebleken dat het privacybewustzijn onder de medewerkers niet groot is.

⁹¹ Het betreft hier een onderzoek gehouden onder 300 Nederlandse organisaties in private en publiekrechtelijke sectoren naar de begripsvorming rondom privacy. Koorn 2010, p. 47-50.

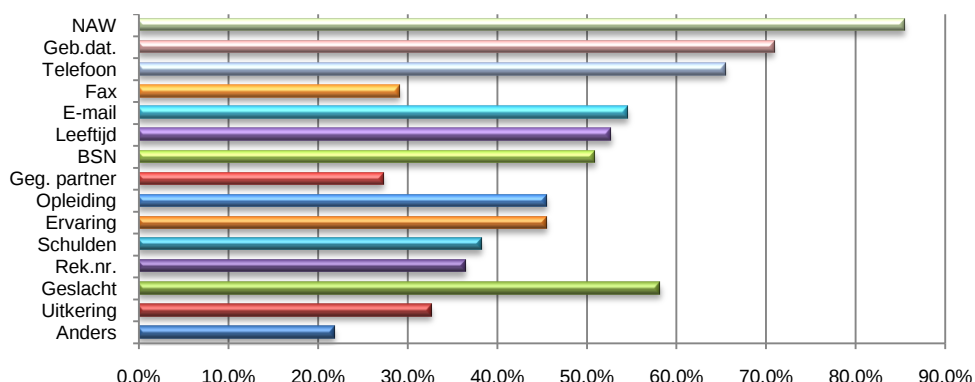
De privacywetgeving, waaronder de Wbp, leeft niet binnen de organisatie. Dit blijkt ook uit het feit dat de kennis van de hoofdlijnen van de Wbp onder de maat is. Daarnaast is gebleken dat medewerkers vaak hun eigen kennis van de Wbp overschatten. Van de medewerkers die aangeven voldoende of meer kennis te hebben van de Wbp, blijkt namelijk uit de overige resultaten van de vragenlijst, dat zij minder op de hoogte zijn dan zij zelf inschatten. Duidelijk is geworden dat de basiskennis van relevante begrippen uit de Wbp vaak ontbreekt en dat medewerkers onvoldoende deskundig zijn om hun eigen handelen te toetsen aan de Wbp. In de volgende paragrafen worden deze stellingen verder onderbouwd.

§ 5.3 Welke persoonsgegevens worden verwerkt en is dit wettelijk toegestaan?

Middels de vragenlijsten is in beeld gebracht welke algemene en bijzondere persoonsgegevens de medewerkers verwerken. Daarbij wordt in deze paragraaf ingegaan op de toereikendheid van de autorisaties en de verschillende verwerkingshandelingen.

§ 5.3.1 De verwerking van algemene persoonsgegevens

Tijdens het invullen van de vragenlijst bleek dat bij de medewerkers veel onduidelijkheid bestond over de begrippen ‘verwerken’ en ‘persoonsgegevens’. De toelichting op deze begrippen bleek niet voldoende helderheid te verschaffen. Medewerkers waren veelal van mening dat zij geen persoonsgegevens verwerkten. Dat kwam enerzijds door de gedachte dat zij niet te maken hadden met persoonsgegevens, anderzijds doordat zij van mening waren dat er geen sprake was van verwerken. Door een mondelinge toelichting of doorvragen bleek dat, op één medewerker na, alle medewerkers persoonsgegevens verwerkten. In onderstaand figuur is per persoonsgegeven weergegeven hoeveel procent van de medewerkers deze verwerkt.



Figuur 2: Verwerking algemene persoonsgegevens

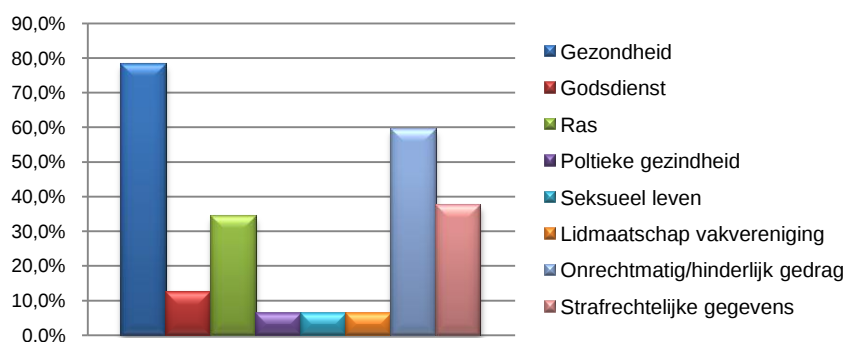
Zoals verwacht worden NAW, geboortedatum en geslacht vaak verwerkt. Wat in bovenstaand figuur echter opvalt, is het feit dat medewerkers relatief vaak gegevens als het BSN, de gegevens van de partner, opleiding, werkervaring, schulden en uitkering verwerken. Dit is enerzijds inherent aan een Sw-bedrijf, anderzijds dient de gegevensverwerking ook dan te voldoen aan de noodzakelijkheidseis. Aangezien deze gegevens verwerkt worden om de verplichting die voortkomt uit de Wsw goed uit te voeren, kan gesteld worden dat deze verwerkingen noodzakelijk zijn. Van de partner wordt voornamelijk naam en adres verwerkt, in verband met de adressering van de post. De medewerker kan aangeven dit liever niet te hebben, hier wordt ook gehoor aan gegeven. Ook deze verwerking is noodzakelijk.

Ruim 20% geeft aan andere persoonsgegevens te verwerken dan hierboven opgesomd. Het bleek voornamelijk te gaan om verzuim- en indicatiegegevens, gegevens over plaatsing binnen de Diamant-groep, persoonlijke omstandigheden, ziekte, voorzieningen, IOP's, functionerings-, ontwikkelings- en salarisgegevens en identiteitsgegevens.

Ook gegevens over iemands werkplek en afdeling, sollicitatiebrieven, curricula Vitae en de omvang van het dienstverband worden als mogelijke persoonsgegevens genoemd. De gegeven antwoorden hebben deels een overlap met andere persoonsgegevens. Zo vallen identiteitsgegevens uiteen in NAW, geboortedatum en BSN. Andere antwoorden kunnen bijzondere persoonsgegevens betreffen, zoals persoonlijke omstandigheden, gegevens over ziekte, verzuim- en indicatiegegevens. Een aantal gegevens zijn mogelijk geen persoonsgegevens, afhankelijk van de precieze gegevens die verwerkt worden. Indien enkel gegevens over een werkplek, afdeling of de omvang van het dienstverband worden verzameld en geen relatie wordt gelegd tussen deze gegevens en de betreffende medewerker, zijn deze gegevens geen persoonsgegevens.

§ 5.3.2 De verwerking van bijzondere persoonsgegevens

Het risico van inbreuk op de privacy van betrokkenen is bij de verwerking van bijzondere persoonsgegevens groter dan bij de verwerking van algemene persoonsgegevens, door het gevoelige karakter van deze gegevens. Verwerking van bijzondere persoonsgegevens is verboden, tenzij de Wbp een ontheffing kent. Uit de resultaten, opgenomen in figuur 3, blijkt dat binnen de Diamant-groep veel bijzondere persoonsgegevens worden verwerkt.



Figuur 3: Verwerking bijzondere persoonsgegevens

§ 5.3.2.1 Gezondheidsgegevens

Uit de resultaten blijkt dat zeer veel medewerkers gezondheidsgegevens verwerken. Daarom zal in deze paragraaf uitgebreid ingegaan worden op de verwerking van deze gegevens. De grondslag om gezondheidsgegevens te verwerken zal normaliter enkel kunnen liggen in een gerechtvaardigd belang van de verantwoordelijke op grond van art. 8 sub f Wbp. Daarnaast is in paragraaf 3.5.1 bepaald dat gezondheidsgegevens slechts verwerkt mogen worden indien sprake is van een ontheffingsgrond. Eén van deze ontheffingsgronden is neergelegd in art. 21 lid 1 onder f sub 1 Wbp en bepaalt dat gezondheidsgegevens verwerkt mogen worden voor zover dat noodzakelijk is voor de uitvoering van wettelijke voorschriften, pensioenregelingen of een collectieve arbeidsovereenkomst.

Voorbeeld uitvoering wettelijk voorschrift - In het kader van art. 8 lid 2 sub e Besluit uitvoering sociale werkvoorziening en begeleid werken, wordt de plaatsing op de wachtlijst beëindigd met ingang van de dag dat de betrokkene niet beschikbaar is een dienstbetrekking in het kader van de Wsw te aanvaarden. Op basis van art. 4 lid 1 sub a Regeling uitvoering sociale werkvoorziening en begeleid werken is dat onder meer het geval als hij in verband met ongeschiktheid ten gevolge van ziekte niet in staat is tot het verrichten van arbeid onder aangepaste omstandigheden gedurende een ononderbroken periode van ten minste dertien weken. Om te bepalen of een medewerker al dan niet van de wachtlijst afgevoerd dient te worden, dienen gezondheidsgegevens verwerkt te worden, zoals medische rapportages van een specialist, het UWV of de bedrijfsarts. Ook het verwerken van gezondheidsgegevens in het kader van de Wet verbetering poortwachter (hierna: WVP) is toegestaan.

Daarnaast mogen gezondheidsgegevens verwerkt worden in het kader van de re-integratie of begeleiding van medewerkers in verband met ziekte of arbeidsongeschiktheid, conform art. 21 lid 1 onder f sub 2 Wbp. In het kader van begeleiding mogen gegevens omtrent de gezondheid van individuele medewerkers worden verwerkt, om te voorkomen dat door het werk schade aan de gezondheid optreedt. Daarnaast mogen deze gegevens verwerkt worden met als doel het terugbrengen van arbeidsongeschikte medewerkers in het arbeidsproces, bijvoorbeeld door het aanbieden van een passende werkplek.⁹²

Voorbeeld begeleiding of re-integratie - De noodzakelijkheidseis brengt met zich mee dat slechts een beperkt aantal gegevens verwerkt mogen worden. Als algemene richtlijn geldt dat een medewerker enkel die gegevens hoeft te verschaffen aan zijn werkgever, die deze nodig heeft om vast te stellen of er recht bestaat op loondoorbetaling. Dit houdt in dat een werkgever alleen gegevens mag verwerken omtrent het feit dat en de mate waarin iemand arbeidsongeschikt is, alsmede de periode van arbeidsongeschiktheid en eventueel de noodzakelijke aanpassingen. De Diamant-groep mag dus geen gegevens verwerken over de medische achtergronden van de arbeidsongeschiktheid van zijn medewerkers, zoals de aard en oorzaak. Een medewerker is ook niet verplicht deze gegevens te verstrekken.⁹³

Indien de rechtvaardiging om gezondheidsgegevens te verwerken niet gevonden kan worden in art. 21 Wbp, kan wellicht één van de algemene ontheffingsgronden uit art. 23 Wbp, zoals besproken in paragraaf 3.5.2 uitkomst bieden. Voor de verwerking van gegevens omtrent de gezondheid zijn de volgende uitzonderingen mogelijk relevant:

- Uitdrukkelijk toestemming van de betrokkene. Bij de zwakste groep medewerkers, die op een beschutte werkplek binnen de muren van de Diamant-groep werkzaam is, valt echter te betwijfelen of er sprake kan zijn van een beslissing die in vrijheid genomen is. Het is namelijk voorstelbaar dat deze groep medewerkers onder druk van de omstandigheden zijn goedkeuring geeft. Daarnaast dient de betrokkene te beschikken over voldoende informatie, zodat hij bewust zijn toestemming geeft. Gezien het niveau van de zwakste doelgroep is het niet altijd aannemelijk dat hiervan sprake is. De Diamant-groep zal dus uiterst zorgvuldig om dienen te gaan met het verwerken van gezondheidsgegevens op deze grond.
- Duidelijke openbaarmaking door de betrokkene zelf. Dit moet volgen uit het gedrag van de zieke medewerker, waaruit nadrukkelijk de intentie blijkt om deze informatie openbaar te maken. Veel medewerkers van de Diamant-groep hebben een zichtbare handicap. Hoewel dit gezondheidsgegeven voor iedereen zichtbaar is, is hierbij geen sprake van een uitdrukkelijke wens tot openbaarmaking door de betrokkene geuit.
- Noodzakelijkheid voor een gerechtelijke procedure.⁹⁴

Opname in verzuimregistratie - Veel medewerkers vertellen uit eigen beweging iets over de aard en oorzaak van hun ziekte. De werkgever verkrijgt deze gegevens dan rechtmatig. De werkgever zal het opnemen van gezondheidsgegevens in de verzuimregistratie normaliter enkel kunnen baseren op art. 8 sub f Wbp (een gerechtvaardigd belang). Tevens dient de verwerking gebaseerd te kunnen worden op een ontheffingsgrond uit art. 21 of art. 23 Wbp. Dit zal veelal niet mogelijk zijn, waardoor het de werkgever slechts in zeer uitzonderlijke gevallen zal vrijstaan om gegevens betreffende de aard en oorzaak op te nemen in de verzuimregistratie.

De Registratiekamer (de voorganger van het CBP) heeft bepaald dat de verwerking van medische gegevens door de werkgever niet is toegestaan.⁹⁵

⁹² Hooghiemstra & Nouwt 2007, p. 109.

⁹³ Hooghiemstra & Nouwt 2007, p. 109-110.

⁹⁴ Lioen & Van Munster-Frederiks/Van de Velde & Terhorst 2008, p. 27-28.

⁹⁵ Rgk 9 maart 1994, zaaknr. 94.E.034.

In het kader van het algemene verzuimbeleid (het maken van verzuimoverzichten, analyseren waar veel en langdurig verzuim voorkomt en oorzaken en oplossingen in kaart brengen) zijn gegevens over de aard en oorzaak van de ziekte van individuele medewerkers voor de werkgever niet noodzakelijk. Daarbij beschikt de werkgever niet over de deskundigheid om deze gegevens te analyseren. Dit dient hij over te laten aan bijvoorbeeld de bedrijfsarts, die gezien zijn wettelijke taak bij de verzuimbegeleiding toegang heeft tot veel informatie en wel over deze deskundigheid beschikt. De bedrijfsarts mag gegevens met betrekking tot de aard en oorzaak van de ziekte niet doorspelen aan de werkgever. Hij dient zich te beperken tot het vermelden van de functionele beperkingen of de rapportage te anonimiseren voor wat betreft deze gegevens. De bedrijfsarts is in beginsel gebonden aan een geheimhoudingsplicht, hoewel deze enigszins wordt beperkt door zijn adviserende functie richting werkgever.⁹⁶

Opname in persoonsdossier - Het is niet toegestaan om gegevens betreffende de aard en oorzaak van de ziekte in persoonsdossiers op te nemen, tenzij de werkgever daarvoor een rechtvaardigingsgrond kan aandragen. Dit zal slecht in zeer uitzonderlijke gevallen zo zijn. De opname van dergelijke gegevens wordt begrensd door het noodzakelijkheidscriterium. Het is namelijk onwenselijk dat medewerkers gedurende hun verdere loopbaan met deze gegevens worden achtervolgd en daarbij bestaat het risico dat de informatie uit zijn context wordt gehaald en een eigen leven gaat leiden. Ook als de gegevens omtrent aard en oorzaak van de ziekte vrijwillig worden verstrekt aan de werkgever, moet deze een goede reden hebben om de gegevens te verwerken. Het consequent noteren van de aard van de ziekte bij alle ziekmeldingen is in ieder geval niet noodzakelijk en dus niet geoorloofd.⁹⁷

Toegang tot gezondheidsgegevens van medewerkers dient enkel voorbehouden te zijn aan direct betrokkenen. Dit zijn bijvoorbeeld de medewerkers van de personeelsadministratie en de direct leidinggevende. Ook in dit kader is het noodzakelijkheidscriterium van belang. Een leidinggevende hoeft slechts te weten welke medewerkers op zijn afdeling ziek zijn en niet welke medewerkers op andere afdelingen ziek zijn.⁹⁸ De Diamant-groep dient in dit kader nog een behoorlijke slag te slaan. Dat heeft voornamelijk te maken met de gegevens die in Compas staan opgenomen. Deze dienen beter afgeschermd te worden, aangezien ze nu voor een te grote groep medewerkers toegankelijk zijn.

Binnen de Diamant-groep worden op structurele basis medische gegevens opgenomen in de persoonsdossiers. Regelmatig blijkt dat volledige medische of psychologische verslagen in Compas staan. Hierdoor zijn deze gegevens voor een relatief grote groep medewerkers toegankelijk en niet slechts voor direct betrokkenen. De Diamant-groep verzuimt hiermee in zijn zorgplicht voor een adequate beveiliging van deze gegevens en voldoet niet aan het noodzakelijkheidscriterium. Toch kan de Diamant-groep een gerechtvaardigd belang hebben om dergelijke gegevens op te nemen in de verzuimregistratie of het persoonsdossier. Ondermeer als een medewerker bijvoorbeeld last heeft van epilepsie of suikerziekte. Collega's of leidinggevendenden moeten hiervan op de hoogte zijn, zodat zij weten hoe te handelen in geval van nood.⁹⁹

De bedrijfsarts - Het is gebleken dat de adviezen van de bedrijfsarts structureel inhoudelijke informatie over de aard en oorzaak van de ziekte of arbeidsongeschiktheid bevatten. Gezien het bovenstaande is dit een behoorlijke inbreuk op de privacy van medewerkers. Hoewel het kaderpersoneel het wellicht als handig ervaart om te beschikken over dergelijke informatie, is het volstrekt overbodig.

⁹⁶ Lioen & Van Munster-Frederiks/Van de Velde & Terhorst 2008, p. 68.

⁹⁷ Lioen & Van Munster-Frederiks/Van de Velde & Terhorst 2008, p. 75-76.

⁹⁸ Lioen & Van Munster-Frederiks/Van de Velde & Terhorst 2008, p. 68-69.

⁹⁹ Lioen & Van Munster-Frederiks/Van de Velde & Terhorst 2008, p. 76.

De bedrijfsarts dient enkel aan te geven of, en zo ja voor welk percentage, een medewerker arbeidsongeschikt is, of een medewerker in staat is zijn eigen of ander passend werk uit te voeren en welke functionele aanpassingen daarvoor noodzakelijk zijn. Op basis van deze informatie is het mogelijk om de medewerker te re-integreren naar passend werk, conform zijn indicatie én het advies van de bedrijfsarts.

De Diamant-groep als uitvoerder van de Wsw - De verwerking van gezondheidsgegevens binnen de Diamant-groep dient geplaatst te worden tegen de achtergrond van het feit dat de Diamant-groep de Wsw uitvoert. Verwerking van bepaalde gezondheidsgegevens is inherent aan een dergelijke organisatie. De Diamant-groep wil zijn wettelijke taak, zoals vastgelegd in de Wsw, goed uitvoeren en stelt om deze reden dat het noodzakelijk is te beschikken over relevante medische informatie. De vraag is in hoeverre deze stelling correct is.

Indien een medewerker zich bij het UWV meldt voor een Wsw-indicatie zal hij, afhankelijk van zijn beperkingen, medisch en/of psychologisch onderzocht worden. De resultaten van deze onderzoeken bundelt het UWV in een indicatie. Uit de indicatie blijkt wat vanuit medisch en psychisch oogpunt passend is en worden de noodzakelijke maatregelen en voorzieningen opgesomd. Vervolgens komt een medewerker met zijn indicatie binnen bij de Diamant-groep. Op dat moment wordt het dossier overgedragen aan de afdeling Arbeidsdiagnose. Na het doorlopen van de wachttijd bepaalt een medewerker van deze afdeling in een intake wat er concreet mogelijk is binnen de Diamant-groep. De uitslag van de intake wordt vertaald naar een start-IOP. Naar aanleiding hiervan wordt de medewerker op een passende werkplek bij één van de bedrijfsonderdelen geplaatst. Als blijkt dat de plaatsing niet passend is, wordt door middel van een tussentijdse evaluatie en op basis van de afgegeven indicatiegegevens getoetst of de getroffen maatregelen en voorzieningen juist zijn. In Compas zijn deze indicatiegegevens opgenomen in het cliëntdossier. Een beperkte groep medewerkers heeft toegang tot deze dossiers, echter een veel grotere groep medewerkers heeft toegang tot documenten. Tussen de documenten staan vaak diverse verslagen en rapportages, waardoor iemands indicatie tamelijk eenvoudig te achterhalen is. Gezien het bovenstaande dient de Diamant-groep alleen te beschikken over de noodzakelijke maatregelen en voorzieningen, zodat de medewerker geplaatst kan worden op een passende werkplek. Verdergaande verwerking is in strijd met de Wbp.

Ten aanzien van de verwerking van gezondheidsgegevens creëert art. 21 lid 2 Wbp een belangrijke waarborg. Dergelijke gegevens mogen alleen verwerkt worden door personen die op enige wijze verplicht zijn tot geheimhouding. Binnen de Diamant-groep wordt in elk arbeidscontract standaard een geheimhoudingsclausule opgenomen in. De geheimhouding van ambtenaren wordt primair geregeld in art. 125a lid 2 Ambtenarenwet en art. 15:1b sub c CAR-UWO. Wat betreft de ambtenaren die werkzaam zijn binnen de Diamant-groep, volgt de organisatie de nota 'zuiver op de graat' van de Gemeente Tilburg. Een bepaling met betrekking tot vertrouwelijkheid en geheimhouding maakt onderdeel van deze nota uit.

§ 5.3.2.2 Strafrechtelijke gegevens

Uit figuur 3 blijkt dat redelijk veel medewerkers gegevens over onrechtmatig of hinderlijk gedrag en strafrechtelijke gegevens verwerken. Zoals in paragraaf 3.5.1 uitgewerkt, mogen deze gegevens slechts op twee gronden verwerkt worden. Enkel de grond in art. 22 lid 2 sub b Wbp is voor de Diamant-groep van belang en zal hieronder besproken worden.

Een verantwoordelijke mag strafrechtelijke gegevens over het verleden van medewerkers verwerken, ter bescherming van zijn belangen voor zover het gaat om strafbare feiten die jegens hem, de organisatie of personen in zijn dienst zijn of mogelijk zullen worden gepleegd. De bescherming kan daarin bestaan dat de betrokkene wordt uitgesloten van toekomstige contracten, beperktere ontplooiingsmogelijkheden heeft of het contract met hem wordt beëindigd.

Bij gegevens die hun oorsprong vinden binnen de organisatie, mag de verantwoordelijke deze gegevens vastleggen en gebruiken wanneer hij slachtoffer is of dreigt te worden van strafbare feiten. De Ondernemingsraad (hierna: OR) moet conform art. 27 lid 1 sub I WOR het instemmingsrecht hebben kunnen uitoefenen bij het vaststellen, wijzigingen of intrekken van de regeling die het mogelijk maakt dergelijke gegevens te verwerken.¹⁰⁰ Art. 22 lid 6 Wbp bepaalt dat art. 22 Wbp van toepassing is op persoonsgegevens betreffende een door de rechter opgelegd verbod naar aanleiding van onrechtmatig of hinderlijk gedrag. Het gaat dan bijvoorbeeld om een straat- of caféverbod.

Binnen de Diamant-groep zijn medewerkers met een detentieverleden werkzaam. Dit feit is een persoonsgegeven in het kader van de Wbp. In verband met plaatsing binnen de Diamant-groep, kan het noodzakelijk zijn dat de Diamant-groep strafrechtelijke gegevens verwerkt. Deze gegevens worden via de indicatiebeschikking van het UWV of via de reclassering aangeleverd. Hierdoor kan bijvoorbeeld voorkomen worden dat een pedofiel geplaatst wordt op een kinderdagverblijf. De Diamant-groep is gemachtigd strafrechtelijke gegevens te verwerken, als het gaat om medewerkers die strafbare feiten dreigen te plegen. Tevens is de verwerking noodzakelijk ter bescherming van de Diamant-groep als organisatie en alle medewerkers werkzaam voor of in dienst van de Diamant-groep. Vaak wordt alleen verwerkt dat een medewerker een detentieverleden heeft en wordt niet verwerkt waar dat verleden uit bestaat. Er zijn echter ook situaties bekend waarin wordt verwerkt waaruit het detentieverleden bestaat. De OR van de Diamant-groep heeft geen toestemming verleend om strafrechtelijke gegevens te verwerken.

Binnen de Diamant-groep worden ook gegevens verwerkt omtrent onrechtmatig of hinderlijk gedrag van medewerkers tijdens de uitoefening van hun werkzaamheden. Dit wordt door de leidinggevende bijgehouden in bijvoorbeeld een voortgangsrapportage. Deze gegevens worden gebruikt bij functionerings- of IOP gesprekken. Deze gegevens vallen niet onder de definitie van art. 22 lid 6 Wbp, aangezien het niet gaat om een opgelegd verbod door de rechter. Deze gegevens zijn daarom in beginsel geen bijzondere persoonsgegevens, tenzij er een overlapping plaatsvindt met andere bijzondere gegevens (zoals seksueel leven). Verwerking van dergelijke gegevens is toegestaan, mits voldaan wordt aan de overige bepalingen in de Wbp. In dit kader geldt binnen de Diamant-groep de 'Regeling ongewenste omgangsvormen' zie hiervoor bijlage X.

§ 5.3.2.3 Gegevens omtrent ras of etniciteit

Uit figuur 3 blijkt dat bijna 35% van de ondervraagden heeft aangegeven gegevens omtrent ras of etniciteit van medewerkers te verwerken. In beginsel geldt een verbod om dergelijke gegevens te verwerken, tenzij één van de uitzonderingen in art. 18 Wbp aan de orde is. In het kader van dit onderzoek is enkel de uitzondering in art. 18 sub a Wbp van belang. Persoonsgegevens betreffende ras of etniciteit mogen verwerkt worden met het oog op identificatie van de betrokkene en slechts voor zover dit voor dit doel onvermijdelijk is. Het begrip ras dient ruim te worden opgevat en omvat ook huidskleur, afkomst en nationaliteit of etnische afstamming.¹⁰¹ Uit een uitspraak van de rechtbank te Rotterdam bleek dat de rechter oordeelde dat een (pas)foto met iemands beeltenis een persoonsgegeven betreffende iemands ras en daarmee een bijzonder persoonsgegeven is.¹⁰²

Op basis van art. 23 Wet op de Identificatieplicht is de Diamant-groep verplicht bij indiensttreding van een medewerker diens identiteit vast te stellen. Deze regel geldt zowel voor nieuwe medewerkers als voor medewerkers die reeds in dienst waren.¹⁰³

¹⁰⁰ Hooghiemstra & Nouwt 2007, p. 116-118.

¹⁰¹ Hooghiemstra & Nouwt 2007, p. 101.

¹⁰² Rechtbank Rotterdam 2 juni 2008, nr. 07/956.

¹⁰³ *Identificatie nieuwe werknemers!*,

<www.gibogroep.nl/Nieuws/Nieuws/Algemeen/Identificatienieuwewerknemers/tabid/713/Default.aspx>.

De Diamant-groep maakt bij indiensttreding standaard een kopie van een identiteitsbewijs. Aangezien ieder identiteitsbewijs is voorzien van een pasfoto, verschaft de kopie gegevens over het ras van de medewerker en valt daarmee onder de reikwijdte van art. 18 onder a Wbp.

In 2005 heeft de regiopolitie aan het CBP advies gevraagd over een intern dienstvoorschrift dat regels stelde over de verwerking van de etnische afkomst van het personeel. Het CBP oordeelde dat gegevens over iemands ras niet mogen worden opgenomen in de personeelsadministratie, tenzij sprake is van een voorkeursbeleid en een aantoonbare achterstand van een bepaalde groepering.¹⁰⁴ Dit betekent dat de kopieën van de identiteitsbewijzen bewaard dienen te worden bij de loonadministratie.

Binnen de Diamant-groep is het echter intern beleid om de kopie te bewaren in het persoonsdossier. Conform de 'Werkwijzer Persoonsarchief' (bijgevoegd in bijlage XI) wordt de kopie van het legitimatiebewijs onder persoonlijke gegevens in het persoonsdossiers bewaard. Dit is een bewuste keuze. De personeelsadministratie heeft, in tegenstelling tot de medewerkers van het archief, onvoldoende mogelijkheden en kennis om de kopieën deugdelijk te beveiligen en de bewaartermijnen na te leven. Het bewaren van de kopieën in de personeelsadministratie levert dus een grotere kans op inbreuk op de privacy van de betrokkene op dan bewaring in het persoonsdossier.

De Diamant-groep verwerkt bovendien om een andere reden gegevens omtrent ras. Voor de medewerkers die op basis van een Wsw-indicatie werkzaam zijn, ontvangt de Diamant-groep subsidie. De Diamant-groep dient aan te kunnen tonen dat voor de juiste personen subsidie is ontvangen. Deze verplichting blijkt uit de verantwoordingsadministratie die afgelegd moet worden aan het Rijk. Indien de Diamant-groep conform art. 13 Wsw niet voor een goede administratie van de uitvoering van de Wsw zorgt of niet aan zijn inlichtingenplicht voldoet, kan de subsidie overeenkomstig art. 9 Wsw teruggevorderd worden.¹⁰⁵ Een kopie van de identiteitsgegevens van de medewerkers is dus noodzakelijk voor identificatie, daarom kan deze verwerking gebaseerd worden op art. 18 onder a Wbp.

In het kader van de digitalisering werd een kopie van het legitimatiebewijs en de bankpas in Compas geplaatst. Het ontbrak aan extra beveiligingsmaatregelen waardoor deze gegevens voor een grote groep medewerkers toegankelijk was. Bovendien waren de medewerkers niet van deze nieuwe verwerking op de hoogte gebracht. Naar aanleiding van een bezwaar tegen het plaatsen van deze kopieën in Compas is besloten dit proces (tijdelijk) te staken. Privacytechnisch stuit deze handelswijze op bezwaren, aangezien de verwerking niet gebaseerd kan worden op art. 18 sub a Wbp (noodzakelijk in verband met identificatie). Het is niet waarschijnlijk dat de verwerking gebaseerd kan worden op één van de algemene ontheffingsgronden uit art. 23 Wbp. De werkgever heeft namelijk geen zwaarwegend algemeen belang, hetgeen betekent dat de verwerking enkel plaats kan vinden als sprake is van uitdrukkelijke toestemming van de betrokkenen conform art. 23 lid 1 sub a Wbp.

Ook videobeelden worden beschouwd als gegevens die informatie verschaffen over het ras of de etniciteit van de betrokkene. Dit betekent dat er zeer terughoudend moet worden omgegaan met het gebruik van cameratoezicht.¹⁰⁶ Uit het beleid en de regeling blijkt dat de Diamant-groep geen overmatig gebruik maakt van het cameratoezicht, aangezien de camera's dienen ter bescherming van de eigendommen. Zie verder bijlage VII.

In de telegids op intranet staan foto's van veel medewerkers van de Diamant-groep. Voor het plaatsen van deze foto's is conform art. 23 lid 1 sub a Wbp uitdrukkelijke toestemming van de betrokkene noodzakelijk, aangezien de noodzaak voor identificatie ontbreekt.

¹⁰⁴ CBP 23 januari 2006, z2005-1355.

¹⁰⁵ *Kamerstukken II* 1995/1996, 24 787, nr. 3, p. 57 (MvT).

¹⁰⁶ Terstegge 2000, p. 38-39.

Op de toegangspasjes die medewerkers hebben om het terrein en de gebouwen te kunnen betreden, staan geen gegevens omtrent ras.

§ 5.3.2.4 Overige bijzondere persoonsgegevens

De gegevens omtrent godsdienst, politieke gezindheid, seksueel leven en het lidmaatschap van een vakvereniging worden binnen de Diamant-groep minder verwerkt. In deze paragraaf zullen deze categorieën bijzondere persoonsgegevens slechts kort worden besproken.

Het is niet toegestaan dat de Diamant-groep persoonsgegevens omtrent godsdienst verwerkt, aangezien verwerking blijkens art. 17 lid 1 Wbp slechts kan geschieden door (kerk)genootschappen op geestelijke grondslag of instellingen op godsdienstige of levensbeschouwelijke grondslag. Voor zover noodzakelijk met het oog op de geestelijke verzorging van de betrokkene, mogen ook andere instellingen deze gegevens verwerken. Ook dit laatste is binnen de Diamant-groep niet aan de orde.

Gegevens met betrekking tot iemands politieke gezindheid mogen ook niet verwerkt worden, aangezien dit conform art. 19 Wbp voorbehouden is aan instellingen op politieke grondslag of met het oog op de eisen die in dit kader redelijkerwijs aan iemand kunnen worden gesteld in verband met de vervulling van functies in bestuursorganen en adviescolleges.

De Diamant-groep kan gegevens met betrekking tot het vakbondslidmaatschap van een medewerker niet verwerken op grond van art. 20 Wbp, aangezien verwerking van deze gegevens enkel is toegestaan door de betreffende vakbond of vakcentrale. De CAO Wsw maakt het echter mogelijk het lidmaatschap van een vakbond te fiscaliseren. In dat geval geeft de medewerker toestemming en is de verwerking van deze gegevens rechtmatig.

Met betrekking tot gegevens over het seksuele leven, is geen specifieke bepaling in de Wbp opgenomen. Er zal dus teruggevallen moeten worden op de algemene ontheffingen uit art. 23 Wbp. Met betrekking tot de uitdrukkelijke toestemming geldt hetzelfde als hierboven in paragraaf 5.3.2.1 is aangehaald. Verder is verwerking wellicht mogelijk als de gegevens door betrokkene zelf duidelijk openbaar zijn gemaakt. Van deze beide gronden zal echter niet snel sprake zijn. Mocht dit echter wel aan de orde zijn, dan nog is verwerking van deze gegevens door de Diamant-groep niet rechtmatig, aangezien de gegevens niet noodzakelijk zijn voor de uitoefening van zijn taken. Ook mogen dergelijke gegevens verwerkt worden als dat noodzakelijk is in aanvulling op de verwerking van gezondheidsgegevens.¹⁰⁷

§ 5.3.3 De toereikendheid van de huidige autorisaties

Aan de medewerkers is gevraagd of zij vonden dat zij voldoende gegevens tot hun beschikking hadden om hun functie naar behoren te vervullen. 85,5% van de ondervraagden gaf aan over voldoende informatie te beschikken, tegenover 14,5% (acht ondervraagden) die dat niet vond. Zes medewerkers vonden dat ze te weinig informatie tot hun beschikking hadden, tegenover twee ondervraagden die juist vonden dat ze toegang hadden tot te veel informatie. Ook werd door een ondervraagde opgemerkt dat Compas slecht gevuld is, hetgeen vanzelfsprekend onwenselijk is.

Tevens is gevraagd over welke persoonsgegevens de medewerkers naar hun mening dienen te beschikken om hun functie naar behoren te kunnen uitoefenen. Bij het verwerken van de resultaten is helaas gebleken dat deze vraag op verschillende wijzen geïnterpreteerd kon worden. Daarnaast vulden opvallend veel medewerkers deze vraag niet of half in, waaruit blijkt dat de vraag voor veel medewerkers onduidelijk was.

¹⁰⁷ <www.dehoogstraat.nl/uploads> revalideren > privacy > privacyreglement en inzage-recht > privacyreglement; alleen te openen met Adobe Reader.

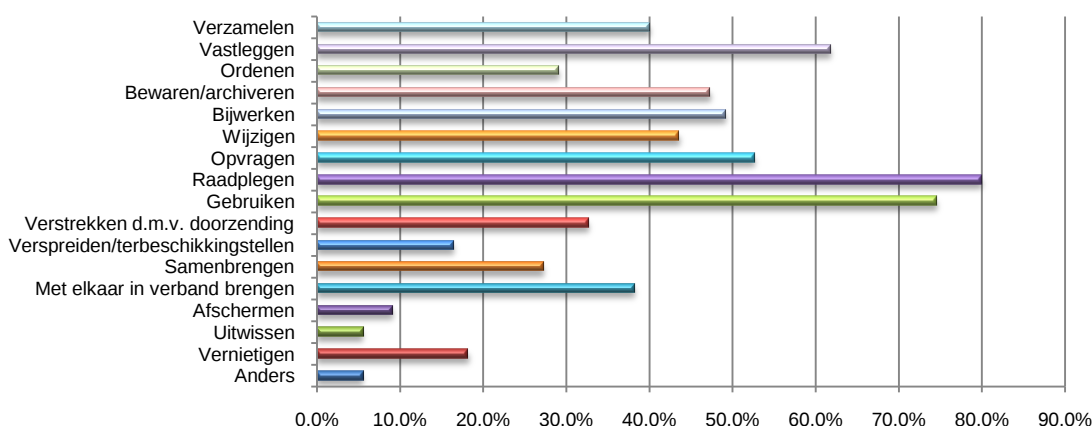
Hoewel getracht is de resultaten op eenduidige wijze in kaart te brengen, bleek het niet mogelijk aan de resultaten met zekerheid een aantal conclusies te verbinden. In verband met de betrouwbaarheid van het onderzoek, is besloten deze resultaten niet verder uit te werken.

Als gekeken wordt naar de antwoorden van de ondervraagden die de vraag wel correct hebben ingevuld, kan met enige voorzichtigheid een aantal algemene conclusies getrokken worden. Volgens de medewerkers klopt gemiddeld in 20% van de gevallen het autorisatieprofiel niet. Veruit de meeste medewerkers vinden hun autorisatieprofiel te beperkt. Opvallend is dat met name op het gebied van inzage in salarisgegevens veel medewerkers vinden dat zij beschikken over te weinig informatie.

Deze constatering onderstrepen slechts de relevantie om binnen de organisatie de discussie op gang te brengen. Dat de organisatie naar zijn digitale informatiesysteem en het daarbij behorende autorisatieprobleem dient te kijken is evident.

§ 5.3.4 De verwerkingshandelingen

In het kader van dit onderzoek is het van belang een beeld te krijgen van de meest voorkomende verwerkingshandelingen. In onderstaande figuur is het overzicht weergegeven.



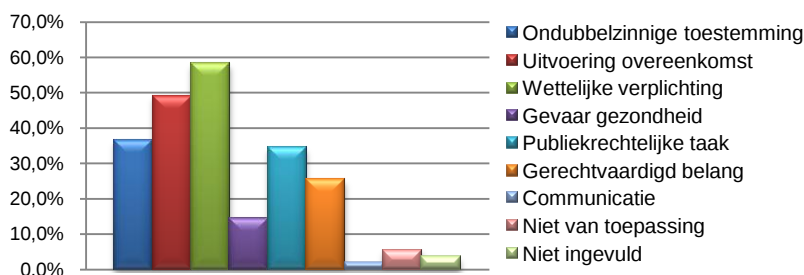
Figuur 4: De verwerkingshandelingen

De meest voorkomende handelingen zijn gebruikelijk binnen een organisatie. Opvallend is dat slechts weinig medewerkers gegevens afschermen, uitwissen en vernietigen, terwijl deze verwerkingen in het kader van de bescherming van persoonsgegevens belangrijk zijn. Dit kan deels verklaard worden door intern beleid binnen de Diamant-groep. Het hoofd Beleids- en Persoonsarchief is verantwoordelijk voor de naleving van de bewaartermijnen met betrekking tot de informatie in de analoge en digitale dossiers. Voor wat betreft handmatige verwerkingen zijn de medewerkers zelf verantwoordelijk voor de naleving van de bewaartermijn. Het is echter onwaarschijnlijk dat de medewerkers hier zelf consequent op letten. Bij 'anders' gaven medewerkers aan dat het ging om uitlenen, interne controle en ondertekenen/accorderen. In dit kader kan alleen uitlenen een 'verwerkingshandeling' in de zin van de Wbp zijn.

Gezien de 347 (!) gegeven antwoorden, blijkt dat de medewerkers erg veel gebruik maken van allerlei verwerkingshandelingen en dus veel persoonsgegevens verwerken. Uit alle verwerkingshandelingen die medewerkers gebruiken, kan geconcludeerd worden dat de medewerkers veelal een uitgebreide autorisatie in Compas hebben.

§ 5.4 De grondslag om gegevens te verwerken

Zoals reeds is besproken in paragraaf 3.4.2 dient elke verwerking van persoonsgegevens gebaseerd te worden op een grondslag uit art. 8 Wbp. In onderstaande figuur is de verhouding tussen de verschillende verwerkingsgrondslagen in een grafiek weergegeven.



Figuur 5: De verwerkingsgrondslag

De verwerkingsgronden zijn limitatief vermeld in art. 8 Wbp, dit is ook in de toelichting op de vragenlijst aangegeven. Desondanks geeft een aantal medewerkers aan dat zij gegevens verwerken op een andere verwerkingsgrond. Zo verwerkt één medewerker gegevens omdat dit noodzakelijk is in verband met de communicatie. Daarnaast gaven meerdere medewerkers aan dat de verwerkingsgrond niet van toepassing is. Deze medewerkers gaven allemaal aan dat zij wel persoonsgegevens verwerkten. Inherent hieraan is dat de verwerking gebaseerd dient te worden op één van de zes gronden, wil er sprake zijn van een rechtmatige verwerking. Er is dus sprake van enige tegenstrijdigheid. Daarnaast valt op dat 15% van de ondervraagden aangeeft gegevens te verwerken in verband met een ernstig gevaar voor de gezondheid van betrokkene. In de toelichting op de vragenlijst stond duidelijk dat deze grond enkel van toepassing is, als de gezondheid van de betrokkene in ernstig gevaar verkeert. Het is niet waarschijnlijk dat binnen de Diamant-groep er sprake is van deze verwerkingsgrondslag.

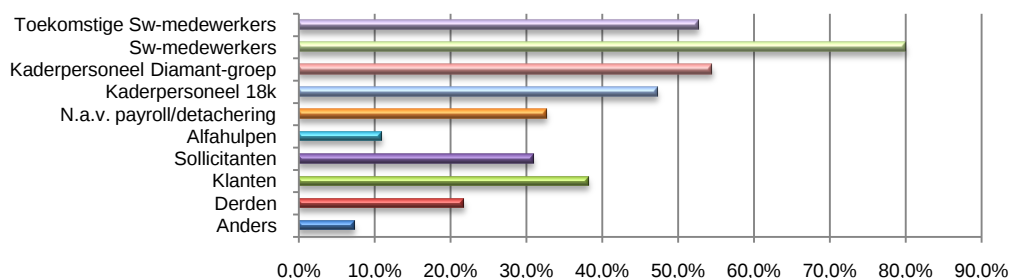
Bijna 60% van de ondervraagden baseert de verwerking op een wettelijke verplichting. Binnen een organisatie als de Diamant-groep is dit te verklaren. Aangezien de Diamant-groep de Wsw uitvoert, is het ziekteverzuim hoger dan in andere organisaties. Daarom worden veel gegevens verwerkt in het kader van de WVP. Daarnaast verwerkt bijna 50% van de ondervraagden gegevens in verband met de uitvoering van een (arbeids)overeenkomst. Op basis van deze arbeidsovereenkomst, worden bijvoorbeeld de salarisgegevens van de medewerkers verwerkt.

Ongeveer 35% verwerkt gegevens op basis van ondubbelzinnige toestemming en naar aanleiding van een publiekrechtelijke taak. Gezien het publiekrechtelijke karakter van de Diamant-groep, vallen alle taken die de Diamant-groep uitvoert namens de gemeenten onder deze grondslag. Dit is ook aangegeven in de toelichting op de vragenlijst. In dit kader was de verwachting dat dit percentage hoger zou liggen. Tot slot heeft ongeveer 25% ingevuld gegevens te verwerken op basis van een gerechtvaardigd belang. Op basis van de resultaten is het niet mogelijk om te achterhalen of dit belang daadwerkelijk een gerechtvaardigd belang is.

Uit deze resultaten blijkt met name dat medewerkers het als erg lastig ervaren om hun eigen handelen te kwalificeren in termen van de Wbp. Dit is niet geheel verwonderlijk, gezien de lastige termen in de Wbp en de resultaten in paragraaf 5.2.

§ 5.5 Van wie worden er persoonsgegevens verwerkt?

Een belangrijke vraag om inzicht te verkrijgen in de omvang van de gegevensverwerkingen binnen de organisatie, is van wie en door wie persoonsgegevens worden verwerkt. Op dit moment zijn er ongeveer 270 Compas-gebruikers. De gegevens van een Sw-medewerker kunnen gezien worden door een wisselende groep van gemiddeld 120 gebruikers. Binnen de organisatie hebben dus veel mensen op enige wijze toegang tot persoonsgegevens. Uit onderstaande figuur blijkt van wie medewerkers de persoonsgegevens verwerken.



Figuur 6: De betrokkenen

Uit de resultaten blijkt dat voornamelijk veel gegevens worden verwerkt van medewerkers met een Wsw-indicatie. Tevens verwerken veel medewerkers gegevens van toekomstige medewerkers met een Wsw-indicatie en het kaderpersoneel van zowel de Diamant-groep en 18k. De groep toekomstige medewerkers met een Wsw-indicatie bestaat vooral uit mensen die op de wachtlijst staan. Van hen bestaat al een indicatiedossier, aangezien zij de intake via de afdeling Arbeidsdiagnose reeds hebben gehad. Daarnaast zijn er medewerkers via een inkooptraject van het UWV of de gemeente binnen de Diamant-groep werkzaam. Deze trajecten dienen ter overbrugging van de wachttijd (die op dit moment bijna drie jaar bedraagt) van de medewerkers, alvorens zij met hun Wsw-indicatie aan de slag kunnen. De mensen die hier voor in aanmerking komen hebben vaak een WWB-uitkering en werken gedurende een periode met behoud van uitkering binnen de Diamant-groep. Deze categorie medewerkers behoort tot de categorie 'toekomstige medewerkers met een Wsw-indicatie'.

Daarnaast is uit het onderzoek naar voren gekomen dat medewerkers vrij veel gegevens verwerken naar aanleiding van payroll en detachering, van sollicitanten, klanten en derden. Ook van deze medewerkers wordt een analoog dossier aangemaakt en worden de persoonsgegevens verwerkt in Compas. 18k verwerkt vooral gegevens van derden naar aanleiding van externe opdrachten naar de arbeidscapaciteiten van een betrokkene. Deze opdrachten kunnen afkomstig zijn van de gemeente Tilburg, het UWV of een extern re-integratiebureau. Ook in het kader van het project Tilburg at Work worden persoonsgegevens van derden verwerkt. De derden in dit kader zijn dus niet de derden zoals deze omschreven zijn in de begrippenlijst.

§ 5.6 Interne en externe verstrekking van persoonsgegevens

Maar liefst 80% van de medewerkers krijgt gegevens aangeleverd van een andere afdeling of bedrijfsonderdeel. Vooral de personeelsteams en de personeels- en salarisadministratie spelen hierin een sleutelrol. Al geven ook veel medewerkers aan dat de gegevens vanuit alle afdelingen binnen de Diamant-groep en 18k kunnen komen. Daarbij krijgen medewerkers veel gegevens aangeleverd van betrokkenen (67%) en derden (47%). De derden zijn bijvoorbeeld gemeenten, het UWV, Achmea, andere Sw-bedrijven en diverse hulpverlenende instellingen. Binnen de organisatie vinden dus zeer grote gegevensstromen plaats.

Deze conclusie wordt onderschreven door het feit dat 71% van de ondervraagden aangeeft intern persoonsgegevens uit te wisselen. Dit is toegestaan mits de uitwisseling gebaseerd kan worden op één van de wettelijke grondslagen uit art. 8 Wbp. De uitwisseling vindt voornamelijk plaats met directe collega's, personeelsteams, de personeels- en salarisadministratie, leidinggevenden, arbeidsdiagnose, trajectbegeleiders en juridische zaken. Daarnaast wisselt 49% gegevens uit met externe organisaties binnen Nederland. De organisaties waarmee medewerkers gegevens uitwisselen en de organisaties waarvan medewerkers gegevens krijgen aangeleverd komen overeen. Zo worden gemeenten, het UWV, Achmea en hulpverlenende instellingen het meest genoemd.

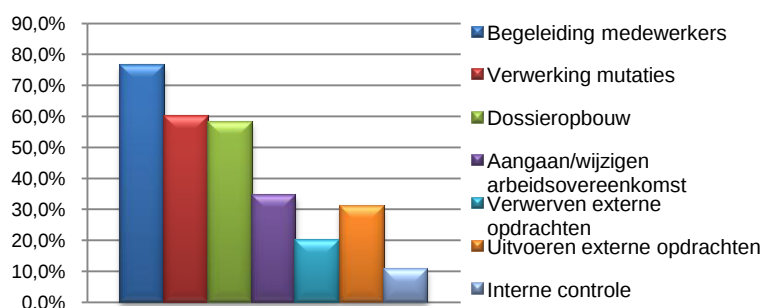
§ 5.7 De wijze waarop de persoonsgegevens worden verwerkt

Bijna 93% van de ondervraagde medewerkers verwerkt op (gedeeltelijk) geautomatiseerde wijze persoonsgegevens. Dit gebeurt vooral in Compas. Daarnaast heeft bijna 53% aangegeven ook handmatig gegevens te verwerken. Handmatige gegevens worden voornamelijk verwerkt in het kader van verslaglegging, gespreksverslagen en aantekeningen van telefoongesprekken. Handmatige verslaglegging gebeurt met name in verband met het functioneren van de medewerkers (73%) en het minst in verband met het opleggen van disciplinaire maatregelen (50%). In mindere mate worden persoonlijke telefoon- of adressenboekjes of persoonlijke notities bijgehouden. Daarnaast gaf een aantal medewerkers aan handmatige gegevens te verwerken in verband met arbeids- en detacheringsovereenkomsten, schaduwdoossiers, werkplekonderzoeken en -aanpassingen.

Handmatige verwerkingen vallen enkel onder de reikwijdte van de Wbp als ze bestemd zijn opgenomen te worden in een bestand. Persoonlijke telefoon- of adressenboekjes en persoonlijke notities vallen onder de uitzondering in art. 2 lid 2 sub a Wbp en vallen dus niet onder de Wbp. Het is evident dat medewerkers toch voorzichtig dienen te zijn met dergelijke gegevens. Voorwaarde is dat documenten niet door meerdere medewerkers worden gebruikt. Met betrekking tot de gegevens in verband met verslaglegging, gespreksverslagen en aantekeningen van telefoongesprekken, zullen vanuit de meeste verwerkingen gedeeltelijk geautomatiseerd plaatsvinden. Handmatige verslagen en aantekeningen worden namelijk nagenoeg altijd geautomatiseerd en in het persoonsdossier en Compas opgeborgen. De verwerking van deze gegevens valt daarmee dus onder het toepassingsbereik van de Wbp.

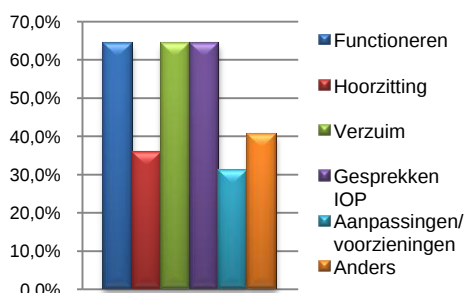
§ 5.8 De doeleinden van de verwerking

De doeleinden voor de verwerkingen dienen welbepaald, uitdrukkelijk en gerechtvaardigd te zijn. De medewerkers is gevraagd aan te geven voor welke doeleinden zij gegevens verwerken. De resultaten zijn weergegeven in figuur 7.

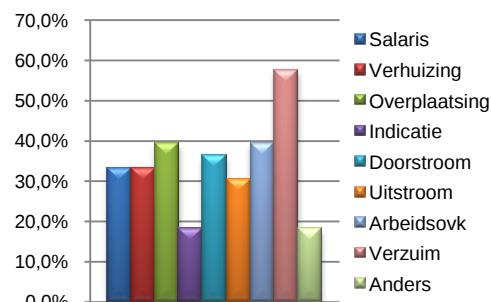


Figuur 7: Doeleinden gegevensverwerking

Veel ondervraagde medewerkers verwerken persoonsgegevens in verband met de begeleiding van medewerkers en het aanbrengen van mutaties. Van deze medewerkers is hieronder in figuur 8 en 9 uitgesplitst voor welke subdoelen de gegevens worden verwerkt.



Figuur 8: Begeleiding medewerkers



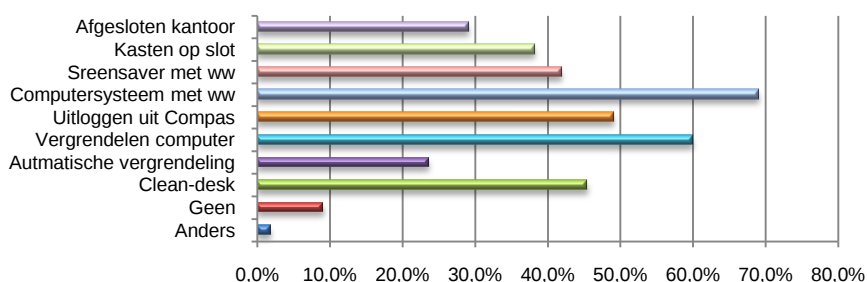
Figuur 9: Verwerking mutaties

In verband met het doel ‘begeleiding medewerkers’ verwerken de medewerkers met name gegevens met betrekking tot het functioneren, het verzuim en IOP-gesprekken. Opvallend is dat ruim 40% andere persoonsgegevens verwerkt. Het bleek hier te gaan om het uitvoeren van diagnoseonderzoeken en gegevens in verband met bezwaren- en klachtencommissies. Ook in het kader van ontslagprocedures en de plaatsing van een medewerker binnen de Diamant-groep worden gegevens verwerkt.

Als men kijkt naar het doel ‘verwerking mutaties’, springt voornamelijk het verzuim in het oog. Er worden veel mutaties aangebracht met betrekking tot het verzuim, bijvoorbeeld: ziekmelding, herstelmelding, consult bedrijfsarts, verzuimrapportage et cetera. Dit zijn alle gerechtvaardigde doeleinden op basis waarvan persoonsgegevens mogen worden verwerkt.

§ 5.9 De toereikendheid van de huidige beschermingsmaatregelen

In dit rapport is het belang van beveiliging en bewaring al meerdere malen onderstreept. In de vragenlijst zijn hieromtrent dan ook enkele vragen gesteld. Zo is onder andere gevraagd welke beveiligingsmaatregelen de medewerkers getroffen hebben om de persoonsgegevens te beveiligen. In figuur 10 worden de resultaten weergegeven. Op het eerste gezicht lijken er behoorlijk wat beveiligingsmaatregelen te zijn getroffen door de medewerkers. Dit blijkt bij nadere bestudering echter tegen te vallen.



Figuur 8: Beveiligingsmaatregelen

§ 5.9.1 Beveiliging

Uit het eerder aangehaalde onderzoek van NPS-Nipo in samenwerking met KPMG volgen een aantal belangrijke conclusies op het gebied van de beveiliging van persoonsgegevens. Ongeveer de helft van de Nederlandse organisaties ziet privacybescherming als synoniem voor informatiebeveiliging. Hierdoor zijn de privacyrisico's binnen deze organisaties mogelijk onvoldoende in kaart gebracht en zijn dus mogelijk onvoldoende maatregelen getroffen om de privacy te kunnen waarborgen. Organisaties dienen te beseffen dat privacy veeleer gaat om verantwoord gebruik van persoonsgegevens en niet louter om de bescherming daarvan.¹⁰⁸ In onderstaande paragraaf zal toch uitgebreid bij de beveiligingsaspecten stil worden gestaan, aangezien de Diamant-groep op dit moment niet voldoet aan de Wbp.

Bijna 70% van de ondervraagden geeft aan een computersysteem met een wachtwoord te hebben. Dit is echter een standaardinstelling, die noodzakelijk is om Windows op te starten. Het systeem herinnert de medewerkers er automatisch aan het wachtwoord één keer per drie maanden te wijzigen. Indien dit niet gebeurt, is inloggen niet meer mogelijk.

Tevens geeft 60% van de ondervraagden aan zijn computer te vergrendelen als hij tijdelijk niet op kantoor aanwezig is. Door het vergrendelen dient de medewerker opnieuw zijn gebruikersnaam en wachtwoord in te voeren alvorens toegang te krijgen tot de computer. Uit de praktijk is echter gebleken dat zeer veel medewerkers dit niet, of niet consequent, doen.

¹⁰⁸ Koorn 2010, p. 47-50.

Medewerkers zijn zich onvoldoende bewust van de veiligheidsrisico's van dergelijk nalatig gedrag. Om te voorkomen dat medewerkers vergeten hun computer te vergrendelen, is het mogelijk centraal een automatische vergrendeling in te stellen wanneer de computer een bepaalde tijd niet gebruikt wordt. Op dit moment wordt hier nog geen gebruik van gemaakt, ondanks het feit dat dit al meerdere malen is aangekaart. Medewerkers kunnen ook zelf de automatische vergrendeling instellen. Dit heeft slechts 24% van de ondervraagden gedaan.

Van de ondervraagden blijkt 42% een screensaver met wachtwoord te hebben. Voordat de screensaver uitgeschakeld kan worden, dient de gebruikersnaam en wachtwoord ingegeven te worden. Deze maatregelen zijn belangrijke mogelijkheden om persoonsgegevens te beveiligen tegen onbevoegde kennisname door anderen. Veel medewerkers hebben (enige) weerstand tegen de automatische vergrendeling en de screensaver met wachtwoord, aangezien zij het lastig vinden steeds hun gebruikersnaam en wachtwoord in te geven.

De medewerkers dienen zich eerst in te loggen op het algemene netwerk, voordat zij zich kunnen inloggen in Compas. Minder dan de helft van de ondervraagden geeft aan zich uit te loggen als ze Compas niet meer gebruiken. Concreet doen ongeveer 140 geautoriseerde medewerkers dit niet. Als deze medewerkers vervolgens hun werkplaats verlaten en hun computer niet vergrendelen, kunnen onbevoegde mensen eenvoudig kennis nemen van de grote hoeveelheden privacygevoelige informatie in Compas. Inmiddels is een deel van dit probleem ondervangen, doordat Compas automatisch uitlogt als het programma een half uur niet gebruikt wordt.

Ook simpele maatregelen blijken vaak niet gehanteerd te worden. Zo sluit slechts 29% het kantoor af als de laatste naar huis gaat en sluit 38% de (dossier)kasten af. Hierbij wordt opgemerkt dat de kantoren in het hoofdgebouw zelfs niet op slot kunnen. Deze maatregelen zorgen voor een basisbeveiliging, die nu dus veelal ontbreekt. Tot slot is gebleken dat slechts ongeveer 45% van de ondervraagden aangeeft de clean-desk methode te hanteren. Dit betekent dat aan het eind van de dag geen belangrijke papieren of dossiers meer op het bureau liggen. Bij 55% blijven dus wel belangrijke documenten op het bureau liggen.

Doordat medewerkers de risico's van dergelijk gedrag onderschatten, ontstaat een direct gevaar voor de privacy van de (over het algemeen kwetsbare) doelgroep van de Diamant-groep. Daarom dient de organisatie zorg te dragen voor een optimaal beveiligingsniveau, dat minimaal voldoet aan art. 13 Wbp. Tevens mag van de medewerkers verwacht worden dat zij ook zelf alles in het werk stellen om misbruik te voorkomen. Ook op basis van het goed werkgeverschap is de Diamant-groep verplicht zorg te dragen voor een goede beveiliging van de persoonsgegevens. Op basis van het bovenstaande wordt vastgesteld dat de Diamant-groep niet aan deze verplichting voldoet.

Het feit dat weinig medewerkers het belang van een passende beveiliging onderkennen, wordt onderstreept door de antwoorden op de vraag wie intern of extern toegang hebben tot de persoonsgegevens. Deze vraag is bewust op open wijze gesteld, met de bedoeling uit de antwoorden af te leiden of medewerkers een idee hebben van welke personen kennis (kunnen) nemen van de informatie die zij bijvoorbeeld in Compas plaatsen. In beginsel heeft iedereen met een autorisatie in Compas en degenen die inzage hebben in het persoons- en beleidsarchief toegang tot de persoonsgegevens. Dit komt neer op de personeelsadviseurs, het management (inclusief staf en directie), medewerkers van juridische zaken, leidinggevenden, de personeels- en salarisadministratie (inclusief de verzuimadministratie) en de afdeling arbeidsdiagnose. Slechts 18% gaf een compleet antwoord, tegenover 31% met een 'fout' antwoord.

Deze medewerkers gaven onder andere aan dat enkel collega's met dezelfde functie, collega's van hetzelfde bedrijfsonderdeel, alle medewerkers, niemand, het UWV, alleen 18k, de vertrouwenspersoon en de Ombudsman toegang hebben tot de persoonsgegevens.

Deze antwoorden tonen aan dat medewerkers onvoldoende besef hebben van de grote groep medewerkers die daadwerkelijk toegang heeft. Tot slot gaf 38% van de ondervraagde medewerkers een gedeeltelijk compleet antwoord. Zij noemden één of twee afdelingen of functiegroepen die toegang hebben tot de persoonsgegevens.

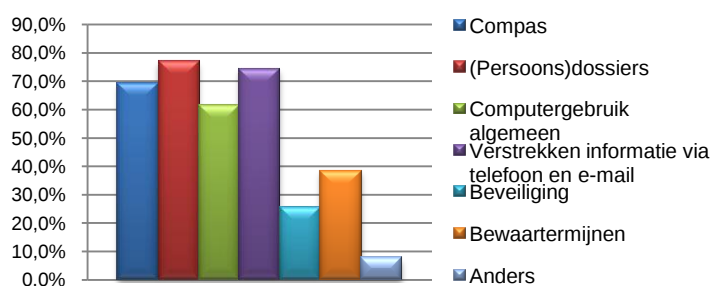
Opgemerkt dient te worden dat de vraag wellicht dermate algemeen was dat enkele medewerkers slechts gekeken hebben naar één aspect van het geheel. Zij hebben de vraag mogelijk beantwoord voor wat betreft de aanwezige dossiers in hun kantoor en hebben vervolgens niet bedacht dat dit niet de enige persoonsgegevens zijn die zij verwerken.

§ 5.9.2 Bewaring

Ten aanzien van de bewaring van persoonsgegevens is al het een en ander uitgewerkt in paragraaf 3.6.3. Met betrekking tot de bewaartermijnen beschikt de Diamant-groep over een selectielijst, die wordt getoetst door een secretaris van de gemeente. De selectielijst is de 'Werkwijzer Persoonsarchief' (opgenomen in bijlage XI), waarin per categorie is aangegeven of en hoe lang de documenten bewaard dienen te blijven. De selectielijst wordt regelmatig bijgewerkt. Wat betreft de bewaartermijnen is het hoofd Beleids- en Persoonsarchief verantwoordelijk voor een correcte naleving van deze termijnen. Vanuit dit beleid is het te verklaren dat 16% van de medewerkers aangeeft op de hoogte te zijn van de normen in deze werkwijzer, maar hier niet op te letten. Tevens geeft 31% aan wel op de hoogte te zijn gebracht en er ook daadwerkelijk naar te handelen. De grootste groep, 45% van de ondervraagden, geeft echter aan niet op de hoogte te zijn gebracht van de voorschriften en waarschijnlijk niet overeenkomstig deze voorschriften te handelen. Hetgeen in de vorige paragraaf voor het belang van een deugdelijke beveiliging gold, geldt in dit kader ook. Met betrekking tot de bewaring van persoonsgegevens is er echter een belangrijke waarborg aangebracht, in de persoon van het hoofd Beleids- en Persoonsarchief, die streng let op een correcte naleving van de werkwijzer. Medewerkers moeten wel zelf de termijnen voor hun handmatige verwerkingen in de gaten houden.

§ 5.9.3 Informatieverstrekking aan nieuwe medewerkers

Middels de vragenlijst is een beeld gevormd van de informatie die aan (nieuwe) medewerkers wordt meegedeeld over diverse privacyrechtelijke onderwerpen. Ruim 70% geeft aan dat hen is meegedeeld welke opstelling van hen werd verwacht. In figuur 11 is weergegeven hoeveel procent van deze ondervraagden is ingelicht over de verschillende onderwerpen.



Figuur 9: Informatieverstrekking aan medewerkers

Ten aanzien van het gebruik van persoonsdossiers, het verstrekken van privacygevoelige informatie via telefoon en e-mail en het gebruik van Compas is aan tamelijk veel medewerkers de gewenste werkhouding meegedeeld. Uit de resultaten van de vragenlijst blijkt echter dat eenduidig beleid hieromtrent ontbreekt. Het is namelijk gebleken dat aan de ene medewerker wel meegedeeld wordt welke houding van hem wordt verwacht, terwijl andere medewerkers weer geen informatie hebben ontvangen. Een verklaring kan gevonden worden in de persoon van de leidinggevende.

Niet alle leidinggevendenden voorzien nieuwe medewerkers namelijk van informatie. Ten aanzien van Compas zou het wenselijk zijn als standaard bepaalde informatie omtrent het gebruik van het programma aan de medewerker ter beschikking wordt gesteld. Ten aanzien van de beveiliging van persoonsgegevens en bewaartermijnen worden relatief weinig medewerkers van informatie voorzien. Dit komt overeen met de resultaten in paragraaf 5.9.

§ 5.10 De verplichtingen van de verantwoordelijke

Zoals reeds in paragraaf 3.6 is aangegeven rust op de verantwoordelijke een aantal verplichtingen. Met name de informatieplicht is in dit kader van groot belang. Middels de vragenlijst is getracht enig inzicht te krijgen in de naleving van deze informatieplicht. Uit de resultaten is gebleken dat 67% van de ondervraagden de betrokkenen op de hoogte stelt van de gegevensverwerking en bijna 24% dit niet doet. Daarnaast heeft ruim 7% aangegeven betrokkenen enerzijds wel op de hoogte te brengen en anderzijds niet. Dit heeft te maken met dubbelfuncties die deze medewerkers vervullen. In sommige gevallen worden de betrokkenen niet op de hoogte gesteld, omdat de verwerking voortvloeit uit het dienstverband. Daarbij dient bijvoorbeeld gedacht te worden aan de verwerking van salarisgegevens door de salarisadministratie. Uit diverse gesprekken is gebleken dat medewerkers niet exact weten wat zij moeten meedelen aan de betrokkenen.

Van de ondervraagden informeert 40% de betrokkenen op het moment van verkrijging, ruim 25% doet dat op het moment van eerste verstrekking aan een derde, 20% op het moment van vastlegging en nog eens 20% informeert de betrokkene gedurende de gegevensverwerking. Conform art. 33 en art. 34 Wbp en paragraaf 3.6.5 hangt het moment waarop de betrokkene geïnformeerd dient te worden samen met de vraag van wie de medewerkers de gegevens hebben verkregen.

In paragraaf 5.5 is uitgewerkt wie de persoonsgegevens aanleveren. Er bestaat een zekere discrepantie tussen de antwoorden op de vraag van wie de persoonsgegevens zijn verkregen en de vraag wanneer de betrokkenen zijn geïnformeerd. Doordat bijna iedere medewerker heeft aangegeven de persoonsgegevens vanuit meerdere kanalen te verkrijgen, is het niet mogelijk te achterhalen of de ondervraagden de betrokkenen op het juiste moment informeren. Gezien de lengte en complexiteit van de vragenlijst is bewust geen koppeling tussen beide vragen aangebracht, mede gelet op de geringe relevantie die een dergelijke aanvulling voor de organisatie heeft.

Deze keuze heeft tot gevolg dat het helaas niet mogelijk is de discrepantie met zekerheid te verklaren, hoewel een aantal mogelijke verklaringen voor de hand ligt. Allereerst kan de betreffende medewerker beoordelen dat hij de betrokkene niet op de hoogte hoeft te stellen van de verwerking. Bijvoorbeeld omdat hij er vanuit gaat dat een collega dit dient te doen. Daarnaast kan de medewerker niet op de hoogte zijn van de informatieplicht die op hem rust of kan sprake zijn van nalatigheid van de medewerker, door bijvoorbeeld gemakzucht of tijdgebrek.

§ 5.11 De rechten van betrokkenen

De rechten van betrokkenen vormen een belangrijke waarborg voor een betrokkene om grip te houden of te krijgen op de gegevens die over hem worden verwerkt. Van de ondervraagden geeft bijna 44% aan op de hoogte te zijn van de rechten die betrokkenen hebben. Bijna 53% gaf daarentegen aan de rechten van betrokkenen niet op te kunnen noemen. Van de ondervraagden die aan hebben gegeven op de hoogte te zijn van de rechten, bleek slechts 12,5% alle rechten op te kunnen noemen. Dit komt neer op drie ondervraagden. Deze resultaten tonen wederom aan dat de nodige kennis van de Wbp ontbreekt en het onderwerp privacy binnen de organisatie weinig aandacht krijgt.

Verder kon één ondervraagde twee rechten opnoemen en negen ondervraagden konden slechts één recht opnoemen. Deze resultaten houden in dat acht medewerkers hun eigen kennis van de Wbp op dit gebied verkeerd inschatten.

Veelal waren de medewerkers op de hoogte van het inzagerecht. Opvallend is dat zes medewerkers rechten noemden die niet in de Wbp zijn vastgelegd, te weten: toestemming voor verwerking, informatie, bezwaar, medische gegevens mogen alleen verstrekt worden met toestemming, geheimhoudingsplicht, toestemming voor verspreiding en inzage in de informatie die aan derden is verstrekt. Sommige antwoorden hebben wel enige overlapping met belangrijke onderwerpen in de Wbp, zoals de geheimhoudings- en informatieplicht. Het is begrijpelijk dat medewerkers de informatieplicht van de verantwoordelijke zien als een informatierecht van de betrokkene. De resultaten geven echter aan dat er (veel) te weinig kennis is bij de medewerkers. Hierdoor weten medewerkers ook niet welke procedure zij moeten volgen als zij een verzoek van een medewerker ontvangen. Uit recente vragen blijkt dat medewerkers niet weten of Sw-medewerkers recht op inzage in hun dossier hebben en of ze kopieën uit dit dossier mogen verstrekken. Daarbij bestaat veel onduidelijkheid over de status van het digitale dossier. Het is voor medewerkers onduidelijk of het inzagerecht ook voor het digitale dossier in Compas geldt.

Ook is gebleken dat de persoonsdossiers (zowel de analoge als de digitale) worden opgeschoond, alvorens het inzageverzoek wordt gehonoreerd. Het mag duidelijk zijn dat dit een onacceptabele handelswijze is. De Diamant-groep loopt achter met het opschonen van de dossiers en er is onvoldoende geld om deze achterstand recht te trekken. Hierdoor kunnen dossiers documenten bevatten die al verwijderd hadden moeten zijn. Betrokkenen hebben hier echter geen boodschap aan, zij hebben namelijk recht op inzage van hun totale dossier. Indien het dossier documenten bevat die verwijderd hadden moeten zijn, kan de betrokkene gebruik maken van zijn correctierecht en verwijdering van deze documenten vorderen.

§ 5.12 Het melden van gegevensverwerkingen bij het CBP en het voorafgaand onderzoek

De Diamant-groep heeft op dit moment geen gegevensverwerkingen gemeld bij het CBP, maar had dit wel reeds lang moeten doen. De organisatie zal daarom op korte termijn over moeten gaan tot het melden van diverse verwerkingen. Daarbij is het mogelijk dat er een aantal vrijstellingen bestaat op basis van het Vb. Een complete inventarisatie van de gegevensverwerkingen binnen de Diamant-groep maken valt buiten de reikwijdte van dit onderzoek, echter is op korte termijn wel noodzakelijk.

Verder is het van belang om vast te stellen of bij een aantal verwerkingen wellicht een voorafgaand onderzoek door het CBP noodzakelijk is. Bij drie categorieën verwerkingen, vastgelegd in art. 31 lid 1 Wbp, is een dergelijk onderzoek verplicht. Een voorafgaand onderzoek is verplicht als persoonsnummers worden gebruikt voor een ander doel dan waarvoor het nummer is verzameld, teneinde gegevens in verband te brengen met gegevens van andere verantwoordelijken, zonder dat dit wettelijk is toegestaan. Van de ondervraagden geeft iets minder dan de helft aan het BSN te verwerken. Deze medewerkers geven aan het BSN te verwerken in verband met het leggen van contact met het UWV, de Belastingdienst, gemeenten en zorgverzekeraars, als zoekfunctie, identificatie, de aanmelding voor een dienstverband, aanvragen van onderzoeken en het herkennen van de alfahulp en -klant. Het gebruik van het BSN voor deze doeleinden is niet onrechtmatig, waardoor een voorafgaand onderzoek niet noodzakelijk is.

Daarnaast is een voorafgaand onderzoek verplicht als de verantwoordelijke voornemens is gegevens vast te leggen op eigen waarneming, zonder de betrokkene daarvan op de hoogte te stellen.

Uit de resultaten is gebleken dat bijna 24% van de medewerkers gegevens vastlegt op eigen waarneming. Het gaan dan om de volgende gegevens: beoordeling van het functioneren, onrechtmatig gedrag, strafrechtelijke gegevens, gespreksverslagen en ziekteverzuim. Een voorafgaand onderzoek is enkel noodzakelijk als de gegevens heimelijk vastgelegd worden. Met betrekking tot het functioneren van medewerkers is geen sprake van heimelijke observatie. De medewerkers weten immers dat zij beoordeeld worden in de uitoefening van hun functie en dat er in dat kader gegevens verzameld worden. Ook de overige observaties gebeuren niet heimelijk en dus is een voorafgaand onderzoek niet verplicht.

Tot slot dient het CBP een voorafgaand onderzoek uit te voeren als de verantwoordelijke strafrechtelijke gegevens of gegevens over onrechtmatig of hinderlijk gedrag ten behoeve van derden verwerkt zonder daarvoor een vergunning te hebben. Ruim 14% geeft aan deze gegevens te verwerken. Medewerkers geven aan dat het gaat om gegevens in het kader van fraude, het niet naleven van de WWB (zoals opgenomen in hoofdstuk 2 van de WWB), het justitieel verleden van betrokkenen, ongewenst gedrag of opstandig gedrag in de training die als informatie dient voor de casemanager bij de gemeente. Een deel van deze gegevens wordt niet ten behoeve van derden verwerkt, maar ten behoeve van de verwerker zelf. Als het echter gaat om fraude, het niet naleven van WWB en de informatie voor casemanagers omtrent opstandig gedrag in de training, gaat het wel om het verwerken van strafrechtelijke gegevens of gegevens over onrechtmatig of hinderlijk gedrag voor derden. Deze verwerkingen zijn dus onderworpen aan een voorafgaand onderzoek.¹⁰⁹

§ 5.13 Het belang van een privacyreglement

Aan de medewerkers is gevraagd of zij het belangrijk vinden dat binnen de Diamant-groep meer geregeld wordt omtrent privacy. Bijna 95% van de ondervraagden onderkent het belang van een privacyreglement. De redenen die het vaakst genoemd worden zijn: medewerkers dienen beschermd te worden (13x), medewerkers moeten weten hoe ze met privacygevoelige gegevens moeten omgaan (8x), behoefte aan duidelijkheid (7x), betere afscherming is noodzakelijk (5x), de werkgever is verplicht hier zorg voor te dragen (4x), eenduidigheid (3x), alleen bepaalde mensen zouden toegang mogen hebben (3x), het reglement moet niet alleen opgesteld, maar ook nageleefd worden (2x), nu kunnen gegevens op straat belanden (2x).

Eén ondervraagde stelde dat een reglement niet zorgt voor de noodzakelijke verandering in het gedrag van medewerkers. Tevens gaf een medewerker aan dat medewerkers vanuit verschillende wetten verplicht zijn vertrouwelijk om te gaan met gegevens. Bij indiensttreding moet deze vertrouwelijkheid worden overeengekomen en zo nodig worden verduidelijkt. Degene die deze vertrouwelijkheid schendt dient ter verantwoording te worden geroepen en indien nodig disciplinair worden gestraft.

Het reeds eerder aangehaalde onderzoek¹¹⁰ onderstreept het belang van een deugdelijk privacyreglement. De onderzoeker heeft op basis van de resultaten een twaalf stappenplan gemaakt, dat organisaties kan helpen bij het waarborgen van de privacy binnen hun organisatie. In bijlage XII is dit stappenplan opgenomen.

¹⁰⁹ Voorafgaand onderzoek (Informatieblad CBP).

¹¹⁰ Koorn 2010, p. 47-50.

Conclusie

Op basis van het uitgevoerde onderzoek kunnen diverse conclusies getrokken worden die van belang zijn voor het opstellen van het nieuwe privacybeleid van de Diamant-groep. De belangrijkste conclusies zijn voortgekomen uit de ingevulde vragenlijsten door diverse medewerkers van de Diamant-groep.

De belangrijkste conclusie is dat medewerkers van de Diamant-groep slecht op de hoogte zijn van de hoofdlijnen uit de Wbp. Veel medewerkers overschatten hun eigen kennis van de Wbp. Dit hangt samen met het feit dat de Wbp niet leeft binnen de organisatie en dientengevolge het privacybewustzijn onder de medewerkers klein is. Medewerkers zijn onvoldoende in staat om hun eigen handelen te toetsen aan de normen in de Wbp. Hieronder wordt deze conclusie in verschillende punten uitgewerkt.

Compas - Binnen de Diamant-groep wordt veel gebruik gemaakt van Compas, het digitale personeelsinformatiesysteem. Compas is al meerdere malen onderwerp van discussies geweest. Op dit moment zijn de belangrijkste problemen met Compas:

- De medewerkers zijn onvoldoende voorgelicht over het gebruik van Compas. Hierdoor gebruiken zij het programma niet altijd even goed en komt het regelmatig voor dat bepaalde documenten en notities niet goed in het programma worden geplaatst. Dit heeft tot gevolg dat deze documenten leesbaar zijn voor een te grote groep medewerkers en de beveiliging niet optimaal is.
- De beveiliging van bepaalde gegevens in Compas is gebrekkig. Dit hangt enerzijds samen met de gebruikte opties van het programma, anderzijds met het gebruik van het programma door medewerkers.
- Er is geen autorisatiebesluit, waardoor het autorisatieproces niet loopt zoals het zou moeten lopen.
- Als een medewerker documenten kan aanmaken, kan hij ook alle documenten inzien en wijzigen.

De voornoemde problemen met Compas zorgen er mede voor dat de privacybescherming op dit moment niet gewaarborgd wordt, zoals dat volgens de Wbp hoort. De kans op inbreuk van het privacyrecht van individuele medewerkers is dan ook behoorlijk groot. Dit komt onder andere doordat er 275 geautoriseerden in Compas zijn.

Schaduwdoossiers - Het is algemeen bekend dat diverse medewerkers schaduwdoossiers bijhouden. Gebleken is dat het oorspronkelijke dossier hierdoor vaak incompleet is en er een grote kans is dat bepaalde documenten verloren gaan. Het bijhouden van schaduwdoossiers, is een inbreuk op het recht van privacy van medewerkers. Daarbij is het houden van schaduwdoossiers niet conform de Wbp. De verwerking, dat wil zeggen het verzamelen van gegevens om het schaduwdoossier aan te leggen, is in strijd met het rechtmatigheidsbeginsel, het beginsel van doelbinding en kan niet gebaseerd worden op een wettelijke grondslag. Bovendien heeft de Diamant-groep hierdoor geen grip op de gegevens die in de dossiers worden opgenomen, hoe de dossiers beveiligd zijn, hoe lang ze bewaard worden en wie er toegang tot heeft.

Doeleinden - De doeleinden van de verwerkingen binnen de Diamant-groep zijn zeer verschillend, doch allemaal rechtmatig te noemen. De doeleinden dienen concreet vastgelegd te worden in het nieuwe privacyreglement, zodat medewerkers geen gegevens verzamelen buiten deze doeleinden om.

Algemene en bijzondere persoonsgegevens - Binnen de organisatie worden veel algemene persoonsgegevens verwerkt. Dit is noodzakelijk in verband met de uitvoering van de wettelijke verplichtingen, zoals deze vastgelegd zijn in de Wsw. Mits de verwerkingen voldoen aan de overige bepalingen in de Wbp, zijn deze rechtmatig.

Daarnaast verwerken medewerkers erg veel bijzondere gegevens. Gezien de, over het algemeen, zwakke en kwetsbare doelgroep van de Diamant-groep, dient de rechtvaardiging om bijzondere gegevens te verwerken bij voorkeur gevonden te worden in één van de specifieke ontheffingsgronden in de Wbp. Het is namelijk niet aannemelijk dat er, gezien het niveau van de allerzwakste medewerkers, sprake is van 'uitdrukkelijke toestemming' (aangeduid als algemene ontheffingsgrond in de Wbp). Toestemming die door deze medewerkers wordt gegeven, voldoet mogelijk niet aan de vereisten. (Bijvoorbeeld dat de beslissing in vrijheid en bewust (op basis van de juiste informatie) genomen dient te zijn). Mocht hier sprake van zijn, dan dient de Diamant-groep niet zonder meer aan te nemen dat de verwerking geoorloofd is.

Gezondheidsgegevens - Binnen de Diamant-groep worden tamelijk structureel gezondheidsgegevens opgenomen in de verzuimregistratie of het persoonsdossier. Dit is echter niet toegestaan. Daarnaast zijn deze gegevens voor een te grote groep medewerkers toegankelijk. Met name in Compas kunnen te veel medewerkers bij deze informatie. De regels omtrent de analoge dossiers worden wel streng nageleefd. Hoewel dit niet toegestaan is, bevatten de adviezen van de bedrijfsarts te vaak gegevens met betrekking tot de aard en oorzaak van de ziekte van medewerkers. De Diamant-groep stelt dat de medische gegevens noodzakelijk zijn om de wettelijke taak uit te kunnen voeren. Deze stelling is niet correct. De medewerkers hebben in beginsel enkel de gegevens met betrekking tot de noodzakelijke maatregelen en voorzieningen nodig, om de medewerkers op een passende werkplaats te kunnen plaatsen. Er dient dus selectiever met het verwerken van gezondheidsgegevens omgegaan moeten worden.

Strafrechtelijke gegevens - De OR heeft geen toestemming gegeven, voor wat betreft de verwerking van strafrechtelijke gegevens die hun oorsprong vinden in de organisatie. Gegevens over het strafrechtelijke verleden (bijvoorbeeld een detentieverleden) van medewerkers mogen slechts verwerkt worden als de verwerking noodzakelijk is ter bescherming van de Diamant-groep en de medewerkers in dienst van de Diamant-groep. Gegevens omtrent onrechtmatig of hinderlijk gedrag zijn geen bijzondere persoonsgegevens, aangezien het niet gaat om een opgelegd verbod door de rechter. Verwerking van deze gegevens is toegestaan, mits er wordt voldaan aan de overige bepalingen in de Wbp.

Gegevens omtrent ras of etniciteit - De Diamant-groep maakt conform de Wet op de Identificatieplicht bij indiensttreding van medewerkers een kopie van een geldig identiteitsbewijs. Deze kopie dient bewaard te worden bij de loonadministratie en niet bij de personeelsadministratie. Binnen de Diamant-groep gebeurt dit bewust wel, aangezien de medewerkers van het archief, in tegenstelling tot de personeelsadministratie, de nodige kennis hebben om de wettelijke bewaartermijnen na te leven. Daarbij is het archief beter beveiligd. Het plaatsen van kopieën van identiteitsbewijzen in Compas, voldoet niet aan het noodzakelijkheids criterium en is daarom niet toegestaan. Indien de Diamant-groep de noodzaak aannemelijk zou kunnen maken, dient in ieder geval zorg gedragen te worden voor een passende beveiliging, hetgeen nu niet het geval is. Op de camerabeelden die op het terrein worden gemaakt, kunnen mogelijk personen staan (en dus worden rasgegevens verwerkt). Deze gegevens mogen echter verwerkt worden, aangezien de Diamant-groep terughoudend met het cameratoezicht omgaat. Zo hangen er geen camera's op de werkplekken. De foto's van medewerkers die in de Telegids staan, zijn daar met toestemming in geplaatst en deze verwerking is dus rechtmatig.

Gegevens omtrent godsdienst, politieke gezindheid, lidmaatschap van een vakvereniging en seksueel leven - Verwerking van deze gegevens door medewerkers van de Diamant-groep is niet toegestaan, aangezien geen specifieke uitzonderingsgrond in de Wbp is die verwerking rechtvaardigt. Alleen voor het verwerken van de gegevens omtrent het lidmaatschap van een vakvereniging van de betrokkene, kan een rechtvaardiging aanwezig zijn. Dit is alleen het geval als de betrokkene de kosten daarvan wenst te fiscaliseren.

Daarnaast zal, gezien de werkzaamheden van de Diamant-groep, niet zo snel sprake zijn van één van de algemene ontheffingsgronden in de Wbp. Mocht dit echter wel het geval zijn, dan nog kan de Diamant-groep niet aannemelijk maken dat deze gegevens noodzakelijk zijn voor de uitoefening van zijn taken.

Noodzakelijkheid - Hoewel de Diamant-groep de neiging heeft zoveel mogelijk gegevens van zijn medewerkers te verzamelen, is dit niet conform de Wbp. Vooral ten aanzien van de verwerking van bijzondere gegevens voldoet de Diamant-groep vaak niet aan het noodzakelijkheids criterium. Hierdoor zijn deze verwerkingen onrechtmatig.

Grondslag - Medewerkers hebben deze vraag, ondanks de toelichting bij deze vraag, als lastig ervaren. Het blijkt niet eenvoudig en eenduidig voor de medewerkers, om de wettelijke grondslag op basis waarvan zijn gegevens verwerken aan te duiden. Medewerkers vinden het lastig hun eigen handelen te kwalificeren volgens normen in de Wbp. Dit is gezien de lastige en vage termen in de Wbp niet zo verrassend.

Gegevensstromen - Binnen de Diamant-groep zijn de gegevensstromen zeer omvangrijk, zowel intern als extern. Veruit de meeste medewerkers krijgen de persoonsgegevens aangeleverd vanuit een andere afdeling of bedrijfsonderdeel. Daarnaast zijn ook veel gegevens afkomstig van betrokkenen of derden. Verder vindt ook een grote uitwisseling van gegevens plaats met externe instellingen. Uitwisseling van gegevens is toegestaan als de verwerking gebaseerd kan worden op een wettelijke grondslag. Voor zover te concluderen valt uit de resultaten, zijn de verstrekkingen aan externe instellingen rechtmatig conform art. 8 sub f Wbp. Op dit moment heeft de Diamant-groep echter weinig vat op deze gegevensstromen. Hierdoor is de kans op privacyinbreuk tamelijk groot.

Handmatige en (gedeeltelijk) geautomatiseerde verwerkingen - De handmatige verwerkingen, te weten de persoonlijke telefoon- of adressenboekjes van medewerkers en persoonlijke notities, vallen niet onder de reikwijdte van de Wbp, aangezien ze bestemd zijn voor persoonlijk gebruik. Medewerkers dienen wel zorg te dragen voor een goede bescherming van deze gegevens, zodat onbevoegden hier geen kennis van kunnen nemen. Gegevens in verband met verslaglegging, gespreksverslagen en aantekeningen van telefoongesprekken betreffen alle gedeeltelijk geautomatiseerde verwerkingen en vallen daarmee wel onder de reikwijdte van de Wbp.

Beveiliging - Eén aspect loopt als een rode draad door de resultaten, namelijk de maatregelen ter bescherming van de persoonsgegevens. Op allerlei vlakken worden onvoldoende beschermingsmaatregelen getroffen en medewerkers beseffen onvoldoende wat de mogelijke gevolgen hiervan zijn. Gezien de kwetsbare doelgroep van de Diamant-groep drukt de beveiligingsverplichting extra zwaar op de Diamant-groep. Zelfs eenvoudige beveiligingsmaatregelen worden slechts door een kleine groep medewerkers toegepast. Dit probleem is terug te leiden naar een gering privacybewustzijn onder de medewerkers. Zoals eerder aangehaald voldoet de huidige inrichting van Compas niet aan de vereiste beveiligingsmaatregelen. Daarnaast is het de verplichting van de Diamant-groep om de kans op misbruik door onbevoegden zo klein mogelijk te houden. Er kan niet anders dan geconcludeerd worden dat de Diamant-groep niet voldoet aan de verplichting om zorg te dragen voor passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. Het feit dat het besef bij medewerkers over relevante onderwerpen met betrekking tot privacy veelal ontbreekt, wordt onderstreept doordat slechts een kleine groep medewerkers kan aangeven wie toegang hebben tot de persoonsgegevens (in de analoge en digitale dossiers).

Autorisaties - Tegen de achtergrond van de problemen met Compas speelt het autorisatieprobleem. Binnen de Diamant-groep ontbreekt een autorisatiebesluit waarin is geregeld wie beslist over het toekennen en aanmaken van nieuwe autorisaties.

Hierdoor is het onduidelijk waar de verantwoordelijkheden op het autorisatiegebied zouden moeten liggen en blijven er discussies ontstaan.

Bewaartermijnen - Ten aanzien van de naleving van bewaartermijnen is een belangrijke waarborg gevormd. Er is een selectielijst aanwezig waarin de bewaartermijnen zijn opgenomen en deze wordt uitgevoerd door het hoofd Beleids- en Persoonsarchief. Deze waarborg is belangrijk, aangezien uit de praktijk is gebleken dat medewerkers zelf moeite hebben om dergelijke termijnen in het oog te houden.

Informatievoorziening - Er ontbreekt eenduidig beleid met betrekking tot de informatievoorziening aan nieuwe medewerkers. Met betrekking tot het telefoon- en e-mailverkeer en Compas zijn tamelijk veel medewerkers voorzien van informatie over de gewenste houding die van hen verwacht wordt. Gebleken is dat het van de leidinggevende afhangt of medewerkers ingelicht worden. Ten aanzien van de beveiliging en bewaring van persoonsgegevens krijgen medewerkers te weinig informatie. Door aan het begin van het dienstverband medewerkers onvoldoende in te lichten, kan in een later stadium niet verwacht worden dat deze medewerkers conform de privacywetgeving handelen.

Informatieplicht - Uit diverse gesprekken is gebleken dat medewerkers niet exact weten welke gegevens zij moeten meedelen aan betrokkenen. Er bestaat een zekere discrepantie tussen het percentage van wie de gegevens worden verkregen en het moment van gegevensverstrekking. Mogelijke oorzaken voor deze discrepantie kunnen zijn: medewerkers zijn van mening dat een collega de betrokkene dient te informeren, de medewerker is niet bekend met de informatieplicht, of er kan sprake zijn van nalatigheid, door bijvoorbeeld gemakzucht of tijdgebrek.

Rechten van betrokkenen - Medewerkers schatten hun eigen kennis op het gebied van de rechten van betrokkenen hoger in dan deze daadwerkelijk is. Ook met betrekking tot dit onderwerp ontbreekt de relevante kennis bij de medewerkers. Slechts drie medewerkers bleken in staat alle rechten van de betrokkenen op te noemen. Daarnaast noemden medewerkers rechten die niet in de Wbp staan. Hieruit vloeit voort dat medewerkers niet op de hoogte zijn van de procedure die zij moeten volgen bij een verzoek van een betrokkene. Het opschonen van persoonsdossiers, voordat het inzageverzoek gehonoreerd wordt, is niet toegestaan. Hierdoor worden de rechten van betrokkenen beperkt.

Melden en voorafgaand onderzoek - Binnen de Diamant-groep zijn er nog geen verwerkingen gemeld bij het CBP. Dit betekent dat er risico bestaat op een boete vanuit het CBP. De kans op een dergelijke boete is niet zo groot, maar wel aanwezig. Ten aanzien van de verwerking van strafrechtelijke gegevens voor derden is een voorafgaand onderzoek door het CBP verplicht. Slechts een enkele medewerker heeft aangegeven in dit kader gegevens te verwerken. Nader onderzoek hiernaar is wellicht noodzakelijk.

FG of privacy officer - Op dit moment is er geen FG of privacy officer aangesteld binnen de Diamant-groep. Gezien de grootte van de organisatie en de kwetsbaarheid van de doelgroep is het opmerkelijk en onwenselijk dat niemand binnen de organisatie deze functie vervult, waardoor dus de nodige kennis op het gebied van het privacyrecht ontbreekt.

Het privacyreglement - Een overgrote meerderheid van de ondervraagden vindt dat binnen de Diamant-groep meer geregeld moet worden op het gebied van privacy. Gezien de grote diversiteit aan verwerkingen binnen de Diamant-groep, is het niet mogelijk het algemene privacybeleid concreet te maken. Verder zal gedurende een langere periode aandacht besteed moeten worden aan het privacyrecht van medewerkers binnen de Diamant-groep. Het opstellen van een privacyreglement is namelijk zinloos als niet ingezet wordt op het vergroten van kennis van medewerkers en affiniteit met de privacy en dientengevolge het gedrag van de medewerkers niet verandert.

Aanbevelingen

Uit de conclusies is een aantal aspecten naar voren gekomen, die op dit moment niet voldoen aan de Wbp of een concrete dreiging voor de privacy vormen. Op basis hiervan wordt een aantal belangrijke aanbevelingen gedaan om de huidige situatie te verbeteren en te komen tot een nieuw privacybeleid dat voldoet aan de normen in de Wbp.

Bewustwording - Eén van de belangrijkste aanbevelingen naar aanleiding van dit onderzoek, is dat binnen de Diamant-groep gewerkt dient te worden aan bewustwording onder de medewerkers. Dit betekent dat de medewerkers voorgelicht moeten worden over het privacyrecht en de gevolgen van een niet goede naleving van de privacywetgeving voor individuele medewerkers en de organisatie. Door vaker aandacht te besteden aan de privacy(bescherming), gaat het onderwerp meer leven binnen de organisatie.

Daarnaast dient de kennis die er op dit moment binnen de organisatie op het gebied van privacy is, vergroot te worden. Slechts enkele medewerkers zijn, voornamelijk in verband met hun functie, op de hoogte van de normen en de wettelijke verplichtingen uit de Wbp. Er dient geïnvesteerd te worden in het op peil brengen van de kennis, zodat medewerkers in de toekomst zelf betere afwegingen kunnen maken en bepaalde verzoeken van betrokkenen zelf kunnen afhandelen. Door het vergroten van de kennis over het privacyrecht, kunnen medewerkers ook beter beoordelen welke informatie (en waar) in Compas moet staan.

Medewerkers hebben behoefte aan concrete informatie over wat zij wel en niet mogen. Naar aanleiding van dit onderzoek is een algemeen privacyreglement opgesteld. Gezien de diversiteit van verwerkingen binnen de Diamant-groep is het niet mogelijk te komen tot een concreet reglement. Daarom is het belangrijk dat naar aanleiding van dit onderzoeksrapport en het privacyreglement diverse werkinstructies en -protocollen worden opgesteld, waarin bepaalde processen omtrent privacy worden uitgewerkt. Er kan dan bijvoorbeeld gedacht worden aan de procedure betreffende het inzagerecht. Mede door heldere werkinstructies wordt het voor medewerkers duidelijk hoe zij met dergelijke verzoeken dienen om te gaan.

Wat verder bij kan dragen aan bewustwording onder de medewerkers, is het geven van eenduidige informatie bij indiensttreding van nieuwe medewerkers. Het privacyrecht is voor elke medewerker van belang, welke functie in de organisatie hij ook vervult. Bij indiensttreding krijgen medewerkers informatie over de rechten en plichten die zij hebben als medewerkers. Voorstaande is dus deels eenvoudig te ondervangen door de hierboven besproken maatregelen onderdeel te laten uitmaken van het introductiebeleid van nieuwe medewerkers. Daarom dient overwogen te worden om in het introductiepakket informatie over privacy op te nemen. De informatie die nu aan medewerkers wordt verschaft is te zeer afhankelijk van de leidinggevende, waardoor medewerkers met dezelfde functie, verschillende informatie krijgen en dus anders handelen.

Door het investeren in bewustwording en kennis onder de medewerkers, gaan medewerkers op een gegeven moment hun eigen handelen toetsen aan de Wbp. Dit betekent dat medewerkers in staat moeten worden geacht te analyseren of zij overeenkomstig de Wbp handelen. Indien dat niet het geval blijkt, kunnen deze medewerkers hier ook op aangesproken worden.

Implementatie privacyreglement - Het opstellen van het privacyreglement, waarin wordt aangegeven wat wel en niet toegestaan is binnen de organisatie op het gebied van privacy, draagt bij aan een grotere bewustwording. Het opstellen van een privacyreglement is dus belangrijk, maar zonder gedragsverandering bij de medewerkers zal het reglement voor de organisatie weinig toegevoegde waarde hebben. Deze gedragsverandering kan mede gerealiseerd worden, door voldoende aandacht te besteden aan de implementatie van het privacyreglement.

Het nieuwe reglement dient kenbaar gemaakt te worden onder de medewerkers. Dit kan bijvoorbeeld gedaan worden door het plaatsen van een bericht op intranet, medewerkers een brief te sturen en het geven van presentaties. Vervolgens dient de organisatie ook aandacht te besteden aan het naleven van het reglement, anders vervallen medewerkers terug in hun oude gedrag. Leidinggevendenden dienen de medewerkers te begeleiden, de nieuwe werkwijze (uiteengezet in het reglement en diverse werkinstructies) te introduceren en uit te voeren en medewerkers actief te corrigeren.

Beveiliging - Ten aanzien van de beveiliging dient binnen de Diamant-groep een flinke slag geslagen te worden. Binnen de organisatie is bekend dat er problemen zijn met Compas. Gezien de problemen die er op dit moment spelen, dient te organisatie te overwegen of Compas wel het meest geschikte informatiesysteem is. Ook dient onderzocht te worden of de organisatie alle mogelijke functies van Compas gebruikt.

In Compas wordt zeer veel informatie opgeslagen door medewerkers. Gebleken is dat niet alle informatie voor medewerkers noodzakelijk is om hun taak uit te kunnen uitvoeren. Er dient dus onderzocht te worden of er optimaal gebruik wordt gemaakt van de beveiligingsmogelijkheden die Compas de gebruiker biedt. Dit punt hangt nauw samen met het ontbreken van kennis en kunde (op het gebied van privacy) bij de medewerkers. Hierdoor plaatsen zij vaak overbodige of subjectieve informatie in Compas. Daarnaast plaatsen zij de informatie vaak op een verkeerde plek, waardoor het beveiligingsniveau niet voldoende is en deze informatie toegankelijk is voor een te grote groep medewerkers.

Verder dient de organisatie aandacht te schenken aan de beveiligingsmaatregelen die medewerkers zelf kunnen treffen om hun persoonsgegevens te beveiligen. Op alle computers dient standaard een automatische vergrendeling geplaatst te worden die ingeschakeld wordt als de computer bijvoorbeeld gedurende vijf minuten niet wordt gebruikt. Indien de medewerker de computer weer wil gebruiken, dient hij zijn gebruikersnaam en wachtwoord in te voeren. Het belang van de bescherming van privacy van individuele medewerkers dient voor te gaan op het belang van de medewerkers die met het systeem werken. Verder dient de organisatie te overwegen sloten op de kantoordeuren in het hoofdgebouw te monteren, zodat deze aan het einde van dag afgesloten kunnen worden. Verder dient de clean-desk methode bedrijfspolicy te worden. Iedereen dient volgens deze methode te handelen. Indien geconstateerd wordt dat dit niet gebeurt, dienen medewerkers hier op aangesproken te worden. Een onderdeel van het vergroten van het privacybewustzijn is het onder de aandacht brengen van het belang van beveiligingsmaatregelen. Medewerkers moeten het belang van beveiliging onderkennen en attenter worden op de naleving van deze voorschriften.

De getroffen beveiligingsmaatregelen en de te volgen (beveiligings)richtlijnen dienen vastgelegd te worden in een beveiligingsprocedure of een beveiligingsplan, dat ter goedkeuring aan het bestuur en de OR wordt voorgelegd.

Autorisaties - De Diamant-groep dient een autorisatiebesluit vast te stellen. Hierdoor worden discussies over de vraag waar bepaalde bevoegdheden liggen vermeden. Alle autorisaties die er op dit moment bestaan dienen in kaart gebracht te worden, evenals de rechten van de verschillende autorisaties. Er zal gekeken moeten worden of bepaalde medewerkers op dit moment onterecht meerdere rechtenprofielen hebben. Indien dit het geval is, zal het aantal rechtenprofielen teruggebracht moeten worden naar één. Ook dient onderzocht te worden of er nagenoeg identieke autorisaties bestaan die samengevoegd kunnen worden. Hierbij is het van belang te bekijken of bepaalde rechten ook daadwerkelijk noodzakelijk zijn voor de uitoefening van de functie van deze medewerker.

Adviezen bedrijfsarts - De adviezen van de bedrijfsarts voldoen vaak niet aan de privacyregels.

Zo bevatten de adviezen regelmatig informatie over de aard en oorzaak van de arbeidsongeschiktheid van een medewerker. Dit is niet toegestaan, want de Diamant-groep heeft deze informatie niet nodig om de medewerker te plaatsen op een passende werkplek. Het is onduidelijk of de bedrijfsarts deze informatie verstrekt omdat hij niet op de hoogte is van de geldende regelingen of omdat medewerkers hebben aangegeven dat zij deze informatie nodig hebben en de bedrijfsarts daar aan tegemoet wil komen. Wellicht dat de bedrijfsarts betrokken kan worden bij het traject voor medewerkers om de bewustwording en kennis over het privacyrecht te vergroten.

Inzage - Het is evident dat het opschonen van het persoonsdossier alvorens het verzoek om inzage wordt gehonoreerd, niet toegestaan is. Er wordt daarom geadviseerd een start te maken met de controle van de dossiers en daaruit te verwijderen wat verwijderd dient te worden conform de Werkwijze Persoonsarchief, zoals die binnen de Diamant-groep geldt.

Noodzakelijkheid - Voornamelijk ten aanzien van de verwerking van de vele bijzondere persoonsgegevens is het noodzakelijkheids criterium niet altijd aanwezig. Het bestuur zal de eigen handelswijze dienen te evalueren en zich af dienen te vragen welke informatie nu daadwerkelijk noodzakelijk is om aan de wettelijke verplichting te kunnen voldoen. Tevens wordt aanbevolen niet zonder meer verder te gaan met het plaatsen van kopieën van legitimatiebewijzen en bankpassen in Compas. De noodzaak hiertoe ontbreekt.

FG/Privacy officer - Gezien de omvang van de organisatie en de kwetsbaarheid van de doelgroep, dient de Diamant-groep te overwegen of zij een privacy officer of een FG aan zullen stellen. Er wordt in eerste instantie geadviseerd een privacy officer aan te stellen. Op deze wijze kunnen de organisatie en zijn medewerkers in kleine stappen wennen aan de verscherpte regels rondom privacy. Na bijvoorbeeld een jaar dient een evaluatiemoment plaats te vinden. Op dat moment kan besloten worden verder te gaan met de privacy officer of wellicht alsnog een FG aan te stellen.

Melden - Op dit moment is er nog geen enkele gegevensverwerking aangemeld bij het CBP. Dit kan eventueel vervelende financiële gevolgen voor de organisatie hebben. Geadviseerd wordt op zeer korte termijn een werkgroep te formeren die zich bezig gaat houden met de melding aan het CBP.

Uitvoeren Quickscan - Het CBP heeft de Quickscan ontwikkeld. Dit is een vragenlijst, waarin een aantal belangrijke onderwerpen met betrekking tot de privacybescherming in een organisatie centraal staan. De Quickscan is bedoeld voor het creëren van bewustwording en kan samen met dit rapport uitstekend dienen als startpunt om de privacy binnen de Diamant-groep beter vorm te geven. Het spreekt voor zich dat de Quickscan slechts een globaal beeld schetst. De Quickscan en bijbehorende toelichting zijn te vinden via de website van het CBP, te weten: www.cbppweb.nl (zoekterm: Quickscan). Ook het stappenplan (bijgevoegd in bijlage XII) kan behulpzaam zijn bij de inrichting van het nieuwe privacybeleid. In de toekomst wordt verder ten eerste aanbevolen gebruik te maken van andere evaluatie instrumenten die het CBP beschikbaar stelt via zijn website, zoals de 'Wbp zelfevaluatie' of de 'privacyaudit'.

Tot slot - De Diamant-groep dient intern een discussie op gang te brengen over de uitgangspunten van het nieuwe privacybeleid. Wat is de doelstelling van de Diamant-groep? Willen zij aan de wettelijke vereisten voldoen, maar meer ook niet, of willen ze zich inspannen om een en ander zo goed mogelijk geregeld te hebben voor alle medewerkers (met als uitgangspunt het behouden van een werkbare situatie)? Kortom: is het doel een 10 of een 6,5? Afhankelijk van deze beslissing, dient het bestuur te besluiten welke maatregelen al dan niet doorgevoerd worden.

Evaluatie

In dit hoofdstuk zal het verloop van het onderzoek worden geëvalueerd. Eerst wordt ingegaan op het proces en vervolgens op het product. De evaluatie van het proces heeft betrekking op het proces van de totstandkoming van dit onderzoeksrapport. Er wordt gekeken hoe dit rapport tot stand is gekomen en welke punten goed en minder goed zijn verlopen. Bij de evaluatie van het product wordt gekeken of de resultaten van het onderzoek antwoord geven op de deelvragen en de centrale vraagstelling wordt beantwoord.

Procesevaluatie - De onderzoeksopzet bleek een belangrijk document, dat gedurende het verdere onderzoek van grote waarde was. Met name de hoofdstukindeling en het overzicht van middelen waren van groot belang. Gedurende het proces is de onderzoeksopzet een aantal malen op kleine puntjes gewijzigd. Zo is besloten minder interviews te houden dan in eerste instantie gepland, omdat meer interviews weinig nieuwe relevante informatie voor het onderzoek zou opleveren. Wel is besloten een interview te houden met een medewerker van de afdeling juridische zaken van de gemeente Tilburg. Gezien de nauwe verwantschap tussen de Diamant-groep en de gemeente, droeg de informatie omtrent de wijze waarop de gemeente haar privacybeleid vormgeeft bij aan het beantwoorden van de deelvragen. Ook zijn wat kleine wijzigingen aangebracht in de deelvragen, zodat deze beter aansloten bij hetgeen in de vragenlijst behandeld werd. Het beantwoorden van de deelvragen is verder volgens planning verlopen.

Gedurende het onderzoek is gebleken dat de deelvragen vroegen om een uitgebreide beantwoording, zodat het geheel ook voor niet juristen goed leesbaar is. Hierdoor is het onderzoeksrapport uitgebreider dan gepland geworden. Het deed echter afbreuk aan het betoog, om relevante informatie weg te laten met als enige reden het rapport enkele pagina's in te korten.

Met betrekking tot de vragenlijsten is de respons een sterk punt van dit onderzoek. Deze respons is bereikt door alle vragenlijsten persoonlijk onder de medewerkers te verspreiden. Hierdoor bleken veel medewerkers bereid te zijn mee te werken aan het onderzoek. Er is één herinneringsmail gestuurd, naar aanleiding hiervan hebben veel medewerkers de vragenlijst nog ingevuld. Dit heeft geleid tot de respons van ruim 82%.

Productevaluatie - Het onderzoek gaat met name in op de huidige wijze van het verwerken van gegevens binnen de Diamant-groep. Alvorens hier toe over te gaan is het wettelijk kader geschetst. De huidige wijze van gegevens verwerken is in kaart gebracht middels de vragenlijsten. De verschillende onderwerpen die in de vragenlijsten aan de orde kwamen, zijn uitgewerkt in subdeelvragen. De combinatie van het wettelijk kader en de uitwerking van de vragenlijsten vormen tezamen de beantwoording van de centrale vraagstelling. Het was lastig om de resultaten uit de vragenlijsten overzichtelijk uit te werken in het onderzoeksrapport. Er is bewust gekozen om de vragen die zich daarvoor leenden uit te werken in grafieken. Dit zorgt voor een overzichtelijke weergave van de resultaten.

Er was reeds een algemeen privacyreglement als concept binnen de organisaties aanwezig. Naar aanleiding van de conclusies en aanbeveling is een nieuw reglement opgesteld, dat ter goedkeuring aan het bestuur wordt voorgelegd.

Het onderzoek en het privacyreglement is van grote waarde voor de organisatie. Aan de hand van het onderzoek is binnen de organisatie duidelijk vast komen te staan waar de knelpunten in het huidige beleid liggen. Een deel van deze knelpunten is weggenomen door het opstellen van het privacyreglement. Een ander deel van de knelpunten dient echter door andere stappen opgelost te worden. Dit onderzoek kan daarbij behulpzaam zijn. In het onderzoek wordt aangegeven wanneer er vervolgonderzoek gewenst zou kunnen zijn.

Literatuurlijst

Boeken

Berkvens & Prins 2007

J.M.A. Berkvens & J.E.J. Prins, *Privacyregulering in theorie en praktijk*, Deventer: Kluwer 2007.

Hooghiemstra & Nouwt 2007

T.F.M. Hooghiemstra & J. Nouwt, *Tekst en toelichting Wet bescherming persoonsgegevens*, Den Haag: Sdu Uitgevers 2007.

Terstegge 2000

J.H.J. Terstegge, *De nieuwe Wet bescherming persoonsgegevens. Handleiding voor de praktijk*, Alphen aan de Rijn: Samsom 2000.

Thole, Van der Jagt & Roerdink 2010

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

De Vries & Rutgers 2001

H.H. de Vries & D.J. Rutgers, *Actualiteiten Sociaal Recht. Wet bescherming persoonsgegevens. Toepassing in arbeidsverhoudingen*, Deventer: Kluwer 2001.

Rapporten en handleidingen

Lioen & van Munster-Frederiks/Van de Velde & Terhorst 2008

S. van de Velde & A.G.I. Terhorst, S. Lioen & M. Th. van Munster-Frederiks. *De zieke werknemer en privacy. Regels voor de verwerking van persoonsgegevens van zieke werknemers* (Achtergrondstudies en verkenningen nr. 27, College Bescherming Persoonsgegevens), Den Haag: Deltahage bv 2008.

Sauerwein & Linnemann 2002

L.B. Sauerwein en J.J. Linnemann, *Handleiding voor verwerkers van persoonsgegevens*, (Ministerie van Justitie), Den Haag: 2002.

Handleiding

Handleiding voor de gebruiker van het Burgerservicenummer. Aanbevelingen voor een goed gebruik van het Burgerservicenummer, 2007.

Handreiking Vrijstellingsbesluit WBP

De Handreiking Vrijstellingsbesluit WBP (College Bescherming Persoonsgegevens).

Onderzoeksrapport College Bescherming Persoonsgegevens 2005

Reïntegratie van zieke werknemers en privacy. Verkennend onderzoek bij drie reïntegratiebedrijven, (College Bescherming Persoonsgegevens), 2005.

Tijdschriften

Koorn 2010

R. Koorn, 'Privacybescherming: het kan én moet beter!', *Informatiebeveiliging* 2010, p. 47-50.

Elektronische bronnen

‘Over Diamant’,
<www.diamant-groep.nl/default.asp?ID=3664>, bezocht: 6 mei 2010.

‘Specialisten in arbeidsontwikkeling en personeelsdiensten’,
<www.18k.nl> producten en diensten > arbeidsontwikkeling/personeelsdiensten, bezocht: 6 mei 2010.

‘Overzicht van de taken en bevoegdheden van het CBP’,
<www.cbpweb.nl/Pages/ind_cbp.aspx>, bezocht: 28 september 2010.

‘De Wet Bescherming Persoonsgegevens. Over de bescherming van uw persoonlijke gegevens’
<www.cbpweb.nl/Pages/bro_wbp.aspx>, bezocht: 22 september 2010.

‘Informatiebladen CBP’
<www.cbpweb.nl>, bezocht: gedurende het gehele onderzoek.

‘Identificatie nieuwe werknemers!’
<www.gibogroep.nl/Nieuws/Nieuws/Algemeen/Identificatienieuwewerknemers/tabid/713/Default.aspx>; bezocht: 6 november 2010.

<www.om.nl/u_en_het_om/juridisch_jargon/>;
zoektermen: materiële schade en immateriële schade, bezocht: 12 oktober 2010.

<www.dehoogstraat.nl> revalideren > privacy > privacyreglement en inzagerecht > privacyreglement, bezocht: 6 november 2010.

Jurisprudentie en uitspraken CBP

EHRM 22 juni 1997, NJ 1998, 506

Rechtbank Rotterdam, 2 juni 2008, nr. 07/956
Rechtbank 's-Hertogenbosch 18 januari 2005, *LJN AT0462*
Voorzieningenrechter Rechtbank 's-Gravenhage 31 maart 2004, nr. AWB04/166

ABRvS 16 maart 2005, *LJN AT0510*.

Rgk 9 maart 1994, zaaknr. 94.E.034
CBP 23 januari 2006 z2005-1355.
CBP 4 februari 2003 z2002-1511.