Je mag alles van me weten, behalve …

Een onderzoek naar de Wet bescherming persoonsgegevens, de Wet meldplicht datalekken en de Algemene Verordening Gegevensbescherming binnen Stichting ORO

Bron: www.fundaments.nl

Stichting ORO

M.P.M.H. (Maartje) Biemans
Helmond, mei 2016

Je mag alles van me weten, behalve …

Een onderzoek naar de Wet bescherming persoonsgegevens, de Wet meldplicht datalekken en de Algemene Verordening Gegevensbescherming binnen Stichting ORO

Auteur	Maartje Biemans
Studentnummer	2059922
Opleiding	HBO Rechten, Juridische Hogeschool Avans-Fontys te ’s-Hertogenbosch
Afstudeeradres	Stichting ORO Baroniehof 165 5709 HL Helmond
Afstudeerperiode	8 februari 2016 – 13 mei 2016
Afstudeermentor	mevrouw drs. C.A. (Corine) Spaans
Eerste afstudeerdocent	mevrouw mr. L.C.P. (Lieke) van Berkel
Tweede afstudeerdocent	mevrouw mr. M.M. (Margo) Kok
Classificatie	Intern

Voorwoord

Voor u ligt mijn praktijkgericht, juridisch onderzoek met betrekking tot de Wet bescherming persoonsgegevens, Wet meldplicht datalekken en de aanstaande Europese Algemene Verordening Gegevensbescherming. Een uitdaging, omdat het privacyrecht slechts kort aangestipt is gedurende mijn opleiding en de geraadpleegde wetgeving grotendeels nieuw is. Dit afstudeeronderzoek is het sluitstuk van mijn opleiding HBO-Rechten aan de Juridische Hogeschool Avans-Fontys te 's-Hertogenbosch. Ik heb mijn afstudeerperiode als intens en uitdagend ervaren.

De verwerking van grote hoeveelheden persoonsgegevens is niet alleen maar een uitkomst in onze huidige samenleving. Ondanks dat door allerlei technische systemen razendsnel persoonsgegevens verwerkt en uitgewisseld kunnen worden, waardoor wij nog sneller en efficiënter kunnen werken, is er ook een keerzijde van de medaille. Er is onvoldoende bewustzijn binnen bedrijven en organisaties over al deze informatiestromen en gegevensuitwisselingen. De welbekende 'dossiers die op straat liggen', staan haast wekelijks in de krant. Ziekenhuizen, politiebureaus, de Belastingdienst en advocatenkantoren: iedereen lijkt met beveiligingsproblemen te kampen. Privacy van medewerkers en andere betrokkenen is een 'hot item'. Ik heb er met dit onderzoek naar gestreefd om ORO voldoende handvatten aan te reiken om zaken rondom privacy conform vigerende en aanstaande wet- en regelgeving te regelen binnen haar bedrijfsvoering.

Graag wil ik een aantal mensen bedanken. Op de eerste plaats wil ik graag mevrouw Spaans bedanken, beleidsadviseur bij ORO, voor haar begeleiding gedurende mijn stage, voor de feedback en input op mijn onderzoek en voor de algemene feedback gedurende mijn gehele stageperiode. Daarnaast bedank ik graag de heer Thijssen, Bestuurssecretaris/Manager Staf en tevens opdrachtgever namens ORO. Ook bedank ik graag mevrouw Van Berkel voor de begeleiding van mijn stage vanuit de Juridische Hogeschool en mevrouw Kok voor het vervullen van de rol als tweede afstudeerdocente. Ik wil mijn vader bedanken voor zijn feedback op de opbouw en structuur van mijn stukken en mijn moeder voor het redigeren van mijn teksten.

Tot slot rest het mij u veel plezier te wensen met het lezen van mijn scriptie 'Je mag alles van me weten, behalve …'[1].

Maartje Biemans
Helmond, mei 2016

[1] De titel is afgeleid van een tv-spotje uit de jaren negentig van de vorige eeuw omtrent de gevaren van het delen van je pincode. 'Je mag alles van me weten, behalve mijn pincode'.

Inhoudsopgave

Samenvatting

ORO is een organisatie die zorg en ondersteuning biedt aan mensen met een verstandelijke en/of lichamelijke beperking. De medewerkers van ORO staan iedere dag circa 1.700 cliënten bij. ORO wil de privacy van medewerkers en cliënten op een juiste manier borgen. De onlangs ingetreden Wet meldplicht datalekken (hierna te noemen: Wmd), onderdeel van de Wet bescherming persoonsgegevens (hierna te noemen: Wbp), en de aanstaande Europese Algemene Verordening Gegevensbescherming (hierna te noemen: AVG) zijn de aanleiding geweest om het huidige privacybeleid van ORO onder de loep te nemen. In overleg met ORO is de volgende centrale onderzoeksvraag geformuleerd: *'Welke maatregelen dient ORO door te voeren binnen haar huidige bedrijfsvoering, zodat bij de verwerking van persoonsgegevens in overeenstemming gehandeld wordt met de Wet bescherming persoonsgegevens, de nieuwe Wet meldplicht datalekken en de aanstaande Europese Algemene Verordening Gegevensbescherming?'.* De doelstelling van dit onderzoek is als volgt geformuleerd: *'Op uiterlijk maandag 30 mei 2016 wordt een adviesrapport overhandigd aan de manager Staf van ORO waarin aanbevelingen staan zodat de huidige bedrijfsvoering binnen ORO dusdanig aangepast kan worden, teneinde in overeenstemming te handelen met de Wet bescherming persoonsgegevens, de nieuwe Wet meldplicht datalekken en de aanstaande Europese Algemene Verordening Gegevensbescherming.'*

Het is ORO onduidelijk of zij voldoet aan de verplichtingen van de Wbp, Wmd en de AVG omtrent de rechtmatige verwerking van persoonsgegevens. Uit dit onderzoek blijkt dat ORO niet voldoet aan alle verplichtingen van de Wbp en Wmd. Niet alle persoonsgegevens hebben een rechtmatige verzamelingsgrond en verwerking van gegevens vindt niet transparant plaats. Het merendeel van de persoonsgegevens van medewerkers wordt langer bewaard dan wettelijke bewaartermijnen toestaan. Persoonsgegevens van cliënten worden nooit vernietigd. De rechten die betrokkenen in kunnen roepen jegens ORO zijn niet vastgelegd in een interne procedure en er is geen aangewezen persoon c.q. afdeling waar betrokkenen een verzoek in kunnen dienen om deze rechten jegens ORO uit te oefenen. Aan hetgeen de Wmd stelt, wordt niet voldaan door ORO, in concreto: er is geen persoon c.q. afdeling belast met de interne verwerking van de melding van een datalek of externe melding van een datalek aan de Autoriteit Persoonsgegevens of betrokkenen.

De Wbp en Wmd vervallen bij inwerkingtreding van de AVG. Verplichtingen uit de Wbp en Wmd worden overgeheveld naar de AVG. De AVG bevat ook nieuwe verplichtingen. Zo wordt het recht van correctie uitgebreid met het 'recht om te wissen'. Aangezien een procedure voor de rechten van betrokkenen reeds ontbreekt, mist dit recht ook. Voorts codificeert de AVG twee beginselen: Privacy by Default en Privacy by Design. Deze beginselen hebben betrekking op de levenscyclus van persoonsgegevens en dienen structureel geborgd te worden in de bedrijfsvoering. Deze borging ontbreekt in het huidige beleid van ORO. De AVG stelt het in dienst hebben van een Functionaris Gegevensbescherming (hierna te noemen: FG) verplicht, als van meer dan 250 betrokkenen gegevens worden verwerkt per kalenderjaar. ORO voldoet ruimschoots de norm, maar heeft geen FG in dienst. Ook stelt de AVG een Privacy Impact Assessment verplicht bij significante veranderingen in de verwerking van persoonsgegevens. ORO heeft hiervoor geen procedure. Tot slot verkort de AVG de meldplichttermijn van de Wmd (72 uur) naar 24 na constatering van een datalek. Deze procedure ontbreekt ook binnen ORO.

Aanbevolen wordt om de verwerkingen van persoonsgegevens inzichtelijk te documenteren en te toetsen op legitimatie. Voorts dienen procedures op voor de rechten van betrokkenen, de meldplicht datalekken en voor het Privacy Impact Assessment ingericht te worden. Als de AVG in werking treedt, dient de procedure voor de rechten van betrokkenen uitgebreid te worden met het 'recht om te wissen'. Ook de verkorte meldingstermijn voor datalekken dient in de procedure vervat te worden. Aanbevolen wordt om bij inwerkingtreding van de AVG een FG in dienst te hebben. Als ORO deze aanbevelingen implementeert, voldoet zij aan alle vigerende wetgeving op het gebied van nationale en Europese privacywetgeving.

Lijst van afkortingen

AP	Autoriteit Persoonsgegevens
AVG	Algemene Verordening Gegevensbescherming
BSN	Burgerservicenummer
BW	Burgerlijk Wetboek
CPO	Contactpersonenoverleg
EU	Europese Unie
e.v.	En volgende
EVRM	Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden
FG	Functionaris gegevensbescherming
Gw	Grondwet
HRS	Afdeling HRS-administratie, onderdeel afdeling HRM
IVBPR	Internationaal Verdrag inzake burgerrechten en politieke rechten
Jo.	Juncto
MvT	Memorie van Toelichting
Nr.	Nummer
ORO	Stichting ORO
PIA	Privacy Impact Assessment
PP	Persoonlijk plan
Privacyrichtlijn	Richtlijn 95/46/EG van het Europese Parlement en de Raad van 24 oktober 1995
RvB	Raad van Bestuur
RvT	Raad van Toezicht
SA	Salarisadministratie, onderdeel afdeling HRM
Sr	Wetboek van Strafrecht
Wbp	Wet bescherming persoonsgegevens
Wbsn-z	Wet gebruik burgerservicenummer in de zorg
Wft	Wet op het financieel toezicht
Wmd	Wet meldplicht datalekken
Wmo	Wet maatschappelijke ondersteuning
WOR	Wet op de ondernemingsraden

Verklarende woordenlijst

Bestand
In navolging van artikel 1 sub c Wbp wordt met ‘bestand’ bedoeld: ‘elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen’.

Betrokkene
In navolging van artikel 1 sub f Wbp: ‘Degene op wie een persoonsgegeven betrekking heeft’.

Bewerker
Degene wie of de instantie die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder hierbij aan zijn rechtstreekse gezag te zijn onderworpen.

Bijzondere persoonsgegevens
In navolging van artikel 16 Wbp wordt met ‘bijzondere persoonsgegevens’ bedoeld: ‘de verwerking van persoonsgegevens betreffende iemand godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele geaardheid, alsmede persoonsgegevens met betrekking tot het lidmaatschap van een vakvereniging, strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag’. De verwerking van deze persoonsgegevens is verboden tenzij hiervoor een expliciet wettelijke grondslag is.

Cliënten van ORO
Een cliënt van ORO is een persoon die zorg geniet, in de breedste zin van het woord, op basis van een zorgdienstverleningsovereenkomst tussen deze persoon of diens wettelijk vertegenwoordiger en ORO.

Datalek
Een datalek wordt omschreven als een inbreuk op de beveiliging in de zin van artikel 13 Wbp, waarbij:
- De verwerkte persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking, of;
- Redelijkerwijs niet uit te sluiten is dat er persoonsgegevens verloren zijn gegaan of onrechtmatig zijn verwerkt.

Inbreuk
Het in het geding zijn van de vertrouwelijkheid van gegevens, alsook het risico op verlies of onrechtmatige wijziging of vernietiging van gegevens.

Kaderwet
Een wet waarin algemene principes, verantwoordelijkheden en procedures staan, maar geen gedetailleerde gegevens opgenomen zijn.

Medewerker van ORO
Een medewerker van ORO is een persoon die actief is binnen ORO op basis van een arbeidsovereenkomst, een leer-arbeidsovereenkomst of een stageovereenkomst. Vrijwilligers die actief zijn binnen ORO vallen buiten de scope van dit onderzoek.

MijnORO
Het digitale personeelsdossier van de medewerkers van ORO.

Ontvanger
In navolging van artikel 1 sub h Wbp: ‘Degene wie of de instantie die ter uitvoering van haar taak bestanden ontvangt van de verantwoordelijke’. De taak van de ontvanger is een taak die ORO zelf niet kan vervullen.

Persoonsgegevens
In navolging van artikel 1 sub a Wbp: alle gegevens betreffende een geïdentificeerde of identificeerbare persoon. In dit onderzoek wordt met persoonsgegevens geduid op de persoonsgegevens van medewerkers en cliënten van ORO. Met persoonsgegevens wordt bedoeld alle niet-bijzondere persoonsgegevens.

Verantwoordelijke
De entiteit die formeel juridisch beslist welke persoonsgegevens worden verwerkt, met welk doel en op welke wijze. In het geval van ORO is de entiteit die dit beslist tevens de wettelijk vertegenwoordiger van de rechtspersoon, te weten: de Raad van Bestuur.

Verkrijging van persoonsgegevens
De verkrijging van persoonsgegevens bij de indiensttreding van medewerkers of gedurende tijdens hun dienstverband of bij het in zorg treden van een cliënt bij ORO dan wel gedurende de zorgdienstverleningsovereenkomst.

Verwerking persoonsgegevens
In navolging van artikel 1 sub b Wbp wordt in dit onderzoek verstaan onder de ‘verwerking van persoonsgegevens: ‘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’. Bij de verwerking van persoonsgegevens wordt gedoeld op niet-bijzondere persoonsgegevens. Wanneer er wordt gedoeld op bijzondere persoonsgegevens conform artikel 16 Wbp, wordt dit expliciet vermeld.

Hoofdstuk 1 Inleiding

In dit algemene hoofdstuk wordt allereerst het probleem van ORO beschreven. Vervolgens wordt de centrale vraag van dit onderzoek, die voortvloeit uit de probleembeschrijving, gesteld. De deelvragen waarmee de centrale vraag beantwoord wordt, worden daarna gegeven. Ook komt de doelstelling van dit onderzoek aan bod. Daaropvolgend worden de methoden en technieken van onderzoek uiteengezet en wordt ook de verantwoording geschetst. Tot slot bevat dit hoofdstuk een leeswijzer.

1.1 Probleembeschrijving

Binnen de nationale privacywetgeving hebben onlangs grote veranderingen plaatsgevonden. Op 1 januari 2016 trad de Wet meldplicht datalekken (hierna te noemen: Wmd) in werking en zijn de bevoegdheden van de Autoriteit Persoonsgegevens (hierna te noemen: AP) uitgebreid. Ondernemingen en instellingen moeten vanaf 1 januari 2016 datalekken in beginsel melden bij de AP. Het niet of niet correct melden van datalekken levert mogelijk forse boetes op. Om datalekken te voorkomen, moeten organisaties persoonsgegevens beveiligen en verwerken in overeenstemming met de Wet bescherming persoonsgegevens (hierna te noemen: Wbp). Beveiliging en (rechtmatige) verwerking van persoonsgegevens wordt door de Wmd structureel geborgd in de bedrijfsvoering.

De Wmd impliceert een ketenaansprakelijkheid. Veel ondernemingen hebben (een deel van hun) werkzaamheden uitbesteed. Bij uitbestedingen worden soms (persoons)gegevens uitgewisseld. Niet elke uitwisseling leidt tot ketenaansprakelijkheid. Om vast te stellen of sprake is van ketenaansprakelijkheid, moet bepaald worden of er uitbesteding is aan een bewerker of een ontvanger. Een ontvanger is een instantie die persoonsgegevens ontvangt voor de uitoefening van haar taak. De taak van deze instantie kan ORO zelf niet uitvoeren. In dat geval is er geen ketenaansprakelijkheid. Een bewerker is een instantie die ook persoonsgegevens ontvangt in de uitvoering van haar taak, maar dit is een taak die ORO zelf ook kan uitvoeren. Het is ORO onduidelijk welke partijen bewerkers en ontvangers zijn en het is tevens onduidelijk wie aansprakelijk is indien er gegevens gelekt worden. Het is ORO ook onduidelijk of ketenaansprakelijkheid ingeperkt dan wel uitgesloten kan worden.

De bevoegdheden van de AP uitgebreid per 1 januari 2016 en vinden grondslag in de Wbp. De uitbreiding heeft met name betrekking op uitbreiding van de sanctionerende bevoegdheden. De AP kan bindende aanwijzingen tot naleving van de Wbp geven aan ondernemingen en instellingen. In geval van een overtreding van de Wbp mag de AP in meer gevallen dan voorheen een bestuurlijke boete opleggen. Boetes kunnen oplopen tot € 810.000,- of 10% van de jaaromzet van een rechtspersoon.

Er is echter nog een verandering op komst. De datum van inwerkingtreding van de Europese Algemene Verordening Gegevensbescherming (hierna te noemen: AVG) is nog onbekend, maar na intreding vinden nog meer wijzigingen plaats binnen de privacywetgeving. De Wbp en Wmd vervallen na inwerkingtreding van de AVG. De verordening heeft vooral gevolgen voor de interne verantwoordelijkheden van ondernemingen. Zo worden ondernemingen verplicht om een privacybeleid te ontwikkelen, dit te integreren in de bedrijfsvoering en adequate beveiligingsmaatregelen te treffen zodat aantoonbaar aan de zorgplicht die de verordening stelt, wordt voldaan. De AVG stelt het in bepaalde gevallen verplicht een Functionaris Gegevensbescherming in dienst te nemen. Het niet voldoen aan de toekomstige wetgeving, kan eveneens forse boetes opleveren.

Concluderend wordt gesteld dat ORO wil weten wat de nieuwe wetgeving voor invloed heeft op haar werkwijzen en wat de nieuwe regels zijn die zij moet naleven met betrekking tot de Wbp, Wmd en de aanstaande AVG. Het is noodzakelijk een definiërend juridisch kader te stellen: wat wordt verstaan onder ‘persoonsgegevens’ en wat is ‘het lekken van datagegevens’? Vervolgens moet de omvang van het begrip ‘lekken van gegevens’ worden

vastgesteld. Behelst dit begrip zowel interne als externe lekken of is dit begrip enger? Om een reëel beeld te schetsen van de huidige situatie binnen ORO, dienen mogelijke risico's in kaart te worden gebracht. Voorts is het van belang dat indien er een lek is, het bekend is wie dat moet melden, hoe dat gemeld moet worden en binnen welke tijd er gemeld moet worden bij de AP. Het is daarnaast essentieel voor ORO om helder te hebben welke bewerkers en ontvangers zij kent en om te bepalen waar ORO risico loopt op ketenaansprakelijkheid. Kan de aansprakelijkheid gereguleerd en ingeperkt of wellicht uitgesloten worden? Tot slot wil ORO weten wat de gevolgen zijn van de aanstaande AVG met betrekking tot de verwerking van persoonsgegevens. Binnen ORO is onvoldoende kennis en capaciteit om dit onderwerp te analyseren en met instrumenten of implementatievoorstellen te komen voor deze kwestie.

1.2 Centrale vraag en deelvragen

De centrale vraag die in dit onderzoek beantwoord wordt, luidt: *'Welke maatregelen dient ORO door te voeren binnen haar huidige bedrijfsvoering, zodat bij de verwerking van persoonsgegevens in overeenstemming gehandeld wordt met de Wet bescherming persoonsgegevens, de nieuwe Wet meldplicht datalekken en de aanstaande Europese Algemene Verordening Gegevensbescherming?'*

Deelvragen waarmee een antwoord geformuleerd wordt op de hoofdvraag, zijn:

1. Welke voorwaarden stellen de Wet bescherming persoonsgegevens en de Wet meldplicht datalekken voor de rechtmatige verwerking van persoonsgegevens?
2. Wat zijn de wijzigingen binnen de Wet bescherming persoonsgegevens met betrekking tot de rechtmatige verwerking van persoonsgegevens na de invoering van de Wet meldplicht datalekken?
3. Wat houdt de aanstaande Europese Algemene Verordening Gegevensbescherming in voor de rechtmatige verwerking van persoonsgegevens?
4. Wat is de huidige situatie met betrekking tot de verwerking van persoonsgegevens binnen ORO?
5. In hoeverre wijkt het huidige beleid van ORO af van de Wet bescherming persoonsgegevens, de Wet meldplicht datalekken en de aanstaande Europese Algemene Verordening Gegevensbescherming?

1.3 Doelstelling

Op basis van voornoemde probleembeschrijving en de centrale vraag, is de volgende doelstelling geformuleerd: *'Op uiterlijk maandag 30 mei 2016 wordt een adviesrapport overhandigd aan de manager Staf van ORO waarin aanbevelingen staan zodat de huidige bedrijfsvoering binnen ORO dusdanig aangepast kan worden, teneinde in overeenstemming te handelen met de Wet bescherming persoonsgegevens, de nieuwe Wet meldplicht datalekken en de aanstaande Europese Algemene Verordening Gegevensbescherming.'*

1.4 Methoden van onderzoek en verantwoording

Bij het onderzoek binnen ORO is sprake van een enkelvoudige casestudy. In het onderzoek is gebruik gemaakt van verschillende onderzoeksmethoden. De beantwoording van de eerste, tweede en derde deelvraag ligt verankerd in de theorie rondom privacywetgeving. Hiervoor heeft een inhoudsanalyse plaatsgevonden. Bij een inhoudsanalyse wordt gebruik gemaakt van bestaand materiaal, waaronder de wet, verdragen en literatuur. De vierde deelvraag heeft betrekking op de huidige situatie binnen ORO. Om deze situatie inzichtelijk te krijgen, is kwalitatieve deskresearch uitgevoerd en daarnaast gebruik gemaakt van semigestructureerde interviews. De interviews zijn gehouden met informanten en respondenten. Als informanten worden beschouwd personen die informatie kunnen leveren over anderen of over situaties,

gebeurtenissen of processen die hij of zij kennen.[2] Informanten zijn, onder andere, wijk- en teammanagers en het bestuur. Respondenten zijn mensen die gegevens kunnen verschaffen over zichzelf en hun eigen ervaringen.[3] Hierbij wordt gedoeld op medewerkers, leerlingen en stagiaires die tijdens hun dagelijkse werkzaamheden te maken hebben met deze gebeurtenissen en processen. Tot slot wordt bij de beantwoording van deelvraag vijf een vergelijking gemaakt tussen de theorie en de praktijk. Deze laatste vraag vormt een toets aan het juridische kader dat opgesteld is bij de eerste drie deelvragen.

Er is gekozen voor de reeds benoemde bronnen en methoden van onderzoek, omdat daarmee effectief, efficiënt, betrouwbaar en valide onderzoek kan plaatsvinden. Rechtsbronnen die zijn geraadpleegd zijn voornamelijk afkomstig van de nationale, formele wetgever en van de wetgevende instanties van de Europese Unie. De geraadpleegde literatuur is geschreven door deskundigen, hoogleraren en/of professoren op het gebied van privacy(wetgeving). De geraadpleegde literatuur is geschreven op basis van feiten, rechtsregels en jurisprudentie. Deskresearch is met name effectief, omdat deze bronnen makkelijk toegankelijk zijn. Bij interne documenten moet gedacht worden aan gedragscodes en richtlijnen. Deze zijn opgesteld door (interne) deskundigen. Daarnaast zijn de interviews effectief, efficiënt en betrouwbaar. Aangezien zowel informanten als respondenten geïnterviewd zijn, is op deze manier vanuit meerdere standpunten antwoord gegeven op de gestelde vragen.

Door middel van triangulatie is de betrouwbaarheid van dit onderzoek geborgd. Door meerdere verschillende theorieën en bronnen te raadplegen, is vastgesteld of de bronnen in overeenstemming zijn met elkaar. Wanneer bronnen in overeenstemming zijn met elkaar, is de kans op mogelijke toevallige fouten beperkt en wordt derhalve de betrouwbaarheid van het onderzoek vergroot. De betrouwbaarheid van een onderzoek maakt het niet per definitie valide, maar betrouwbaarheid is wel een voorwaarde voor validiteit. Bij dit onderzoek is sprake van interne validiteit: het onderzoek met de daaruit voortvloeiende conclusies is gerechtvaardigd voor de situatie binnen ORO. Van externe validiteit is deels sprake: er is mogelijkheid om de uitkomsten van dit onderzoek te generaliseren binnen andere situaties of ondernemingen, maar slechts in beperkte mate. Aangezien het onderzoek specifiek verricht is binnen en voor ORO, kan alleen gegeneraliseerd worden als de situatie of onderneming in grote lijnen dezelfde huidige situatie heeft als de heersende situatie binnen ORO.

1.5 Verantwoording

Deze paragraaf stelt de algemene verantwoording. Indien bepaalde keuzes betrekking hebben op een enkel onderdeel in de tekst, zijn ze daar vermeld. De scope van dit onderzoek beperkt zich tot de cliënten en medewerkers van ORO. Vrijwilligers die actief zijn bij ORO, vallen buiten de scope van dit onderzoek. Voor deze afbakening is gekozen omdat het merendeel van de verwerkingen van persoonsgegevens betrekking heeft op cliënten en medewerkers. Daarnaast ligt aan verwerking van persoonsgegevens van vrijwilligers een andere administratieve procedure ten grondslag dan bij voornoemde groepen. Verwerking van foto's en videobeelden wordt in verband met verwikkeling met andere wet- en regelgeving en de minimale relevantie binnen ORO ook buiten beschouwing gelaten in dit onderzoek.

1.6 Leeswijzer

Hoofdstuk 2 stelt het relevante juridische kader voor dit onderzoek. Hoofdstuk 3 geeft de huidige situatie binnen ORO weer. In hoofdstuk 4 wordt vervolgens het geschetste juridische kader getoetst aan de huidige situatie binnen ORO. In hoofdstuk 5 volgen de conclusies en aanbevelingen die voortvloeien uit dit rapport. In dit hoofdstuk worden de hoofd- en deelvragen van dit rapport, zoals gesteld in §1.2, beantwoord.

[2] Van Schaaijk 2011, p. 85.
[3] Van Schaaijk 2011, p. 92.

Hoofdstuk 2 Juridisch kader

Dit hoofdstuk zet het juridisch kader van de Wet bescherming persoonsgegevens, de Wet meldplicht datalekken en de Algemene Verordening Gegevensbescherming uiteen. Wat zijn persoonsgegevens en wat wordt verstaan onder de verwerking hiervan? Ook wordt ingegaan op de wijzigingen die de onlangs geïmplementeerde Wet meldplicht datalekken teweeg bracht en welke wijzigingen zijn aanstaande met het oog op de Algemene Verordening Gegevensbescherming.

2.1 Wet bescherming persoonsgegevens

2.1.1 Achtergrondinformatie en reikwijdte

De Wet bescherming persoonsgegevens (hierna te noemen: Wbp) dateert uit 2001 en is de uitwerking van Europese richtlijn nr. 95/46/EG[4] uit 1995 (hierna te noemen: de Privacyrichtlijn). Het doel van de Privacyrichtlijn is dat de lidstaten van de Europese Unie (hierna te noemen: EU) bij de bescherming van de verwerking van persoonsgegevens dezelfde maatstaven hanteren.[5] Iedere lidstaat heeft op basis van deze richtlijn eigen privacywetgeving opgesteld, met als gevolg dat de wetgeving in de lidstaten niet volledig is geharmoniseerd.[6]

De Wbp is een kaderwet met ruime toepassing. Een kaderwet is een wet met algemene principes, verantwoordelijkheden en procedures en bevat dus geen gedetailleerde gegevens. Gevolg daarvan is dat de Wbp niet toegesneden is op bijvoorbeeld arbeids- of cliëntverhoudingen.[7] De Wbp bevat regels voor de (deels) geautomatiseerde verwerking van de gegevens. Voorheen werd daarmee de verwerking met behulp van een computer bedoeld: tegenwoordig valt daar de 'cloud' ook onder.[8] Bij de (deels) geautomatiseerde verwerking van persoonsgegevens worden gegevens opgenomen in een bestand of bestaat intentie hiertoe.[9]

2.1.2 Inkadering begrippen

De Wbp is van toepassing op persoonsgegevens. Persoonsgegevens zijn onderverdeeld in persoonsgegevens en bijzondere persoonsgegevens.

Begrip, betekenis	**Uitwerking**
Persoonsgegevens: Alle gegevens betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.	Voorbeelden van persoonsgegevens zijn NAW-gegevens, medische dossiers en foto's. De definitie spreekt over een geïdentificeerde of identificeerbare persoon. Als naasten een persoon herkennen aan de hand van de gegevens, is dat voldoende om te spreken van een geïdentificeerde of identificeerbare persoon.[10] In de Privacyrichtlijn is het begrip 'identificeerbare gegevens' uitgediept in 'direct' en 'indirect' identificeerbare gegevens.[11] Direct identificeerbare gegevens zijn gegevens die zo specifiek zijn dat ze direct herleiden naar één persoon, bijvoorbeeld het burgerservicenummer (hierna te noemen: BSN). Indirecte gegevens wijzen samen gecombineerd terug naar één persoon.

Wanneer in dit onderzoek gesproken wordt over persoonsgegevens, worden daarmee niet-bijzondere persoonsgegevens bedoeld. Wanneer gedoeld wordt op de bijzondere persoonsgegevens van artikel 16 Wbp, wordt dit expliciet vermeld.

[4] Richtlijn 95/46/EG van het Europese Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (Pb*EG* L281).
[5] De Vries en Rutgers 2001, p. 13.
[6] Richtlijn 95/46/EG (MvT).
[7] De Vries en Rutgers 2001, p. 17.
[8] Coöperatie Surf, *'Cloud computing: het juridisch kader'*, Van Elk en Van Elswijk 2015, p. 3.
[9] Artikel 2 lid 1 Wbp.
[10] Artikel 1 onder a Wbp.
[11] Artikel 2 onder a Richtlijn 95/46/EG.

Begrip	Betekenis
Bijzondere persoonsgegevens[12]	Gegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, seksuele geaardheid, alsook persoonsgegevens betreffende lidmaatschap van een vakvereniging, strafrechtelijke persoonsgegevens en gegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.

Met persoonsgegevens wordt geduid op de persoonsgegevens van de medewerkers en cliënten van ORO.

Begrip, betekenis	Opmerkingen
Medewerkers van ORO: De personen die binnen ORO werkzaam zijn op grond van een arbeidsovereenkomst voor bepaalde of onbepaalde tijd, een leer-arbeidsovereenkomst of een stageovereenkomst.	Persoonsgegevens van vrijwilligers die actief zijn binnen ORO vallen buiten de scope van dit onderzoek. Potentiële cliënten die na een vrijblijvend oriëntatiegesprek geen zorg af gaan nemen bij ORO, vallen eveneens buiten de scope van dit onderzoek.
Cliënten van ORO: De personen die binnen ORO zorg afnemen op grond van een zorgdienstverleningsovereenkomst.	Een zorgdienstverleningsovereenkomst is vergelijkbaar met een geneeskundige behandelingsovereenkomst. De zorgdienstverleningsovereenkomst is specifiek bedoeld voor cliënten met een beperking in de breedste zin van het woord.

De medewerkers en cliënten van ORO worden ook wel aangeduid als betrokkene(n).

Begrip, betekenis	Betekenis
Betrokkene	De persoon van wie persoonsgegevens worden verwerkt door de verantwoordelijke.

Zoals uit voorgaande definitie blijkt, worden gegevens verwerkt door een verantwoordelijke.

Begrip, betekenis	Uitwerking
Verantwoordelijke: degene die formeel juridisch de bevoegdheid heeft om doel en middelen van de verwerking van persoonsgegevens te bepalen.[13]	Met de formeel juridische bevoegdheid wordt gedoeld op de wettelijke vertegenwoordiging van de rechtspersoon. Bij ORO is dit de Raad van Bestuur (hierna te noemen: RvB). De RvB van ORO bestaat uit dhr. drs. J.G.J.H.-M. (Jan) Roelofs MBA.

Wanneer in dit onderzoek gesproken wordt over de verwerking van persoonsgegevens, wordt daarmee de wettelijke definitie gevolgd.[14]

Begrip	Betekenis
Verwerking van persoonsgegevens	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.

[12] Artikel 16 Wbp.
[13] Artikel 1 sub d Wbp.
[14] Artikel 1 sub b Wbp.

Het verzamelen van persoonsgegevens is de verkrijging daarvan.

Begrip	Betekenis
Verkrijging van persoonsgegevens medewerkers van ORO	Verkrijging van persoonsgegevens bij het aangaan of tijdens hun dienstverband door functioneringsgesprekken, gegevens rondom ziekte, zwangerschap, verhuizing, bevalling, relevante medische gegevens en scholing.
Verkrijging van persoonsgegevens cliënten van ORO	Verkrijging van persoonsgegevens bij het aangaan van een overeenkomst tot zorgverlening dan wel verkrijging van persoonsgegevens tijdens de uitvoering of ter uitvoering van die overeenkomst.

De uitwisseling van persoonsgegevens kan plaatsvinden tussen personen en tussen instanties. Bij het uitwisselen van gegevens wordt gesproken over uitwisseling van bestanden.

Begrip	Betekenis
Bestand	Elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen.[15]

Het uitwisselen van bestanden kan plaatsvinden met personen en organisaties. Deze uitwisseling wordt verdeeld in het uitwisselen van bestanden met ‘ontvangers’ en ‘bewerkers’.

Begrip, betekenis	Uitwerkingen
Bewerker: Een persoon of instantie die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreekse gezag te zijn onderworpen.[16]	Bewerkers voeren werkzaamheden uit in opdracht van ORO. Deze werkzaamheden zijn door ORO zelf uit te voeren, maar worden vanwege bepaalde redenen, zoals tijd, geld of capaciteit, uitbesteed. Een bewerker is bijvoorbeeld een accountant.
Ontvanger: Degene aan wie persoonsgegevens worden verstrekt ten behoeve van de uitoefening van haar taak.	In dit onderzoek is de wettelijke definitie van het begrip ‘ontvanger’ iets verruimd.[17] Het verschil met de rol van bewerker is dat een ontvanger bestanden ontvangt om een taak uit te oefenen die de verantwoordelijke zelf niet kan uitvoeren. Voorbeeld van een ontvanger is Brocacef. Zij levert medicatie voor de cliënten. ORO kan deze taak niet zelf vervullen.

2.1.3 Voorwaarden rechtmatige verwerking van persoonsgegevens

Om persoonsgegevens te verwerken, worden ze eerst verzameld. Dit mag wanneer aan ten minste één van onderstaande wettelijke voorwaarden van artikel 8 Wbp voldaan is.

- Betrokkene heeft toestemming gegeven voor de verzameling van persoonsgegevens;
- Verzameling is noodzakelijk ten behoeve van de uitvoering van een overeenkomst;
- Verzameling is noodzakelijk ter nakoming van een wettelijke verplichting;
- Verzameling is noodzakelijk ter vrijwaring van een vitaal belang;
- Verzameling is noodzakelijk ter uitvoering van een publiek belang;
- Verzameling is noodzakelijk voor de behartiging of het gerechtvaardigde belang van de verantwoordelijke of een derde aan wie gegevens worden verstrekt, tenzij fundamentele rechten van de betrokkene prevaleren.[18]

[15] Artikel 1 sub c Wbp.
[16] Artikel 1 sub e Wbp.
[17] Artikel 1 sub h Wbp.
[18] De wet noemt in artikel 8 sub f Wbp als voorbeeld van fundamentele rechten in het bijzonder ‘het recht op bescherming van de persoonlijke levenssfeer’ uit artikel 10 Gw, artikel 8 EVRM en artikel 17 IVBPR.

Uitleg van de redenen tot verzameling van persoonsgegevens en de hierbij horende wettelijke grondslagen zijn opgenomen in Bijlage 1. Voor de verzameling van persoonsgegevens is een uitdrukkelijk omschreven doel vereist.[19] Bij de verwerking van persoonsgegevens dienen een aantal eisen en beginselen in acht te worden genomen.[20] Deze zijn opgenomen in Bijlage 1.

De verwerking van bijzondere persoonsgegevens is gebonden aan striktere regelgeving.[21] Louter een reden tot verzameling van artikel 8 Wbp is onvoldoende: er moet een expliciete, wettelijke grondslag zijn en een bepaald doel, welke niet overschreden mag worden. De verboden die artikel 16 Wbp stelt met betrekking tot verwerking van bijzondere gegevens, worden in artikelen 17 tot en met 24 Wbp opgeheven, mits voldaan aan de voorwaarden die deze artikelen stellen. Zo staat in artikel 24 lid 1 Wbp dat een nummer ter identificatie van een persoon alleen verwerkt mag worden als een wettelijk doel dit expliciet voorschrijft. Een nummer ter identificatie dat van cliënten en medewerkers van ORO verwerkt wordt, is het BSN. Bij de gegevensverwerking van medewerkers mag het BSN gevraagd worden op grond van artikel 6a Wet op de Loonbelasting 1964. ORO is een zorgaanbieder en daarom geldt naast de Wbp nog een andere wet met betrekking tot het BSN: de Wet gebruik BSN in de zorg (hierna te noemen: Wbsn-z). Verwerking op grond van deze wet ziet toe op de verwerking van het BSN van cliënten. Het BSN van cliënten moet conform deze wet worden opgeslagen en gecontroleerd aan de hand van een geldig legitimatiebewijs.[22]

2.1.4 De rechten van betrokkenen

Betrokkenen hebben rechten met betrekking tot de verwerking van hun persoonsgegevens. Deze rechten kunnen zij inroepen tegenover de verantwoordelijke.

Recht	**Betekenis**	**Wettelijke grondslag**
Recht van inzage	Het recht van inzage biedt de betrokkene de mogelijkheid te controleren of en hoe gegevens worden verwerkt door de verantwoordelijke.	Artikel 35 Wbp
Recht van correctie	Wanneer tijdens inzage blijkt dat gegevens onjuist verwerkt of geregistreerd zijn, heeft een betrokkene het recht van correctie. Een verzoek tot correctie kan ingediend worden bij de verantwoordelijke.	Artikel 36 Wbp
Recht van verzet	Tegen bepaalde vormen van gegevensverwerking kan de betrokkene zich verzetten, als gevolg waarvan de gegevensverwerking wellicht gestaakt moet worden.	Artikel 40 en 41 Wbp

2.1.5 Voorwaarden bewaren en vernietigen van persoonsgegevens

Naast voornoemde eisen, geldt voor het bewaren en vernietigen van persoonsgegevens nog een aantal specifieke artikelen en termijnen. Deze zijn weergegeven in Bijlage 2.

2.1.6 Handhaving

Niet-naleving van de Wbp kan bestuursrechtelijk, strafrechtelijk en civielrechtelijk gehandhaafd worden.[23] De drie vormen sluiten elkaar niet uit: één overtreding kan drie keer beboet worden.

2.1.6.1 Bestuursrechtelijke handhaving

De Autoriteit Persoonsgegevens (hierna te noemen: AP) is een onafhankelijk orgaan[24] dat toezicht houdt op naleving van wetgeving met betrekking tot de verwerking van persoonsgegevens.[25] De AP kan ambtshalve onderzoek instellen naar gegevensverwerking

[19] Artikel 7 Wbp.
[20] Artikel 6 Wbp.
[21] Artikelen 17 tot en met 24 Wbp.
[22] Artikel 4 en 5 Wbsn-z.
[23] Autoriteit Persoonsgegevens, *Naslag Artikel 66,* www.autoriteitpersoonsgegevens.nl (zoek op *artikel 66*).
[24] Artikel 52 lid 2 Wbp.
[25] Artikel 51 Wbp.

binnen organisaties.[26] Onderzoek kan tevens geïnitieerd worden door een belanghebbende. De AP kan ook bestuursdwang toepassen.[27] De verantwoordelijke moet een overtreding van de Wbp in dat geval ongedaan maken op straffe van een dwangsom. Daarnaast kan de AP een bestuurlijke boete opleggen.[28] Door inwerkingtreding van de Wet meldplicht datalekken zijn de sanctiebevoegdheden van de AP verruimd, waarover meer in §2.3.

2.1.6.2 Strafrechtelijke handhaving
Overtreding van artikel 4 lid 3 of artikel 78 lid 2 Wbp is handhaafbaar met een geldboete van de derde categorie.[29] Is de overtreding opzettelijk, dan is de bestraffing maximaal zes maanden gevangenisstraf of een boete van de vierde categorie.[30] Deze artikelen zien toe op verwerkingen door verantwoordelijken gevestigd buiten de EU en doorgifte van gegevens buiten de EU. Uit naslagwerk van de AP blijkt dat strafrechtelijke vervolging nooit is ingezet.[31]

2.1.6.3 Civielrechtelijke handhaving
Een betrokkene wiens gegevens onrechtmatig verwerkt worden, kan zich wenden tot de civiele rechter en een procedure starten. Zo kan een onrechtmatige verwerking wellicht teruggedraaid of gestopt worden, dan wel een schadevergoeding gevorderd worden.

2.2 Wet meldplicht datalekken

2.2.1 Achtergrondinformatie en reikwijdte
De Wet meldplicht datalekken (hierna te noemen: Wmd) is ingetreden per 1 januari 2016 als onderdeel van de Wbp. De meldplicht houdt in dat zowel bedrijven als overheden onverwijld melding moeten doen bij de AP bij een ernstig datalek. In sommige gevallen dient het lek gemeld te worden aan de betrokkene(n).[32] Dat is bijvoorbeeld aan de orde als het lek de persoonlijke levenssfeer van de betrokkene(n) schaadt. De beveiliging en verwerking van persoonsgegevens wordt door invoering van de Wmd structureel geborgd in de bedrijfsvoering van organisaties. Met deze wetswijziging is uitvoering gegeven aan het regeerakkoord van kabinet-Rutte II ‘Bruggen slaan’ van 29 oktober 2012.[33] Met deze wetswijziging wordt beoogd dat naleving van de Wbp door overheden en bedrijven bevorderd wordt.[34] De Wmd loopt voor op de Algemene Verordening Gegevensbescherming (hierna te noemen: AVG), waarover meer in §2.4.

2.2.2 Inkadering begrippen
Aangezien de Wmd onderdeel is van de Wbp, komen de begrippen overeen met de begripsomschrijvingen van de Wbp (§2.1.2).

Artikel 34a Wbp behelst de meldplicht datalekken. Het artikel geeft geen definitie van een ‘datalek’, maar wijst terug naar artikel 13 Wbp. Dit artikel ziet toe op de ‘technische en organisatorische maatregelen die de verantwoordelijke op dient te leggen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking’. Bij het nemen van maatregelen moet een organisatie in overeenstemming handelen met de stand van de techniek, maar in combinatie met kosten van tenuitvoerlegging moet een passend doch haalbaar beveiligingsniveau nagestreefd worden. Maatregelen dienen erop gericht te zijn om onnodige verwerking van persoonsgegevens te voorkomen.

[26] Artikel 60 Wbp.
[27] Artikel 61 lid 4 Wbp jo. artikel 65 Wbp.
[28] Artikel 66 Wbp.
[29] Artikel 75 lid 1 Wbp jo. artikel 23 Sr.
[30] Artikel 75 lid 2 Wbp jo. artikel 23 Sr.
[31] Autoriteit Persoonsgegevens, *Naslag Artikel 66,* www.autoriteitpersoonsgegevens.nl (zoek op *artikel 66*).
[32] Kamerstukken II 2012/13, 33662, nr. 3, p. 1 (MvT).
[33] Kamerstukken II 2014/15, 33662, nr. 9, p. 4.
[34] Kamerstukken II 2014/15, 33662, nr. 9, p. 4.

Begrip	Uitwerking
Datalek Een inbreuk op de beveiliging van persoonsgegevens in de zin van artikel 13 Wbp, waarbij tevens: - De verwerkte persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking; of - Redelijkerwijs niet uit te sluiten is dat er persoonsgegevens verloren zijn gegaan of onrechtmatig zijn verwerkt.	Een datalek is altijd een beveiligingsincident: een beveiligingsincident niet altijd een datalek. Een beveiligingsincident is een lek door een zwakke plek in de beveiliging van een systeem.[35] Een datalek kan onopzettelijk of opzettelijk plaatsvinden. Bij opzettelijke datalekken worden beveiligingsmaatregelen bewust omzeild. Dat kan door een hacker, maar ook door een medewerker. Bij onopzettelijke datalekken wordt het lek niet doelbewust veroorzaakt. Volgens Ponemon Institute[36] waren in 2015 de oorzaken van datalekken te wijten aan 25% menselijk falen, 29% technisch falen en 46% moedwillig lekken.[37] De Wmd maakt geen onderscheid in opzettelijk of onopzettelijke inbreuken.

2.2.3 Melden datalek aan de Autoriteit Persoonsgegevens

Niet elk lek hoeft bij de AP gemeld te worden. Dat zou leiden tot immense belasting van de AP en tot enorme belasting bij de verantwoordelijke. De meldplicht is gebaseerd op een risicocriterium. Dat houdt in dat objectief gekeken wordt of het lek heeft geleid tot intreden van een aannemelijk gevolg.[38] Dat aannemelijk gevolg betekent dat verwerkte persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking, dan wel dat dat redelijkerwijs niet uitgesloten kan worden. Een datalek kan intern of extern zijn.[39]

2.2.3.1 Is de inbreuk een datalek?

Allereerst moet worden vastgesteld of een inbreuk een datalek is. De AP geeft hiervoor handvatten.[40] Om de leesbaarheid van dit rapport te borgen, zijn de stroomschema's opgenomen in de bijlagen. Het stroomschema van deze vraag is toegevoegd op Bijlage 3.

Is er een inbreuk op de beveiliging?

Artikel 12 Wbp e.v. stellen beveiligingseisen aan de verwerking van persoonsgegevens. Specifiek artikel 13 Wbp verplicht de verantwoordelijke om passende technische en organisatorische maatregelen ten uitvoer te leggen bij de verwerking van persoonsgegevens. De maatregelen van artikel 13 Wbp zijn op te delen in vijf categorieën.[41]

Maatregel	Toelichting
Preventieve maatregel	Maatregelen waarmee voorkomen wordt dat een dreiging leidt tot een beveiligingsincident
Detectieve maatregel	Maatregelen waarmee gedetecteerd wordt dat er een beveiligingsincident is of dreigt
Repressieve maatregel	Maatregelen waarmee de negatieve gevolgen van een beveiligingsincident worden beperkt
Herstelmaatregel	Maatregelen waarmee de negatieve gevolgen van een beveiligingsincident worden verholpen
Correctieve maatregel	Maatregelen waarmee de gebleken tekortkomingen van een beveiligingsincident worden hersteld

Zijn bij de inbreuk gegevens verloren gegaan?

Als bij een incident persoonsgegevens vernietigd of op een andere manier verloren zijn gegaan, is in beginsel sprake van verlies van gegevens. Als er een complete en actuele

[35] CBP-richtsnoeren: beveiliging van persoonsgegevens, p. 11.
[36] Ponemon Institute is een instituut dat onafhankelijk onderzoek doet naar privacy, bescherming van persoonsgegevens en informatiebeveiliging binnen circa 500 multinationals. Ponemon Institute, *About us*, www.ponemon.org.
[37] Hutter, Katus, Terstegge en Vermissen 2015, p. 21.
[38] Kamerstukken II 2012/13, 33662, nr. 3, p. 5 (MvT).
[39] Hutter, Katus, Terstegge en Vermissen 2015, p. 18.
[40] Autoriteit Persoonsgegevens, 'Beleidsregels voor toepassing van artikel 34a Wbp', p. 19.
[41] Autoriteit Persoonsgegevens, 'Beleidsregels voor toepassing van artikel 34a Wbp', p. 19.

reservekopie van de gegevens is, is er geen sprake van verlies. De Memorie van Toelichting (hierna te noemen: MvT) stelt dat geen sprake is van een datalek indien persoonsgegevens verloren zijn gegaan als gevolg van een calamiteit en geen actuele kopie beschikbaar is[42], maar de AP weerlegt dit standpunt[43] en stelt melding in een dergelijke situatie verplicht.

Kan redelijkerwijs worden uitgesloten dat persoonsgegevens onrechtmatig zijn verwerkt?
Onder 'onrechtmatige verwerking' vallen de aantasting, onbevoegde kennisname of wijziging en de verstrekking van persoonsgegevens.[44] Kan onrechtmatige verwerking redelijkerwijs niet uitgesloten worden, is de inbreuk een datalek. De AP geeft handvatten (Bijlage 4).[45]

2.2.3.2 Dient het datalek gemeld te worden aan de AP?
De vragen van het stappenplan van Bijlage 4 worden hieronder toegelicht.

Is sprake van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens?
Een datalek hoeft alleen gemeld te worden als deze leidt tot (een aanzienlijke kans) op ernstige gevolgen voor de bescherming van persoonsgegevens.[46] Dit wordt een geclausuleerde meldplicht genoemd. De verantwoordelijke dient per lek zelf te bepalen of sprake is van een aanzienlijke kans op dan wel een ernstig nadelig gevolg voor de bescherming van persoonsgegevens. Ook hiervoor is een schema opgesteld (Bijlage 5).[47]

2.2.3.3 Leidt het lek tot een (aanzienlijke kans op) nadelig gevolg voor de bescherming van persoonsgegevens?
De vragen van het stappenplan van Bijlage 5 worden hieronder toegelicht.

Zijn er gegevens van gevoelige aard gelekt?
Het is van belang vast te stellen wat de aard van de gelekte gegevens is. Gevoelige gegevens leiden bij verlies of onrechtmatige verwerking mogelijk tot uitsluiting of stigmatisering van de betrokkene, tot schade aan de gezondheid, financiële schade of tot (identiteits-)fraude.[48]

Bij persoonsgegevens van gevoelige aard moet in ieder geval gedacht worden aan[49]:
- bijzondere persoonsgegevens ex artikel 16 Wbp;
- gegevens over de financiële of economische situatie van betrokkene, onder andere, maar niet enkel, gegevens over schulden, salarisbetalingen en betalingsgegevens;
- andere gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene, zoals gegevens over verslavingen, prestaties binnen school- of werksfeer en problemen in de privésfeer van betrokkene;
- gebruikersnamen, wachtwoorden of andere inloggegevens;
- gegevens die misbruikt kunnen worden voor (identiteits)fraude, zoals biometrische gegevens (vingerafdrukken en irisscans), kopieën van legitimatiebewijzen of BSN;
- gegevens die onder een beroepsgeheim[50] vallen, zoals het medisch beroepsgeheim.

Wanneer sprake is van een lek waarbij (mogelijk) gegevens van gevoelige aard zijn gelekt, dient onverwijld melding gedaan te worden aan de AP. Wanneer geen gevoelige gegevens zijn gelekt, kan melding alsnog vereist zijn.

[42] Kamerstukken II 2012/13 33 662, nr. 3, p. 5 en 6 (MvT).
[43] Autoriteit Persoonsgegevens, 'Beleidsregels voor toepassing van artikel 34a Wbp', p. 21.
[44] Kamerstukken II 2014/15, 33 662, nr. 11, p. 5.
[45] Autoriteit Persoonsgegevens, 'Beleidsregels voor toepassing van artikel 34a Wbp', p. 23.
[46] Artikel 34a lid 1 Wbp.
[47] Autoriteit Persoonsgegevens, 'Beleidsregels voor toepassing van artikel 34a Wbp', p. 24.
[48] Kamerstukken II 2013/14, 33 662, nr. 6, p. 19 en Kamerstukken II 2014/15, 33 662, nr. 11, p. 5.
[49] Autoriteit Persoonsgegevens, 'Beleidsregels voor toepassing van artikel 34a Wbp', p. 26 en 27.
[50] Artikel 9 lid 4 Wbp.

Leiden aard en omvang van de inbreuk tot (een aanzienlijke kans op) ernstig nadelige gevolgen voor de betrokkene(n)?
Aard en omvang van het lek zijn mede bepalend gevolgen van het lek.[51] Een lek kan grote gevolgen hebben voor de betrokkene(n), ondanks dat er geen gevoelige gegevens gelekt zijn. Onderstaande punten dienen in overweging genomen te worden door de verantwoordelijke:

- Omvang van de groep personen waarvan gegevens gelekt zijn;
- Hoe ingrijpend zijn de beslissingen die de verantwoordelijke normaliter maakt op basis van de gegevens;[52]
- De keten waarin de gegevens verstrekt zijn. Hoe groter de keten, hoe meer kans dat een betrokkene langer last ondervindt van het lek.

Wanneer sprake is van een grote groep betrokkenen, is sprake van (een aanzienlijke kans op) ernstig nadelige gevolgen. De heer A.G. (Gerard) Schouw, destijds D66-lid van de Tweede Kamer, heeft ten tijde van de besluitvorming rondom de Wmd aandacht gevraagd voor kwetsbare groepen.[53] Als deze vragen beantwoord worden omtrent een groep kwetsbare personen, is eerder sprake van (een aanzienlijke kans op) ernstig nadelige gevolgen. Op 12 april 2016 werd bekend dat door een blunder van de gemeente Amersfoort van circa 1.500 inwoners die (jeugd)zorg krijgen, NAW-gegevens gelekt zijn.[54] NAW-gegevens zijn geen gevoelige gegevens volgens voorgaande definitie, maar de groep personen is groot en uit de verklaring van de gemeente is af te leiden dat deze 1.500 inwoners zorgbehoevend en kwetsbaar zijn. In dergelijke gevallen zijn er naar waarschijnlijkheid (een aanzienlijke kans op) ernstige gevolgen voor de betrokkenen.

De AP geeft in haar beleidsregels, naar aanleiding van en gebaseerd op de MvT, een aantal voorbeelden van datalekken die wel en niet gemeld moeten worden. [55]

Wel melden bij de AP	**Niet melden bij de AP**
Door een technische storing zijn medische gegevens ingezien door onbevoegden	Een brief wordt verzonden naar het verkeerde adres, maar wordt ongeopend retour gezonden
Een medewerker verliest een laptop met daarop onversleutelde, financiële gegevens van klanten, medewerkers of cliënten	Een deugdelijk versleutelde laptop met persoonsgegevens blijft achter in de trein, Via 'gevonden voorwerpen' komt de laptop ongeopend terug bij de rechtmatige eigenaar
Een bedrijf krijgt te maken met een hack waarbij wachtwoorden zijn ontvreemd	
Een tablet wordt gestolen uit de auto van een medewerker	

2.2.3.4 Melding aan de Autoriteit Persoonsgegevens
Wanneer uit het voorgaande blijkt dat sprake is van een datalek dat gemeld moet worden bij de AP, dient dit onverwijld na constatering van het lek te geschieden.[56] Melding wordt gedaan door de verantwoordelijke en kan schriftelijk of digitaal.[57] De verantwoordelijke ontvangt per omgaande een ontvangstbevestiging van de melding.[58] De AP hanteert voor de onverwijlde melding een termijn van 72 uur na constatering van het lek.[59] Mocht het incident niet binnen die termijn gemeld kunnen worden, wordt dat zo spoedig mogelijk na verloop van die termijn

[51] Kamerstukken II 2012/13 33 662, nr. 3, p. 7 (MvT).
[52] De 'Beleidsregels voor toepassing van artikel 34a Wbp' noemt op pagina 26 als voorbeeld gegevens voor marketingdoeleinden en de gegevens waarom iemands kredietwaardigheid wordt gebaseerd. De laatste gegevens zijn ingrijpender dan de gegevens die gebruikt worden voor marketingdoeleinden.
[53] Handelingen II 2014/15, nr. 51, item 9, p. 1.
[54] Gemeente Amersfoort lekt zorggegevens 12 april 2016, *Algemeen Dagblad*, www.ad.nl (zoek op: *gegevenslek*).
[55] Autoriteit Persoonsgegevens, 'Beleidsregels voor toepassing van artikel 34a Wbp', p. 25 t/m 28.
[56] Artikel 34a lid 1 Wbp.
[57] Autoriteit Persoonsgegevens, 'Meldloket Datalekken', www.autoriteitpersoonsgegevens.nl (zoek op *melding*).
[58] Autoriteit Persoonsgegevens, 'Beleidsregels voor toepassing van artikel 34a Wbp', p. 30.
[59] Autoriteit Persoonsgegevens, 'Beleidsregels voor toepassing van artikel 34a Wbp', p. 31, gebaseerd op Kamerstukken II 2013/14, 33 662, nr. 6, p. 16.

gedaan. De verantwoordelijke is dan verplicht zijn melding te motiveren.[60] Melding kan door de verantwoordelijke aangevuld en ingetrokken worden. Een aanvulling kan betrekking hebben op informatie over het lek dat na de melding bekend geworden is. Intrekken van een melding kan bijvoorbeeld indien na melding blijkt dat het lek geen datalek is.

2.2.4 Melden van een datalek aan de betrokkene(n)

Een datalek dat gemeld moet worden aan de AP, behoeft niet per definitie aan de betrokkene(n) gemeld te worden. De verantwoordelijke maakt bij een lek zelf de afweging om een lek al te melden aan de betrokkene(n). De AP geeft hiervoor handvatten (Bijlage 6).[61] De vragen van het stappenplan van Bijlage 6 worden hieronder toegelicht.

Ben ik een financiële onderneming als bedoeld in de Wet op het financieel toezicht?

Voor een financiële onderneming ex artikel 1:1 Wft geldt een uitzondering op de meldplicht.[62] Artikel 1:1 Wft geeft een negental financiële ondernemingen weer: ORO valt hier niet onder. Dit houdt in dat de eerste vraag van dit stappenplan negatief beantwoord moet worden en daarmee ook dat deze uitzonderingsgrond niet van toepassing is voor ORO. Het stappenplan dient verder gevolgd te worden.

Biedt de toegepaste cryptografie voldoende bescherming?

Als voldaan is aan de technische beschermingsmaatregelen, zijn de gelekte gegevens niet toegankelijk voor onbevoegden. De betrokkene hoeft dan niet op de hoogte gesteld te worden van het lek.[63] In de MvT[64] alsook de CBP Richtsnoeren: beveiliging persoonsgegevens[65] wordt als voorbeeld van technische maatregelen cryptografie genoemd. Cryptografie is 'de kunst van beveiliging met behulp van informatie'[66] en is een verzamelnaam voor mogelijke wijzen van versleuteling. Twee cryptografische bewerkingen waar de CBP Richtsnoeren op ingaat zijn encryptie (versleuteling van gegevens) en hashing (omzetten van gegevens in een unieke code).[67] Deze wijzen van informatiebeveiliging vloeien voort uit een NEN-normering.[68] Deze normering is algemeen. Voor de zorgsector is er ook een specifieke NEN-normering opgesteld met betrekking tot informatiebeveiliging: de NEN-7510. Daarnaast ziet de NEN-7512 toe op informatiebeveiliging met betrekking tot de uitwisseling van persoonsgegevens in de zorg.

Wanneer bovenstaande bewerkingen juist worden toegepast, kan een onbevoegde het systeem niet ontsleutelen. Een lek hoeft dan niet gemeld te worden aan de betrokkene(n). Wanneer de adequaatheid van deze maatregelen discutabel is, moet het lek gemeld worden aan de betrokkene(n). Deze afweging wordt door de verantwoordelijke gemaakt: de AP geeft opnieuw een stappenplan (Bijlage 7).[69] Voordat verder gegaan wordt met het stappenplan op Bijlage 6, is het van belang dat het stappenplan op Bijlage 7 doorlopen wordt.

Zijn de persoonsgegevens blootgesteld aan vernietiging of aantasting?

Ondanks dat persoonsgegevens adequaat versleuteld zijn volgens technische beveiligingsmaatregelen, kunnen deze bij een lek worden vernietigd. De AP benoemt mogelijkheden tot aantasting of onbevoegde wijziging door zogenaamde 'cryptoware'.[70] Bij cryptoware worden reeds versleutelde gegevens nogmaals versleuteld door bijvoorbeeld hackers. De tweede sleutel kan de verantwoordelijke alleen tegen betaling verkrijgen. Wanneer sprake is van onbevoegde kennisname, verlies of een andere vorm van

[60] Autoriteit Persoonsgegevens, 'Beleidsregels voor toepassing van artikel 34a Wbp', p. 31.
[61] Autoriteit Persoonsgegevens, 'Beleidsregels voor toepassing van artikel 34a Wbp', p. 32.
[62] Artikel 34a lid 10 Wbp.
[63] Artikel 34a lid 6 Wbp.
[64] Kamerstukken II 2012/13 33 662, nr. 3, p. 20 (MvT).
[65] CBP Richtsnoeren: beveiliging persoonsgegevens, p. 12.
[66] Tel 2006, p. 8.
[67] CBP Richtsnoeren: beveiliging persoonsgegevens, p. 12.
[68] De algemene NEN-normering voor Informatietechnologieën, Beveiligingstechnieken en Managementsystemen voor informatiebeveiliging is de NEN-ISO/IEC 27001+C11:2014+C1:2014+C2:2015.
[69] Autoriteit Persoonsgegevens, 'Beleidsregels voor toepassing van artikel 34a Wbp', p. 34.
[70] Autoriteit Persoonsgegevens, 'Beleidsregels voor toepassing van artikel 34a Wbp', p. 35.

onrechtmatige verwerking, heeft dit mogelijk ongunstige gevolgen voor de persoonlijke levenssfeer en er dient daarom melding gedaan te worden aan de betrokkene(n).

Waren alle persoonsgegevens versleuteld op het moment dat de inbreuk plaatsvond?
Versleutelde gegevens zijn alleen beschermd tegen een inbreuk als ze op het moment van het lek versleuteld zijn. Wanneer een datalek plaatsvindt en gegevens niet versleuteld zijn, kan dit ongunstige gevolgen hebben voor de betrokkene(n). Melding aan betrokkene(n) is dan vereist.

Is de versleuteling adequaat?
De verantwoordelijke beoordeelt of de versleuteling adequaat is.[71] Aangezien cryptografie voortdurend blijft ontwikkelen, is de cryptografische beveiliging van gegevens mogelijk niet meer toereikend. Het is belangrijk om de cryptografie regelmatig te beoordelen en vast te stellen of deze nog voldoende bescherming biedt.

De AP verwijst in haar beleidsregels[72] naar Europese Verordening 611/2013[73]. Deze Verordening geeft invulling aan het begrip 'adequate versleuteling'. Gegevens zijn adequaat versleuteld als:

- Ze zijn versleuteld met een standaardalgoritme, de sleutel voor decryptie door geen enkele inbreuk gevaar heeft gelopen en zodanig gegenereerd is dat onbevoegden de sleutel met de beschikbare technologische middelen niet kunnen vinden[74], of;
- Ze zijn vervangen door een met een cryptografisch versleutelde hashfunctie berekende hashwaarde, de sleutel die daarvoor is gebruikt door geen enkele inbreuk gevaar heeft gelopen en dat deze voor datahashing gebruikte sleutel zodanig is gegenereerd onbevoegden de sleutel niet kunnen vinden met de beschikbare technologische middelen.[75]

Aandachtspunten bij de beoordeling van een adequate versleuteling zijn[76]:

- Het algoritme of de wijze waarop dit is toegepast. Het kan kwetsbaarheden vertonen waardoor encryptie of hashing niet de verwachte bescherming biedt;
- Encryptie is omkeerbaar en een onbevoegde die over de juiste sleutel beschikt, of deze zonder te veel moeite kan vinden, kan de gelekte gegevens ontsleutelen;
- Hashing is herhaalbaar. Wanneer bij hashing geen salt[77] is toegepast, of als een onbevoegde over de gebruikte salt beschikt of deze zonder te veel moeite kan vinden, kan hij de gebruikte hashingmethode toepassen op een lijst met veelgebruikte waarden en daardoor bijvoorbeeld wachtwoorden achterhalen.

Is het restrisico acceptabel?
Uit beantwoording van voorgaande vragen komt een duidelijk beeld naar voren van het beveiligingsniveau van de gelekte gegevens. Afhankelijk hiervan wordt het restrisico vastgesteld. Is het risico dat door het lek nadelige gevolgen optreden voor de betrokkene(n) significant? Of is de kans nihil dat de betrokkene(n) hinder (gaan) ondervinden van het lek? Deze afweging dient per lek gemaakt te worden door de verantwoordelijke.

Als voorgaande vragen beantwoord zijn, wordt doorgegaan met het schema van Bijlage 6.

[71] Kamerstukken II 2013/14, 33 662, nr. 6, p. 31 en 32.
[72] Autoriteit Persoonsgegevens, 'Beleidsregels voor toepassing van artikel 34a Wbp', p. 36.
[73] Verordening (EU) Nr. 611/2013 van de Commissie van 24 juni 2013 betreffende maatregelen voor het melden van inbreuken in verband met persoonsgegevens op grond van Richtlijn 2002/58/EG van het Europese Parlement en de Raad betreffende privacy en elektronische communicatie.
[74] Artikel 4 lid 2 sub a Verordening 611/2013.
[75] Artikel 4 lid 2 sub b Verordening 611/2013.
[76] Autoriteit Persoonsgegevens, 'Beleidsregels voor toepassing van artikel 34a Wbp', p. 37.
[77] Een 'salt' is extra informatie die bij hashing wordt toegevoegd aan de oorspronkelijke gegevens om het kraken of hacken van de hashcode te bemoeilijken.

Bieden de andere toegepaste technische beschermingsmaatregelen voldoende bescherming om de melding aan de betrokkene achterwege te laten?
Een andere beveiligingsmaatregel 'remote wiping'.[78] Remote wiping is het op afstand wissen van gegevens op een gegevensdrager. Het wissen van deze gegevens maakt ze ontoegankelijk. De AP stelt randvoorwaarden voor een geslaagde remote wipe[79]:

- De remote wipe dient tijdig in gang te worden gezet, zodat een eventuele aanvaller geen kans heeft gehad om kennis te nemen van de gelekte gegevens;
- Het apparaat waarop de wipe is uitgevoerd dient intact te zijn en correct te werken;
- De toepassing die gebruikt wordt om de wipe uit te voeren, dient correct te werken.

Bij remote wiping, dienen de specifieke omstandigheden van het geval afgewogen te worden in combinatie met voornoemde randvoorwaarden om vast te stellen of sprake is van een geslaagde remote wipe. Bij een geslaagde wipe is melding aan de betrokkene(n) niet vereist.[80] Een andere beveiligingsmaatregel is het pseudonimiseren en anonimiseren van gegevens. Deze maatregel houdt in dat persoonsgegevens niet direct gekoppeld kunnen worden aan de identiteit van een persoon. Wanneer gegevens dusdanig gepseudonimiseerd of geanonimiseerd zijn dat onbevoegden de gegevens niet kunnen lezen of begrijpen, is er sprake van geslaagd pseudonimiseren of anonimiseren. Melding aan betrokkene(n) is dan niet vereist.[81] Voor het pseudonimiseren en anonimiseren van gegevens is door de Europese Toezichthouders advies uitgebracht.[82] Wanneer organisaties gegevens pseudonimeseren of anonimiseren, kan dit advies gebruikt worden als richtlijn.

Heeft het datalek (waarschijnlijk) ongunstige gevolgen voor de persoonlijke levenssfeer van betrokkene(n)?
Als een datalek (waarschijnlijk) ongunstige gevolgen heeft voor de persoonlijke levenssfeer van betrokkene(n), dient het lek gemeld te worden aan de betrokkene(n).[83] Betrokkenen kunnen door verlies, onrechtmatig gebruik of misbruik van persoonsgegevens in hun belangen worden geschaad. Dit schaden kan in materiële en immateriële zin. Immateriële schade omvat onrechtmatige publicatie, discriminatie of aantasting in eer en goede naam.[84]

De verantwoordelijke beslist per datalek of melding gedaan wordt aan de betrokkene(n). Indien sprake is van een lek met gevoelige persoonsgegevens, is melding aan de betrokkene(n) vereist. 'Gevoelige persoonsgegevens' is in dezen hetzelfde als het begrip van Bijlage 6.

2.2.4.1 Zwaarwegende belangen
Op grond van artikel 43 Wbp mag melding aan de betrokkene(n) achterwege gelaten worden wanneer dit noodzakelijk is op grond van de in dit artikel genoemde, zwaarwegende belangen.

2.2.4.2 Melding aan de betrokkene(n)
Wanneer melding aan de betrokkene(n) vereist is, gebeurt dit onverwijld.[85] De melding behelst in ieder geval de aard van de inbreuk, de instanties waar de betrokkene meer informatie kan krijgen over het lek en de maatregelen die de verantwoordelijke de betrokkene aanbeveelt om negatieve gevolgen van de inbreuk te beperken.[86] Het schrijven vermeldt ook de contactgegevens van de verantwoordelijke. De verantwoordelijke mag meer informatie toevoegen aan de kennisgeving: dit is niet verplicht.[87] Artikel 34a lid 5 Wbp stelt dat kennisgeving aan de betrokkene, gelet op de aard van de inbreuk, de geconstateerde (en feitelijke) gevolgen van de inbreuk voor de verwerking van persoonsgegevens, de kring van

[78] Kamerstukken II 2013/14, 33 662, nr. 7, p. 6.
[79] Autoriteit Persoonsgegevens, 'Beleidsregels voor toepassing van artikel 34a Wbp', p. 38.
[80] Artikel 34a lid 6 Wbp.
[81] Artikel 34a lid 6 Wbp.
[82] Groep Gegevensbescherming artikel 29, 'Advies 5/2014 over anonimiseringstechnieken'.
[83] Artikel 34a lid 2 Wbp.
[84] Kamerstukken II 2013/14, 33 662, nr. 6, p. 19.
[85] Artikel 34a lid 2 Wbp.
[86] Artikel 34a lid 3 Wbp.
[87] Kamerstukken II, 2012/13, 33 662, nr. 3, p. 21 en 22 (MvT).

betrokkenen en de kosten van tenuitvoerlegging, op een behoorlijke en zorgvuldige wijze geschiedt. Het melden van een datalek aan de betrokkene(n) is informatief. De betrokkene kan hierop eventueel zelf de verantwoordelijke aansprakelijk stellen om schade te verhalen.[88]

2.2.5 Registratie datalekken

Iedere verantwoordelijke dient een register bij te houden van de meldplichtincidenten. Per lek bevat het register in ieder geval de feiten en gegevens omtrent de aard van het lek. Als het lek gemeld is aan de betrokkene(n), dient hiervan de kennisgeving bewaard te worden in het register.[89] De wet geeft geen bewaartermijn voor het register. De AP adviseert het register minimaal één jaar te bewaren[90], maar geeft aan dat er gevallen zijn waarbij het register langer bewaard moet worden. Voor deze gevallen geeft de AP een beslismodel (Bijlage 8).[91]

2.2.5.1 Bewaartermijn melding

De AP gaat ervan uit dat gegevens worden bewaard in het register om lering te trekken uit het datalek en de wijze waarop het afgehandeld is en antwoord te kunnen geven op vragen van betrokkenen. Gegevens worden tevens bewaard om te verstrekken aan betrokkenen indien dit niet is gebeurd en omstandigheden dit achteraf alsnog vereisen.[92] Wanneer een datalek leidt tot een juridische procedure, kan het register een bewijsstuk zijn en een opgenomen logboek kan de keuzes die gemaakt zijn ten tijde van het lek weerspiegelen.

2.2.6 Gevolgen (onrechtmatig nalaten) melding datalek

Na het melden van een datalek aan de AP, krijgt de verantwoordelijke per omgaande een ontvangstbevestiging.[93] De AP verifieert of het gemelde lek daadwerkelijk afkomstig is van de verantwoordelijke en stelt mogelijk inhoudelijke vragen over het lek. De AP houdt intern een register bij van de gemelde datalekken. Dit register is niet openbaar.

Het is aan de verantwoordelijke om de oorzaak van het lek op te sporen en hiertegen maatregelen te treffen: ook om herhaling te voorkomen. De AP biedt als toezichthouder geen ondersteuning bij de afhandeling van een datalek. De AP kan op grond van ontvangen meldingen wel adequate beveiligingsmaatregelen vorderen bij organisaties. Als uit ontvangen meldingen blijkt dat de beveiliging van de persoonsgegevens niet voldoet aan de normen van de Wbp, kan de AP een onderzoek starten naar het naleven van de normen uit de Wbp[94] en eventueel een sanctie opleggen, waarover meer in §2.2.7.

Het onrechtmatig nalaten van melding van een datalek aan de AP of de betrokkene(n) blijft niet zonder gevolgen. Onrechtmatig nalaten van een melding aan de AP kan gesanctioneerd worden, waarover meer in §2.2.7 Handhaving. Bij het onrechtmatig nalaten van melden aan betrokkenen, kan de AP van de verantwoordelijke eisen dat deze alsnog kennisgeving doet aan de betrokkene(n).[95] Dit staat gelijk met een bindende aanwijzing.[96] Niet nakomen van deze eis kan eveneens bestraft worden, waarover meer in §2.2.7.

2.2.7 Handhaving

Tegen een overtreding van de meldplicht kan de AP op verschillende manieren optreden. In beginsel legt zij een bindende aanwijzing op, alvorens zij een bestuurlijke boete geeft.[97] De AP kan de overtreder een termijn stellen waarbinnen de aanwijzing moet worden opgevolgd. Bij niet nakoming van de bindende aanwijzing kan de AP een bestuurlijke boete opleggen van ten hoogste € 810.000,-. Wanneer de AP dat bedrag onvoldoende passend vindt, kan zij de boete

[88] Artikel 49 Wbp.
[89] Artikel 34a lid 8 Wbp.
[90] Autoriteit Persoonsgegevens, 'Beleidsregels voor toepassing van artikel 34a Wbp', p. 46.
[91] Autoriteit Persoonsgegevens, 'Beleidsregels voor toepassing van artikel 34a Wbp', p. 46.
[92] Autoriteit Persoonsgegevens, 'Beleidsregels voor toepassing van artikel 34a Wbp', p. 47.
[93] Autoriteit Persoonsgegevens, 'Beleidsregels voor toepassing van artikel 34a Wbp', p. 48.
[94] Artikel 60 Wbp.
[95] Artikel 34a lid 7 Wbp.
[96] Kamerstukken I 2014/15, 33 662, nr. C, p. 23.
[97] Artikel 66 lid 3 Wbp.

ophogen tot maximaal 10% van de jaaromzet van de rechtspersoon. Bij het opleggen van een bestuurlijke boete houdt de AP rekening met de omstandigheden van het specifieke geval.[98] Wanneer een overtreding opzettelijk is gepleegd of sprake is van ernstig verwijtbare nalatigheid, kan de AP direct een bestuurlijke boete opleggen.[99] Wanneer vaker sprake is geweest van eenzelfde overtreding, wordt nalatigheid sneller aangenomen.[100]

2.3 Wijzigingen Wet bescherming persoonsgegevens ten aanzien van de invoering Wet meldplicht datalekken

2.3.1 Uitbreiding sanctionerende bevoegdheden Autoriteit Persoonsgegevens

Met inwerkingtreding van de Wmd heeft de AP de bevoegdheid gekregen om vaker en hogere bestuurlijke boetes op te leggen bij overtredingen van de Wbp. Voor inwerkingtreding kon de AP alleen bij overtreding van een administratieve verplichting een boete opleggen. Deze boete was ten hoogste € 4.500,-. Door de beperkte sanctioneringsgronden en de beperkte hoogte van sancties, werd de AP 'tandeloze tijger' genoemd. Door inwerkingtreding van de Wmd kan de AP bij overtreding van alle bepalingen van de Wbp boetes opleggen: ook bij overtreding van materiële normen. De hoogte van de sancties is verruimd tot € 810.000,- of, indien dat bedrag te laag is naar oordeel van de AP, tot 10% van de jaaromzet van een onderneming. Met de overtreding van materiële normen wordt bedoeld overtredingen van onder meer het rechtmatigheidsbeginsel (artikel 6 Wbp), het beginsel van doelbinding (artikel 7 Wbp), maar ook overtredingen bij onrechtmatig gebruik van het BSN (artikel 24 Wbp).

2.3.2 Handhaving door de Autoriteit Persoonsgegevens

Een andere manier van handhaving is een bindende aanwijzing. In beginsel legt de AP een bindende aanwijzing op alvorens zij boetes oplegt. Een bindende aanwijzing is een zelfstandige last: deze wordt opgelegd ter bevordering van de naleving van bepaalde wettelijke voorschriften.[101] De AP geeft in de bindende aanwijzing aan om welk wettelijk voorschrift het gaat en legt mogelijk een termijn op waarbinnen aan de aanwijzing voldaan dient te zijn. De AP geeft in de bindende aanwijzing ook aan wat gedaan moet worden om de overtreding (deels) te herstellen. De bindende aanwijzing wordt bij besluit opgelegd en de verantwoordelijke kan derhalve in bezwaar en beroep gaan. Wanneer de bindende aanwijzing niet nageleefd wordt, kan de AP alsnog een bestuurlijke boete opleggen (zie §2.2.7 en 2.3.1).

De AP is van tandeloze tijger na de invoering van de Wmd veranderd in een echte tijger: zowel de gronden voor sancties als de hoogte van de sancties zijn flink verruimd. Daarnaast is het niet meer de AP die op onderzoek uit moet om overtredingen vast te stellen: de verantwoordelijke dient de organisatie in de gaten te houden en bij een lek melding te doen. Dit neemt niet weg dat de AP een rol blijft houden in het onderzoek naar overtredingen en ambtshalve onderzoek kan verrichten indien zij dit wenselijk acht.

2.3.3 Ketenaansprakelijkheid verwerkingen persoonsgegevens op grond van de Wbp

Zoals uit de begripsbepalingen (§2.1.2 en 2.2.2) blijkt, maakt de wet onderscheid tussen een verantwoordelijke, bewerker en een ontvanger. Met de inwerkingtreding van de Wmd impliceert de Wbp een ketenaansprakelijkheid voor verwerking van persoonsgegevens. De verantwoordelijke is in beginsel (eind)verantwoordelijk voor de verwerking van de gegevens. Verwerkingen van gegevens kunnen uitbesteed worden aan bewerkers. Een bewerker handelt op instructie van de verantwoordelijke, maar is niet onderworpen aan diens gezag. Of een bewerker verantwoordelijk is voor de verwerking van persoonsgegevens en daarmee ook voor mogelijke datalekken, is afhankelijk van de mate van zeggenschap die de bewerker heeft over

[98] Kamerstukken II 2014/15, 33 662, nr. 24.
[99] Artikel 66 lid 4 Wbp.
[100] Kamerstukken II 2013/14, 33 662, nr. 16, p. 1.
[101] Conform artikel 1 sub q jo. sub r Wbp is deze zelfstandige last een zelfstandige last in de zin van artikel 5:2 lid 2 Awb: 'Geen bestuurlijke sanctie is de enkele last tot het verrichten van bepaalde handelingen'.

de verwerking van de gegevens.[102] Wanneer de bewerker een aanzienlijke mate van zeggenschap heeft, wordt deze als verantwoordelijke aangemerkt. Een ontvanger verwerkt gegevens ten behoeve van een taak die de verantwoordelijke zelf niet kan vervullen. Bij deze uitwisseling ontstaat geen ketenaansprakelijkheid.

2.3.3.1 De bewerkersovereenkomst

De verantwoordelijke is verplicht een bewerkersovereenkomst te sluiten met bewerkers.[103] De verantwoordelijke moet voldoende technische en organisatorische beveiligingsmaatregelen treffen ten aanzien van de verwerkingen van persoonsgegevens. Bij uitbesteding aan een bewerker worden middels deze overeenkomst afspraken gemaakt over de wijzen waarop de bewerker de technische en organisatorische maatregelen waarborgt in haar processen. Uitgangspunt is contractvrijheid: het staat partijen vrij de inhoud van de overeenkomst te regelen.[104] In hoeverre de verantwoordelijke zorg draagt voor de technische en organisatorische maatregelen bij de bewerker, wordt in deze overeenkomst vastgelegd. Afhankelijk wat overeengekomen is, kan de verantwoordelijke die zijn verplichtingen niet nakomt, aansprakelijk worden gesteld.[105] Datzelfde geldt voor de bewerker.[106]

2.4 Algemene Verordening Gegevensbescherming

2.4.1 Achtergrondinformatie en reikwijdte

De Privacyrichtlijn[107] waarop de Wbp gebaseerd is, stamt uit 1995. Sindsdien is de technologie enorm gegroeid: de privacyrichtlijn en de Wbp zijn hier onvoldoende op toegespitst. De Europese Commissie heeft daarom op 25 januari 2012 een nieuw privacybeschermingspakket gepresenteerd. Het pakket bestaat onder meer uit de AVG[108] en een Richtlijn Bescherming persoonsgegevens opsporing en vervolging[109]. Op 12 maart 2014 is het voorstel voor de AVG door het Europees Parlement aangenomen.[110] De precieze datum van inwerkingtreding is nog onbekend: naar verwachting treedt de AVG eind 2016 in werking. De AVG trekt de touwtjes rondom privacy strak aan. Aangezien de AVG een Europese verordening is, heeft deze directe werking.[111] De Wbp is vanaf inwerkingtreding van de AVG niet langer rechtsgeldig. De tekst van de Wbp wordt grotendeels overgenomen, waardoor de AVG feitelijk voornamelijk een aanvullend karakter heeft. Lidstaten hebben een implementatietermijn van twee jaar om aan de nieuwe wetgeving te voldoen.

De verordening is, evenals de huidige Wbp, van toepassing op geheel of gedeeltelijk geautomatiseerde verwerkingen van persoonsgegevens, alsmede op de niet-geautomatiseerde verwerkingen van gegevens die in een bestand zijn opgenomen dan wel de gegevens die verzameld zijn met de intentie om deze op te nemen in een bestand. De tekst van de AVG heeft het over ‘verwerkers’. Aangezien met verwerker dezelfde rol bedoeld wordt als die van bewerker, wordt bewerker gehanteerd om verwarring te voorkomen.

2.4.2 Rol bewerker en ontvanger

De AVG wijdt hoofdstuk III aan de rechten van betrokkenen en aan de rollen van verantwoordelijke en bewerker. Een bewerker die niet uitsluitend op instructie van de verantwoordelijke handelt, wordt als gezamenlijk verantwoordelijke beschouwd.

---

[102] Thole, Van der Jagt en Roerdink 2014, p. 109.
[103] Artikel 14 Wbp.
[104] Brahn/Reehuis 2010, p. 240.
[105] Artikel 15 Wbp.
[106] Artikel 49 Wbp.
[107] Richtlijn 95/46/EG van het Europese Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (Pb*EG* L 281).
[108] COM (2012) 11 def.
[109] COM (2012) 10 def.
[110] Aangenomen Teksten Europees Parlement, 1314, vergadering 12 maart 2014 deel I, PE 531.357.
[111] Artikel 288 VwEU.

2.4.3 Rechten van betrokkenen

Rechten van betrokkenen staan ook in de AVG. Het huidige correctierecht wordt uitgebreid.

Recht	**Uitwerking**
Recht om te wissen (artikel 17 AVG)	Het huidige recht van correctie (artikel 36 Wbp) wordt uitgebreid met het recht om te wissen. De betrokkene kan de verantwoordelijke verzoeken om gegevens die van hem openbaar zijn gemaakt te wissen en de verspreiding van de gegevens stop te zetten. Grondslagen voor dit verzoek zijn: - Gegevens zijn niet langer noodzakelijk in verband met de doeleinden waarvoor ze verzameld dan wel verwerkt werden; - Betrokkene trekt de door hem gegeven toestemming in; - Een regelgevende instantie die rechtsgeldig uitspraak heeft gedaan, heeft besloten dat de gegevens gewist moeten worden; - De gegevens zijn onrechtmatig verwerkt (artikel 17 lid 1 AVG). De verantwoordelijke dient eventuele (sub)bewerkers ook op de hoogte te stellen van het ingeroepen recht om te wissen en dient alle (technische) maatregelen te nemen om de gegevens te wissen (artikel 17 lid 2 AVG).

2.4.4 Beginselen

In de AVG worden twee privacybeginselen gecodificeerd. Door de codificatie dienen verantwoordelijke en de bewerker zowel bij het vaststellen van doeleinden, de middelen ter verwerking en de daadwerkelijke verwerking zelf, passende maatregelen ten uitvoer te leggen. Deze beginselen borgen de rechten van betrokkenen structureel in de bedrijfsvoering.

2.4.4.1 Privacy by Design

Privacy by Design ligt verankerd in artikel 23 lid 1 AVG. Het beginsel stelt dat aandacht voor procedures met betrekking tot vertrouwelijkheid, integriteit, veiligheid en de verwijdering van persoonsgegevens structureel geborgd moet worden in de bedrijfsvoering.

2.4.4.2 Privacy by Default

Het andere beginsel is Privacy by Default. De nadruk bij dit beginsel ligt op systeeminstellingen. Niet de cyclus, maar waarborging van gegevens in het systeem staat centraal bij dit beginsel.[112] Digitale gegevensminimalisering en firewalls zijn voorbeelden van waarborgen.

Invoering van de AVG houdt in dat de twee beginselen op nieuwe gegevensverwerkingen van toepassing zijn, maar ook op huidige verwerkingen. Om in kaart te brengen wat er binnen organisaties geregeld is, wordt een instrument aangereikt: het Privacy Impact Assessment.

2.4.4.3 Privacy Impact Assessment

Artikel 33 AVG stelt dat het recht op bescherming van persoonsgegevens bij de verwerking van die gegevens continu gemonitord moet worden. Om de risico's van de bewerkingen in kaart te brengen, kan de verantwoordelijke een risicoanalyse uitvoeren: een Privacy Impact Assessment (hierna te noemen: PIA). Wanneer een onderneming grote wijzigingen aanbrengt in procedures met betrekking tot de verwerking van persoonsgegevens, waarbij in een periode van twaalf maanden risicovolle persoonsgegevens van betrokkenen zijn verwerkt, stelt de AVG een PIA verplicht.[113] Een grote wijziging is bijvoorbeeld de aanschaf van een nieuw administratiesysteem. Bij het uitvoeren van een PIA worden de verwerkingen en de bescherming van gegevens tijdens die verwerkingen onderzocht. Het PIA geeft een beeld over de mogelijke kans van de aantasting van de persoonsgegevens van betrokkenen. Ook brengt het de risico's per bedrijfsonderdeel in beeld. De Functionaris Gegevensbescherming (hierna te noemen: FG) van een onderneming of organisatie, wordt nauw betrokken bij de uitvoering van een PIA.

[112] A. Duthler en A. Biesheuvel, *Het Europees privacyrecht in beweging, Overzicht van actuele ontwikkelingen en mogelijke consequenties voor werkzaamheden van IT-auditors*, februari 2013.
[113] Artikel 33 AVG.

2.4.5 Functionaris Gegevensbescherming

De functie FG bestaat reeds in de Wbp, maar de Wbp stelt deze niet verplicht. Met de inwerkingtreding van de AVG is de aanstelling van een FG verplicht voor overheidsinstanties en voor ondernemingen die in een periode van twaalf maanden van meer dan 250 betrokkenen gegevens hebben verwerkt, alsook organisaties die hoofdzakelijk belast zijn met de verwerkingen die regelmatig en stelselmatige observatie van betrokkenen vereisen of de waarbij de kernactiviteit van de onderneming bestaat uit de verwerking van bijzondere gegevens.[114] Het niet aanstellen van een FG als deze verplicht is, kan dit beboet worden (zie §2.4.7). ORO is vanaf inwerkingtreding van de AVG verplicht een FG in dienst te hebben.

2.4.5.1 Functietaken

De FG is een natuurlijk persoon die wordt aangewezen op grond van diens professionele kwaliteiten, in het bijzonder de kwaliteiten met betrekking tot deskundigheid op het gebied van (privacy)wetgeving en praktijkervaring met de bescherming van persoonsgegevens.[115] Een louter juridische achtergrond is onvoldoende: de FG dient knowledge en knowhow te hebben van ICT en informatiebeveiliging. Artikel 37 AVG vermeldt de minimumfunctie-eisen van een FG. De FG heeft twee 'petten' op: die van adviseur en toezichthouder. De FG houdt onder meer toezicht op de uitvoering van Privacy by Default en Privacy by Design, informeert betrokkenen over hun rechten en is degene die bewustzijn onder medewerkers creëert.

2.4.5.2 Positie Functionaris Gegevensbescherming binnen een organisatie

Artikel 36 AVG beschrijft de positie van de FG binnen de organisatie. Een FG vervult zijn taken en plichten onafhankelijk en ontvangt geen instructies van de verantwoordelijke. De FG brengt direct verslag uit aan het bestuur of de directie. De FG hoeft niet in dienst te zijn van een organisatie: de AP houdt FG-registers bij waaruit een passende FG geselecteerd kan worden voor een bepaald type organisatie. Wanneer de FG in dienst treedt bij de organisatie, is dat voor een minimumperiode van vier jaar. Als de FG extern wordt ingeleend, is dat voor een minimumperiode van twee jaar. De FG geniet ontslagbescherming gedurende deze periode: ontslag is alleen mogelijk wanneer niet voldaan wordt aan de taken die aan de functie verbonden zijn.[116] De eindverantwoordelijkheid voor het voldoen aan privacywetgeving binnen een organisatie blijft bij de verantwoordelijke.

2.4.6 Meldplicht datalekken

De AVG bevat ook een meldplicht datalekken. Om hierop vooruit te lopen, is in Nederland per 1 januari 2016 de Wmd in werking getreden. Het kader van die meldplicht is reeds geschetst (§2.2). In grote lijnen is de meldplicht van de AVG hetzelfde als die van de Wmd. Verschil met de Wmd is dat de meldplicht van de AVG onder 'onverwijld melden' een termijn van 24 uur na kennisname van het lek verstaat, terwijl deze termijn bij de Wmd 72 uur bedraagt.[117] Melding geschiedt bij de toezichthouder. De toezichthouder is de toezichthouder in het land waar de onderneming haar hoofdvestiging heeft. In Nederland is dit de AP.

2.4.7 Handhaving

De invoering van de Wmd maakt het mogelijk om hoger boetes op te leggen bij overtreding van de Wbp. Binnen de AVG is de mogelijkheid tot het opleggen van hoge boetes ook opgenomen. De Europese Commissie betoogt dat doeltreffende, afschrikkende sancties essentieel zijn om handhaving te kunnen garanderen. Boetes worden opgelegd door de toezichthouder en bedragen maximaal € 1 miljoen of 5% van de wereldwijde omzet van een onderneming.[118]

[114] Artikel 35 AVG.
[115] Artikel 37 AVG.
[116] Artikel 35 lid 7 AVG.
[117] Artikel 31 AVG.
[118] Artikel 79 lid 2 onder c AVG.

Hoofdstuk 3 Huidige situatie

In dit hoofdstuk wordt de huidige situatie ten aanzien van de verwerking van persoonsgegevens en mogelijk andere regelingen op het gebied van privacy binnen ORO uiteengezet. Er wordt gekeken welke verwerkingen van persoonsgegevens plaatsvinden en hoe deze plaatsvinden binnen ORO.

3.1 Stichting ORO

ORO is een middelgrote organisatie die zorg en ondersteuning biedt aan mensen met een verstandelijke en/of lichamelijke beperking. Verankerd in regio Zuidoost-Brabant staan de medewerkers van ORO iedere dag circa 1.700 cliënten bij. Deze zorg varieert van 24-uurs-zorg tot begeleiding bij een tandartsbezoek. Binnen ORO zijn 1.400 mensen werkzaam.[119] ORO heeft circa 80 locaties en 174 adressen, zo bleek uit het interview met de Projectleider Beheer, Onderhoud en Facilitaire zaken (zie Bijlage 17).

3.2 Organisatie(structuur)

Aangezien ORO organen heeft die mogelijk betrokken worden bij de aanstaande interne wijzigingen teneinde te voldoen aan de wetgeving, wordt allereerst de organisatiestructuur uiteengezet. ORO is organisatorisch verdeeld in twee regio's: Regio I en Regio II. Regio I is de regio Deurne[120], ook wel Regio Intensieve zorg. Regio II zijn de overige Peelgemeenten. Beide regio's hebben hun eigen directeur. Uit de organogrammen blijkt dat de tweede managementlaag bestaat uit wijkmanagers. Zij dragen zorg voor dagbesteding, wonen en ambulante hulpverlening: voor zowel de zaken rondom cliënten als medewerkers. Naast wijkmanagers zijn er teammanagers en meewerkend teammanagers. De organogrammen zijn weergegeven op Bijlage 9.

Naast de twee regio's is een apart organogram met de structuur van de afdelingen Kennis en Behandeling. Deze twee afdelingen hebben gezamenlijk één manager. De tak Behandeling heeft tevens een eigen teammanager.

Voorts is er de topstructuur van ORO. De Raad van Bestuur (hierna te noemen: RvB) van ORO: deze is eenhoofdig. De bestuurder wordt bijgestaan door de bestuurssecretaris, die tevens de rol van Manager Staf bekleedt. De RvB staat in directe verbinding met de Raad van Toezicht (hierna te noemen: RvT). Tot slot is er een ondernemingsraad (hierna te noemen: OR) en een Centrale Cliëntenraad (hierna te noemen: CCR). Zie voor deze organogrammen tevens Bijlage 9.

3.2.1 Raad van Bestuur en Raad van Toezicht

De dagelijkse leiding van ORO is in handen van de RvB. Deze is verantwoordelijk voor de realisatie van de doelstellingen, de strategie en de daaruit voortvloeiende resultaten.[121] De heer Roelofs is sinds 2012 werkzaam als bestuurder binnen ORO. Vanaf 1 mei 2015 is hij de enige bestuurder van ORO: in de periode van januari 2012 tot mei 2015 had ORO twee bestuurders, voor 2012 was de RvB ook eenhoofdig.

De RvT houdt toezicht op de wijze waarop de RvB van ORO de organisatie bestuurt.[122] ORO voldoet aan de eisen van transparantie en inrichting van de bedrijfsvoering, zoals vastgelegd

[119] Over ORO, *ORO,* www.oro.nl (zoek op '*Over ORO*').
[120] Er is één locatie in Deurne die valt onder Regio II, te weten de locatie 'Smalle Haven'.
[121] Raad van Bestuur, *ORO*, www.oro.nl (zoek op '*Raad van Bestuur*).
[122] Raad van Toezicht, *ORO*, www.oro.nl (zoek op *'Raad van Toezicht'*).

in de Zorgbrede Governance Code.[123] De RvT bestaat uit zeven leden (een voorzitter, een vicevoorzitter en vijf leden).

3.2.2 Ondernemingsraad en Centrale Cliëntenraad

Vanwege de omvang van de organisatie, heeft ORO een verplichte OR.[124] De OR bestaat uit vijftien leden. De OR komt wekelijks bijeen en vergadert minstens éénmaal per kalendermaand. Daarnaast is er eenmaal per zes weken een vergadering met de RvB. Ook vindt tweemaal jaarlijks een achterbanoverleg plaats met geselecteerde contactpersonen (hierna te noemen: CPO). Iedere medewerkers van ORO kan zichzelf aanmelden als CPO.[125] Onlangs is de zittingstermijn van de OR afgelopen en zijn er OR-verkiezingen geweest. De OR heeft meerdere rechten, waaronder het adviesrecht, instemmingsrecht en initiatiefrecht.[126] Wanneer nieuwe regelingen vastgesteld worden die grote gevolgen hebben voor medewerkers, dient de OR om advies te worden gevraagd. Aangezien er wijzigingen aankomen teneinde aan de wetgeving te voldoen, dient de OR mogelijk om advies of instemming gevraagd te worden.

De mening van cliënten, ouders, familieleden en vrijwilligers over onderwerpen zoals veilig wonen en werken, staat binnen ORO centraal. Samen met deze groepen mensen wordt binnen de wijkraden en met de CCR over deze onderwerpen gesproken. Iedere wijk van ORO heeft een wijkraad. Een wijkraad bestaat uit onder meer cliënten, vrijwilligers en familieleden. Cliënten in een wijkraad worden bijgestaan door een cliëntencoach. Een coach legt moeilijke onderwerpen aan cliënten uit in voor hen begrijpelijke taal. Momenteel telt ORO circa twintig wijkraden. Een wijkraad komt minimaal viermaal per kalenderjaar bijeen en de wijkmanager van een wijk sluit ten minste tweemaal per kalenderjaar aan bij deze vergaderingen. De CCR bestaat uit vertegenwoordigers van iedere wijkraden. Elke twee maanden overlegt de CCR met de RvB. Onderwerpen die aan bod komen, hebben vaak betrekking op meerdere wijken of zijn zelfs ORO-breed. De CCR kan over onderwerpen gevraagd en ongevraagd advies geven. Dit advies is niet bindend, maar wanneer er besluiten genomen worden die ingrijpend zijn voor de cliënten van ORO, wordt aangeraden de CCR om advies te vragen.

3.3 Stakeholders

ORO heeft te maken met een grote hoeveelheid in- en externe stakeholders, waaronder zorgaanbieders, samenwerkingsverbanden, gemeentes en leveranciers. Met een deel van deze instanties worden gegevens uitgewisseld: deze instanties zijn derhalve ontvangers ofwel bewerkers. Een overzicht van de stakeholders is weergegeven op Bijlage 10.

Het is ORO onduidelijk welke stakeholders bewerkers, ontvangers of louter stakeholders zijn in het kader van de Wbp. Het is tevens niet helder met welke bewerkers een bewerkersovereenkomst gesloten is. Uit de afgenomen interviews met onder meer de Manager HRM en de Manager ICT blijkt dat onlangs (medio eind 2015) met AFAS een bewerkersovereenkomst gesloten is (zie Bijlage 17). AFAS is de leverancier van MijnORO: alle persoonsgegevens hangen in de ‘cloud’ van AFAS. De voornoemde overeenkomst met AFAS is vertrouwelijk en is derhalve niet als bijlage toegevoegd. De overeenkomst met AFAS is echter geen bewerkersovereenkomst in de juridische zin van het woord. De overeenkomst regelt inderdaad een en ander rondom privacy en het omgaan met persoonsgegevens. Dit is echter te beknopt om te spreken van een volwaardige bewerkersovereenkomst. Uit het interview met de Manager ICT blijkt dat naar waarschijnlijkheid tevens een

[123] Voor alle leden van GGZ Nederland geldt de Zorgbrede Governancecode. Deze code geeft regels voor het afleggen van de maatschappelijke verantwoording door de zorginstelling aan de belanghebbenden van de instelling. Zorgbrede Governancecode, *GGZ Nederland*, www.ggznederland.nl (zoek op *‘Zorgbrede Governancecode’*).
[124] Artikel 2 WOR stelt een OR verplicht voor een onderneming met circa 50 medewerkers. ORO voldoet met haar 1.400 medewerkers ruimschoots aan deze drempel.
[125] Deze informatie is verkregen via de intranetpagina van ORO en is derhalve geen openbaar toegankelijke informatie.
[126] Artikel 23 t/m 25, 27 en 30 WOR.

bewerkersovereenkomst gesloten is met Nedap.[127] Nedap is de leverancier van het ONS-systeem. Persoonsgegevens in dit systeem hangen in de 'cloud' van Nedap. Nedap heeft aangekondigd naar aanleiding van de nieuwe wetgeving haar bewerkersovereenkomsten te gaan wijzigen teneinde de nieuwe wetgeving in te bedden, zo bleek uit het interview met de Adviseur Persoonlijk plan/Medewerker Startpunt (zie Bijlage 17).

3.4 Overzicht verwerkingen van persoonsgegevens binnen ORO

Aangezien binnen ORO zowel cliëntgegevens als gegevens van medewerkers verwerkt worden, is het van belang dat de verantwoordelijke voldoende inzichtelijk heeft wat er voor verwerkingen plaatsvinden en door wie deze geschieden. In Bijlage 11 is een overzicht opgesteld van de persoonsgegevens die verwerkt worden van medewerkers en cliënten binnen ORO. Bijlage 12 bevat een overzicht van de bewaartermijnen van deze gegevens. Bijlage 13 geeft de wettelijke grondslagen van verwerkingen die plaatsvinden binnen ORO weer.

3.5 Documentatie

Gedurende dit onderzoek is geïnventariseerd wat binnen ORO vastligt om de huidige stand van zaken omtrent privacy in kaart te brengen. Onderstaande zaken zijn binnen ORO schriftelijk geregeld.

3.5.1 Geheimhouding

Bij indiensttreding tekent een medewerker een arbeidsovereenkomst. In deze overeenkomst ligt een artikel verankerd aangaande geheimhouding. Het beding is als onderstaand opgenomen in de overeenkomsten.

'De werknemer/stagiaire heeft een geheimhoudingsplicht. Daarbij gaat de werknemer zorgvuldig en correct om met informatie waarover hij beschikt, uit hoofde van de functie en bij uitvoering van de werkzaamheden. De geheimhoudingsplicht blijft ook na beëindiging van het dienstverband van kracht'.

3.5.2 Gedragscode Social Media

Medewerkers ontvangen bij indiensttreding het document 'Gedragscode Social Media'. Dit document is een algemene gedragscode, waarbij enkel volgend punt ingaat op privacy: 'Wij respecteren de privacy van de ander en doen dit onder meer door zorgvuldig en correct om te gaan met informatie waarover wij uit hoofde van onze functie beschikken.'

3.5.3 Toestemmingsverklaring cliëntdossier, het persoonlijk plan en privacyreglement voor cliënten

Een cliënt (of diens wettelijk vertegenwoordiger) vult een aanmeldingsformulier en een toestemmingsverklaring in en retourneert deze ondertekend. Vanaf dat moment treedt de cliënt bij ORO in zorg en wordt door Startpunt een elektronisch cliëntdossier aangelegd. Middels de toestemmingsverklaring geeft de cliënt (of diens wettelijk vertegenwoordiger) toestemming om gegevens uit te wisselen met andere instanties in het kader van de zorg die aan de cliënt verleend wordt. Toestemming kan te allen tijde worden ingetrokken door de cliënt (of diens wettelijk vertegenwoordiger).

Als de cliënt bij ORO in zorg treedt, wordt er een persoonlijk plan (hierna te noemen: PP) geschreven. Het PP is een belangrijk hulpmiddel voor de zorgverleners in de ondersteuning van de cliënten en maakt deel uit van het elektronisch cliëntdossier. Het plan is de weergave van de inhoudelijke afspraken tussen de cliënt(vertegenwoordiger) en ORO over de

[127] Uit navraag bij de afdeling Beleidsadvies blijkt dat Nedap ORO een bewerkersovereenkomst heeft toegezonden, maar dat deze nooit bekrachtigd is.

overeengekomen ondersteuning en de wijze waarop getracht wordt deze te bereiken c.q. uit te voeren. Alle afspraken in het PP zijn gericht op de bevordering dan wel het in stand houden van de kwaliteit van bestaan van de cliënt. Binnen ORO is het uitgangspunt een cliënt heeft één zorgcoördinator, één PP en één PP-bespreking. Samen met de cliënt(vertegenwoordiger), betrokken deskundigen en eventueel andere persoonlijk betrokkenen uit het netwerk van de cliënt wordt het PP opgesteld door de zorgcoördinator. Het plan wordt jaarlijks besproken en ten minste tweejaarlijks vernieuwd. Het plan bevat persoonsgegevens en mogelijk medische gegevens of indicaties van de cliënt.

Voor cliënten is er een privacyreglement (zie Bijlage 14). Het reglement wordt niet (meer) verstrekt aan cliënten: het is verouderd en daardoor inhoudelijk niet meer juist. Het reglement is intern te raadplegen via Intranet[128].

3.6 Overige regelingen en voorzieningen

Uit interviews met onder meer de receptioniste/telefoniste van het Centraal Bureau en de Medewerker HRS-administratie blijkt dat de HRS-administratie en de recepties binnen ORO zich zeer bewust zijn van het feit dat zij geen persoonsgegevens mogen verstrekken aan derden (zie Bijlage 17). Deze afspraak ligt echter niet vast op schrift in procedures of werkafspraken.

Uit de interviews met voorgaande dames bleek eveneens dat op het Centraal bureau wordt gewerkt met papier- en vernietigbakken. De papierbakken bevatten oud papier: de vernietigbakken bevatten oud papier met gevoelige informatie. De vernietigbakken op het Centraal Bureau worden eenmaal per week geleegd door een medewerker van de Atlant Groep[129]. Deze cliënt verzamelt de inhoud van alle vernietigbakken en gooit dit in de afsluitbare vernietigcontainer die buiten het pand staat. De sleutel van deze container wordt bewaard bij de receptie van het Centraal Bureau. Medewerkers kunnen deze sleutel vragen wanneer zij hun vernietigbak zelf (eerder) willen legen. Andere locaties hebben geen vernietigbakken en –container. Aangezien op de andere locaties vrijwel geen administratie gevoerd wordt (met uitzondering van het Dienstencentrum en locatie de Rakthof), zijn deze locaties niet voorzien van een vernietigcontainer, maar van versnipperapparaten.

ORO werkt momenteel met reguliere printers op elke locatie: de printers zijn bijvoorbeeld niet uitgerust van een follow-me-systeem[130]. Geprinte stukken die niet opgehaald worden bij de printer, worden op verschillende locaties bewaard in een bak naast de printer: ‘vergeten printjes’. Er zijn ook locaties die een dergelijke bak niet hebben en alle achtergebleven stukken aan het einde van de werkdag in de vernietigbak stoppen of versnipperen. De printers worden geleased bij Ricoh. Het leasecontract loopt af medio september van dit jaar.

ORO heeft (nog) een eigen ICT-afdeling. Deze afdeling wordt grotendeels dit jaar nog geoutsourced naar een derde partij. Het systeem van ORO is, gelet op het grote aantal locaties en adressen, een complexe aangelegenheid. Vandaar dat ervoor gekozen is deze taak over te dragen aan een gespecialiseerde partij. Momenteel wordt binnen ORO op de locaties met name gewerkt met ‘thin clients’[131] (circa 400 stuks). Van deze thin clients zijn de USB-poorten door afdeling ICT uitgeschakeld. Enkele werkplekken zijn voorzien van een fat client[132] (circa 40 stuks). De USB-poorten van deze computers zijn niet uitgeschakeld.

[128] Intranet is een privaat netwerk dat alleen te raadplegen is binnen de organisatie waar het netwerk toe behoort. Met intranet wordt in dit rapport het private netwerk van ORO bedoeld.
[129] Atlant Groep zorgt voor duurzame participatie in het arbeidsproces voor iedereen die dat niet zelf kan. Visie en missie, *Atlant Groep*, www.atlantgroep.nl (zoek op: *missie*).
[130] Een printopdracht kan dan gegeven worden aan iedere willekeurige multifunctional binnen een organisatie, waarbij de opdrachtgever zelf kan kiezen wanneer de printopdracht uit de multifunctional moet komen.
[131] Een kleine, relatief zwakke computer die de hoofdmoot van het benodigde computercapaciteit van een server, een centrale computer betrekken en één gebruiker tegelijk ‘bediend’.
[132] Een netwerkcomputer waarop de meeste middelen lokaal geïnstalleerd zijn. Een fat client biedt functionaliteiten die onafhankelijk van een centrale server gebruikt kunnen worden.

Binnen ORO geldt een clear screen-policy. Dit houdt in dat een medewerker zijn of haar computer vergrendeld op het moment dat de werkplek verlaten wordt. Na verstrijken van een aantal minuten vergrendeld de computer automatisch. MijnORO is de naam van het digitale personeelsdossiers van medewerkers. Bij de implementatie van MijnORO is aandacht besteed aan het clear screen-policy. Wanneer een medewerker ingelogd is op een computer van ORO, kan het digitale personeelsdossier zonder extra inlog geopend worden.

Alle locaties waar fysieke documenten bewaard worden, zijn voorzien van afsluitbare (archief)kasten. Gedurende het onderzoek is geconstateerd dat niet al deze kasten daadwerkelijk afgesloten worden. Daarnaast zijn alle werkruimten afsluitbaar. Ook dat gebeurt niet op iedere locatie. In principe zijn alle bureaus aan het einde van de werkdag leeg: documenten worden in de afsluitbare kasten bewaard. Geconstateerd is dat dit niet door iedereen gebeurt. Uit het interview met de receptioniste/telefoniste van het Centraal Bureau bleek dat bij de receptie van het Centraal Bureau slechts één kast afsluitbaar is. Bij andere recepties is voldoende afsluitbare kastruimte.

Uit onder meer de interviews met de Projectleider Beheer, Onderhoud en Facilitaire zaken, de receptioniste/telefoniste van het Centraal Bureau en de Adviseur Persoonlijk Plan/Medewerker Startpunt blijkt het sleutelsysteem van (bijna) elke locatie van ORO een gelaagde structuur heeft. Het uitgangspunt is dat een sleutel de medewerker slechts toegang geeft tot de poort van de locatie, de voordeur en diens werkplek. Tevens zijn er enkele medewerkers voorzien van een loper en zijn enkele medewerkers geautoriseerd om alarmsystemen van bepaalde locaties in of uit te schakelen. Locatie de Rakthof en het Centraal Bureau regelen intern het sleutelbeleid. Bij de rest van de locaties worden de sleutels geregeld en beheerd door afdeling Huisvesting.

Tot slot bleek uit onder meer het interview met een wijkmanager dat de medewerkers die zorg verlenen vaak per locatie een Whatsapp-groep hebben (zie Bijlage 17). Het doel van deze groepen is om inval te regelen bij bijvoorbeeld ziekte. Het is echter voorgevallen dat in de gesprekken informatie en gegevens werden gedeeld die niet in een Whatsapp-groep thuishoren. Dit is besproken met de medewerkers en ook benoemd in het wijkoverleg. Hierover is op centraal niveau niets geregeld.

Hoofdstuk 4 Toetsing huidige situatie aan het juridisch kader

In dit hoofdstuk wordt het juridisch kader uit hoofdstuk 2 met de huidige situatie binnen ORO, zoals opgenomen in hoofdstuk 3, vergeleken. Uit deze analyses blijkt wat juist is geregeld en wat ORO nog dient in te richten om aan de Wet bescherming persoonsgegevens en de Wet meldplicht datalekken te voldoen. Daarnaast wordt gekeken in hoeverre ORO al voldoet aan de Algemene Verordening Gegevensbescherming en wat er nog geregeld moet worden om daaraan te voldoen.

4.1 Analyse IST-situatie

Om te weten waar de organisatie aan moet (gaan) voldoen, is het essentieel om te weten wat het vertrekpunt van de organisatie is.[133] Anders gezegd: stel vast wat er allemaal geregeld is binnen ORO met betrekking tot de privacybescherming van persoonsgegevens conform de Wbp, de Wmd en de aanstaande AVG.

4.1.1 Aanleiding

ORO is een organisatie die met persoonsgegevens van verschillende groepen betrokkenen werkt. De corebusiness van ORO is het verlenen van zorg: er worden derhalve cliëntgegevens verwerkt. Verwerking vindt eveneens plaats bij gegevens van de grote groep medewerkers en voor de lange lijst met stakeholders die ORO kent. De aanleiding van ORO om onderzoek te laten doen naar de wijzigingen binnen de privacywetgeving is tweeledig. Allereerst staat bij ORO privacy van haar cliënten en medewerkers hoog in het vaandel en streeft zij ernaar alle (juridische) zaken conform de wet te regelen. Om aan de wet- en regelgeving te voldoen, wenst zij inzicht te krijgen in de adequate beheersmaatregelen die hiertoe noodzakelijk zijn. Daarnaast zijn de wetswijzigingen met betrekking tot de sanctionerende bevoegdheden van de AP voor ORO een extra aanleiding geweest om de huidige situatie in kaart te brengen.

4.1.2 IST-situatie

Uit onder meer het interview met de Bestuurssecretaris/Manager Staf, de Manager HRM, Adviseur Persoonlijk plan/medewerker Startpunt en een wijkmanager blijkt dat medewerkers van ORO zich ervan bewust zijn dat er onlangs wijzigingen plaats hebben gevonden dan wel plaats gaan vinden privacywetgeving (zie Bijlage 17). Zo bleek uit het interview met de Adviseur Persoonlijk plan/medewerker Startpunt dat zij bij Nedap naar een bijeenkomst is geweest over de aanstaande wetswijzigingen die de AVG teweeg gaat brengen. De manager HRM vertelde dat bij het digitaliseren van de personeelsdossiers veel aandacht besteed is aan het selecteren van een gecertificeerd bedrijf voor de uitvoering van de digitalisering. Met dat bedrijf is, ook met het oog op eventuele datalekken, een bewerkersovereenkomst gesloten. Bij de integratie van MijnORO is aandacht besteed aan het vergrendelen van de werkplek wanneer een medewerker deze verlaat, omdat een collega met één klik het digitale dossier kan openen. De Bestuurssecretaris/Manager Staf is opdrachtgever voor dit onderzoek en is zich derhalve ook bewust van het feit dat er veranderingen plaatsgevonden hebben en op komst zijn op het gebied van privacy.

Er is een en ander schriftelijk geregeld met betrekking tot privacy binnen ORO. Zoals omschreven in hoofdstuk 3, tekenen de medewerkers van ORO een arbeidsovereenkomst met daarin een geheimhoudingsverklaring. Ook voor cliënten is er een zorgdienstverleningsovereenkomst en een separate toestemmingsverklaring om gegevens uit te wisselen met andere instanties. De meeste afspraken omtrent de verwerking van persoonsgegevens en privacy zijn echter mondeling gesloten of er is niets geregeld. Medewerkers van ORO tekenen bij indiensttreding hun arbeidsovereenkomst. Hierin is een basaal, triviaal artikel opgenomen omtrent geheimhouding. Voorts wordt bij de arbeidsovereenkomst als bijlage een ‘Gedragscode Social Media verstrekt’. Ook deze gaat slechts basaal in op privacy. Er is voor de cliënten een Reglement persoonsgegevens cliënten.

[133] Analyse IST-analyse, *Ben en Wil – Business, ICT en Alignment,* www.ben-en-ik.nl (zoek op *IST*).

Dit reglement is verouderd: wetswijzigingen zijn niet bijgehouden en bewaartermijnen in het reglement kloppen derhalve niet. Het reglement wordt derhalve niet meer aan cliënten verstrekt. Het is alleen via intranet intern te raadplegen door medewerkers. Het reglement is toegevoegd op Bijlage 14.

Elke werkplek is voorzien van afsluitbare (archief)kasten en kantoren. Op locatie de Rakthof is het archief alleen voorzien van een afsluitbare deur: de archiefkasten zijn niet af te sluiten. Bij het Startpunt, de HRS-administratie en de receptie van het Centraal Bureau is mondeling is afgesproken dat geen persoonsgegevens door worden gegeven aan derden (zie Bijlage 17). De clean screen-policy is tevens mondeling afgestemd.

4.1.3 Ontbrekende documentatie

Het is belangrijk om vast te stellen wat er geregeld is binnen een organisatie, maar ook om vast te stellen wat niet geregeld is binnen een organisatie. Binnen ORO zijn op veel afdelingen mondelinge afspraken, maar er ligt vrijwel niets schriftelijk vast. Op de volgende pagina staat een niet-limitatieve opsomming van wat er niet (schriftelijk) vastgelegd is binnen ORO.

Wat is er niet (op papier) geregeld binnen ORO?

- Er is geen privacyreglement voor medewerkers;
- Er is geen algemeen privacystatement of een algemene privacyverklaring;
- Er is geen privacy(awareness)beleid;
- Er is geen standaard bewerkersovereenkomst;
- Er is geen overzicht van bewerkers en ontvangers;
- Er is geen (officieel) overzicht van de verwerkingen van persoonsgegevens die plaatsvinden binnen ORO;
- Er zijn geen protocollen voor (het melden van) beveiligingslekken en datalekken;
- Er is geen aangewezen persoon of afdeling die datalekken registreert en, indien vereist, meldt aan de AP of aan de betrokkene(n);
- Er is geen document met betrekking tot bewaartermijnen van persoonsgegevens;
- Er is geen document met betrekking tot de rechten van betrokkenen en het is onbekend waar zij hun verzoek met betrekking tot deze rechten in kunnen dienen;
- Er is geen FG-functiebeschrijving voor ORO;
- Er is geen FG in dienst binnen ORO.

4.2 Analyse SOLL-situatie

Nadat vastgesteld is wat het vertrekpunt van de organisatie is, wordt bepaald wat de veranderingen uiteindelijk teweeg dienen te brengen binnen een organisatie.[134] De SOLL-situatie in de casus van ORO is gebaseerd op de onlangs ingetreden wetgeving en de aanstaande AVG. Uit hoofdstuk 2 is een tabel gedestilleerd die de wettelijke verplichtingen naar aanleiding van deze wetten weergeeft.[135] De tabel is opgenomen in Bijlage 15.

4.3 Overzicht huidige stand van zaken binnen ORO (GAP-analyse)

Een GAP-analyse geeft het verschil weer tussen de huidige situatie en de gewenste situatie.[136] Deze analyse is opgenomen in Bijlage 16. In Bijlage 11 is een overzicht van de verwerkingen van persoonsgegevens van medewerkers en cliënten opgenomen. Dit overzicht is opgemaakt gedurende dit onderzoek. Het overzicht is dan ook geen officieel document dat binnen ORO gebruikt wordt. Het geeft, samen met Bijlage 12 en 13, inzicht in hetgeen binnen ORO conform wet- en regelgeving verzameld, verwerkt, bewaard en vernietigd wordt, maar ook welke handelingen onrechtmatig plaatsvinden. Aan de hand van deze bijlagen en de bevindingen uit

[134] Analyse SOLL-analyse, *Ben en Wil – Business, ICT en Alignment,* www.ben-en-ik.nl (zoek op *SOLL*).
[135] Bij het opstellen van deze SOLL-analyse is tevens het privacy-normenkader van Duthler Associates geraadpleegd. Dit document is geclassificeerd als vertrouwelijk/geheim en is derhalve niet toegevoegd als bijlage.
[136] Analyse GAP-analyse, *Ben en Wil – Business, ICT en Alignment,* www.ben-en-ik.nl (zoek op *GAP*).

de interviews (zie Bijlage 17) is voornoemde GAP-analyse van Bijlage 16 opgesteld. Aangezien er geen officiële documentatie inzake de inventarisatie van de verwerking van persoonsgegevens door ORO is, wordt aan veel punten van de GAP-analyse niet of slechts deels voldaan. In de kolom 'Toelichting en actiepunt(en)' wordt aangegeven waar wel, niet of deels aan voldaan wordt, gevolgd door een uitleg en eventuele actiepunten waardoor wel aan het gegeven voldaan kan worden. Als actiepunten voortvloeien uit de aanstaande AVG, is dit vermeld. De AVG treedt waarschijnlijk dit jaar in werking: er start dan een implementatietermijn van twee jaar. De Wbp en Wmd zijn rechtsgeldig: aan hetgeen dat voortvloeit uit deze wetgeving dient derhalve zo snel mogelijk voldaan te worden. Deze items hebben dan ook de hoogste prioriteit.

4.4 Risicoanalyse

Nu bekend is wat de IST-situatie en de SOLL-situatie zijn en daarmee ook de GAP-analyse gemaakt is, kan een risicoanalyse plaatsvinden. Een risicoanalyse is een overzicht van alle mogelijke risico's met betrekking tot een bepaald item: in dit geval is dat item 'privacy'. Voor bepaling van de risico-omvang is uitgegaan van onderstaand classificeringsmodel, waarbij als uitgangspunten de impact en de kans van het risico gebruikt zijn. Het classificeringsmodel ziet er als onderstaand uit.

Classificeringsmodel

		Impact		
		Hoog	**Middel**	**Laag**
Kans	**Hoog**			
	Middel			
	Laag			

Als de kans op het intreden van het risico hoog is en de impact van het risico hoog is, wordt het risico dus geclassificeerd als 'hoog' (rood). Als de kans op het intreden 'middel' is, maar de impact 'laag', wordt het risico geclassificeerd als 'laag' (groen). De impact van een risico is hoog, middel of laag, afhankelijk van de financiële impact en de mogelijke imagoschade die het risico ten gevolge heeft.

In onderstaande tabel wordt het begrip 'impact' geclassificeerd.

Classificatie	Impact
Hoog	Het financiële risico voor ORO is zodanig hoog dat het een bedreiging vormt voor de continuïteit van de onderneming (10% van de jaaromzet, circa € 7,5 miljoen)[137] en/of de imagoschade dusdanig groot is dat de kwaliteit van de zorgdienstverlening landelijk van ORO ter discussie komt te staan en waarbij een significant deel van de cliënten hun behandelovereenkomst met ORO ontbinden en overstappen naar een andere zorgverlener.
Middel	Het financiële risico voor ORO is zodanig hoog dat een significant beroep gedaan moet worden op financiële reserves (€ 3 miljoen tot € 7,5 miljoen) en/of de imagoschade dusdanig groot is dat de kwaliteit van de zorgdienstverlening van ORO ter discussie komt te staan, waarbij een deel van de cliënten hun behandelingsovereenkomst met ORO ontbinden en overstappen naar een andere zorgverlener.
Laag	Het financiële risico voor ORO is minder dan € 3 miljoen en/of de gevolgen van de imagoschade zijn lager dan weergegeven bij classificatie 'Middel'.

Nadat bepaald is hoe hoog de impact van een mogelijk risico is, is het van belang om vast te stellen hoe groot de kans is dat een bepaald risico intreedt. Wanneer een risico een hoge

[137] Uit de laatste, nog niet definitieve, jaarcijfers van ORO (2015), blijkt dat haar omzet over het jaar 2015 circa € 72 miljoen bedroeg. De jaarcijfers van ORO zijn na vaststelling openbaar toegankelijk. Uit het interview met de Bestuurssecretaris/Manager Staf (zie Bijlage 17) blijkt dat de continuïteit van de onderneming in gevaar komt bij een boete ten hoogte van 10% van de jaaromzet (circa € 7,5 miljoen). Aan de hand hiervan zijn de geldbedragen van de impactclassificatie vastgesteld.

impact heeft, maar de kans op het intreden van het risico vrijwel nihil is, kan een verantwoordelijke mogelijk de afweging maken dat er geen maatregelen getroffen worden omdat de kans van intreden zo klein is.

In onderstaande tabel wordt het begrip ‘kans’ geclassificeerd.

Classificatie	Kans
Hoog	De kans dat het risico optreedt, is meer dan eenmaal per kalendermaand (dus minimaal twaalf keer per jaar).
Middel	De kans dat het risico optreedt, is meer dan tweemaal per jaar, maar minder dan twaalf keer per jaar.
Laag	De kans dat het risico optreedt is één à twee keer per jaar.

Het vaststellen van de kans en impact levert gecombineerd een classificatie op. Een hoge impact en lage kans leveren een middel (oranje) classificatie van het risico op: een middel impact en een lage kans leveren een lage (groene) classificatie van het risico op. Wanneer deze risicoanalyse toegepast wordt op de SOLL-analyse van Bijlage 15, levert dit vier hoofdgroepen risico’s op. Deze vier hoofdrisico’s worden hieronder geanalyseerd. Allereerst wordt het huidige risico geclassificeerd en toegelicht. Eventuele reeds genomen maatregelen worden beschreven. Vervolgens worden aanbevolen beheersmaatregelen beschreven. Als ORO deze maatregelen op een juiste manier ten uitvoer legt, wordt het beschreven risico verkleind. Het resterend risico wordt bij ‘restrisico-omvang’ geclassificeerd.

4.4.1 Risico: onvoldoende inzicht in privacyrisico’s

ORO heeft onvoldoende inzicht in verwerkingen van persoonsgegevens door haar medewerkers en door bewerkers en ontvangers. Zij heeft hierdoor onvoldoende inzicht in de mogelijke privacyrisico’s die zij loopt bij haar verwerkingen en kan daarom worden geconfronteerd met onverwachte incidenten en de daarbij horende (gevolg)schades en mogelijke boetes.

Risico-omvang	Midden (hoge kans, lage impact)	
Toelichting	Ten tijde van de uitvoering van de analyse heeft ORO niet inzichtelijk welke verwerkingen en handelingen met betrekking tot persoonsgegevens er plaatsvinden. Dit ontbrekende c.q. beperkte inzicht kan ertoe leiden dat er onverwacht incidenten plaatsvinden die (gevolg)schade met zich meebrengen of mogelijk leiden tot een boete van de AP. Ten tijde van het onderzoek is geconstateerd dat in ieder geval bij de HRS-administratie persoonsgegevens onrechtmatig verzameld worden (zie Bijlage 13, Wettelijke grondslagen van rechtmatige verwerking van persoonsgegevens van medewerkers en cliënten binnen ORO). Deze onrechtmatige verzameling vindt bij indiensttreding van medewerkers van ORO plaats. Per jaar treden er meer dan twaalf personen in dienst: dit levert een hoge kans classificatie op. Naar verwachting is de impact van de (gevolg)schade laag. Hierbij is de kans op boetes van de AP buiten beschouwing gelaten: deze zijn apart gekwalificeerd in §4.4.2.	
Reeds genomen maatregelen voor analyse	N.v.t.	
Aanbevolen maatregelen	Wanneer de actiepunten van de GAP-analyse worden uitgevoerd met betrekking tot het inzichtelijk krijgen van de gegevensverwerkingen binnen ORO, ontstaat er een duidelijk beeld van de privacyrisico’s die ORO loopt en waar ORO deze loopt. Op deze manier zijn risico’s inzichtelijk en kan tijdig geanticipeerd worden op mogelijke incidenten en de gevolgen daarvan.	
Restrisico-omvang	Laag (lage kans, lage impact)	

4.4.2 Risico: (significante) boetes opgelegd door de Autoriteit Persoonsgegevens

ORO voldoet met haar huidige beleid (IST-situatie, zoals weergegeven in §4.1) niet aan de nieuwe wetgeving van de Wbp en Wmd. Zij loopt daarom het risico beboet te worden door de AP. Er zijn meerdere redenen waarvoor een boete opgelegd kan worden. Momenteel is ORO bezig met het inzichtelijk krijgen wat er moet gebeuren om aan de wetgeving te voldoen (SOLL-situatie, zoals weergegeven in §4.2).

Risico-omvang	Midden (hoge kans, lage impact)
Toelichting	Zoals reeds gesteld vinden er binnen ORO, in ieder geval op de HRS-administratie, onrechtmatige verwerkingen van persoonsgegevens plaats. Er treden meer dan twaalf medewerkers per jaar in dienst. Dat houdt in dat er meer dan twaalf keer per jaar onrechtmatig persoonsgegevens van medewerkers verwerkt worden (kansclassificatie: hoog). Mogelijke boetes van de AP voor niet-naleving van de Wbp lopen op tot € 810.000,- of, indien dat naar oordeel van de AP onvoldoende hoog is, tot 10% van de jaaromzet van een rechtspersoon. De hoogte van deze boete moet verenigbaar zijn met de overtreding. Bij een boete van 10% van de jaaromzet van ORO, is de impact hoog. Het verschil tussen een boete van 10% van de jaaromzet en € 810.000,-, is bij ORO erg groot. In beginsel geeft de AP een bindende aanwijzing alvorens zij beboet. De kans dat de AP direct een boete oplegt die € 810.000,- overschrijdt is daarom klein. Een boete van € 810.000,- wordt geclassificeerd als laag, nu de financiële reserves niet aangetast worden en de continuïteit van de onderneming daarmee geen gevaar loopt.
Reeds genomen maatregelen voor analyse	Beheersmaatregelen zoals de toestemmingsverklaring uitwisseling gegevens voor cliënten die in zorg treden en het geheimhoudingsbeding in de arbeidsovereenkomsten met medewerkers.
Aanbevolen maatregelen	Wanneer de actiepunten van de gehele GAP-analyse worden uitgevoerd (met uitzonderingen van de punten die pas verplicht worden als de AVG in werking treedt), wordt voldaan aan de gehele Wbp en Wmd. Het boeterisico neemt daardoor af: er wordt immers aan de wet voldaan en daarmee is ook al het mogelijke gedaan om verwerkingen rechtmatig te laten geschieden en het risico op datalekken zo beperkt mogelijk te maken.
Restrisico-omvang	Laag (lage kans, lage impact)

4.4.3 Risico: ketenaansprakelijkheid

ORO heeft veel stakeholders waarvan niet inzichtelijk is wie bewerker, ontvanger of louter stakeholder is. Dit houdt in dat de ketenaansprakelijkheid voor bewerkers dus niet of onvoldoende afgedekt is en ORO als verantwoordelijke aansprakelijk kan worden gesteld voor geleden schade door betrokkene(n) en derde partijen.

Risico-omvang	Hoog (hoge kans, hoge impact)
Toelichting	ORO heeft veel stakeholders (circa 150, zie Bijlage 10). Het is niet c.q. slechts beperkt inzichtelijk welke stakeholders bewerkers, ontvangers of louter stakeholders zijn. Door het niet of onvoldoende afdekken van aansprakelijkheid met bewerkers van persoonsgegevens van ORO kan ORO als verantwoordelijke aansprakelijk worden gesteld voor geleden schaden door betrokkenen en mogelijke derde partijen. Uit de interviews met de Manager ICT en de manager HRM blijkt dat ORO niet standaard bewerkersovereenkomsten sluit en dat van slechts een tweetal bewerkers bekend is dat met hen een overeenkomst gesloten is (zie Bijlage 17). Hierdoor komt verantwoordelijkheid naar verwachting bij ORO te liggen.
Reeds genomen maatregelen	N.v.t.
Aanbevolen maatregelen	- Inzichtelijk documenteren gegevensverwerkingen door derden (zowel bewerkers als ontvangers);

	- Sluit met de partijen die gekwalificeerd zijn als bewerker een deugdelijke bewerkersovereenkomst die de aansprakelijkheid voldoende inbedt.
Restrisico-omvang	Midden tot laag (midden tot lage kans, midden tot lage impact, mede afhankelijk in hoeverre de betrokken partijen willen participeren)

4.4.4 Risico: (significante) boetes opgelegd door de Autoriteit Persoonsgegevens in het kader van de AVG

ORO voldoet met haar huidige beleid (IST-situatie, zoals weergegeven in §4.1) niet aan de aanstaande AVG. Momenteel is ORO bezig met het inzichtelijk krijgen van wat er moet gebeuren om aan de wetgeving te voldoen (SOLL-situatie, zoals weergegeven in §4.2). De datum van inwerkingtreding van de AVG is nog onbekend, maar wanneer deze inwerking treedt, wijzigt er nog meer op het gebied van privacy. Wanneer de AVG in werking treedt, start een implementatietermijn van twee jaar.

Risico-omvang	Middel (hoge kans, lage impact)
Toelichting	Zoals reeds gesteld vinden er binnen ORO, in ieder geval op de HRS-administratie, onrechtmatige verwerkingen van persoonsgegevens plaats. Er treden meer dan twaalf medewerkers per jaar in dienst. Dat houdt in dat er meer dan twaalf keer per jaar onrechtmatig persoonsgegevens van medewerkers verwerkt worden (kansclassificatie: hoog). Mogelijke boetes van de AP voor niet naleving van de AVG lopen op tot € 1 miljoen, of, indien dat naar oordeel van de AP onvoldoende hoog is, tot 5% van de wereldwijde jaaromzet van een rechtspersoon (impactclassificatie: laag tot middel). De hoogte van deze boete moet verenigbaar zijn met de overtreding. De datum van inwerkingtreding van de AVG is nog niet bekend en wanneer de AVG in werking treedt, start er een implementatietermijn van twee jaar. ORO heeft daarom nog voldoende tijd om de regels van de AVG te implementeren voordat zij risico loopt op boetes (bijstelling impactclassificatie: laag).
Reeds genomen maatregelen	N.v.t.
Aanbevolen maatregelen	- Inzichtelijk documenteren welke wijzigingen de AVG teweeg brengt (die de Wmd nog niet teweeg heeft gebracht) en hierop anticiperen; - Stel tijdig een FG aan.
Restrisico-omvang	Laag (lage kans, lage impact)

Hoofdstuk 5 Conclusies en aanbevelingen

In dit hoofdstuk worden de conclusies en aanbevelingen gegeven die voortvloeien uit dit onderzoek. De conclusies vloeien voort uit de in het vorige hoofdstuk opgenomen GAP-analyse op basis van wetgeving en semigestructureerde interviews. De aanbevelingen zijn afgeleid van de conclusies.

De conclusies en aanbevelingen beantwoorden samen de hoofdvraag van dit onderzoek: 'Welke maatregelen dient ORO door te voeren binnen haar huidige bedrijfsvoering, zodat bij de verwerking van persoonsgegevens in overeenstemming gehandeld wordt met de Wet bescherming persoonsgegevens, de nieuwe Wet meldplicht datalekken en de aanstaande Europese Algemene Verordening Gegevensbescherming?'. De scope van dit onderzoek is beperkt tot verwerking van persoonsgegevens van de cliënten en medewerkers van ORO.

5.1 Conclusies

Het onderzoek heeft uitgewezen dat er verschillende eisen ten grondslag liggen aan de rechtmatige verwerking van persoonsgegevens voor zowel de huidige wetgeving als de aanstaande wetgeving. De huidig wetgeving, bestaande uit de Wet bescherming persoonsgegevens (hierna te noemen: Wbp) en de Wet meldplicht datalekken (hierna te noemen: Wmd), vervalt bij inwerkingtreding van de aanstaande Europese Algemene Verordening Gegevensbescherming (hierna te noemen: AVG). De datum van inwerkingtreding van de AVG is nog onbekend. De conclusies zijn tweeledig: allereerst wordt ingegaan op de huidige wetgeving, daarna wordt ingegaan op de aanstaande wetgeving. De laatste alinea van deze paragraaf vat de conclusies samen.

Het juridisch kader schetst op basis van wetgevings- en literatuuronderzoek de verplichtingen voor de verwerking van persoonsgegevens uit de Wbp en Wmd. Verwerking van persoonsgegevens is een breed begrip: het omvat de gehele levenscyclus van gegevens van verzameling tot en met vernietiging. De verzameling van persoonsgegevens vereist een wettelijk doel tot verzameling. Een voorbeeld van een wettelijke verzamelingsgrond is verzameling ter uitvoering van een overeenkomst. Verwerking van persoonsgegevens mag alleen dan plaatsvinden als de verwerking een uitdrukkelijk omschreven wettelijk gerechtvaardigd doel dient. Voorts mag verwerking enkel plaatsvinden op een wijze die verenigbaar is met het doel waarvoor de gegevens verzameld zijn. De verzamelde gegevens moeten juist, nauwkeurig, adequaat en ter zake dienend zijn, maar mogen niet bovenmatig zijn. Ook dient de verwerking een voor de betrokkene(n) transparante wijze te geschieden. Om bijzondere persoonsgegevens, als bedoeld in artikel 16 Wbp, te mogen verzamelen, moet sprake zijn van een expliciet wettelijke grondslag. Een bijzonder persoonsgegeven dat binnen ORO verwerkt wordt, is het BSN van medewerkers en cliënten. Voor deze verwerking is een expliciet wettelijke grondslag aanwezig en de verwerking is derhalve rechtmatig.

Uit dit onderzoek blijkt dat het binnen ORO onduidelijk is welke verwerkingen van persoonsgegevens plaatsvinden. Dat geldt voor zowel verwerkingen intern door medewerkers als verwerkingen extern door bewerkers. Met dit onderzoek zijn de interne verwerkingen in kaart gebracht en beoordeeld op rechtmatigheid conform de eisen van de Wbp en Wmd. Geconstateerd is dat er onrechtmatige interne verwerkingen plaatsvinden binnen ORO. Deze onrechtmatige verwerkingen dient ORO per direct stop te zetten en, indien en voor zover mogelijk, ongedaan te maken. Uit dit onderzoek is eveneens gebleken dat ORO een groot aantal stakeholders heeft. Deze stakeholders zijn niet gekwalificeerd: het is ORO derhalve onduidelijk welke stakeholders bewerkers zijn. Welke verwerkingen geschieden door bewerkers en de rechtmatigheid hiervan, dient ORO vast te stellen en te toetsen op legitimatie.

Gegevens mogen niet langer bewaard worden dan de verwerking vereist, tenzij de wet een andere termijn stelt. Met dit onderzoek is in kaart gebracht hoelang ORO documenten bewaard alvorens zij deze vernietigd. De meeste wettelijke bewaartermijnen worden overschreden.

Enkele documenten worden geheel niet vernietigd. Uit de wet vloeien rechten van betrokkenen voort. Een interne procedure voor de betrokkenen om deze rechten uit te kunnen oefenen jegens ORO, ontbreekt. Er is geen aangewezen persoon c.q. afdeling waar betrokkenen hun verzoek in kunnen dienen teneinde hun rechten uit te oefenen tegen ORO.

Een verantwoordelijke is op grond van de Wmd verplicht om een beveiligingsincident te kwalificeren als mogelijk datalek conform artikel 34a Wbp. Niet ieder datalek behoeft melding aan de Autoriteit Persoonsgegevens (hierna te noemen: AP) De meldplicht is gebaseerd op een risicocriterium. Dat houdt in dat objectief gekeken wordt of het lek heeft geleid tot het intreden van een aannemelijk gevolg. Dat aannemelijk gevolg is dat de verwerkte persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking, dan wel dat dat redelijkerwijs niet uitgesloten kan worden. Wordt hieraan voldaan dan is melding aan de AP vereist. Vervolgens dient de verantwoordelijke af te wegen of het lek (mogelijk) nadelige gevolgen heeft voor de persoonlijke levenssfeer van de betrokkene(n). Indien dat het geval is, dient het lek ook aan de betrokkene(n) gemeld te worden. Onderzoek wijst uit dat een procedure meldplicht datalekken, die zowel de interne melding door medewerkers als externe melding aan de AP en mogelijk de betrokkene(n) regelt, ontbreekt binnen ORO.

De Wmd, ingetreden per 1 januari 2016, heeft een drietal wijzigingen teweeg gebracht binnen de Wbp.

- Allereest zijn de sanctionerende bevoegdheden van de AP verruimd. Voorheen kon de AP slechts bij overtreding van administratieve voorschriften een boete opleggen van maximaal € 4.500,-. In de nieuwe situatie kan de AP boetes opleggen bij overtreding van alle voorschriften van de Wbp, waaronder ook de materiële voorschriften, waarbij het maximum van de boete € 810.000,- bedraagt, of, indien dat naar oordeel van de AP onvoldoende hoog is, 10% van de jaaromzet van een rechtspersoon;
- Ten tweede reikt de Wbp de AP een nieuw handhavingsinstrument aan: de bindende aanwijzing. De AP legt in beginsel een bindende aanwijzing op alvorens zij beboet. De bindende aanwijzing is een besluit tot naleving van de Wbp;
- Tot slot impliceert de Wbp na inwerkingtreding van de Wmd een ketenaansprakelijkheid voor de verantwoordelijke en de bewerkers van gegevens. De verantwoordelijke is in beginsel eindverantwoordelijk voor de verwerkingen door bewerkers. Door middel van bewerkersovereenkomsten kunnen afspraken gemaakt worden over de aansprakelijkheid van partijen.

Wanneer de AVG in werking treedt, vervallen de Wbp en Wmd. Ook de inwerkingtreding van de AVG brengt wijzigingen teweeg op het gebied van privacywetgeving. Het juridisch kader schetst op basis van wetgevings- en literatuuronderzoek ook de verplichtingen voor de verwerking van persoonsgegevens op grond van de aanstaande AVG. De rechten van betrokkenen worden uitgebreid met het ‘recht om te wissen’. Ook stelt de AVG stelt een Functionaris Gegevensbescherming (hierna te noemen: FG) verplicht bij de verwerking van persoonsgegevens van 250 betrokkenen per kalenderjaar. Nu ORO de persoonsgegevens van meer 250 betrokkenen per kalenderjaar verwerkt, voldoet zij aan deze norm. De FG is een natuurlijk persoon die wordt aangewezen op grond van diens professionele kwaliteiten, in het bijzonder de kwaliteiten met betrekking tot deskundigheid op het gebied van (privacy)wetgeving en praktijkervaring met bescherming van persoonsgegevens. De FG vervult zowel de rol van adviseur als toezichthouder binnen een organisatie. De FG opereert onafhankelijk van ORO: een FG staat niet onder toezicht van de Raad van Bestuur en hoeft derhalve ook geen verantwoording af te leggen. De AVG codificeert tevens twee privacybeginselen: Privacy by Design en Privacy by Default. Deze beginselen hebben betrekking op de gehele levenscyclus van persoonsgegevens. Deze beginselen dienen structureel in de bedrijfsvoering te worden opgenomen, teneinde verwerkingen van persoonsgegevens rechtmatig te laten geschieden. Om de bescherming van persoonsgegevens bij de verwerking hiervan continu te monitoren, reikt de AVG een instrument aan: het Privacy Impact Assessment (hierna te noemen: PIA). Indien er grote

wijzigingen plaatsvinden in de wijze van verwerking van persoonsgegevens, dient de verantwoordelijke een PIA uit te voeren. Een PIA is een risicoanalyse die de verantwoordelijke inzet bij grote wijzigingen in registratie- of verwerkingssystemen van gegevens van betrokkenen. Daarnaast bevat ook de AVG een meldplicht datalekken. Deze is grotendeels hetzelfde als de huidige Wmd: de meldplicht van de AVG verengd de termijn voor onverwijlde melding aan de autoriteit van 72 naar 24 uur na constatering. Tot slot biedt de AVG de autoriteit sanctionerende bevoegdheden. Bij overtreding van de rechtmatige verwerking van persoonsgegevens, kan een boete opgelegd worden van maximaal € 1 miljoen of 5% van de wereldwijde omzet van een onderneming.

Naast de voorgaande wettelijke vereisten omtrent de verwerking van persoonsgegevens, zijn er binnen ORO maatregelen genomen om de beveiliging van persoonsgegevens te borgen. Zo tekenen cliënten die in zorg treden bij ORO een toestemmingsverklaring omtrent het uitwisselen van hun persoonsgegevens met andere zorginstanties. Er is ook een reglement persoonsgegevens voor cliënten, maar dit is verouderd en wordt niet meer aan cliënten verstrekt. Medewerkers tekenen bij indiensttreding een overeenkomst met daarin een artikel omtrent geheimhouding. Voorts krijgen zij een gedragscode Social Media uitgereikt. Op locaties van ORO waar administratie gevoerd wordt, werkt men met oud-papier- en vernietigbakken. De vernietigbakken bevatten oud papier met gevoelige dan wel persoonsgegevens. Deze bakken worden éénmaal per week door een medewerker van Atlant-groep geleegd in een afsluitbare container. ORO werkt met reguliere printers die niet uitgerust zijn met bijvoorbeeld een follow-me-systeem. Binnen ORO heerst een clear-screen-policy: dat houdt in dat een medewerker het computerscherm dient te vergrendelen wanneer de werkplek verlaten wordt. USB-poorten voor computers zijn in beginsel uitgeschakeld. Er wordt gewerkt met een gelaagde sleutelstructuur op de locaties. Iedere medewerker heeft een sleutel van de poort, voordeur en diens eigen kantoor. Enkele medewerkers hebben de autorisatie het alarm van een locatie in- of uit te schakelen en er zijn ook medewerkers die een loper hebben van een locatie. Op het Centraal Bureau is ieder kantoor voorzien van afsluitbare (archief)kasten. Op locatie de Rakthof is alleen de deur van het archief af te sluiten, maar de archiefkasten niet. Tot slot zijn er enkele afdelingen en teams die een Whatsapp-groep hebben voor werk-gerelateerde onderwerpen.

Samenvattend wordt geconcludeerd dat ORO voldoet niet aan de Wbp en Wmd en dus ook nog niet aan de AVG. Er vinden onrechtmatige verwerkingen van persoonsgegevens plaats. Bij deze onrechtmatige verwerkingen ontbreekt het verzamelingsdoel conform artikel 8 Wbp of wordt niet aan het kwaliteitsbeginsel van artikel 11 Wbp voldaan. Een onrechtmatige verwerking is bijvoorbeeld de verzameling van de partnergegevens van de medewerkers van ORO. Ook worden gegevens langer bewaard dan wettelijke bewaartermijnen toestaan. Sommige gegevens worden geheel niet vernietigd. Er zijn geen interne procedures opgesteld waarmee betrokkene(n) om hun rechten jegens de verantwoordelijke uit kunnen te oefenen: ook niet voor het nieuwe ‘recht om te wissen’ dat uit de AVG voortvloeit. Verwerkingen van persoonsgegevens vinden niet transparant plaats. De verplichtingen omtrent de Wmd heeft ORO niet geborgd in haar bedrijfsvoering en –processen. Zij voldoet daarmee geheel niet aan hetgeen de Wmd stelt. De verplichtingen die voortvloeien uit de AVG heeft ORO niet ingeregeld, maar deze wetgeving is nog niet ingetreden. De beginselen Privacy by Design en Privacy by Default zijn niet geborgd in de bedrijfsprocessen van ORO en ORO heeft geen Functionaris Gegevensbescherming in dienst.

5.2 Aanbevelingen

Op de volgende pagina staan de aanbevelingen die voortvloeien uit voornoemde conclusies. De aanbevelingen zijn opgedeeld in wettelijke aanbevelingen en algemene aanbevelingen.

Wettelijke aanbevelingen
Per aanbeveling staat aangegeven op welke wet(ten) de aanbeveling betrekking heeft.

Verwerkingen persoonsgegevens (Wbp, Wmd)
Gedurende dit onderzoek zijn de verwerkingen van persoonsgegevens intern, door medewerkers van ORO, in kaart zijn gebracht. Aanbevolen wordt om dit document officieel vast te stellen dan wel aan te vullen. Indien de verwerkingen worden aangevuld, toets de bewerkingen dan op rechtmatigheid. Stop direct met verwerkingen die onrechtmatig zijn en maak, indien en voor zover mogelijk, de onrechtmatige verwerkingen ongedaan. In Bijlage 18 is een kader opgesteld om legitimatie van gegevensverwerking te toetsen.

Breng in kaart welke stakeholders bewerkers zijn van persoonsgegevens. Legitimeer van de externe verwerkingen of deze rechtmatig plaatsvinden. Indien verwerkingen onrechtmatig plaatsvinden, stop dan per direct met deze verwerkingen en maak, indien en voor zover mogelijk, de onrechtmatige verwerkingen ongedaan.

Bewerkersovereenkomst (Wbp, Wmd)
Aanbevolen wordt om met bewerkers een bewerkersovereenkomst te sluiten. Hiervoor dienen eerst de stakeholders gekwalificeerd te worden als mogelijk bewerker. De enige bewerker waarvan bekend is dat hiermee een bewerkersovereenkomst is gesloten, is AFAS. Wanneer de bewerkers gekwalificeerd zijn, dient met hen een bewerkersovereenkomst gesloten te worden. In Bijlage 19 is een voorbeeld opgenomen van een bewerkersovereenkomst. Deze bewerkersovereenkomst is toegespitst op de verplichtingen van de Wbp en Wmd omtrent verwerkingen van persoonsgegevens.

Wanneer ORO een andere bewerkersovereenkomst opstelt, dient deze ten minste te bevatten: welke persoonsgegevens de bewerker in opdracht van de verantwoordelijke verwerkt en welke maatregelen de bewerker dient te nemen bij deze verwerkingen. Het is gebruikelijk om voor de verantwoordelijke een controlemogelijkheid te scheppen in de vorm van een audit. Indien van toepassing, neem op hoe deze audit uitgevoerd wordt en op wiens kosten.

Voorts regelt de overeenkomst de looptijd en de beëindigingsmogelijkheden van de overeenkomst alsook wat er na afloop van de overeenkomst met de persoonsgegevens gebeurt. Hecht de separate bewerkersovereenkomst aan de hoofdovereenkomst die reeds bestaat met de bewerker.

Rechten van betrokkenen (Wbp, AVG)
De rechten van betrokkenen vloeien voort uit de wet. Stel een interne procedure voor betrokkenen en beschrijf in deze procedure wat de rechten van betrokkenen inhouden en bij welke aangewezen persoon c.q. afdeling betrokkenen hun verzoek in kunnen dienen. Er is een procedure opgesteld voor ORO in Bijlage 20.

Wijs een persoon of afdeling aan die deze verzoeken in behandeling neemt en verwerkt. Zorg ervoor dat deze aangewezen persoon c.q. afdeling voldoende mandaat verkrijgt van de verantwoordelijke: in dezen de Raad van Bestuur.

Breid de procedure bij inwerkingtreding van de AVG uit met het ‘recht om te wissen’ en stel betrokkenen van deze uitbreiding en de inhoud van de uitbreiding op de hoogte.

Meldplicht datalekken (Wbp, Wmd, AVG)
Aanbevolen wordt een procedure meldplicht datalekken op te stellen. De procedure is tweeledig.

Stel intern een procedure op voor medewerkers die een lek constateren. Neem op waar medewerkers een lek kunnen melden, hoe ze deze melding moeten doen en van welke bescheiden deze melding voorzien moet zijn. Koppel aan de melding een termijn, waarbij het haalbaar is voor de aangewezen persoon of afdeling die de melding verwerkt, het lek binnen

een termijn van 72 uur na constatering te melden aan de AP. In Bijlage 22 is een opzet voor deze interne en externe meldingsprocedure opgenomen.

Stel daarnaast een procedure op voor de aangewezen persoon c.q. afdeling die de meldingen ontvangt en verwerkt. Geef deze aangewezen persoon of afdeling mandaat namens de verantwoordelijke en geef de persoon of afdeling handvatten voor de beoordeling van het lek. De stroomschema's, zoals opgenomen in Bijlagen 3 tot en met 8, zijn handvatten afkomstig van het AP en kunnen derhalve geraadpleegd worden bij de beoordeling van een lek. Neem in deze procedure ook de plicht op om een register van de meldingen bij te houden.

Zorg dat voornoemde procedure eenduidigheid geeft over de wijze van melden bij de AP (dus schriftelijk of digitaal) en doe hetzelfde voor de melding aan de betrokkene(n). Wanneer de Functionaris Gegevensbescherming aangesteld is, kunnen deze taken aan deze persoon worden overgedragen. Wijzig de procedure bij inwerkingtreding van de AVG: de AVG verengd de termijn van onverwijld melden van 72 uur naar 24 uur na constatering van het lek.

Functionaris Gegevensbescherming (AVG)
Aanbevolen wordt om een functieprofiel op te stellen voor een Functionaris Gegevensbescherming waarbij gelet wordt op het type onderneming dat ORO is. Zorg dat bij inwerkingtreding van de AVG de Functionaris Gegevensbescherming in dienst is bij ORO.

Privacy Impact Assessment (AVG)
Aanbevolen wordt een procedure op te stellen omtrent het Privacy Impact Assessment. Beschrijf in deze procedure wanneer een PIA plaats dient te vinden binnen ORO en hoe deze PIA uitgevoerd gaat worden.

Afhankelijk van welke groep betrokkenen de PIA treft (medewerkers of cliënten), wordt aanbevolen de OR dan wel de CCR te betrekken bij het opstellen van deze procedure.

Privacy by Design en Privacy by Default (AVG)
Aanbevolen wordt om bij inwerkingtreding van de AVG deze twee beginselen reeds ingebed te hebben in de bedrijfsvoering van ORO. Privacy by Design en Privacy by Default zijn beginselen die beiden betrekking hebben op de gehele levensduur van persoonsgegevens.

Privacy by Design stelt dat aandacht voor vertrouwelijkheid, integriteit, veiligheid en voor de verwijdering van persoonsgegevens structureel geborgd moet worden in de bedrijfsvoering. Aan Privacy by Design wordt bijvoorbeeld voldaan wanneer ORO rekening houdt met dataminimalisatie. Dat wil zeggen dat bij ieder gegeven dat verzameld wordt continu getoetst wordt of dat het gegeven noodzakelijk is voor de verwerking. Indien dat niet het geval is, wordt het gegeven niet verwerkt. Rekening houden met privacy bij de ontwikkeling of aanschaf van nieuwe verwerkingssystemen past bij dit beginsel.

Privacy by Default houdt in dat systeeminstellingen van apps en computers dusdanig zijn ingesteld dat maximale privacy betracht wordt. Pas als iemand iets 'aanvinkt' op de website, worden er gegevens van hem of haar verzonden, in plaats dat er het verzenden stopt als je iets 'aanvinkt'. Eerst goedkeuring van de betrokkene, pas dan het verzenden van gegevens.

Algemene aanbevelingen
Onderstaand de algemene aanbevelingen ter bevordering van de situatie met betrekking tot privacy binnen ORO. Deze aanbevelingen vloeien niet direct uit een wettelijke verplichting voort, maar faciliteren een situatie binnen ORO waardoor de kans op overtreding van de wettelijke voorschriften verkleind wordt.

Intern privacy-awareness beleid

Aanbevolen wordt een intern privacy-awareness beleid te voeren voor medewerkers van ORO. Medewerkers zijn de ogen en oren van een organisatie: een datalek wordt naar verwachting dan ook meestal geconstateerd door een medewerker. Het is van belang dat een medewerker weet wat een datalek is en inhoud: anders wordt een lek ook niet gemeld aan de daartoe gemandateerde persoon c.q. afdeling.

Aanbevolen wordt om in het beleid onder meer aandacht te schenken aan de items (interne en externe) datalekken, clear-screen-policy, de rechten van betrokkenen, informatie-uitwisseling via Whatsapp en het beheer van het eigen, digitale personeelsdossier. Awareness beleid kan gevoerd worden door middel van posters en flyers, maar ook middels informatieve bijeenkomsten of workshops.

Printers/multifunctionals

Aanbevolen wordt bij het afsluiten van een nieuw leasecontract voor printers/multifunctionals de nieuwe en aanstaande privacywetgeving in acht te nemen. Het leasecontract van de printers van ORO loopt medio september van dit jaar af. De huidige printers zijn reguliere printers, die niet uitgerust zijn met een follow-me-systeem.

Aanbevolen wordt de nieuwe printers/multifunctionals uit te rusten met bijvoorbeeld een follow-me-systeem, druppel of pincode. De kans dat medewerkers documenten met gevoelige informatie afdrukken en vervolgens niet ophalen bij de printer/multifunctional is dan minimaal. Interne datalekken (met betrekking tot niet-opgehaalde printopdrachten) worden zo maximaal beperkt.

Bronnen- en literatuurlijst

Literatuur

Brahn & Reehuis 2010
O.K. Brahn & W.H.M Reehuis, *Zwaartepunten van het vermogensrecht*, Deventer: Kluwer 2010.

Duthler & Biesheuvel 2013
A. Duthler & A. Biesheuvel, *Het Europees privacyrecht in beweging, Overzicht van actuele ontwikkelingen en mogelijke consequenties voor werkzaamheden van IT-auditors*, februari 2013.

Van Elk & Van Elswijk 2015
W.-J. van Elk & M. van Elswijk, *Cloud Computing: het juridisch kader*, Utrecht 2015.

Fennell, Kroes & Koppejan 2015
S. Fennel, R. Kroes & F. Koppejan, *Privacy wetgeving – inclusief voorgestelde meldplichten, boetes en concept Algemene Verordening Gegevensbescherming*, Deventer: Kluwer 2015.

Grit 2011
R. Grit, *Projectmanagement*, Deventer: Kluwer 2011.

Hutter, Katus, Terstegge & Vermissen 2015
J. Hutter, S. Katus, J. Terstegge & K. Vermissen, *Grip op datalekken*, Deventer: Kluwer 2015.

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

Leidraad voor Juridische auteurs 2013
M.H. Bastiaans e.a., *Leidraad voor Juridische auteurs 2013*, Deventer: Kluwer 2013.

Mouwe 2011
K. Mouwe, *Handboek strategisch management voor de non-profit organisatie*, Koninklijke van Gorcum, 2011.

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

Tel 2006
G. Tel, *Cryptografie: de beveiliging van de digitale maatschappij*, Utrecht, 2006.

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.

Handleidingen

Autoriteit Persoonsgegevens, *Beleidsregels voor toepassing van artikel 34a Wbp*, 2015.

Autoriteit Persoonsgegevens, *Naslag artikel 66 Wbp*, 2016.

College bescherming persoonsgegevens, *CBP Richtsnoeren beveiliging van persoonsgegevens,* 2013.

Groep Gegevensbescherming artikel 29, 'Advies 5/2014 over anonimiseringstechnieken'.

Kamerstukken
Kamerstukken I 2014/2015 33 662 nr. C, *Memorie van Antwoord Wet Meldplicht Datalekken*

Kamerstukken II 2012/2013 33 662 nr. 3, *Memorie van Toelichting Wet Meldplicht Datalekken*

Kamerstukken II 2013/2014 33 662 nr. 6, *Nota naar aanleiding van het verslag*

Kamerstukken II 2013/2014 33 662 nr. 7, *Nota van wijziging*

Kamerstukken II 2014/2015 33 662 nr. 9, *Tweede nota van wijziging*

Kamerstukken II 2014/2015 33 662 nr. 11, *Nota naar aanleiding van het nader verslag*

Kamerstukken II 2014/2015 33 662 nr. 24, *Gewijzigde motie van het lid Oskam C.S. ter vervanging van die gedrukt onder nr. 21*

Handelingen Tweede Kamer 2014/2015 33 662 nr. 51, item 9, *Vergadering Tweede Kamer van 5 februari 2015 inzake de behandeling van het wetsvoorstel 'Wijziging van de Wet bescherming persoonsgegevens en enige andere wetten in verband met de invoering van een meldplicht bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens, alsmede uitbreiding van de bevoegdheid van het College bescherming persoonsgegevens om bij overtreding van het bepaalde bij of krachtens de Wet bescherming persoonsgegevens een bestuurlijke boete op te leggen (meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid Cbp) (33 662)'.*

Rechtshandelingen Europese Unie
COM (2012) 10 def.

COM (2012) 11 def.

Aangenomen Teksten Europees Parlement, 1314, vergadering 12 maart 2014 deel I, PE 531.357.

Artikelen
Gemeente Amersfoort lekt zorggegevens 12 april 2016, *Algemeen Dagblad*, www.ad.nl (zoek op: *gegevenslek*), laatst geraadpleegd op 3 mei 2016.