
JE HOEFT NIET ALLES TE WETEN

Een praktijkgericht juridisch onderzoek naar de verwerkingsprocessen van de persoonsgegevens van de burger, in het kader van de inwerkingtreding van de Algemene verordening gegevensbescherming, binnen de gemeente Oosterhout.



Projectnaam: Je hoeft niet alles te weten

Projectomschrijving: Onderzoeksrapport

Opdrachtgever: gemeente Oosterhout

Begeleider: mevrouw mr. J.J.J. (Jolanda) Kerremans

Auteur: Milou Boeren (2071704)

Onderzoekperiode: februari tot en met mei 2018

Plaats en datum: Oosterhout, 28 mei 2018

Eerste docent: de heer mr. B.C.M. (Bart) Hooijdonk

Tweede docent: de heer Drs. J.R.H.V.J. (Jasper) Oltheten

Opleidingsinstituut: Juridische Hogeschool Avans-Fontys, te Tilburg

JE HOEFT NIET ALLES TE WETEN

Een praktijkgericht juridisch onderzoek naar de verwerkingsprocessen van de persoonsgegevens van de burger, in het kader van de inwerkingtreding van de Algemene verordening gegevensbescherming, binnen de gemeente Oosterhout.

Projectnaam: Je hoeft niet alles te weten.

Projectomschrijving: Onderzoeksrapport

Opdrachtgever: gemeente Oosterhout

Begeleider: mevrouw mr. J.J.J. (Jolanda) Kerremans

Auteur: Milou Boeren (2071704)

Onderzoekperiode: februari tot en met mei 2018

Plaats en datum: Oosterhout, 28 mei 2018

Eerste docent: de heer mr. B.C.M. (Bart) Hooijdonk

Tweede docent: de heer Drs. J.R.H.V.J. (Jasper) Oltheten

Opleidingsinstituut: Juridische Hogeschool Avans-Fontys, te Tilburg

Voorwoord

Voor u ligt het onderzoeksrapport 'Je hoeft niet alles te weten' omtrent het rechtmatig verwerken van persoonsgegevens door de gemeente Oosterhout, naar aanleiding van de inwerkingtreding van de Algemene verordening gegevensbescherming. Dit onderzoeksrapport is geschreven ter afsluiting van mijn opleiding HBO-Rechten aan de Juridische Hogeschool Avans-Fontys en is het sluitstuk van een afstudeerstage bij de gemeente Oosterhout. Het onderzoeksrapport is specifiek geschreven op basis van de verwerkingsprocessen die bij de gemeente Oosterhout worden uitgevoerd. Het onderzoek is in een periode van vier maanden uitgevoerd. Gedurende deze periode heb ik veel mogen leren. Het combineren van wettelijke verplichtingen en praktische oplossingen was de grootste uitdaging.

Ik ben dankbaar voor de kans die mij is geboden door de opdrachtgever, de gemeente Oosterhout, om het onderzoek naar eigen inzichten in te vullen. Mijn tevredenheid over het eindresultaat is mede dankzij de hulp van Jolanda Kerremans en Gildardo Gaviria. Bedankt voor alle begeleiding en steun de afgelopen maanden. Dankzij de opbouwende feedback en brainstormsessies heb ik veel geleerd en met veel plezier gewerkt.

Daarnaast wil ik alle geïnterviewden bedanken voor alle tijd die is vrijgemaakt in hun drukke agenda's voor het beantwoorden van al mijn vragen. De medewerkers van de afdeling BCA bedank ik voor de gezellige werksfeer en alle koffierondjes. De heer Hooijdonk en de heer Oltheten bedank ik voor de antwoorden op al mijn vragen, die vaak dezelfde dag nog per e-mail werden beantwoord.

Rest mij niets meer dan u veel plezier toe te wensen tijdens het lezen.

Milou Boeren

Oosterhout, 28 mei 2018

Inhoudsopgave

Samenvatting

Lijst met afkortingen

Hoofdstuk 1: Inleiding.....	7
§1.1 Probleembeschrijving	7
§1.2 Doelstelling, centrale vraag en deelvragen.....	7
§1.3 Verantwoording.....	8
§1.4 Leeswijzer	9
Hoofdstuk 2: De introductie van de Avg & de tegenstrijdigheid van transparantie en vertrouwelijkheid.....	10
§2.1 De tien speerpunten van de Algemene verordening gegevensbescherming	10
§2.2 De spanning tussen openbaarheid van bestuur en vertrouwelijkheid van persoonsgegevens	12
§2.3 De dagelijkse bedrijfsvoering binnen de gemeente Oosterhout	14
§2.4 Samenvatting en conclusie	15
Hoofdstuk 3: Wat is de verantwoording van de verwerkingsverantwoordelijke?	16
§3.1 Het verwerkingsregister.....	16
§3.2 De verwerkingsovereenkomst	17
§3.3 Het data protection impact assessment	18
§3.4 Functionaris gegevensbescherming.....	20
§3.5 Verantwoording aan het college van burgemeester en wethouder	20
§3.6 Samenvatting.....	21
Hoofdstuk 4: De uitvoering van het data protection impact assessment.....	22
§4.1 Verplichtingen vanuit de Avg.....	22
§4.2 Het toetsingskader van NOREA.....	22
§4.3 NOREA in de praktijk.....	23
§4.4 Samenvatting en conclusie	24
Hoofdstuk 5: Welke rechten heeft de burger?	26
§5.1 Verplichtingen vanuit de Algemene verordening gegevensbescherming.....	26
§5.2 Beroepbare rechten.....	28
§5.3 De procedure omtrent de beroepbare rechten.....	30
§5.4 Datalekken.....	31
§5.5 Samenvatting.....	33

Hoofdstuk 6: De beroepbare rechten van de burger vòòr de Avg.....	34
§6.1 De vier beroepbare rechten van de basisregistratiepersonen.....	35
§6.2 De werkwijze van de frontoffice	36
§6.3 De inhoudelijke behandeling bij de backoffice	37
§6.4 Samenvatting en conclusie	39
Hoofdstuk 7: Het nieuwe bedrijfsproces	40
§7.1 Het nieuwe bedrijfsproces in vijf stappen	40
§7.2 De deelnemers van het nieuwe primaire proces	42
§ 7.3 Samenvatting.....	43
Hoofdstuk 8: De datalekprocedure van de gemeente Oosterhout.....	44
§8.1 Datalekken in de praktijk	44
§8.2 Samenvatting en conclusie	45
Hoofdstuk 9: Conclusies en aanbevelingen	46
§9.1 Conclusies.....	46
§9.2 Aanbevelingen	48
Hoofdstuk 10: Literatuurlijst.....	49
§10.1 Literatuur	49
§ 10.2 Elektronische bronnen.....	50
§10.3 Jurisprudentie.....	50
§10.4 Wet- en regelgeving	51

Samenvatting

De Algemene verordening gegevensbescherming (hierna te noemen: 'Avg') treedt op 25 mei 2018 in werking. De gemeente Oosterhout zal vanaf dat moment alle persoonsgegevens moeten verwerken volgens de Avg. De Avg zorgt middels tien speerpunten voor een groot aantal waarborgen van de persoonsgegevens. De speerpunten zijn: bewustwording van de komst van de Avg, de nieuwe rechten van de burger waarborgen, de gemeente moet een verwerkingsregister opstellen, de gemeente moet data protection impact assessments (hierna te noemen: 'DPIA's') uitvoeren op risicovol beleid met betrekking tot de verwerking van persoonsgegevens, bij het opstellen van het beleid moet al gekeken worden of de verwerking van persoonsgegevens noodzakelijk is en op welke manier dit gebeurt, er moet een functionaris gegevensbescherming aangewezen worden en alle datalekken moeten gedocumenteerd worden.

Naast het waarborgen van de persoonsgegevens zal de gemeente Oosterhout als bestuursorgaan ook transparant moeten handelen. Deze twee plichten kunnen voor tegenstrijdigheid zorgen bij het openbaren van stukken met een bestuurlijk karakter. Hierbij is te denken aan bezwaar dat is ingediend door een burger naar aanleiding van een bestemmingsplan. Deze stukken moeten in het kader van transparantie geopenbaard worden, maar in deze stukken staan ook persoonsgegevens vermeld.

Een van de speerpunten is het uitvoeren van DPIA's. De gemeente Oosterhout gebruikt hiervoor NOREA. In NOREA worden de wettelijke verplichtingen rondom de DPIA meegenomen. NOREA beoordeelt het verwerkingsproces op acht punten: het type project, de persoonsgegevens die gebruikt worden, de partijen die betrokken zijn bij de uitvoering, het verzamelen van persoonsgegevens, het gebruiken van persoonsgegevens, het bewaren en vernietigen van persoonsgegevens, het beveiligen van persoonsgegevens en de meldplicht datalekken.

Een ander speerpunt is het waarborgen van de nieuwe rechten van de burger. De burger heeft acht beroepbare rechten gekregen en kan een actief beroep doen op grond van deze rechten. De burger kan een verzoek indienen om zijn of haar persoonsgegevens in te zien of te laten wijzigen, wissen, beperkt laten verwerken, versturen naar een andere verwerkingsverantwoordelijke, bezwaar maken, geautomatiseerde besluitvorming stoppen en om een schadevergoeding vragen. De gemeente Oosterhout is verplicht aan deze verzoeken gehoor te geven. De wettelijke vereisten moeten wel in acht genomen worden. Na het observeren en bestuderen van het (be)handelen van de bestaande rechten binnen de gemeente Oosterhout, is besloten om een nieuw verwerkingssysteem te maken. In het nieuwe systeem worden de rechten van de burgers behandeld. De behandeling van het verzoek op een beroepbare recht is in vijf stappen opgedeeld. Stap 1 is het verzoek aannemen. Het aannemen kan zowel digitaal als analoog. Stap 2 is het beoordelen van het verzoek. De beoordeling is formeel en inhoudelijk. Nadat de beoordeling is afgerond, wordt het verzoek naar de afdelingen gestuurd voor de uitvoering, dit is stap 3. Wanneer de afdeling het verzoek heeft uitgevoerd wordt nogmaals gecontroleerd of het verzoek goed is uitgevoerd. Het tweede controle moment is stap 4. Als laatste stap, stap 5, wordt het besluit omtrent het verzoek naar de burger verzonden.

Het laatste speerpunt dat binnen dit onderzoek wordt behandeld is het datalekprotocol. De gemeente Oosterhout heeft een meldingsprotocol rondom de constatering van een datalek opgesteld. Aan de hand van twee casussen is te zien dat het protocol daadwerkelijk wordt gevolgd.

[Lijst met afkortingen](#)

Awb	Algemene wet bestuursrecht
Avg	Algemene verordening gegevensbescherming
Bibob	Wet bevordering integriteitsbeoordelingen door het openbaar bestuur
BSN	burgerservicenummer
BRP	Wet basisregistratie personen
DPIA	Data protection impact assessment
EVRM	Europees Verdrag voor de Rechten van de Mens en de Fundamentele Vrijheden
Wbp	Wet bescherming persoonsgegevens
Wob	Wet openbaarheid van bestuur

Hoofdstuk 1: Inleiding

In het eerste hoofdstuk wordt de aanleiding van het onderzoek besproken. Vervolgens wordt gekeken welke vragen centraal staan in het onderzoek en voor welke onderzoeksmethoden zijn gekozen.

§1.1 Probleembeschrijving

De gemeente Oosterhout is een informatieverwerkende organisatie. Dienstverlenende organisaties (en andere instellingen) verschaffen de gemeente Oosterhout een groot aantal persoonsgegevens. De burgers vullen deze persoonsgegevens vaak ook nog aan. De gemeente Oosterhout heeft deze persoonsgegevens nodig om de publiekrechtelijke taken uit te voeren en om te voldoen aan de wettelijke verplichtingen. Het verwerken van de persoonsgegevens is noodzakelijk voor een goed functionerende gemeente. Hierbij is te denken aan het verstrekken van paspoorten en uitkeringen, maar ook om de openbare orde te beschermen. Om de gegevensstroom in goede banen te leiden is het van belang dat de privacywetgeving wordt nageleefd en de persoonsgegevens van de burger worden beschermd. De gemeente Oosterhout verwerkt persoonsgegevens van eenieder die woonachtig is in Oosterhout, Dorst, Oosteind en Den Hout.

Vanuit Europa is een verordening opgesteld genaamd de Avg waar vanaf 25 mei 2018 aan voldaan moet worden. De gemeente Oosterhout moet dus vanaf 25 mei 2018 handelen conform de Avg. De gehele verordening moet geïmplementeerd worden en naast de huidige nationale wetgeving worden uitgevoerd. Dit zorgt voor een aantal knelpunten. Het eerste knelpunt is het dilemma tussen een open overheid en gegevensbescherming. De gemeente Oosterhout heeft als overheidsorgaan de verplichting om zo transparant mogelijk te werk te gaan, maar de persoonsgegevens moeten ook worden beschermd. Tussen deze twee waarden zal een middenweg moeten worden gevonden. Het tweede knelpunt gaat over de inrichting van de verantwoordingsplicht binnen de gemeente Oosterhout. De verwerkingsprocessen met betrekking tot de verwerking van persoonsgegevens zullen inzichtelijk gemaakt moeten worden. Op deze manier kan gekeken worden naar de veiligheid van de persoonsgegevens. Het derde knelpunt dat binnen dit project wordt belicht zijn de rechten de burger. Voor de burger zijn er al procedures opgesteld voor het recht op inzage, correctie en bezwaar. Voor de overige rechten van de burger zal nog een procedure moeten worden opgesteld. Deze rechten moeten goed uit te voeren zijn en eenvoudig beroepbaar. Daarnaast wordt ook gekeken naar de procedure en maatregelen naar aanleiding van de geconstateerde datalekken. Dit is het vierde knelpunt. Om aan de Avg te voldoen, moet de gemeente Oosterhout nog een aantal verwerkingsprocessen van persoonsgegevens onder de loop nemen.

§1.2 Doelstelling, centrale vraag en deelvragen

Doelstelling: 28 mei 2018 heb ik een procedure opgesteld om de beroepbare rechten van de burgers volgens de Algemene verordening gegevensbescherming te waarborgen en is er een data protection impact assessment opgesteld om het privacygevoelig beleid van de gemeente Oosterhout te testen.

Centrale vraag: Aan welke juridische voorwaarden moet de gemeente Oosterhout voldoen om haar verwerkingsprocessen van persoonsgegevens van de burgers in overeenstemming met de Algemene verordening gegevensbescherming te laten lopen?

Deelvraag 1: Wat moet de gemeente Oosterhout doen om te voldoen aan de wettelijke bepalingen vanuit de Algemene verordening gegevensbescherming, die zien op de waarborging van persoonsgegevens en de Wet openbaarheid van bestuur waarin een transparante overheid centraal staat?

Deelvraag 2: Welke eisen stelt de Algemene verordening gegevensbescherming aan de gemeente Oosterhout met betrekking tot de verantwoordingsplicht?

Subdeelvraag 2.A: Aan welke voorwaarden moet een procedure voldoen voor de uitvoering van een data protection impact assessment, zoals omschreven in de Algemene verordening gegevensbescherming, om aan te sluiten bij de bedrijfsvoering van de gemeente Oosterhout?

Deelvraag 3: Welke eisen stelt de Algemene verordening gegevensbescherming aan de gemeente Oosterhout met betrekking tot de rechten van de burgers en de procedure datalekken?

Subdeelvraag 3.A: Hoe wordt voor de inwerkingtreding van de Algemene verordening gegevensbescherming door de gemeente Oosterhout omgegaan met de beroepbare rechten van de burger vanuit de Wet basisregistratie personen?

Subdeelvraag 3.B: Welke handelingen zijn van belang voor het waarborgen van de beroepbare rechten van de burgers op basis van de Algemene verordening gegevensbescherming in de dagelijkse bedrijfsvoering van de gemeente Oosterhout?

Subdeelvraag 3.C: Wat is de huidige handelingswijze van de Gemeente Oosterhout bij het signaleren van een datalek?

§1.3 Verantwoording

Deelvraag 1 is een theoretische vraag. Om deze reden is vooral gekeken naar wetgeving, literatuur en jurisprudentie. Alleen de arresten van de Raad van State zijn gebruikt voor het onderzoek, omdat de Raad van State als de hoogste bestuursrechter van Nederland een rechtsregel vaststelt. Naast het theoretisch kader is ook gekeken naar de handelswijze van de gemeente Oosterhout met betrekking tot een verzoek op basis van de Wet openbaarheid van bestuur (hierna te noemen: 'Wob'). Er is gekozen om dit in kaart te brengen door een interview af te nemen met een ambtenaar van de afdeling Juridische Zaken. In het interview zijn ook naar een aantal praktijkvoorbeelden gevraagd. Aan de hand van de praktijkvoorbeelden is gekeken hoe daadwerkelijk wordt gehandeld.

Deelvraag 2 is beantwoord door het analyseren van de Avg en literatuur van de Autoriteit Persoonsgegevens. In het hoofdstuk komen alle aspecten van de verantwoordingsplicht terug die de Autoriteit Persoonsgegevens beschrijft.

In subdeelvraag 2.A worden de DPIA's behandeld. Het toetsingsmodel genaamd: 'NOREA' is als startpunt genomen. Dit model zorgt voor een goed startpunt, omdat de wettelijke vereisten erin zijn opgenomen en de Autoriteit Persoonsgegevens NOREA mede heeft opgesteld. De gemeente Oosterhout voerde voorheen geen soortgelijke toetsingen uit, dus naar de huidige stand van zaken is in dit onderzoek geen aandacht besteed. Er is gekozen om op het verwerkingsproces omtrent het Leerlingenvervoer een DPIA uit te voeren, omdat het een relatief klein verwerkingsproces is dat binnen een afdeling afgehandeld wordt. Het proces is goed in beeld te krijgen en daarom kan er een DPIA binnen korte tijd worden uitgevoerd. Het verwerkingsproces van de Bibob is gekozen, omdat dit een gecompliceerder verwerkingsproces is. Er worden veel (bijzondere) persoonsgegevens verzameld en met meerdere partijen worden deze persoonsgegevens gedeeld. Aan de hand van dit verwerkingsproces kan gekeken worden hoe wordt samengewerkt met andere partijen en hoe NOREA hieraan toetst.

Deelvraag 3 is een theoretische vraag. In deelvraag 3 is een beperking gemaakt op het begrip betrokkene. Onder het begrip betrokkene wordt binnen de reikwijdte van dit onderzoek verstaan: alle inwoners van de gemeente Oosterhout. Na deze groep wordt verwezen onder de noemer 'burger'. Deze keuze is gemaakt omdat het onderzoek in een kort tijdsbestek wordt uitgevoerd.

In deelvraag 3.A is onderzoek uitgevoerd naar de huidige methode van het behandelen van verzoeken op basis van de rechten van de burger. De Wet basisregistratie personen (hierna te noemen: 'BRP') is als uitgangspunt genomen voor het praktijkonderzoek. De Avg en de BRP geven de burgers soortgelijke rechten. Daarnaast is een procedure opgesteld voor de verzoeken op basis van de BRP. Omdat de gemeente Oosterhout al jaren werkt via een vast proces, leent het proces zich voor het uitvoeren van een praktijkonderzoek. Het onderzoek heeft betrekking op de handelswijze van de afdeling Burgerzaken bij het behandelen van de rechten van de burger op basis van de BRP. Om dit in beeld te krijgen is als eerste bij de frontoffice geobserveerd hoe de verzoeken worden aangenomen. Middels de observatieschema's is gedurende drie dagen gekeken welke persoonsgegevens werden opgevraagd en in welk systeem de gegevens verwerkt. Aan de hand van de observaties zijn interviews afgenomen. Tijdens de interviews zijn aan alle medewerkers die geobserveerd zijn soortgelijke vragen gesteld. Door het stellen van dezelfde vragen kan gekeken worden of het protocol daadwerkelijk wordt gevolgd. Alle medewerkers die geobserveerd zijn, zijn al minimaal twee jaar werkzaam bij de frontoffice. Dit vergroot de validiteit van het onderzoek. Naast het observeren van het innemen van de verzoeken is ook gekeken naar de beoordeling van de verzoeken. Om alle handelingen in kaart te brengen is gekozen voor een open observatieschema. Vervolgens is een interview afgenomen met een medewerker van de backoffice. De medewerker is al dertig jaar werkzaam bij de gemeente Oosterhout op de afdeling Burgerzaken. De interviews en de observatieschema's zijn terug te vinden in bijlage 6. Voordat de interviews zijn afgenomen is een cursus interviewtechnieken gevolgd door de auteur van dit onderzoek om de betrouwbaarheid te vergroten.

Subdeelvraag 3.B beschrijft het nieuw systeem wat de rechten van de burgers moet gaan waarborgen. Het proces is geschreven nadat de huidige methode was geanalyseerd. Vervolgens is in samenwerking met een ICT-specialist gekeken naar de technische mogelijkheden.

Subdeelvraag 3.C beschrijft het beleid en de handelswijze rondom de datalekken binnen de gemeente Oosterhout. De twee casussen die worden besproken in het hoofdstuk zijn datalekken die de gehele procedure al doorlopen hebben. De gemeente Oosterhout houdt sinds oktober 2017 een datalekregister bij. Er is gekozen om alleen oudere datalekken op te nemen in het hoofdstuk omdat de maatregelen die zijn genomen goed te analyseren zijn.

[§1.4 Leeswijzer](#)

De deelvragen worden in meerdere hoofdstukken besproken. Deelvraag 1 wordt in hoofdstuk 2 behandeld. Deelvraag 2 wordt in hoofdstuk 3 behandeld. Subdeelvraag 2.A wordt in hoofdstuk 4 en de bijlagen uiteengezet. Deelvraag 3 wordt in hoofdstuk 5 besproken. Subdeelvraag 3.A wordt in hoofdstuk 6 besproken. Subdeelvraag 3.B wordt in hoofdstuk 7 behandeld en in het beroepsproduct. De laatste Subdeelvraag 3.C wordt in hoofdstuk 8 behandeld. In hoofdstuk 9 worden conclusies getrokken en aanbevelingen gegeven.

Hoofdstuk 2: De introductie van de Avg & de tegenstrijdigheid van transparantie en vertrouwelijkheid

Nederland is een lidstaat van de Europese Unie. Binnen de Europese Unie zijn verdragen van kracht die iets zeggen over de werkwijze van de Europese Unie. Een verdrag waarin de werking van de Europese Unie uiteen wordt gezet is het werkingsverdrag van de Europese Unie. Volgens het werkingsverdrag van de Europese Unie heeft een verordening een directe werking binnen de lidstaten. Een verordening kan gezien worden als een wet op Europees niveau. Een verordening is afdwingbaar binnen de lidstaten en hoeft niet te worden omgezet in nationale wetgeving.¹ Verordeningen zijn dus rechtsgeldig binnen Nederland. De Avg is een verordening. Dit betekent dat de Avg van kracht is in Nederland. Iedereen die persoonsgegevens verwerkt, zal dit dus conform de Avg moeten doen. De gemeente Oosterhout zal daarom conform de Avg moeten handelen wanneer persoonsgegevens worden verwerkt. De vraag rijst welke eisen de Avg stelt aan de gemeente Oosterhout. Volgens het toezichthoudende orgaan, de Autoriteit Persoonsgegevens, wordt de Avg op een correcte wijze geïmplementeerd wanneer de tien speerpunten worden nageleefd. De Autoriteit Persoonsgegevens heeft tien speerpunten² opgesteld op basis van de veranderingen die de Avg met zich meebrengt. Deze speerpunten moeten dus in het oog worden gehouden door de gemeente Oosterhout. Vervolgens wordt ingegaan op de wettelijke tegenstrijdigheden en verplichtingen waarbinnen de gemeente Oosterhout te werk moet gaan. De vraag die in dit hoofdstuk centraal staat is: *‘Wat moet de gemeente Oosterhout doen om te voldoen aan de wettelijke bepalingen vanuit de Algemene verordening gegevensbescherming, die zien op de waarborging van persoonsgegevens en de Wet openbaarheid van bestuur waarin een transparante overheid centraal staat?’*

§2.1 De tien speerpunten van de Algemene verordening gegevensbescherming

Het eerste speerpunt is de bewustwording van de komst van de Avg. Binnen de gemeente Oosterhout wordt veelvuldig gewerkt met persoonsgegevens. Hierbij is te denken aan het verstrekken van uitkeringen of paspoorten. Om te zorgen dat er zorgvuldig en conform de Avg wordt gewerkt, is de gemeente Oosterhout in december 2017 al gestart met een bewustwordingscampagne. Middels filmmateriaal en casussen werd aangegeven hoe gehandeld moet worden conform de Avg. Door middel van e-learning modules worden de 10 speerpunten van de Avg uitgelegd. Een ander onderdeel van de bewustwordingscampagne is het spel datalekken. Hiermee wordt het melden van datalekken gestimuleerd. De gemeente Oosterhout heeft al zeer veel stappen ondernomen wat betreft het eerste speerpunt.

Het tweede speerpunt is de rechten van de burger. Dit speerpunt wordt uitgebreid besproken in hoofdstuk 5, maar zal nu kort worden toegelicht. De burger heeft een groot aantal nieuwe rechten gekregen waar een beroep op kan worden gedaan. De gemeente Oosterhout heeft daarentegen aan een groot aantal nieuwe verplichtingen richting haar burgers te voldoen. Het doel van het creëren van rechten en plichten richting de burger, is om de burger de mogelijkheid te geven om te participeren bij de verwerking van zijn of haar persoonsgegevens.

Voor het derde speerpunt wordt een verwerkingsregister bijgehouden. In het verwerkingsregister wordt gedocumenteerd welke persoonsgegevens worden verwerkt, met welk doel, waar deze gegevens vandaan komen en met wie ze worden gedeeld. Het verwerkingsregister is te vinden op de website van de gemeente Oosterhout. Alle burgers kunnen op een eenvoudige wijze alle informatie omtrent de verwerking van hun persoonsgegevens inzien.

Het vierde speerpunt geeft aan dat bij risicovolbeleid met betrekking tot de verwerking van persoonsgegevens een toetsing uitgevoerd moet worden. Men spreekt van beleid met een verhoogd

¹ Artikel 288 van het Verdrag betreffende de werking van de Europese Unie

² in 10 stappen voorbereid op de AVG, *autoriteitpersoonsgegevens*, 5 maart 2018, autoriteitpersoonsgegevens.nl (zoek op: 10 stappen).

risico, wanneer het gaat om de verwerking van persoonsgegevens: van een kwetsbare groep zoals ouderen, wanneer sprake is van profilering, gevoelige gegevens zoals medische gegevens, wanneer grootschalig wordt verwerkt, geautomatiseerd wordt verwerkt waarop een besluit wordt gebaseerd, er een gekoppelde database is of wanneer gebruik wordt gemaakt van nieuwe technologieën.³ De toetsing van het risicovolbeleid met betrekking tot de verwerking van persoonsgegevens wordt uitgevoerd aan de hand van een DPIA. De gemeente Oosterhout heeft momenteel nog geen DPIA-model. Hier zal in hoofdstuk 3 en 4 verder op worden ingegaan.

Het vijfde speerpunt zet de gemeente Oosterhout aan om al bij het ontwikkelen van beleid privacy verhogende maatregelen te bedenken. De privacy verhogende maatregelen moeten ervoor zorgen dat de persoonsgegevens zo goed mogelijk gewaarborgd worden. De verplichting wordt verder ingevuld door de twee beginselen, namelijk: privacy by design en –default. Dit betekent dat gekeken moet worden of persoonsgegevens verwerkt moeten worden voor de doelstelling van het beleid. Met andere woorden, is het noodzakelijk persoonsgegevens van de burger te verwerken voor de uitvoering van het beleid? Het tweede beginsel gaat over de manier van verwerken. De verwerking dient zo min mogelijk nadelige effecten voor de betrokkene te veroorzaken. Binnen het kader van dit project zal aan de beginselen van privacy by design en –default verder geen aandacht besteed worden.

Het zesde speerpunt stelt sommige verwerkingsverantwoordelijken verplicht een persoon aan te wijzen die zich bezighoudt met de toezicht op de naleving van de Avg en dient als contactpersoon richting burgers en de Autoriteit Persoonsgegevens. Deze persoon vervult de functie van functionaris gegevensbescherming. De gemeenten zijn verplicht een functionaris gegevensbescherming aan te wijzen. Binnen de gemeente Oosterhout is dit mevrouw mr. J.J.J. Kerremans. Mevrouw Kerremans is sinds 1 september 2017 functionaris gegevensbescherming voor de gemeente Oosterhout.

Het zevende speerpunt heeft betrekking op de procedure omtrent de datalekken. We spreken van een datalek als er problemen zijn rondom de beveiliging waarbij persoonsgegevens kwijt raken of onrechtmatig worden verwerkt.⁴ Het melden van datalekken wordt intern gestimuleerd. Het stimuleren van deze meldplicht wordt onder de aandacht gebracht door een spelvorm binnen de afdelingen. Over het verdere verloop van de procedure binnen de gemeente Oosterhout zal in hoofdstuk 8 verder op worden ingegaan.

Het achtste speerpunt heeft betrekking op de samenwerking met andere gegevensverwerkers (hierna te noemen: ‘verwerkers’). De gemeente Oosterhout werkt met meerdere dienstverlenende organisaties samen om (sociale) voorzieningen te verwezenlijken. Om deze samenwerking conform de Avg in te richten, moet een verwerkingsovereenkomst worden opgesteld met de andere organisaties. In de verwerkingsovereenkomst wordt onder andere vastgesteld welke gegevens uitgewisseld worden en met welk doel, hoelang de gegevens opgeslagen worden en wat met de gegevens wordt gedaan als de doelstelling is verwezenlijkt. De gemeente Oosterhout is druk bezig om met verschillende verwerkers de overeenkomsten op te stellen. Binnen dit project zal hier verder geen aandacht aan besteed worden. Het negende speerpunt is ook niet van toepassing, omdat het betrekking heeft op bedrijven of instellingen die in verschillende lidstaten actief zijn.

Het tiende en laatste speerpunt heeft betrekking op de grondslag van verwerking. Om persoonsgegevens te mogen verwerken moet er sprake zijn van een legitieme verwerkingsgrond. De verwerkingsgronden staan limitatief opgesomd in de Avg. De gemeente kan persoonsgegevens op meerdere gronden verwerken. De gemeente kan onder andere verwerken op basis van: toestemming, voor de uitvoering van een overeenkomst, om te voldoen aan een wettelijke

³ ‘In welke gevallen moet ik een DPIA uitvoeren’, *autoriteitpersoonsgegevens*, 18 maart 2018, autoriteitpersoonsgegevens.nl (zoek op: DPIA).

⁴ ‘Meldplicht datalekken’, *autoriteitpersoonsgegevens*, 7 april 2018, autoriteitpersoonsgegevens.nl (zoek op: datalek).

verplichting, voor de vervulling van een taak van algemeen belang of het openbaar gezag.⁵ Een verwerkingsgrond is het verwerken op grond van de toestemming. De Avg stelt zwaardere eisen aan deze verwerkingsgrond om zeker te zijn dat de toestemming vrijwillig is gegeven. Er kan worden aangenomen dat de toestemming vrijwillig is gegeven wanneer:

- de vraag om op basis van toestemming te verwerken helder is geformuleerd; en
- er geen sprake is van hiërarchie tussen de betrokkene en de gemeente Oosterhout.

Binnen dit project zullen speerpunten nummer twee, vier en zeven verder uitgewerkt worden. Voordat op een van deze speerpunten verder wordt ingegaan, wordt binnen dit hoofdstuk stilgestaan bij het spanningsveld tussen openbaarheid van bestuur en vertrouwelijkheid van persoonsgegevens. Dit spanningsveld kan voor de gemeente Oosterhout voor problemen zorgen. Om transparant te werken moeten stukken geopenbaard worden, maar veel stukken bevatten persoonsgegevens. De vraag rijst hoe de gemeente Oosterhout beslist omtrent de openbaarmaking.

§2.2 De spanning tussen openbaarheid van bestuur en vertrouwelijkheid van persoonsgegevens

Het is voor een democratische samenleving van belang dat de burger kan participeren in de besluitvorming. De overheid tracht daarom openbaarheid bij de uitvoering van haar taken te verschaffen.⁶ Deze openbaarheid moet natuurlijk wel bij wet voorzien zijn. De wet die de gemeente Oosterhout van deze taak voorziet is de Wob, de Wet openbaarheid van bestuur. De Wob geeft de gemeente de taak om informatie met betrekking tot de uitvoering van een bestuurlijke aangelegenheid openbaar te maken. De informatie over de bestuurlijke aangelegenheid kan persoonsgegevens bevatten.

Het openbaar maken van persoonsgegevens valt onder de definitie ‘verwerken’ op basis van de Avg.⁷ Openbaar maken van persoonsgegevens staat dus gelijk aan het verwerken van persoonsgegevens. Het openbaren van stukken omtrent een bestuurlijke aangelegenheid, waar ook persoonsgegevens in worden vermeld, moet dus conform de Avg gebeuren. De openbaarmakingsplicht uit de Wob en de bescherming van persoonsgegevens volgens de Avg vormen een knelpunt.⁸ De vraag rijst hoe het knelpunt kan worden weggenomen zonder afbreuk te doen aan een van deze twee plichten.

De Avg stelt dat persoonsgegevens alleen verwerkt, en dus geopenbaard, mogen worden wanneer een verwerkingsgrondslag aanwezig is. Zoals in het tiende speerpunt van de Avg te lezen is, is een wettelijke plicht een verwerkingsgrondslag. De Wob zorgt voor een wettelijke basis voor de verwerking van persoonsgegevens voor de gemeente Oosterhout. Er is een verwerkingsgrondslag, de Wob. De persoonsgegevens mogen verwerkt worden. De Wob geeft zelfs meerdere wettelijke grondslagen voor de verwerking van persoonsgegevens. Onderstaand worden de grondslagen besproken.

Eenieder kan op basis van artikel 3 van de Wob een verzoek om informatie indienen. De verzoeker hoeft hier geen enkel belang bij te hebben. Een Wob-verzoek (een verzoek op basis van de Wob) moet wel betrekking hebben op een bestuurlijke aangelegenheid van het desbetreffende bestuursorgaan. Met een bestuurlijke aangelegenheid wordt bedoeld: een aangelegenheid die betrekking heeft op beleid van een bestuursorgaan, daaronder inbegrepen de voorbereiding en de uitvoering ervan.⁹ Naast Wob-verzoeken kan de gemeente Oosterhout ook uit eigen beweging gegevens, waaronder persoonsgegevens, openbaar maken. De gemeente maakt gegevens openbaar op basis van artikel 2 juncto 8 van de Wob. Wanneer informatie op basis van artikel 2 juncto 8 Wob wordt geopenbaard, moet het gaan om informatie over:

⁵ Artikel 6 van de Algemene verordening gegevensbescherming

⁶ Artikel 110 van de Grondwet

⁷ Artikel 4 van de Algemene verordening gegevensbescherming

⁸ Artikel 2, 8, 9 van de Wet openbaarheid van bestuur juncto artikel 4,5,6 van de Algemene verordening gegevensbescherming

⁹ Artikel 1 van de Wet openbaarheid van bestuur

- het beleid, de voorbereiding of de uitvoering ervan;
- het belang van de democratische samenleving en bestuursvoering staan voorop; en
- het is een bestuurlijke aangelegenheid.

Artikel 8 van de Wob stelt specifiekere eisen. Er wordt slechts openbaar gemaakt wanneer het in het belang is van een goede democratische bestuursvoering. Artikel 8 geeft het bestuursorgaan een zwaardere toets voordat de informatie wordt geopenbaard. Daarnaast is het nog altijd aan de gemeente zelf om de informatie te openbaren. Bij het Wob-verzoek van artikel 3 Wob is elk document dat iets te maken heeft met beleid, vatbaar voor openbaarmaking.¹⁰ Daarnaast heeft de gemeente Oosterhout niet de extra weigeringsgrond (het belang van de democratische samenleving moet voorop staan) en moet de gemeente gemotiveerd aangeven waarom niet aan het Wob-verzoek wordt voldaan.¹¹

Artikel 3 van de Wob geeft de indruk dat alle persoonsgegevens zonder enige waarborg worden geopenbaard zolang de stukken betrekking hebben op een bestuurlijke aangelegenheid. Dit zou grote gevolgen hebben voor de waarborging van persoonsgegevens. De wetgever heeft met de persoonsgegevens van de burger echter wel enigszins rekening gehouden bij het opstellen van de Wob. Artikel 10 van de Wob geeft aan wanneer niet voldaan hoeft te worden aan artikel 2, 3, en 8 Wob. Artikel 10 lid 1 geeft de absolute weigeringsgronden weer. De absolute weigeringsgronden zijn weigeringsgronden waar geen speelruimte in zit. Valt een Wob-verzoek onder een van deze gronden, dan moet het verzoek afgewezen worden. Artikel 10 lid 1 van de Wob geeft aan dat bijzondere persoonsgegevens niet geopenbaard hoeven te worden, tenzij het de persoonlijke levenssfeer van de betrokkene niet raakt. Bijzondere persoonsgegevens zijn gegevens omtrent iemands ras, etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond, biometrische gegevens met het oog op de unieke identificatie van een persoon, gegevens over gezondheid, gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid, volgens de Avg.¹² In de Wob wordt momenteel nog verwezen naar de Wet bescherming persoonsgegevens (hierna te noemen: 'Wbp'), maar per 25 mei 2018 komt deze wet te vervallen en zal de Avg leidend worden. Artikel 10 lid 1 Wob stelt dat al deze bijzondere persoonsgegevens alleen op basis van de Wob geopenbaard worden, als het de persoonlijke levenssfeer van de burger niet raakt. Lid 2 van artikel 10 van de Wob geeft de relatieve uitzonderingsgronden weer. Van de relatieve uitzonderingsgronden kan afgeweken worden, mits er een motivatie wordt gegeven. Wanneer een beroep wordt gedaan op een van deze gronden wordt gekeken welk belang prevaleert. Onder de werking van lid 2 vallen de 'gewone' persoonsgegevens. Met gewone persoonsgegevens wordt bedoeld: alle gegevens die niet onder de definitie van bijzondere persoonsgegevens vallen en waaraan een persoon te identificeren is. Een voorbeeld is een adres, naam of foto. De persoonsgegevens worden in beginsel wel openbaar gemaakt. De uitzondering is dat het de persoonlijke levenssfeer van de betrokkene niet mag beïnvloeden, tenzij dit belang niet opweegt tegen het verzoek. De leden 1 en 2 van artikel 10 van de Wob maken een identieke belangenafweging, maar beide leden gaan over een ander soort persoonsgegeven. De vraag is wanneer de persoonlijke levenssfeer wordt geraakt en hoe wordt deze belangenafweging verder ingevuld? Voor de beantwoording van deze vraag wordt gekeken naar andere wetgeving.

In de Algemene wet bestuursrecht¹³ (hierna te noemen: 'Awb') wordt aangegeven dat een bestuursorgaan de belangen van de burger omtrent het besluit afweegt. De benadeling van de burger mag niet onevenredig zijn in verhouding tot het met het besluit te dienen doel. Artikel 8 van het Europees verdrag van de Rechten van de Mens en de Fundamentele Vrijheden (hierna te

¹⁰ 'openbaarheid van bestuur', Koninklijke vermande, Sdu Uitgevers 2003, toelichting bij artikel 8 van de Wet openbaarheid van bestuur, 3 februari 2010, ECLI:NL:RVS:2010:BL1831.

¹¹ 3:2 juncto 3:46 van de Algemene wet bestuursrecht

¹² Artikel 9 van de Algemene verordening gegevensbescherming

¹³ Artikel 3:4 van de Algemene wet bestuursrecht

noemen: 'EVRM') geeft aan dat inmenging van een bestuursorgaan in het privéleven enkel is toegestaan voor zover dit bij wet is voorzien en in het belang is van de democratische samenleving. Het begrip privéleven staat gelijk aan de persoonlijke levenssfeer als wordt bedoeld in de Wob. De persoonlijke levenssfeer is een zeer ruim begrip en omvat ook de persoonsgegevens van een Europees burger.¹⁴ Artikel 8 EVRM stelt dat de gemeente Oosterhout de persoonsgegevens van de burger alleen mag openbaren wanneer dit noodzakelijk is. De beginselen van subsidiariteit en proportionaliteit komen om de hoek kijken. Deze beginselen houden in dat er een zo min mogelijk ingrijpend middel gebruikt moet worden en de manier van toepassing zo gunstig mogelijk moet zijn voor de burger. Er wordt dus in bovenstaande wettelijke bepalingen aangegeven dat per geval bekeken wordt of de persoonlijke levenssfeer wordt geraakt en welk belang prevaleert. De wetgever verschaft geen duidelijk toetsingskader wat betreft de invulling van de eerbiediging van de persoonlijke levenssfeer. Het hoogst sprekende bestuursrechtelijke orgaan in Nederland, de Raad van State, geeft hier een duidelijkere invulling aan.

De Raad van State stelt dat het openbaar maken van namen en adressen de persoonlijke levenssfeer van de burger raakt.¹⁵ De Raad van State stelt dat wanneer een Wob-verzoek afgewezen wordt, omdat anders de persoonlijke levenssfeer van een burger geraakt wordt, dit moet worden verantwoord. Het Wob-verzoek kan ook worden afgewezen wanneer de openbaarmaking van de gegevens het publiek belang van een goede en democratische bestuursvoering niet dient. Met andere woorden: een Wob-verzoek moet een zekere mate van algemeen belang hebben, ondanks het feit dat je geen belang hoeft te hebben bij het indienen van het verzoek.¹⁶ Een Wob-verzoek indienen om op deze manier bewijsmateriaal te verzamelen voor een rechtsvordering valt dus niet onder de toepassing van de Wob.¹⁷ De persoonsgegevens moeten een toegevoegde waarde hebben voor de maatschappij. Wanneer de gegevens niet noodzakelijk geopenbaard hoeven te worden, zal dit ook niet gebeuren. Het moet dus van belang zijn dat de burger weet op wie de bestuursvoering betrekking heeft. Een voorbeeld is de inspectie van horecagelegenheden.¹⁸ Hierbij is het van belang dat de burger weet welk restaurant niet door de keuring is gekomen of bij welke eigenaar de vergunning is ingetrokken. De vraag blijft hoe vult de gemeente Oosterhout deze belangenafweging in de dagelijkse bedrijfsvoering in?

§2.3 De dagelijkse bedrijfsvoering binnen de gemeente Oosterhout

Binnen de gemeente Oosterhout is de tweestrijd tussen de wettelijke bepalingen niet onopgemerkt gebleven. De juridische medewerker vertelt er het volgende over: *"Het probleem is dat je geen belang hoeft te hebben bij het indienen van een Wob-verzoek. Dit maakt het maken van een afweging lastig en het speelveld heel groot."* In de belangenafweging geeft de gemeente Oosterhout uitdrukkelijk de voorkeur aan de eerbiediging van de persoonlijke levenssfeer van de burger. *"We maken eigenlijk niet zomaar persoonsgegevens openbaar."* Toch zal de mogelijkheid tot inzage van bepaalde bestuurlijke stukken niet geweigerd kunnen worden. De gemeente Oosterhout heeft hier een zeer praktische oplossing voor gevonden. *"We strepen de persoonsgegevens in deze vallen door."* Er is een situatie waarin documenten met persoonsgegevens wel geopenbaard worden. *"In een geval waar we het wel doen is bij een uniforme voorbereidingsprocedure van bijvoorbeeld een bestemmingsplan. De gegevens hebben dan al ter inzage gelegen en iedereen heeft ze in kunnen zien. Wanneer dit het geval is worden de gegevens ook op basis van een Wob verzoek geopenbaard."* De persoonsgegevens van de burger worden dus slechts geopenbaard middels een Wob-verzoek, wanneer de gegevens al middels een andere procedure voor het publiek inzichtelijk zijn geweest. De juridisch medewerker vat het standpunt krachtig samen met de uitspraak: *"We beschermen de*

¹⁴ EHRM 16 december 1992, ECLI:NL:XX:1992:AD1800, NJ 1993/400 (Niemietz tegen Duitsland) en EHRM 16 februari 2000, no. 27798/95 (Amann t. Zwitserland) en EHRM 28 januari 2003, nr. 44647/98 (Peck tegen het Verenigd Koninkrijk).

¹⁵ Uitspraak 201106670/1/A3, woensdag 25 juli 2012, Onder 2.4.1, Afdeling van 3 februari 2010, ECLI:NL:RVS:2010:BL1844

¹⁶ RvS 28 augustus 2013, ECLI:NL:RVS:2013:910.

¹⁷ RvS 18 februari 2015, ECLI:NL:RVS:2015:426 en RvS 22 februari 2017, ECLI:NL:RVS:2017:498.

¹⁸ RvS 2 augustus 2017, ECLI:NL:RVS:2017:2086.

burger en de ambtenaar liever iets te goed. We zijn hier niet om burgers te pesten. Wat moet dat moet, maar ook zeker niet meer dan dat.” Op basis van de Wob zullen persoonsgegevens niet snel openbaar worden gemaakt door de gemeente Oosterhout.¹⁹

§2.4 Samenvatting en conclusie

De eerste deelvraag luidt: *‘Wat moet de gemeente Oosterhout doen om te voldoen aan de wettelijke bepalingen vanuit de Algemene verordening gegevensbescherming, die zien op de waarborging van persoonsgegevens en de Wet openbaarheid van bestuur waarin een transparante overheid centraal staat?’*

Na het analyseren van de Avg, de Wob en de dagelijkse bedrijfsvoering van de gemeente Oosterhout kan deze vraag worden beantwoord. De Avg zorgt middels de tien speerpunten voor een groot aantal waarborgen voor persoonsgegevens. De speerpunten zijn: bewustwording van de komst van de Avg, de nieuwe rechten van de burger, de gemeente moet een verwerkingsregister opstellen, de gemeente moet een DPIA uitvoeren op risicovol beleid met betrekking tot de verwerking van persoonsgegevens, bij het opstellen van beleid moet al gekeken worden of de verwerking van persoonsgegevens noodzakelijk is en op welke manier dit gebeurt, er moet een functionaris gegevensbescherming aangewezen worden, alle datalekken moeten gedocumenteerd worden en er moet een procedure worden opgesteld, er zal een verwerkingsovereenkomst opgesteld moeten worden tussen verwerkers, wanneer een organisatie meerdere vestigingen in de EU-lidstaten heeft zal een leidende toezichthouder aangewezen moeten worden en voor de verwerking op basis van toestemming geldt een zwaardere toetsing om met zekerheid vast te stellen dat de toestemming vrijwillig is gegeven.

Middels de Wob wordt de Avg, gedeeltelijk, te niet gedaan. Volgens de wettelijke bepalingen mogen veel persoonsgegevens middels een Wob-verzoek worden opgevraagd. Zolang het verzoek betrekking heeft op een bestuurlijke aangelegenheid, waar binnen een bestuursorgaan al snel sprake van is, worden persoonsgegevens afgegeven. Artikel 10 van de Wob zorgt dan ook voor weinig bescherming. Jurisprudentie zorgt dat tijdens de belangenafweging wel wordt gekeken naar het maatschappelijk belang. Ook het doel van het indienen van een Wob-verzoek wordt meegenomen. De gemeente Oosterhout geeft een duidelijke invulling aan de belangenafweging van artikel 10 van de Wob. De eerbiediging van de persoonlijke levenssfeer prevaleert in bijna alle gevallen. Middels deze afweging zorgt de gemeente Oosterhout zelf voor een strikte invulling van het privacybeleid. De gemeente Oosterhout anonimiseert stukken door persoonsgegevens door te strepen. Op deze manier wordt voldaan aan de verplichtingen van een openbaar bestuur, maar blijven persoonsgegevens vertrouwelijk. Dankzij de invulling van de belangenafweging tussen openbaarheid van bestuur en vertrouwelijkheid van persoonsgegevens door de Raad van State en de gemeente Oosterhout, worden aan beide wettelijke verplichtingen voldaan.

¹⁹ Het interview is terug te vinden in bijlage 1.

Hoofdstuk 3: Wat is de verantwoording van de verwerkingsverantwoordelijke?

Een bedrijf, instelling of persoon is een verwerkingsverantwoordelijke wanneer het bedrijf, de instelling of de persoon het doel van de verwerking van persoonsgegevens vaststelt en bepaalt met welk middel wordt verwerkt. Een middel kan een applicatie zijn of een archief bijhouden.²⁰ De verwerkingsverantwoordelijke hoeft de daadwerkelijke verwerking zelf niet uit te voeren, maar dit kan natuurlijk wel. De uitvoering van de verwerking kan uitbesteed worden aan een andere partij. Deze partij heet de verwerker. De verwerker verwerkt persoonsgegevens namens de verwerkingsverantwoordelijke.²¹

De gemeente Oosterhout is een verwerkingsverantwoordelijke, omdat de gemeente Oosterhout het doel en middelen rondom de verwerking van persoonsgegevens vaststelt. Alle verwerkingsverantwoordelijken die gegevens verzamelen of verwerken binnen de Europese Unie moeten volgens de Avg aan de verantwoordingsplicht voldoen. Deze plicht houdt in dat de verwerkingsverantwoordelijke moet aantonen dat er op een juiste manier met de persoonsgegevens wordt omgegaan. Een uitzondering op deze plicht is de verwerking binnen huiselijke kringen.²² Hierbij is te denken aan alle verwerking van persoonsgegevens binnen een gezin. Aan het eind van dit hoofdstuk zal de vraag beantwoord worden: *“Welke eisen stelt de Algemene verordening gegevensbescherming aan de gemeente Oosterhout met betrekking tot de verantwoordingsplicht?”*

De verantwoordingsplicht kan in een aantal aspecten worden opgedeeld volgens de Autoriteit Persoonsgegevens. Onder de verantwoordingsplicht vallen:

- het verwerkingsregister;
- de verwerkingsovereenkomst;
- de DPIA;
- het datalekregister;
- het vragen van toestemming aan de betrokkene voor de verwerking en;
- het aanstellen van een functionaris gegevensbescherming.

Bovenstaande aspecten zullen in dit hoofdstuk besproken worden, behalve het datalekregister wat in hoofdstuk 8 wordt besproken. Het verwerken op grond van de toestemming van de betrokkene wordt ook niet behandeld. De meeste taken die de gemeente Oosterhout uitvoert hebben een wettelijke grondslag of worden in het kader van een publiek openbare taak of openbaar gezag uitgevoerd. Hierbij is te denken aan het verstrekken van uitkeringen of het handhaven van de veiligheid. In deze gevallen is het vragen van toestemming aan de betrokkene niet vereist, omdat er al een andere verwerkingsgrondslag aanwezig is. Aangezien de gemeente Oosterhout sporadisch verwerkt op grond van toestemming, zal dit gedeelte buiten beschouwing worden gelaten binnen dit onderzoek.²³

§3.1 Het verwerkingsregister

Het eerste onderdeel van de verantwoordingsplicht is het opstellen van een verwerkingsregister.²⁴ Een verwerkingsregister is een schema waarin alle activiteiten rondom de verwerking van de persoonsgegevens worden weergegeven. De gemeente Oosterhout geeft voor elke verwerking van persoonsgegevens in het verwerkingsregister aan: wat de verwerkingsdoeleinden zijn, de wettelijke grondslag, een beschrijving van de categorieën van persoonsgegevens en categorieën burgers, welk bedrijf of instelling deze gegevens krijgt toegestuurd, het termijn van verwerking, de maatregelen om veiligheid te waarborgen en welke verwerkingen door welke afdelingen zijn uitgevoerd.

²⁰ Artikel 4 zevende lid van de Algemene verordening gegevensbescherming

²¹ Artikel 4 achtste lid van de Algemene verordening gegevensbescherming

²² Artikel 3 van de Algemene verordening gegevensbescherming

²³ Artikel 6 juncto artikel 7 van de Algemene verordening gegevensbescherming

²⁴ Artikel 30 juncto artikel 31 van de Algemene verordening gegevensbescherming

Daarnaast worden ook de contactgegevens van de gemeente Oosterhout en de functionaris gegevensbescherming genoemd.

De gemeente Oosterhout heeft het verwerkingsregister op de website geplaatst. Op deze manier kan eenieder inzien hoe de gemeente Oosterhout de persoonsgegevens verwerkt. De burger heeft het recht om het verwerkingsregister in te zien.²⁵ Door het verwerkingsregister op de website te plaatsen is aan deze verplichting voldaan.²⁶

§3.2 De verwerkingsovereenkomst

Het tweede deel van de verantwoordingsplicht is het opstellen van een verwerkingsovereenkomst.²⁷ De verwerkingsovereenkomst wordt tussen de verwerkingsverantwoordelijke en verwerker opgesteld. Een voorbeeld van een verwerker waarmee de gemeente Oosterhout samenwerkt is de Stichting Theek 5 Oosterhout in het kader van de invulling van een sociale voorziening.²⁸ Stichting Theek 5 Oosterhout voorziet Oosterhout van een bibliotheek. De gemeente Oosterhout werkt met veel meer externe partijen waarmee persoonsgegevens worden uitgewisseld. Deze externe partijen kunnen een lokale buurtvereniging of een ICT bedrijf zijn maar ook andere overheidsinstellingen. Voor al deze samenwerkingen waarbij persoonsgegevens worden uitgewisseld, moeten verwerkingsovereenkomsten opgesteld worden.

In de verwerkingsovereenkomst staat op welke wijze de verwerker en / of verwerkingsverantwoordelijke de persoonsgegevens verwerkt. De Europese wetgever heeft bepaald dat een aantal onderwerpen in de verwerkingsovereenkomst opgenomen moeten worden. De vereiste onderwerpen en een beknopte uitleg staan in het schema.

Vereisten	Uitleg
Algemene beschrijving	Een omschrijving van het onderwerp, de duur, de aard en het doel van de verwerking, het soort persoonsgegevens, de categorieën van betrokkenen en de rechten en verplichtingen als verwerkingsverantwoordelijke.
Instructiebevoegdheid	De verwerker mag de persoonsgegevens enkel verwerken voor zover daar instructie voor is gegeven door de verwerkingsverantwoordelijk, in dit geval de gemeente Oosterhout.
Geheimhoudingsplicht	De verwerker is verplicht vertrouwelijk om te gaan met de persoonsgegevens. De gemeente Oosterhout kan een boetebeding opnemen in de verwerkingsovereenkomst. Wanneer de verwerker de geheimhoudingsplicht niet nakomt, is de verwerker verplicht een boete te betalen.
Beveiligingsmaatregelen	De gemeente Oosterhout moet ervoor zorgen dat de verwerker passende technische en organisatorische maatregelen neemt om de persoonsgegevens te beveiligen tegen verlies.
Sub-verwerkers	In de verwerkingsovereenkomst wordt vastgelegd of, en onder welke voorwaarden, de verwerker sub-verwerkers mag inschakelen.
Rechten van burgers	De verwerker is verplicht mee te werken wanneer de burger een beroep doet op zijn of haar beroepbare rechten. De beroepbare rechten worden verder besproken in hoofdstuk 5.
Data protection impact assessment	De verwerker werkt mee om andere verplichtingen na te komen zoals het melden van een datalek en een DPIA uit te voeren.
Audit	De gemeente Oosterhout moet kunnen controleren of de verwerker zich houdt aan de gemaakte afspraken. Dit gebeurt vaak in de vorm van een onderzoek door de gemeente Oosterhout of door een onafhankelijke derde. In de verwerkersovereenkomst kunnen partijen hier nadere afspraken over maken.

²⁵ Artikel 15 van de Algemene verordening gegevensbescherming (meer informatie is terug te vinden in hoofdstuk 5 onder de beroepbare rechten.)

²⁶ 'verantwoordingsplicht', *autoriteitpersoonsgegevens* 3 mei 2018, autoriteitpersoonsgegevens.nl (zoek op: *verantwoording*).

²⁷ Artikel 28 van de Algemene verordening gegevensbescherming

²⁸ Artikel 172 eerste lid van de Gemeentewet

Gegevens verwijderen	Na afloop van de verwerkingsdiensten verwijdert de verwerker de gegevens of worden de persoonsgegevens terug gegeven aan de gemeente Oosterhout. Kopieën worden ook verwijderd, tenzij de verwerker wettelijk verplicht is de persoonsgegevens te bewaren. De verwerker heeft een bewijslast. Het is dus aan de verwerker om aan te tonen dat de persoonsgegevens daadwerkelijk zijn verwijderd.
Aansprakelijkheid	De Avg bepaalt dat de gemeente Oosterhout kan worden aangesproken als iemand schade lijdt doordat de Avg niet wordt nageleefd. Dit geldt zelfs als de schade het gevolg is van nalatigheid van de verwerker. De verwerker en de gemeente Oosterhout maken afspraken over de verdere invulling van de kostenverdeling en mate van aansprakelijkheid richting elkaar. ²⁹

Naast de wettelijke vereisten kunnen meerdere bepalingen opgenomen worden in de verwerkingsovereenkomst. Hierbij is te denken aan een wekelijkse afspraak om de gang van zaken te bespreken of de manier van afgifte van de gegevens. De vormgeving en de (aanvullende) invulling van de overeenkomst wordt open gelaten door de Europese wetgever. Met andere woorden, naast de bovenstaande verplichten onderwerpen worden geen aanvullende eisen gesteld aan de verwerkingsovereenkomst. Zolang de verwerker en / of verwerkingsverantwoordelijke conform de Avg handelen, mogen de partijen zelf besluiten hoe de verwerkingsovereenkomst eruit ziet. Wanneer tussen twee verwerkingsverantwoordelijken persoonsgegevens worden uitgewisseld, kan worden volstaan met een ingeperkte verwerkingsovereenkomst. Aangezien beide partijen zelfde wettelijke verplichtingen hebben hoeven sommige bepalingen, zoals bijvoorbeeld een instructiebevoegdheid, niet te worden opgenomen in de geminimaliseerde verwerkingsovereenkomst.³⁰ Een voorbeeld hiervan is de gegevensuitwisseling met de gemeente Oosterhout en zorgaanbieders.

§3.3 Het data protection impact assessment

Het derde deel van de verantwoordingsplicht is het uitvoeren van het DPIA. Een DPIA is een toetsingsmodel. Aan de hand van deze toetsing kan gekeken worden of op een juiste manier met persoonsgegevens om wordt gegaan. De vormgeving van het DPIA zal in hoofdstuk 4 besproken worden. In dit hoofdstuk wordt gekeken wanneer een DPIA uitgevoerd moet worden.

Een DPIA is een methode om privacyrisico's van een gegevensverwerking in kaart te brengen en vervolgens maatregelen te kunnen nemen om de risico's te verkleinen. Een DPIA stimuleert organisaties om proactief na te denken over vragen als: Wat is de impact van het beoogde project op de privacy van de betrokkenen? Wat zijn de risico's voor de betrokkenen en voor de organisatie? Is een aanpak die minder gevolgen heeft voor de privacy ook mogelijk?³¹ Een DPIA hoeft alleen uitgevoerd te worden wanneer sprake is van een verhoogd privacyrisico bij de gegevensverwerking. De vraag rijst wanneer er sprake is van een privacyrisico bij de gegevensverwerking. Om deze afweging niet volledig aan de gemeente Oosterhout over te laten, is voor een aantal situaties besloten dat er sprake is van een privacyrisico. Hiervan is sprake wanneer:

- systematisch en uitvoerig persoonlijke aspecten worden geëvalueerd, hieronder valt bijvoorbeeld profilering voor marketingdoeleinden;
- op grote schaal bijzondere persoonsgegevens worden verwerkt, een voorbeeld hiervan is iemands religie; of
- op grote schaal en systematisch mensen worden geobserveerd in een publiek toegankelijk gebied. Hierbij is te denken aan cameratoezicht op het treinstation.

²⁹ 'verantwoordingsplicht', *autoriteitpersoonsgegevens* 3 mei 2018, *autoriteitpersoonsgegevens.nl* (zoek op: verantwoording).

³⁰ 'gemeentedomein sociaal', *autoriteitpersoonsgegevens* 15 mei 2018, *autoriteitpersoonsgegevens.nl* (zoek op: gemeente).

³¹ 'privacy impact assessment', *norea* 28 februari 2018, *norea.nl*. (zoek op: norea).

Wanneer sprake is van een van deze drie situaties, moet een DPIA uitgevoerd worden. Een groot aantal gegevensverwerkingen zijn echter niet te categoriseren onder deze drie gevallen. Om de gemeente Oosterhout te helpen te bepalen of er sprake is van een verhoogd privacyrisico zijn criteria opgesteld. Een DPIA moet uitgevoerd worden wanneer de verwerking aan 2 of meer van de onderstaande criteria voldoet. Wanneer aan 1 van deze criteria wordt voldaan en er geen DPIA uitgevoerd wordt, moet de gemeente Oosterhout deze afweging motiveren.³² De criteria zijn:

- geautomatiseerde beslissingen;

Hiervan is sprake wanneer op basis van een volledig geautomatiseerde verwerking van persoonsgegevens besluiten worden gemaakt. Volledig geautomatiseerd wil zeggen zonder menselijke tussenkomst. De computer verwerkt de persoonsgegevens zelfstandig. Op basis van deze verwerking wordt een besluit gemaakt. Dit besluit moet wel gevolgen hebben voor de burger. Hierbij is te denken aan het afwijzen van een vergunning.

- grootschalige gegevensverwerkingen;

De Avg geeft geen definitie voor 'grootschalige gegevensverwerkingen'. Een deskundige adviesgroep³³ heeft wel een definitie opgesteld. De adviesgroep stelt dat de volgende criteria bepalen of sprake is van grootschalige gegevensverwerking: de hoeveelheid mensen van wie gegevens worden verwerkt; de hoeveelheid gegevens of de verscheidenheid aan gegevens die worden verwerkt; de tijdsduur van de gegevensverwerking en de geografische reikwijdte van de gegevensverwerking. Deze criteria kunnen bepalen of een verwerking grootschalig is of niet. Exacte aantallen worden door de adviesgroep niet genoemd om de afweging te maken. De invulling van de afweging blijft dus bij de gemeente Oosterhout zelf liggen.

- gekoppelde databases;

Een gekoppelde databases houdt in dat persoonsgegevens uit meerdere systemen worden gehaald. Deze systemen kunnen persoonsgegevens verzamelen om verschillende doelen (lees: doelstellingen) te verwezenlijken of voor verschillende verwerkingsverantwoordelijken. Met andere woorden, de persoonsgegevens zijn van verschillende locaties afkomstig en worden met (een) ander(e) doel(en) verwerkt. Wanneer sprake is van gekoppelde databases en de burger hier redelijkerwijs niet van op de hoogte kan zijn, spreekt men van een privacyrisico. Een voorbeeld ter illustratie: In 2008 zijn de individuele reisgegevens van OV-chipkaarthouders gebruikt voor marketingdoeleinden. De OV-chipkaarthouders kregen advertenties toegestuurd. De advertenties sloten aan bij het reisgedrag van de OV-chipkaarthouders. De reisgegevens werden gehaald vanuit de gegevensopslag van Arriva en NS.³⁴ Er is er dus sprake van gekoppelde databases.

- gegevens van kwetsbare personen;

Kwetsbare personen zijn personen die niet in staat zijn zelf de beslissing te nemen of ze toestemming willen geven voor de verwerking van hun persoonsgegevens. Het kan hierbij gaan om kinderen, gehandicapten of ouderen.

- gebruik van nieuwe technologieën; of

De gemeente Oosterhout kan gebruik maken van nieuwe technologieën bij de verwerking van de persoonsgegevens. Wanneer de betrouwbaarheid van deze technologieën nog niet gegarandeerd kan worden, voert de gemeente Oosterhout een DPIA uit. Wanneer blijkt dat de gegevensverwerking een groot risico voor de waarborging van de persoonsgegevens met zich meebrengt, neemt de gemeente Oosterhout contact op met de Autoriteit Persoonsgegevens. Wanneer de Autoriteit

³² 'data-protection-impact-assessment', autoriteitpersoonsgegevens 18 april 2018, autoriteitpersoonsgegevens.nl (zoek op: PIA).

³³ Richtlijn voor gegevensbeschermingseffectbeoordelingen en bepalingen of een verwerking "waarschijnlijk een hoog risico inhoudt" in de zin van de verordening 2016/679, groep gegevensbescherming artikel 29, 17/nl wp 248 rev.01, 4 oktober 2017.

³⁴ 'geen algemene direct marketing met reisgegevens ov-chipkaart zonder toestemming klant', autoriteitpersoonsgegevens 15 april 2018, autoriteitpersoonsgegevens.nl (zoek op: marketing).

Persoonsgegevens van mening is dat de verwerking inbreuk maakt op de Avg wordt schriftelijk advies gegeven. De Autoriteit Persoonsgegevens kan ook handhavende bevoegdheden inzetten om een correcte verwerking van de persoonsgegevens af te dwingen. Een voorbeeld hiervan is het opleggen van een bestuurlijke boete.³⁵

- blokkering van een recht, dienst of contract.

Het gaat hierbij om gegevensverwerking met een direct gevolg voor de burger. Met gevolg wordt bedoeld dat de burger van een bepaald recht of dienst geen gebruik kan maken. Een voorbeeld is de verwerking van persoonsgegevens door een bank om te bepalen of een lening aan de burger verstrekt wordt. Een DPIA wordt uitgevoerd op gegevensverwerking met een privacyrisico. Een privacyrisico kan ook later ontstaan door veranderende omstandigheden. Hierbij is te denken aan het ophangen van camera's om te handhaven in plaats van buitengewone opsporingsambtenaren te laten patrouilleren. De methode van handhaven is veranderd dus zal er opnieuw gekeken moeten worden naar het privacyrisico. De DPIA hoeft niet uitgevoerd te worden, wanneer er geen verhoogd risico aanwezig is of al een soortgelijke toetsing is uitgevoerd.

§3.4 Functionaris gegevensbescherming

De gemeente Oosterhout is als overheidsorgaan verplicht een functionaris gegevensbescherming aan te stellen.³⁶ De functionaris gegevensbescherming houdt toezicht op de naleving van de Avg, informeert en adviseert de medewerkers over de uitvoering van de Avg, controleert de naleving van het beleid met betrekking tot de bescherming van persoonsgegevens en wijst verantwoordelijkheden toe. De functionaris zorgt voor bewustwording, geeft advies over het uitvoeren van DPIA's en werkt indien nodig samen met de Autoriteit Persoonsgegevens. De functionaris gegevensbescherming is het contactpunt tussen de gemeente Oosterhout en de Autoriteit Persoonsgegevens.³⁷

De gemeente Oosterhout heeft sinds september 2017 een functionaris gegevensbescherming aangesteld. De functionaris gegevensbescherming, mevrouw Kerremans, helpt de afdelingen met het beantwoorden van vraagstukken met betrekking tot privacy. Hierbij is te denken aan het instellen van onderzoeken bij datalekken, het adviseren van afdelingen over een praktische aanpak, de indeling van applicaties, het adviseren bij het opstellen van verwerkingsovereenkomsten en het uitvoeren van DPIA's. Momenteel heeft de functionaris gegevensbescherming een uitvoerende rol binnen de gemeente Oosterhout. Aangezien de gemeente Oosterhout bezig is alle verwerkingsprocessen conform de Avg te laten verlopen, is er een grote behoefte aan kennis. De functionaris gegevensbescherming is momenteel de enige medewerker die zich alleen bezig houdt met de implementatie van de Avg en dus geen andere functie bekleedt. Er zijn meerdere medewerkers die zich bezig houden met de implementatie van de Avg, de privacybeheerders, maar deze medewerkers hebben ook een andere functie. De privacybeheerders zijn werknemers die naast hun functie een rol spelen bij de implementatie. De kennis over de Avg komt hoofdzakelijk van de functionaris gegevensbescherming en dus heeft de functionaris gegevensbescherming een adviserende en uitvoerende taak.

§3.5 Verantwoording aan het college van burgemeester en wethouder

Het college van burgemeester en wethouders is integraal verantwoordelijk voor de uitvoering van de Avg. Het college van burgemeester en wethouders stelt formeel het privacybeleid binnen de gemeente Oosterhout vast. De invulling van het privacybeleid wordt dagelijks uitgeoefend door de afdeling Bestuur, Control en Advies (hierna te noemen: 'afdeling BCA'). De afdeling BCA rapporteert een keer per jaar aan het college van burgemeester en wethouders over de voortgang. De

³⁵ Artikel 35 juncto 36, 57, 60 van de Algemene verordening gegevensbescherming

³⁶ Artikel 37 van de Algemene verordening gegevensbescherming

³⁷ Artikel 39 van de Algemene verordening gegevensbescherming

functionaris gegevensbescherming is ook werkzaam op de afdeling BCA en stelt de rapportage voor het college van burgemeester en wethouders op. Om het privacybeleid geheel op te nemen in de dagelijkse bedrijfsvoering, zijn er privacybeheerders op de afdelingen aangesteld. De privacybeheerders zijn ambtenaren die al werkzaam zijn op de desbetreffende afdelingen. De privacybeheerders vormen de schakel tussen de werkvloer en het team Gegevensmanagement. Zij hebben een cursus gevolgd over de Avg. De privacybeheerders zijn dus zowel op de hoogte van de wettelijke verplichtingen als vakkennis. Op deze manier wordt getracht de Avg en het privacybeleid zo praktisch mogelijk te vertalen voor elke afdeling. De taken van de privacybeheerders zijn:

- het uitdragen van privacy binnen de afdeling;
- nieuwe ontwikkelingen vanuit het werkveld en bijbehorende wetgeving inpassen in het privacybeleid;
- signaleren van nieuwe ontwikkelingen en melden aan de functionaris gegevensbescherming;
- toetsing van de afdeling op het gebied van privacybescherming;
- zorgen voor de toepassing van privacy voorschriften;
- uitvoeren van de DPIA's; en
- het uitvoeren van werkzaamheden voor de oplossing van privacy issues of werkzaamheden voor verbetermaatregelen vanuit privacy adviezen.

§3.6 Samenvatting

Het hoofdstuk begon met de vraag: *“Welke eisen stelt de Algemene verordening gegevensbescherming aan de gemeente Oosterhout met betrekking tot de verantwoordingsplicht?”* Er kan geconstateerd worden dat de verantwoordingsplicht uit meerdere onderdelen bestaat. Het eerste deel is het bijhouden van een verwerkingsregister. In dit verwerkingsregister staat welke persoonsgegevens de gemeente Oosterhout verwerkt en op welke manier. Het verwerkingsregister is te vinden op de website van de gemeente Oosterhout. Het tweede onderdeel is het opstellen van een verwerkingsovereenkomst. De verwerker is de partij die persoonsgegevens verwerkt namens de gemeente Oosterhout. De verwerkingsovereenkomst geeft invulling aan de manier van verwerken. De gemeente Oosterhout is momenteel druk bezig met het maken van verwerkingsovereenkomsten met alle partners waarmee persoonsgegevens worden gedeeld.

Het derde onderdeel is het uitvoeren van een DPIA. Een DPIA is een toetsingsmodel. De toetsing wordt uitgevoerd op gegevensverwerking met een privacyrisico. In meerdere omstandigheden kan sprake zijn van een privacyrisico. Er wordt uitgegaan van een privacyrisico wanneer: systematisch en uitvoerig persoonlijke aspecten worden geëvalueerd, op grote schaal bijzondere persoonsgegevens verwerkt worden of op grote schaal en systematisch mensen worden geobserveerd in een publiek toegankelijk gebied. De Europese toezichthouder heeft nog een aantal punten opgesteld. Aan de hand van deze punten kan de gemeente Oosterhout beslissen of een DPIA noodzakelijk is.

Het vierde onderdeel van de verantwoordingsplicht is het aanstellen van een functionaris gegevensbescherming. De gemeente Oosterhout heeft sinds september 2017 een functionaris gegevensbescherming aangesteld. De functionaris heeft momenteel een uitvoerende taak, maar dit zou na verloop van tijd een toezichthoudende functie moeten worden. Om de toetsing van de functionaris gegevensbescherming zo zuiver mogelijk te houden, zou de functionaris gegevensbescherming de implementatie van de Avg niet zelf uit moeten voeren. De gemeente Oosterhout voldoet conform de Avg aan de verantwoordingsplicht, wanneer alle vier de onderdelen van de verantwoordingsplicht worden nageleefd. Momenteel is hier nog geen sprake van.

Hoofdstuk 4: De uitvoering van het data protection impact assessment

Een DPIA uitvoeren is verplicht bij de verwerking van persoonsgegevens met een verhoogd privacyrisico. In hoofdstuk 3 is besproken wanneer sprake is van een verhoogd privacyrisico. Aan de hand van de criteria kan worden beslist bij welk werkingsproces een DPIA uitgevoerd moet worden. In dit hoofdstuk wordt besproken hoe een DPIA uitgevoerd moet worden. De vraag die centraal staat is dit hoofdstuk luidt: *“Aan welke voorwaarden moet een procedure voldoen voor de uitvoering van een data protection impact assessment, zoals omschreven in de Algemene verordening gegevensbescherming, om aan te sluiten bij de bedrijfsvoering van de gemeente Oosterhout?”*

§4.1 Verplichtingen vanuit de Avg

De Avg stelt een aantal verplichtingen aan de uitvoering van de DPIA. De Avg stelt dat er gekeken moet worden naar:

- een systematische beschrijving van de (beoogde) verwerkingen;
- de verwerkingsdoeleinde(n);
- een beoordeling van de noodzaak en de evenredigheid van de verwerkingen met betrekking tot de doeleinden;
- een beoordeling van de risico's voor de rechten van de betrokkenen;
- de beoogde maatregelen om de risico's aan te pakken; en
- of de goedgekeurde gedragscodes naar behoren in aanmerking genomen worden.

Wanneer uit het uitgevoerde DPIA blijkt dat de verwerking een hoog risico kan opleveren en geen maatregelen worden genomen om dit risico in te perken, raadpleegt de gemeente Oosterhout voorafgaand aan de verwerking de Autoriteit Persoonsgegevens. De Autoriteit Persoonsgegevens beoordeelt of de voorgenomen verwerking inbreuk maakt op Avg. De Autoriteit Persoonsgegevens kijkt met name of de gemeente Oosterhout het risico voldoende heeft beperkt. Wanneer de gemeente Oosterhout de Autoriteit Persoonsgegevens verzoekt te adviseren omtrent een risicovolle verwerking van persoonsgegevens, moeten de volgende gegevens worden verstrekt:

- de verantwoordelijkheden van de gemeente Oosterhout;
- bij de verwerking betrokken verwerkingsverantwoordelijken en verwerkers;
- de doeleinden en de middelen van de voorgenomen verwerking;
- de maatregelen en waarborgen die worden geboden ter bescherming van de rechten van betrokkenen;
- de contactgegevens van de functionaris voor gegevensbescherming;
- een overzicht van de DPIA die is uitgevoerd op de risicovolle verwerking van de persoonsgegevens; en
- alle andere informatie waar de Autoriteit Persoonsgegevens om verzoekt.

§4.2 Het toetsingskader van NOREA

Voor het uitvoeren van een DPIA is een toetsingsmodel nodig. Zowel de Rijksoverheid³⁸ als de beroepsorganisatie van IT-auditors hebben een DPIA-model opgesteld. De gemeente Oosterhout heeft de keuze om een van deze twee modellen als uitgangspunt te nemen voor het uitvoeren van een DPIA. De Autoriteit Persoonsgegevens verwijst naar het toetsingskader dat door de beroepsorganisatie van IT-auditors is opgesteld, genaamd: NOREA.³⁹ Door de functionaris gegevensbescherming is NOREA gekozen als uitgangspunt te nemen om een tweetal DPIA's binnen de gemeente Oosterhout uit te voeren.⁴⁰ Het toetsingskader van NOREA bestaat uit 8 stappen:

³⁸ 'model gegevensbeschermingseffectbeoordeling rijksdienst pia', *rijksoverheid* 22 april 2018, [rijksoverheid.nl](https://rijksoverheid.nl/onderwerpen/gegevensbeschermingseffectbeoordeling) (zoek op: gegevensbeschermingseffectbeoordeling).

³⁹ 'data-protection-impact-assessment', *autoriteitpersoonsgegevens* 18 april 2018, [autoriteitpersoonsgegevens.nl](https://autoriteitpersoonsgegevens.nl/onderwerpen/data-protection-impact-assessment) (zoek op: PIA).

⁴⁰ 'privacy impact assessment', *norea* 28 februari 2018, [norea.nl](https://norea.nl/onderwerpen/privacy-impact-assessment) (zoek op: norea).

- Stap 1. het type project;
- Stap 2. de persoonsgegevens die gebruikt worden;
- Stap 3. de partijen die betrokken zijn bij de uitvoering;
- Stap 4. het verzamelen van persoonsgegevens;
- Stap 5. het gebruiken van persoonsgegevens;
- Stap 6. het bewaren en vernietigen van persoonsgegevens;
- Stap 7. het beveiligen van persoonsgegevens; en
- Stap 8. de meldplicht datalekken.⁴¹

Alle stappen zijn onder te verdelen in een tiental gesloten vragen. De gesloten vragen helpen het verwerkingsproces duidelijk in kaart te brengen. Op deze manier kan vastgesteld worden waar de risico's omtrent de verwerking zitten. Aan de hand van twee verwerkingsprocessen, een in het sociaal domein en de ander met betrekking op veiligheid, zal gekeken worden of het toetsingskader van NOREA aansluit bij de werkwijze van de gemeente Oosterhout. De uitgevoerde DPIA's zijn terug te vinden in bijlage 3. In onderstaande paragraaf worden de bevindingen aan de hand van de uitgevoerde DPIA's besproken.

§4.3 NOREA in de praktijk

Het eerste verwerkingsproces omtrent persoonsgegevens komt uit het sociaal domein. Het verwerkingsproces wordt door de afdeling Informatie- en Servicecentrum uitgevoerd. Het verwerkingsproces genaamd 'Leerlingenvervoer' verwerkt persoonsgegevens van minderjarigen. De minderjarigen zijn een kwetsbare doelgroep. Het verwerken van persoonsgegevens van een kwetsbare groep is een van de gronden om een DPIA uit te voeren. De verwerking omtrent het Leerlingenvervoer is vrij klein en heeft daarom geen of nauwelijks invloed op de manier van verwerking noch op de persoonlijke levenssfeer van de burger. Vanwege deze kleinschalige verwerking is gekozen om een eerste DPIA uit te voeren op dit verwerkingsproces. Deze keuze heeft met het tijdsbestek van het onderzoek te maken. Daarnaast is een klein en overzichtelijk verwerkingsproces handig om NOREA te testen, omdat er weinig wet- en regelgeving is. Er kan dus enkel naar NOREA gekeken worden zonder dat er naar een groot aantal andere bepalingen gekeken moet worden. Wanneer duidelijk is of NOREA zich leent voor de dagelijkse bedrijfsvoering binnen de gemeente Oosterhout, zal er nog een complexer verwerkingsproces worden getoetst. De DPIA van het verwerkingsproces genaamd Leerlingenvervoer, is terug te vinden in bijlage 3.

Het tweede verwerkingsproces omtrent persoonsgegevens komt uit het domein veiligheid. Het verwerkingsproces wordt door de afdeling Informatie- en Servicecentrum, unit veiligheid en handhaving uitgevoerd. Het verwerkingsproces genaamd: 'Bibob', verwerkt de volgende persoonsgegevens: naam, adres, woonplaats, geboortedatum, burgerservicenummer, telefoonnummer, contactgegevens van de curator, opeisbare schulden, financieringen, objecten, verzekeringen, vergunningshistorie, strafrechtelijke gegevens, justitiële- en politiedocumentatie, belastinggegevens, profiel relatie afkomstig van dienst justitie en de conclusie van het onderzoek van het landelijke bureau Bibob. De Wet bevordering integriteitsbeoordelingen door het openbaar bestuur (hierna te noemen: 'wet Bibob') geeft een bestuursorgaan de mogelijkheid om een vergunning in te trekken, omdat de integriteit van de aanvrager in het geding is. Met andere woorden, op basis van de wet Bibob kan een bestuursorgaan de burger bepaalde rechten ontfeggen om op deze manier criminaliteit tegen te gaan. Een voorbeeld hiervan is een café-eigenaar een vergunning op grond van de Drank- en Horecawet ontfeggen, omdat de café-eigenaar meerdere keren is veroordeeld voor mishandeling en binnen het café vaak gevochten wordt.

Het uitvoeren van een DPIA is verplicht, omdat de integriteitsbeoordeling op basis van de wet Bibob kan zorgen voor de blokkering van een recht. Op basis van deze beoordeling kan een vergunning

⁴¹ 'privacy impact assessment', norea 28 februari 2018, norea.nl. (zoek op: norea).

worden ingetrokken. Daarnaast worden veel bijzondere persoonsgegevens verwerkt van de burger. Het uitvoeren van een DPIA is dus noodzakelijk. Van deze plicht kan niet worden afgeweken. Het DPIA is terug te vinden in bijlage 3.

§4.4 Samenvatting en conclusie

Het hoofdstuk begon met de vraag: *"Aan welke voorwaarden moet een procedure voldoen voor de uitvoering van een data protection impact assessment, zoals omschreven in de Algemene verordening gegevensbescherming, om aan te sluiten bij de bedrijfsvoering van de gemeente Oosterhout?"*

De Avg stelt niet zeer veel eisen aan het uitvoeren van een DPIA. Volgens de Avg moet er sprake zijn van:

- een systematische beschrijving van de (beoogde) verwerkingen;
- de verwerkingsdoeleinden, waaronder de gerechtvaardigde belangen die door de verwerkingsverantwoordelijke worden behartigd;
- een beoordeling van de noodzaak en de evenredigheid van de verwerkingen met betrekking tot de doeleinden;
- een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen;
- de beoogde maatregelen om de risico's aan te pakken, waaronder de veiligheidsmaatregelen en mechanismen om de bescherming van persoonsgegevens te garanderen en om aan te tonen dat aan deze verordening is voldaan, met inachtneming van de rechten en gerechtvaardigde belangen van de betrokkenen en andere personen in kwestie; en
- de goedgekeurde gedragscodes.

De wettelijke vereisten zijn (gedeeltelijk) terug te vinden in NOREA.

In stap 1.1 tot en met 1.11 worden verschillende aspecten van het verwerkingsproces in kaart gebracht. De vraag rijst of dit een systematische beschrijving is. Wanneer dit niet het geval blijkt te zijn, wordt aan het eerste wettelijke vereiste niet voldaan. De verwerkingsdoeleinden zijn terug te vinden in stap 1.5 van NOREA. De noodzakelijkheid en evenredigheid van de verwerking wordt onder stap 2.1 tot en met 2.3 behandeld. Stap 4 richt zich op de betrokkenen. In stap 4 en stap 5.9 tot en met 5.11 wordt gekeken naar de rechten van de betrokkenen. De beveiliging van de verwerking wordt in stap 7 besproken. NOREA behandelt geen gedragscode. Aan de hand van de twee verwerkingsprocessen, Leerlingenvervoer en Bibob, kan gesteld worden dat NOREA een goed uitgangspunt is om de DPIA's uit te voeren. Het toetsingskader van NOREA bestaat uit 8 stappen: stap 1. het type project, stap 2. de persoonsgegevens die gebruikt worden, stap 3. de partijen die betrokken zijn bij de uitvoering, stap 4. het verzamelen van persoonsgegevens, stap 5. het gebruiken van persoonsgegevens, stap 6. het bewaren en vernietigen van persoonsgegevens, stap 7. het beveiligen van persoonsgegevens en stap 8. de meldplicht datalekken.

Om aan te sluiten bij de dagelijkse bedrijfsvoering binnen de gemeente Oosterhout zal NOREA bijgeschaafd moeten worden. Zie hiervoor bijlage 3.

Uit de toetsing met NOREA van het eerste verwerkingsproces, Leerlingenvervoer, is gebleken dat het verwerkingsproces in overeenstemming met de Avg wordt uitgevoerd. De gegevens worden enkel voor de van te voren omschreven doeleinden gebruikt. De gegevens worden door de burger zelf aangedragen door het invullen van het verzoek. Het verwerkingsproces zorgt niet voor privacyrisico's. Over NOREA kan gesteld worden dat het een zeer uitgebreid toetsingsmodel is. NOREA houdt rekening met de aard van de verwerking door de verwerkingsverantwoordelijke door te sturen naar bepaalde vragen die van toepassing zijn op de verwerking. NOREA behandelt zowel de categorie persoonsgegevens, de methode van verwerking, samenwerking met externe partijen en de veiligheidsmethoden. NOREA behandelt deze onderwerpen in acht stappen. Aan NOREA hoeven geen stappen toegevoegd te worden voor het uitvoeren van een DPIA op het

verwerkingsproces genaamd Leerlingenvervoer. Om de toetsing makkelijker te maken voor de afdelingen, zou het wel mogelijk zijn enkele stappen te schrappen. De vragen omtrent de datalekken, stap 8, kunnen weggelaten worden. De gemeente Oosterhout heeft een datalekprocedure opgesteld. In deze procedure wordt beschreven bij wie de melding wordt gemaakt en hoe hiermee moet worden omgegaan. Dit hoeft dus niet nogmaals meegenomen te worden in de DPIA.

Uit de toetsing met NOREA van het tweede verwerkingsproces, Bibob, is gebleken dat het verwerkingsproces risicovol is. De persoonsgegevens worden met een groot aantal partijen gedeeld. Het delen van de persoonsgegevens is cruciaal om een profiel te maken van de burger. Aan de hand van dit profiel wordt beoordeeld of de integriteit in het geding komt. Daarnaast is de burger niet op de hoogte van de verwerking. Wanneer de burger hiervan op de hoogte zou zijn, zou dit gevolgen kunnen hebben voor het integriteitsonderzoek. NOREA geeft bij stap 1.7 aan dat er geen verdere DPIA uitgevoerd hoeft te worden. Het verwerkingsproces is omvangrijk, er worden bijzondere persoonsgegevens verwerkt en met een groot aantal partijen samengewerkt. Het niet uitvoeren van een DPIA zorgt, gezien de aard van de verwerking, voor een onveiliger verwerkingsproces. Een periodieke DPIA moet zorgen voor de waarborging van persoonsgegevens en een veilige verwerking. Stap 1.7 kan verwijderd worden uit NOREA. Wanneer, uit de in hoofdstuk 3 genoemde criteria, blijkt dat er een DPIA uitgevoerd moet worden kan NOREA deze verplichting niet wegnemen. Stap 3 gaat in op de partijen waarmee wordt samengewerkt. In NOREA zou opgenomen kunnen worden: wat de grondslag van de andere partijen is om persoonsgegevens te verwerken, of er een verwerkingsovereenkomst ten grondslag ligt en of deze overeenkomst voldoet aan de wettelijke verplichtingen.

Als de volgende stappen worden toegevoegd aan NOREA wordt zowel aangesloten bij de wettelijke verplichtingen als de dagelijkse bedrijfsvoering binnen de gemeente Oosterhout:

Stap 1.0 Beschrijf de verwerkingsketen van het verwerkingsproces.

Stap 3.2.1 Is het noodzakelijk een verwerkingsovereenkomst met de externe partijen op te stellen?

Stap 3.2.2 (Bij 'Ja' op vraag 3.2.1) Is er een verwerkingsovereenkomst opgesteld en ondertekenend met de externe partijen die voldoet aan alle wettelijke verplichtingen?

Stap 3.2.3 (Bij 'Ja' op vraag 3.2.2) Komt het beleid en de handelswijze van beide partijen overeen met de afspraken die gemaakt zijn in de verwerkingsovereenkomst?

Stap 9.0 Is er beleid of een gedragscode opgesteld omtrent de verwerking?

Stap 9.1 (Bij 'Ja' op vraag 9.0) Voldoet de gedragscode of het beleid aan de Avg?

Stap 9.2 (Bij 'Ja' op vraag 9.1) Wordt de gedragscode of het beleid nageleefd?

Wanneer een van deze vragen met 'nee' beantwoord wordt, loopt het verwerkingsproces een verhoogd risico. De gemeente Oosterhout zal maatregelen moeten nemen zodat de bovenstaande stappen alsnog met een 'ja' beantwoord kunnen worden.

Hoofdstuk 5: Welke rechten heeft de burger?

De Europese wetgever heeft een groot aantal rechten opgenomen in de Avg. Als eerste zullen al deze rechten worden toegelicht. Vervolgens wordt het wettelijk kader van de datalekken besproken. De vraag die in dit hoofdstuk centraal staat luidt: *‘Welke eisen stelt de Algemene verordening gegevensbescherming aan de gemeente Oosterhout met betrekking tot de rechten van de burgers en de procedure datalekken?’* De burger heeft meerdere soorten rechten gekregen op basis van de Avg. Deze rechten kunnen in twee categorieën worden opgedeeld. De eerste categorie zijn de rechten die verplichtingen geven aan de gemeente Oosterhout richting de burger. Naar deze groep rechten zal verwezen worden onder de noemer: ‘plichten’. Deze plichten zeggen iets over de wijze waarop de gemeente Oosterhout richting haar burgers handelt. De tweede categorie zijn de rechten van de burger. Hiernaar wordt verwezen onder de noemer: ‘beroepbare rechten’.

De plichten vanuit de Avg stellen eisen aan de gemeente Oosterhout met betrekking tot de manier van verwerking. De wettelijke bepalingen zeggen hoe de gemeente moet handelen. De burger kan deze verplichte handelswijze niet afdwingen bij de gemeente Oosterhout. Ondanks het feit dat het een recht is dat er op een bepaalde manier wordt gehandeld door de gemeente Oosterhout, kan de burger dit niet afdwingen. De enige die toezicht houdt op de naleving van deze plichten is de Autoriteit Persoonsgegevens. De Autoriteit Persoonsgegevens houdt toezicht op de naleving van alle bepalingen die vanuit de Avg worden gesteld en dus ook de plichten. Een niet afdwingbaar recht lijkt een tegenstelling te veroorzaken. Toch zijn er meer niet afdwingbare rechten te vinden. In de Grondwet onder artikel 19 staat: *‘Bevordering van voldoende werkgelegenheid is voorwerp van zorg der overheid.’* Dit betekent dat de overheid zorg moet dragen voor voldoende werkgelegenheid. Dit recht geeft de overheid de plicht om iets te bewerkstellen voor haar burgers. Deze bepaling heeft dus dezelfde werking als de plichten die vanuit de Avg worden gesteld. Toch is artikel 19 van de Grondwet niet afdwingbaar. Een werkeloze burger kan niet bij de Staten-Generaal aankloppen en zich beroepen op dit recht. De rechten die een plicht geven vanuit de Avg beschermen niet de burger, maar het proces rondom de verwerking. De burger is wel gediend bij een deugdelijk proces. De rechten die een plicht geven hebben een indirecte werking op de positie van de burger.

De tweede categorie rechten, zijn de beroepbare rechten. Deze rechten hebben een directe werking. De burger kan een verzoek indienen op basis van een van deze rechten en de gemeente Oosterhout moet hier gehoor aan geven. Met andere woorden, de beroepbare rechten zijn afdwingbaar. Een verzoek moet worden behandeld door de gemeente Oosterhout. De nationale wetgever heeft in het concept van de Uitvoeringswet Algemene verordening gegevensbescherming gesteld dat de beslissing op een beroepbaar recht een besluit is. Dit betekent dat de burger tegen de beslissing op het verzoek in bezwaar kan bij de gemeente Oosterhout en in beroep bij de bestuursrechter.⁴² Een beroepbaar recht is ook terug te vinden in de Grondwet. Een voorbeeld is artikel 1 van de Grondwet. *“Allen die zich in Nederland bevinden, worden in gelijke gevallen gelijk behandeld. Discriminatie wegens godsdienst, levensovertuiging, politieke gezindheid, ras, geslacht of op welke grond dan ook, is niet toegestaan.”* Het discriminatieverbod dat in artikel 1 van de Grondwet wordt gegeven is ook direct afdwingbaar. Beroepbare rechten, van zowel de Grondwet als de Avg, kunnen worden afdgewongen bij de rechter.

§5.1 Verplichtingen vanuit de Algemene verordening gegevensbescherming

In deze paragraaf worden de eerste categorie rechten, de plichten richting de burger, besproken. De eerste plicht is de plicht tot transparantie. De gemeente moet transparant, rechtmatig en behoorlijk met persoonsgegevens omgaan. De vraag is hoe de gemeente Oosterhout dit kan bewerkstellen. Om deze verplichting verder in te vullen heeft de Europese wetgever een zestal punten opgenomen.⁴³

⁴² Artikel 34 van de Uitvoeringswet Algemene verordening gegevensbescherming

⁴³ Artikel 5 van de Algemene verordening gegevensbescherming

De gemeente Oosterhout voldoet aan de plicht, indien niet verder wordt verwerkt dan de doeleinden (1). Dit betekent dat de gemeente Oosterhout de persoonsgegevens alleen gebruikt voor het doel waarvoor de persoonsgegevens zijn verzameld. De gemeente Oosterhout probeert de doelstelling te verwezenlijken met zo min mogelijk persoonsgegevens (2). Dit houdt in dat de gemeente alleen persoonsgegevens verwerkt die noodzakelijk zijn voor het doel van de verwerking. De persoonsgegevens die de gemeente Oosterhout gebruikt zijn actueel (3). De gemeente Oosterhout bewaart de persoonsgegevens alleen als het noodzakelijk is voor het doel waarvoor ze zijn verzameld (4). Om de veiligheid te waarborgen neemt de gemeente passende technische en organisatorische maatregelen om te voorkomen dat gegevens onrechtmatig worden verwerkt (5). Een passende maatregel is werken met een beveiligingssysteem of om een slot op de archiefkast plaatsen. De gemeente is verantwoordelijk om aan bovenstaande eisen te voldoen (6). De gemeente moet de naleving hiervan ook kunnen aantonen. Dit kan door het bijhouden van een verwerkingsregister.

De tweede plicht is de plicht tot informatieverstrekking. Burgers moeten geïnformeerd worden over de komst van de Avg en hun veranderende rechten. De informatie wordt op begrijpelijke wijze geformuleerd en op passende wijze verstrekt. Een voorbeeld van een correcte uitvoering van de informatieplicht is informatie op de website van de gemeente Oosterhout plaatsen voor de burger over wat er gaat veranderen met de komst van de Avg.⁴⁴

De derde plicht is de meldplicht. De gemeente maakt melding bij de burger wanneer zij in bezit komt van nieuwe persoonsgegevens van de desbetreffende burger. De melding is vrij uitgebreid. Zo geeft de gemeente Oosterhout aan wie de persoonsgegevens verwerkt, wie verantwoordelijk is voor de verwerking en wie de functionaris gegevensbescherming is. Op deze manier weet de burger waar zijn of haar persoonsgegevens zijn, wie de gegevens verwerkt en aan wie vragen gesteld kunnen worden. Daarnaast wordt ook medegedeeld voor welk doel de gegevens worden verwerkt en of de gegevens aan derden worden doorgestuurd. De termijn van verwerken wordt genoemd en of de persoonsgegevens volledig geautomatiseerd worden verwerkt. Vervolgens wordt ook vermeld dat de burger gebruik kan maken van zijn of haar beroepbaar recht. De gemeente Oosterhout mag alleen persoonsgegevens verwerken wanneer er een grondslag is. Een veel voorkomende grondslag is een wettelijke plicht. Een andere grondslag is de toestemming van de burger zelf. Wanneer de burger toestemming geeft voor de verwerking, kan de burger deze toestemming zelf ook weer intrekken. De mogelijkheid om die toestemming in te trekken, wordt ook door de gemeente gemeld. De gemeente Oosterhout heeft ook de plicht om aan te geven dat er bij de Autoriteit Persoonsgegevens een klacht ingediend kan worden, wat de noodzaak of verplichting is van het verstekken van de persoonsgegevens en de gevolgen wanneer deze gegevens niet verstrekt worden. Aan deze meldplicht hoeft niet voldaan te worden wanneer de burger al in bezit is van deze verwerkingsinformatie.⁴⁵

Wanneer de persoonsgegevens niet van de burger zelf afkomstig zijn, maar van de gemeente Oosterhout of door een andere partij zijn verzameld, moet de gemeente voldoen aan een uitgebreide meldingsplicht aan de burger. De gemeente dient te vermelden⁴⁶ waar de persoonsgegevens vandaan komen. De meldplicht wordt binnen een maand na verkrijging van de persoonsgegevens, tijdens het eerste contact met burger of wanneer gegevens worden overgedragen uitgevoerd. De meldplicht geldt niet wanneer de burger al reeds beschikt over de informatie, als het onevenredig veel moeite is of een ander zwaarwegend belang dit tegenwerkt. Een zwaarwegend belang kan zijn de openbare orde beschermen. Een andere uitzonderingsgrond is een wettelijke verplichting of beroepsmatige geheimhouding.

⁴⁴ Artikel 12 van de Algemene verordening gegevensbescherming

⁴⁵ Artikel 13 van de Algemene verordening gegevensbescherming

⁴⁶ Artikel 14 van de Algemene verordening gegevensbescherming

§5.2 Beroepbare rechten

Het eerste beroepbare recht van de burger is het recht op inzage. Het recht op inzage heeft betrekking op alle persoonsgegevens van de burger die de gemeente Oosterhout verwerkt. Alle persoonsgegevens en verwerkingsgegevens die de gemeente Oosterhout bezit, mag de burger inzien. Verwerkingsgegevens zijn gegevens over de manier van verwerken. Hieronder vallen de doeleinden, wie de ontvangers zijn en wanneer er sprake is van doorgifte aan derde, de mogelijkheid om een klacht in te dienen bij de Autoriteit Persoonsgegevens, de bron van de persoonsgegevens en de mate van geautomatiseerde besluitvorming. Wanneer een verzoek tot inzage binnenkomt verstrekt de gemeente Oosterhout een kopie van de persoonsgegevens en de verwerkingsgegevens aan de burger. Wanneer om extra kopieën worden verzocht, kan er een administratieve vergoeding worden gerekend. Wanneer het verzoek elektronisch wordt ingediend, zal het ook elektronisch beantwoord worden. Bij het recht op inzage wordt de privacy van andere persoonsgegevens van andere burgers in acht genomen.⁴⁷

Het tweede beroepbare recht van de burger is het recht op correctie. Met dit recht kunnen onjuiste of onvolledige persoonsgegevens worden aangevuld of gewijzigd. De doeleinden moeten wel in acht worden genomen. Met andere woorden, de correctie moet iets toevoegen aan de verwerking van de persoonsgegevens. Dit recht is niet bedoeld om aanvullende informatie te geven zonder dat het iets bijdraagt. De betrokkene moet zelf aantonen dat de gegevens onvolledig of onjuist zijn voordat de persoonsgegevens gewijzigd of aangevuld worden. De betrokkene kan dit aantonen door brondocumenten aan te leveren, hierbij is te denken aan een trouwakte om een achternaam te wijzigen.⁴⁸

Het derde beroepbare recht is het recht op gegevenswissing. De gemeente is verplicht de persoonsgegevens te verwijderen op verzoek van de burger wanneer de persoonsgegevens onder een van de omschreven categorieën vallen. De persoonsgegevens zijn niet (meer) nodig voor de uitvoering van de doeleinden waarvoor ze zijn verzameld. Een voorbeeld hiervan zijn de persoonsgegevens van een oud-medewerker tien jaar lang te bewaren. De gegevens hoeven niet bewaard te worden, omdat de medewerker er niet meer werkt en de verplichte wettelijke bewaartermijn voorbij is.⁴⁹ Een andere grond is het intrekken van de toestemming om de persoonsgegevens te verwerken. Van deze grond kan alleen gebruik worden gemaakt wanneer de verwerkingsverantwoordelijke geen andere bevoegdheid (lees: grondslag) heeft om deze persoonsgegevens te verwerken. De persoonsgegevens moeten verwijderd worden wanneer de verwerking onrechtmatig is of de verwijdering een wettelijke verplicht is. Wanneer persoonsgegevens moeten worden verwijderd, moeten ook de koppelingen en kopieën van deze persoonsgegevens worden verwijderd.

Aan een verzoek met betrekking tot gegevenswissing hoeft niet altijd te worden voldaan. Wanneer er een ander belang prevaleert zal het verzoek niet gehonoreerd worden. Een ander belang is bijvoorbeeld de vrijheid van meningsuiting van een ander of het nakomen van een wettelijke verplichting. Er wordt bij het afwegen van de belangen ook gekeken naar de rest van de samenleving. De openbare orde mag hier niet onder leiden. De laatste weigeringsgrond heeft betrekking op onderzoek of een gerechtelijke procedure. Wanneer wetenschappelijk, historisch onderzoek of statistische doeleinden de persoonsgegevens gebruiken of de persoonsgegevens nodig zijn voor een rechtsoverweging, worden de persoonsgegevens bewaard.⁵⁰

⁴⁷ Artikel 15 van de Algemene verordening gegevensbescherming

⁴⁸ Artikel 16 van de Algemene verordening gegevensbescherming

⁴⁹ Artikel 655 van boek 7 van het Burgerlijk Wetboek en 'bewaren van persoonsgegevens', *autoriteitpersoonsgegevens* 19 maart 2018, autoriteitpersoonsgegevens.nl (zoek op: *bewaren van persoonsgegevens*).

⁵⁰ Artikel 17 van de Algemene verordening gegevensbescherming

Het vierde beroepbare recht is het recht op beperking van de verwerking. De burger kan een verzoek indienen om zijn of haar persoonsgegevens minder uitgebreid te verwerken. Op dit recht kan slechts in een aantal gevallen een beroep op worden gedaan. Op dit recht kan een verzoek worden gedaan wanneer de burger aan heeft gegeven dat zijn of haar persoonsgegevens onjuist zijn en hier een onderzoek naar is ingesteld. Een andere grond is wanneer de verwerking onrechtmatig is, maar de burger wil niet dat zijn of haar gegevens verwijderd worden. De burger kan ook gebruik maken van dit recht wanneer de persoonsgegevens niet meer nodig zijn voor de doeleinden, maar de burger heeft deze gegevens nodig voor een rechtelijke procedure. Wanneer sprake is van een of meerdere van de bovengenoemde situaties worden persoonsgegevens alleen bewaard en niet verwerkt.⁵¹

Wanneer een succesvol beroep op de tweede, derde of vierde beroepbare rechten wordt gedaan en deze persoonsgegevens aan ontvangers worden gegeven, moeten de ontvangers op de hoogte gesteld worden van de wijzigingen. Een ontvanger kan een andere gemeente zijn of de politie. De burger kan de gemeente Oosterhout verzoeken een afschrift van de reactie van de derde partijen toe te zenden. Op deze manier kan gecontroleerd worden dat alle partijen de juiste en meeste actuele persoonsgegevens bezitten.⁵²

Het vijfde beroepbare recht is het recht op dataportabiliteit. Dit recht beschrijft dat de gemeente de persoonsgegevens waarover zij beschikt, op verzoek van de burger aan een andere verwerkingsverantwoordelijke doorgeeft. De verwerking moet dan wel via geautomatiseerde procedures worden verricht. Hierbij is te denken aan een applicatie waarin de persoonsgegevens worden verwerkt. De gemeente Oosterhout zal niet snel verplicht zijn dit recht uit te voeren. Dit recht hoeft alleen uitgevoerd te worden wanneer de persoonsgegevens verwerkt worden op basis van toestemming van de burger of de uitvoering van een overeenkomst die met de burger is afgesloten.⁵³ Aan de hand van het verwerkingsregister is te zien dat de gemeente Oosterhout persoonsgegevens meestal verwerkt vanuit een wettelijke plicht of in het kader van een publiekrechtelijke taak.⁵⁴

Het zesde beroepbare recht geeft de mogelijkheid tot bezwaar. De burger mag altijd bezwaar maken tegen de verwerking van zijn of haar persoonsgegevens. Het bezwaar van verwerking zal alleen door de gemeente Oosterhout gehonoreerd worden wanneer de persoonsgegevens worden verwerkt in het kader van het algemeen belang of openbaar gezag. Hierbij is bijvoorbeeld te denken aan de veiligheid binnen de gemeente Oosterhout. Wanneer de gemeente Oosterhout gegevens verwerkt voor marketing doeleinden of gebruik maakt van profilering kan de burger succesvol bezwaar maken. Profilering houdt in dat door middel van geautomatiseerde verwerking, persoonsgegevens aan de hand van bepaalde persoonlijke aspecten worden verwerkt. Een voorbeeld hiervan is contactgegevens van inwoners boven de 65 jaar op een lijst zetten voor een cursus digitaliseren.

De verwerkingsverantwoordelijke staakt de verwerking gedurende het onderzoek naar het bezwaar, tenzij er sprake is van een zwaarwegend belang. Wanneer persoonsgegevens worden verwerkt met het oog op wetenschappelijk of historisch onderzoek of statistische doeleinden, heeft de burger ook het recht bezwaar te maken tegen de verwerking. Er zijn wel uitzonderingen op van toepassing zoals de uitvoering van een taak van algemeen belang.⁵⁵

Het zevende beroepbare recht heeft betrekking op de mogelijkheid om de burger te beschermen tegen het onderworpen worden aan een uitsluitend geautomatiseerde besluitvorming. Dit betekent

⁵¹ Artikel 18 van de Algemene verordening gegevensbescherming

⁵² Artikel 19 van de Algemene verordening gegevensbescherming

⁵³ Artikel 20 van de Algemene verordening gegevensbescherming en Richtlijn inzake het recht op gegevensoverdraagbaarheid 5 april 2017, groep gegevensbescherming artikel 29.

⁵⁴ 'Register van verwerking', gemeenteoosterhout 20 mei 2018, gemeenteoosterhout.nl (zoek op: privacy).

⁵⁵ Artikel 21 van de Algemene verordening gegevensbescherming

dat de verwerking van persoonsgegevens kan geschieden zonder menselijke tussenkomst. We spreken dan van volledig geautomatiseerde verwerking. Wanneer op basis van deze geautomatiseerde verwerking een besluit wordt gemaakt, spreekt men van een geautomatiseerde besluitvorming. Het moet wel gaan om besluitvorming waar een rechtsgevolg voor de burger uit volgt. Een voorbeeld van een geautomatiseerde besluitvorming met een rechtsgevolg is het volledig geautomatiseerd afwijzen van een omgevingsvergunning. Op het nemen van een geautomatiseerd besluit rust een verbod. Dit verbod mag doorbroken worden. Dit mag echter alleen wanneer: de geautomatiseerde besluitvorming noodzakelijk is voor de naleving van een overeenkomst of een wettelijke bepaling of de betrokkene zelf de gemeente Oosterhout toestemming geeft.⁵⁶

Het achtste en laatste beroepbare recht van de burger is het recht op schadevergoeding. Een succesvol beroep op dit recht vereist een drietal voorwaarden.

De burger moet dus aantonen dat:

- er een inbreuk is gemaakt op de Avg;
- dat de burger door de inbreuk materiële of immateriële schade heeft geleden; en
- dat de inbreuk door de gemeente Oosterhout is veroorzaakt.

Wanneer de schade is veroorzaakt door een partij die persoonsgegevens voor de gemeente Oosterhout verwerkt, is de gemeente Oosterhout ook aansprakelijk. De burger kan in dit geval beide partijen volledig aansprakelijk stellen voor de schade. De gemeente Oosterhout en de verwerkers kunnen het bedrag van de schade onderling naar mate van betrokkenheid en aansprakelijkheid verdelen. De gemeente Oosterhout kan het verzoek natuurlijk ook afwijzen. De burger heeft niet de mogelijkheid hier bezwaar tegen te maken, omdat dit beroepbare recht niet gelijk wordt gesteld aan een besluit. De burger kan het verzoek wel voorleggen aan de bestuursrechter.⁵⁷

§5.3 De procedure omtrent de beroepbare rechten

De Europese wetgever heeft enkele bepalingen opgesteld om te zorgen dat de beroepbare rechten op een juiste manier uitgevoerd worden door de verwerkingsverantwoordelijke. De gemeente Oosterhout zal ook aan deze procedurele voorwaarden moeten voldoen.

Wanneer de burger een beroep doet op een van de beroepbare rechten geeft de gemeente Oosterhout binnen een maand antwoord. Wanneer het verzoek dermate complex is, kan dit termijn met nogmaals twee maanden worden verlengd. Wanneer de burger gebruik wil maken van zijn of haar rechten mogen hier geen kosten voor in rekening gebracht worden. Wanneer een verzoek buitensporig is, mag de gemeente een redelijke vergoeding rekenen voor administratieve kosten of weigeren aan het verzoek te voldoen. De gemeente moet zelf aantonen dat een verzoek buitensporig is of kennelijk ongegrond.

Voordat een verzoek gehonoreerd wordt, moet gekeken worden of de burger zijn eigen persoonsgegevens opvraagt en niet die van een ander. De identiteit van de burger moet dus worden vastgesteld. Wanneer vaststaat dat de verzoeker tevens betrokkenen is, kan het verzoek worden beoordeeld. Een verzoek op basis van een beroepbaar recht wordt afgewezen wanneer het een gevaar oplevert voor onderstaande belangen en dit mogelijke gevaar zwaarder weegt dan het recht van de betrokkene. De onderstaande belangen zijn de uitzonderingsgronden.

- de nationale veiligheid;
- landsverdediging;
- de openbare veiligheid;
- andere belangrijke doelstellingen van algemeen belang;
- de bescherming van de onafhankelijkheid van de rechter en gerechtelijke procedures;

⁵⁶ Artikel 22 van de Algemene verordening gegevensbescherming

⁵⁷ Artikel 82 juncto artikel 79 lid 2 Algemene verordening gegevensbescherming

- geheimhoudingsplicht vanuit de uitoefening van een beroep;
- het openbaar gezag;
- de bescherming van de betrokkene of van de rechten en vrijheden van anderen; of
- een gerechtelijke procedure.⁵⁸

De beslissingen omtrent de beroepbare rechten zijn besluiten. Tegen besluiten van een bestuursorgaan, staat bezwaar en beroep open. De burger kan dus tegen de (gedeeltelijke) afwijzing van een verzoek op een beroepbaar recht in bezwaar en beroep gaan.⁵⁹

In het laatste onderdeel van dit hoofdstuk worden de wettelijke bepalingen omtrent de datalekken besproken. In onderstaande paragraaf zal besproken worden wat datalekken inhouden en welke handelingen er volgens de Avg en de Autoriteit Persoonsgegevens genomen moeten worden na constatering van een datalek.

§5.4 Datalekken

Men spreekt van een datalek wanneer er een beveiligingsincident heeft plaatsgevonden, waarbij persoonsgegevens verloren zijn gegaan of (mogelijk) onrechtmatig worden verwerkt.⁶⁰ Denk hierbij aan het verliezen van een USB-stick, een gestolen laptop of brand. Het verschil tussen een beveiligingsincident en een datalek is dat een datalek gevolgen heeft voor de persoonsgegevens die verwerkt worden. Wanneer er sprake is van een datalek moet actie ondernomen worden. Zodra het lek verholpen is zal gekeken of er een meldplicht is. Een datalek moet gemeld worden bij de Autoriteit Persoonsgegevens wanneer er een grote kans is dat het datalek ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens. Er is een grote kans dat het datalek ernstige gevolgen heeft voor de bescherming van persoonsgegevens als:

- het gaat om bijzondere persoonsgegevens;

Hierbij is te denken aan gegevens omtrent iemands ras of geloof, economische status, gebruiksnamen en wachtwoorden die achterhaald kunnen worden of de gegevens kunnen leiden tot stigmatisering of identiteitsfraude. Ook gegevens waar een wettelijk of beroepsmatige geheimhoudingsplicht voor geldt vallen onder deze categorie.

- de aard of de omvang kunnen er ook voor zorgen dat de gevolgen ernstig zijn;

Denk hierbij aan een datalek bij de Belastingdienst of een verzekeraar. Datalekken bij de overheid kunnen grote gevolgen hebben voor de burger. Daarnaast kan gekeken worden of de gegevens gevoelig zijn voor misbruik vanuit het crimineel circuit.

- persoonsgegevens van kwetsbare groepen.

Hierbij is te denken aan burgers die in blijf-van-mijn-lijfhuizen worden opgevangen. Wanneer dergelijke gegevens openbaar worden gemaakt, worden deze groepen onevenredig zwaar geraakt.

Wanneer het datalek onder een van de bovenstaand genoemde categorieën valt, wordt er een melding bij de Autoriteit Persoonsgegevens gemaakt. De melding geschiedt via een webformulier. Het melden gebeurt binnen 72 uur nadat kennis is genomen van het datalek. Als er niet wordt gemeld binnen de gestelde 72 uur, zal een nadere motivering mee worden gestuurd naar de Autoriteit Persoonsgegevens. In de melding aan de Autoriteit Persoonsgegevens worden de volgende onderwerpen behandeld:

- de aard van de inbreuk;

⁵⁸ Artikel 23 van de Algemene verordening gegevensbescherming

⁵⁹ Artikel 34 van de Uitvoeringswet Algemene verordening gegevensbescherming juncto artikel 1:3, 7:1, 8:1 van de Algemene wet bestuursrecht

⁶⁰ 'richtsnoeren meldplicht datalekken', *autoriteitpersoonsgegevens* 2 mei 2018, autoriteitpersoonsgegevens.nl (zoek op: *meldplicht datalekken*, p. 19-20, 23-24, 27-28, 32-35, 36-39, 43-50).

- de naam en contactgegevens van de functionaris voor de gegevensbescherming;
- de gevolgen van de inbreuk; en
- de maatregelen die de gemeente Oosterhout heeft gesteld om de inbreuk tegen te gaan en om in de toekomst soortgelijke lekken te voorkomen.

De verwerkingsverantwoordelijke documenteert alle inbreuken en de genomen maatregelen.⁶¹ Ondanks de meldingsplicht is het aan de gemeente Oosterhout om het datalek op te sporen en maatregelen te nemen en niet aan de Autoriteit Persoonsgegevens. Wanneer de melding niet wordt gemaakt en dit wel verplicht is, kan dit bestraft worden met een (bestuurlijke) boete. Wanneer naar aanleiding van de melding blijkt dat de gegevensbescherming niet op orde is, kan er nader onderzoek ingesteld worden naar de bedrijfsvoering. De Autoriteit Persoonsgegevens houdt een register bij van de gemelde datalekken. Wanneer tijdens het onderzoek meerdere wettelijke overtredingen worden geconstateerd kan er ook een (bestuurlijke) boete op worden gelegd. Wanneer er geen sprake is van ernstige verwijtbare nalatigheid of aanzienlijk onzorgvuldig en onachtzaam handelen, zal eerst een bindende aanwijzing gegeven worden. Naast het maken van een melding bij de Autoriteit Persoonsgegevens kan er ook een melding worden gemaakt bij de burger zelf. Dit is echter niet verplicht wanneer er voldoende maatregelen zijn genomen om de persoonlijke levenssfeer van de burger te beschermen. De Autoriteit Persoonsgegevens heeft aangegeven dat twee vormen (cryptografie of remote wiping) zorgen voor een effectieve waarborg van de persoonsgegevens.

Cryptografie is het versleutelen van data. Wanneer wordt getracht data zonder toestemming van de gemeente Oosterhout te verkrijgen, wordt de data voor de illegale ontvanger onleesbaar. Wanneer deze maatregel is toegepast gaat de Europese- en nationale wetgever ervan uit dat dit voldoende waarborging biedt. Het wordt gezien als voornaamste beschermingsmaatregel. De melding aan de betrokkene kan dan achterwege worden gelaten. Wel moet de versleuteling lastig zijn te verbreken. Wanneer de data niet ten tijde van het lek versleuteld is of de gegevens vernietigd, aangetast of gelezen kunnen worden, moet alsnog een melding worden gemaakt. Er zijn meerdere manieren om gelekte gegevens voor een derde onleesbaar te maken. Wanneer deze methode voldoende effectief is, blijft de meldplicht uit.

Een van die andere manieren van technische gegevenswaarborging is remote wiping. Dit wil zeggen dat men op afstand gegevens kan verwijderen. Wel moeten de gegevens gewist worden voordat de onbevoegde de gegevens in kan zien, aantasten of verspreiden. Wanneer deze methode is toegepast op de gelekte gegevens kan een melding ook achterwege worden gelaten. Als laatste wordt ook nog gekeken of er zwaarwegende belangen zijn die ervoor zorgen dat de melding aan de burger achterwege gelaten kan worden. Hierbij is te denken aan een algemeen belang van de samenleving of de openbare orde. Wanneer de gemeente Oosterhout de meldplicht bij de burger achterwege laat vanwege een zwaarwegend belang, zal dit goed gemotiveerd moeten worden. Wanneer de burger wordt geïnformeerd meldt men de aard van de inbreuk, bij welke instantie het lek heeft plaatsgevonden en de maatregelen die getroffen zijn. De gemeente Oosterhout is als verwerkingsverantwoordelijke ook verplicht om een register bij te houden van alle datalekken. Het overzicht omvat de aard en overige gegevens van het lek. Het overzicht wordt minimaal een jaar bewaard. Wanneer de betrokkene niet geïnformeerd is of het datalek nadelige effecten kan hebben, geldt het bewaartermijn voor minimaal drie jaar.⁶²

⁶¹ Artikel 33 juncto 34 van de Algemene verordening gegevensbescherming

⁶² 'De meldplicht datalekken', *autoriteitpersoonsgegevens* 12 februari 2018, autoriteitpersoonsgegevens.nl (zoek op: *datalek*).

§5.5 Samenvatting

Het hoofdstuk begon met de vraag: *‘Welke eisen stelt de Algemene verordening gegevensbescherming aan de gemeente Oosterhout met betrekking tot de rechten van de burgers en de procedure datalekken?’*

De rechten van de burger zijn besproken. De Avg geeft de gemeente Oosterhout de plicht om transparant te werken, de burger te informeren over de veranderingen en een melding te maken wanneer nieuwe persoonsgegevens verwerkt worden. Wanneer de burger actiever betrokken wil worden in de verwerking van zijn of haar persoonsgegevens, heeft de burger acht manieren om dit te verwezenlijken. De burger kan zijn of haar persoonsgegevens inzien, wijzigen, wissen, beperkt laten verwerken, versturen naar een andere verwerkingsverantwoordelijke, bezwaar maken, geautomatiseerde besluitvorming stoppen en om een schadevergoeding vragen. De gemeente Oosterhout is verplicht aan deze verzoeken gehoor te geven, mits aan de wettelijke vereiste wordt voldaan. De gemeente is verplicht het verzoek door middel van een besluit binnen een maand te beantwoorden. Wanneer sprake is van een datalek, is de gemeente Oosterhout verplicht om de persoonsgegevens zo snel mogelijk veilig te stellen. Dit kan door middel van meerdere technologische mogelijkheden. Daarnaast wordt de Autoriteit Persoonsgegevens op de hoogte gesteld wanneer het datalek gevolgen heeft voor de verwerking van de persoonsgegevens. De burger wordt op de hoogte gesteld wanneer het datalek zijn of haar persoonlijke levenssfeer kan raken.

Hoofdstuk 6: De beroepbare rechten van de burger vòòr de Avg

De vraag die in dit hoofdstuk centraal staat luidt: *‘Hoe wordt voor de inwerkingtreding van de Algemene verordening gegevensbescherming omgegaan met de beroepbare rechten van de burger vanuit de Wet basisregistratie personen?’* Om deze vraag te beantwoorden zal de dagelijkse bedrijfsvoering bij de gemeente Oosterhout onder de loep worden genomen.

De gemeente Oosterhout behandelt geen verzoeken die voortvloeien uit Wbp. De Wbp is een wet die aangeeft hoe persoonsgegevens verwerkt moeten worden. De Wbp was voor de komst van de Avg van kracht in Nederland. De Wbp is de voorloper van de Avg. Het zou logisch zijn om de Wbp daarom als uitgangspunt te nemen bij het praktijkonderzoek naar de handelswijze van de gemeente Oosterhout omtrent de beroepbare rechten. Aangezien de gemeente Oosterhout de Wbp niet heeft geïmplementeerd, is dit geen optie.

De gemeente Oosterhout behandelt wel verzoeken op basis van de BRP. Volgens de Uitvoeringswet Algemene verordening gegevensbescherming⁶³ valt de BRP niet onder de reikwijdte van de Avg. Dit betekent dat de wettelijke bepalingen van de Avg niet van toepassing zijn op de BRP, maar wanneer de Avg en de BRP naast elkaar worden gehouden is te zien dat deze verordening en wet zeer veel overeenkomsten hebben. De BRP geeft de burger een aantal soortgelijke beroepbare rechten die ook terug te vinden zijn in de Avg (1). De beroepbare rechten van de BRP zijn het recht op: inzage, correctie, geheimhouding en bezwaar.⁶⁴ Een andere overeenkomst tussen de Avg en de BRP is het toezichthoudende orgaan, de Autoriteit Persoonsgegevens (2). De Autoriteit Persoonsgegevens houdt toezicht op de uitvoering van de BRP en de Avg.⁶⁵ De Avg en de BRP zien beide toe op de verwerking van persoonsgegevens (3). Vanwege deze drie overeenkomsten is gekozen om de uitvoering van de BRP te gebruiken om een beeld te schetsen van de werkwijze omtrent de beroepbare rechten van de burger binnen de gemeente Oosterhout.

In dit hoofdstuk wordt naar de behandeling van de beroepbare rechten op basis van de BRP gekeken. De BRP geeft de burger meerdere rechten. Om het praktijkonderzoek zo goed mogelijk bij de beroepbare rechten van de Avg aan te laten sluiten, zijn slechts een aantal rechten vanuit de BRP meegenomen in het onderzoek. De overige rechten vanuit de BRP verschillen te veel om een goede vergelijking met de rechten van de Avg te kunnen maken. De Avg geeft de burger het recht op: inzage, correctie en bezwaar.⁶⁶ Deze rechten zijn ook terug te vinden in de BRP.⁶⁷ De handelswijze rond deze drie beroepbare rechten wordt onderzocht.

De BRP geeft de burger ook de mogelijkheid de verstrekking van persoonsgegevens aan derden tegen te gaan. Dit recht heet geheimhouding.⁶⁸ De Avg geeft de burger de mogelijkheid de verwerking van zijn of haar persoonsgegevens te beperken.⁶⁹ Dit recht, de beperking van de verwerking, zorgt ervoor dat de persoonsgegevens niet bovenmatig worden verwerkt. Een vorm van bovenmatig verwerken is het verstrekken van de gegevens aan derden zonder dat de verstrekking noodzakelijk is voor de verwezenlijking van het doel van de verwerking. De beperking van verwerking geeft de burger, onder andere, bescherming tegen de verstrekking van zijn of haar persoonsgegevens aan derden. Ondanks dat het recht van beperking van verwerking meer omvattend is dan het recht op geheimhouding, kan de betrokkene met beide rechten de verstrekking van zijn of haar persoonsgegevens aan derden aan banden leggen.

⁶³ Artikel 2 tweede lid van de Uitvoeringswet Algemene verordening gegevensbescherming

⁶⁴ Artikel 2:60 van de Wet basisregistratie personen juncto artikel 1:3, 7:1, 8:1 van de Algemene wet bestuursrecht

⁶⁵ Artikel 4:1- 4:3 van de Wet basisregistratiepersonen juncto artikel 1:13 van de Wet basisregistratie personen

⁶⁶ Artikel 15,16 en 21 van de Algemene verordening gegevensbescherming

⁶⁷ Artikel 2.54, 2.60, 3.24, 2.56, 2.58 van de Wet basisregistratie personen

⁶⁸ Artikel 2.57 van de Wet basisregistratie personen

⁶⁹ Artikel 18 van de Algemene verordening gegevensbescherming

De rechten geheimhouding van de BRP en beperking van verwerking van de Avg, bieden de burger dus een soortgelijke bescherming. Om deze reden wordt het recht op geheimhouding ook meegenomen in het onderzoek.

De verzoeken met betrekking tot de vier beroepbare rechten van de BRP worden bij de frontoffice (lees: balie) van de afdeling Burgerzaken ingediend. De backoffice van de afdeling Burgerzaken behandelt het verzoek verder inhoudelijk. Om de werkwijze in kaart te brengen zijn bij de front- en backoffice observaties en interviews gehouden. De interviews, observatieschema's en formulieren waarop de verzoeken worden genoteerd (lees: standaard formulieren) zijn terug te vinden in de bijlagen 4, 5 en 6. Om voldoende helderheid te geven over de beroepbare rechten op basis van de BRP, zullen deze beroepbare rechten eerst kort worden toegelicht.

§6.1 De vier beroepbare rechten van de basisregistratiepersonen

Het eerste recht, is het recht op inzage. Het verzoek om inzage betreft zowel op de persoonsgegevens zelf als de verwerkingsgegevens. Het recht op inzage heeft dus eenzelfde werking als in de Avg wordt gesteld. De burger geeft aan welke gegevens hij of zij in wil zien en deze worden vervolgens verzameld. Het verzoek wordt geweigerd wanneer een ander belang prevaleert, zoals de bescherming van de openbare orde.⁷⁰ De burger krijgt kopieën opgestuurd van de opgevraagde gegevens, indien er geen ander belang prevaleert.⁷¹

Het tweede recht is het recht op correctie. Wanneer een burger van mening is dat de persoonsgegevens waarover de gemeente Oosterhout beschikt onjuist, onvolledig of in strijd met een wettelijke bepaling zijn, kan er een verzoek tot correctie worden ingediend. De burger zal wel zelf aan moeten tonen dat de persoonsgegevens onjuist of onvolledig zijn. De burger kan dit aantonen door brondocumenten, zoals een geboorteakte of trouwakte, aan te leveren. Een verzoek tot correctie kan op meerdere aspecten betrekking hebben. Hierbij is te denken aan een naamswijziging of wijziging van de burgerlijke stand.⁷²

Het derde recht is het recht op geheimhouding. De burger kan bezwaar maken tegen het verstrekken van zijn of haar persoonsgegevens aan andere partijen. In de basisregistratie wordt dan een aantekening gemaakt over deze beperking.⁷³ In principe worden de gegevens alleen verstrekt aan:

- een overheidsinstelling die deze persoonsgegevens nodig heeft voor een goede taakvervulling;
- een private instelling indien dit voortvloeit uit een algemeen verbindend voorschrift;

In de memorie van toelichting zijn algemeen verbindende voorschriften omschreven als: *“naar buiten werkende, voor de daarbij betrokkenen bindende regels, uitgegaan van het openbaar gezag dat de bevoegdheid daartoe aan de wet ontleent”*.⁷⁴ Een algemeen verbindend voorschrift is een besluit van algemene strekking. Een algemeen verbindend voorschrift geeft rechtsregels aan die een overheidsinstelling heeft opgesteld. Een voorbeeld hiervan is de Algemene Plaatselijke Verordening. In de Algemene Plaatselijke Verordening staat de gemeentelijke regelgeving op het gebied van openbare orde en veiligheid. Elke gemeente heeft een eigen Algemene Plaatselijke Verordening die geldt voor iedereen binnen de gemeente. De Algemene Plaatselijke Verordening wordt vastgesteld door de gemeenteraad. Een algemeen verbindend voorschrift kan ook een wet in materiële zin worden genoemd. Een wet in materiële zin wil zeggen dat de wet niet tot stand is gekomen in de

⁷⁰ Artikel 2:60 juncto 2:55 van de Wet basisregistratie personen

⁷¹ Bijlagen 4,5,6,7.

⁷² Artikel 2:56-2:58 van de Wet basisregistratie personen

⁷³ Artikel 2:59 van de Wet basisregistratie personen

⁷⁴ Kamerstukken II 1993/ 94, 23700, nr. 3.

Staten-Generaal, maar middels een andere overheidsinstelling. Het woord ‘algemeen’ in algemeen verbindend voorschrift geeft aan dat de maatregel niet op een specifiek geval is gericht, maar belang heeft voor allerlei burgers in meerdere situaties.⁷⁵

Een private instelling is een bedrijf dat geen onderdeel is van de overheid. Een privaat bedrijf die deze gegevens op kan vragen op basis van een algemeen verbindend voorschrift is een advocaat. Een advocaat heeft een uittreksel uit de basisregistratie nodig voor een gerechtelijke procedure.

- Eenieder indien de burger toestemming heeft gegeven.⁷⁶

Het vierde en laatst beroepbare recht dat binnen de reikwijdte van dit project valt, is het recht op bezwaar. Bezwaar kan ingesteld worden tegen elk besluit. Een afwijzing van een verzoek op inzage, correctie of geheimhouding is een besluit. Tegen een besluit staat de mogelijkheid tot bezwaar en beroep open. Wanneer hiertegen bezwaar wordt gemaakt, is de gemeente Oosterhout verplicht een heroverweging te maken. In de volgende paragraaf zal gekeken worden hoe wordt omgegaan met deze rechten in de praktijk.⁷⁷

§6.2 De werkwijze van de frontoffice

De medewerkers bij de frontoffice zijn geobserveerd om op deze manier in kaart te brengen hoe wordt omgegaan met de beroepbare rechten. Tijdens deze observatie is gekeken naar de manier waarop de burger wordt geïdentificeerd, welke gegevens verder worden uitgevraagd en in welke applicatie de gegevens worden gezet. In het observatieschema zijn deze drie punten terug te vinden. Er is gekozen om tijdens de observatie niet enkel naar persoonsgegevens met betrekking tot de beroepbare rechten van de BRP te kijken. Deze keuze is genomen, omdat deze verzoeken niet frequent binnenkomen. Om toch een juist beeld te schetsen van de handelswijze bij de frontoffice zijn meerdere verzoeken van de burger meegenomen. Hierbij is te denken aan een verstrekking van een rijbewijs of het doorgeven van een verhuizing. Er kan beargumenteerd worden dat er te veel informatie wordt verzameld tijdens de observaties, omdat niet enkel is gekeken naar de beroepbare rechten van de BRP. Deze ‘extra’ informatie is bijvangst. De bijvangst kan het onderzoek beïnvloeden, omdat deze informatie betrekking heeft op de onderzoeksvraag van dit hoofdstuk. Dit ‘probleem’ is opgelost door het gebruik van de standaard formulieren. De standaard formulieren worden gebruikt om een verzoek op de beroepbare rechten van de BRP aan te nemen. Aan de hand van deze formulieren kan dus alsnog precies afgelezen worden welke informatie voor welk verzoek wordt uitgevraagd.

Uit de observering blijkt dat van de 38 verzoeken er 32 betrekking hadden op de persoonsgegevens van de burger zelf. Van de 32 verzoeken werden er 31 burgers aan de hand van legitimatie geïdentificeerd. In 37 gevallen van de 38 verzoeken werd gevraagd naar (aanvullende) persoonsgegevens. Uit de interviews met de medewerkers van de frontoffice is naar voren gekomen dat het vaststellen van de identiteit van de burger middels het adres of geboortedatum gebeurt. Aan de hand van de observatie bleek echter dat een identiteitskaart in haast alle gevallen werd gevraagd. De bevindingen en de verklaringen spreken elkaar tegen.

De medewerkers werken hoofdzakelijk vanuit het systeem genaamd Key2Burgerzaken. Dit is het systeem waarin de basisregistratie van de burger wordt weergegeven. Key2Burgerzaken werd 31 keer geraadpleegd. In Key2Burgerzaken kunnen wijzigingen aangebracht worden in de basisregistratie. De wijzigingen die betrekking hebben op de vier beroepbare rechten van de BRP worden niet door de frontoffice afgehandeld, hoewel sommige medewerkers bij de frontoffice wel

⁷⁵ Artikel 8:2 juncto 8:3 van de Algemene wet bestuursrecht

⁷⁶ Artikel 3:4-3:18 van de Wet basisregistratie personen

⁷⁷ Artikel 2.60 juncto 3.24 van de Wet basisregistratie personen

de autorisatie hebben om dit te doen. Aangezien het tijdrovend werk is om een verzoek op een beroepbaar recht inhoudelijk te behandelen, vindt de beoordeling niet bij de frontoffice plaats. Zo kan de medewerker van het Informatie- en Servicecentrum eerste lijn (lees: de telefooncentrale) geen wijzigingen in de basisregistratie aanbrengen.

Naast het systeem Key2Burgerzaken, wordt ook gewerkt in het zaaksysteem. Alle digitale verzoeken komen hierop binnen. Daarnaast worden de verzoeken hier ook in opgeslagen zodat ze altijd terug te vinden zijn. Het zaaksysteem werd 11 keer gebruikt gedurende de observatie. In 10 van de 11 keer werd het zaaksysteem naast Key2Burgerzaken gebruikt.

De medewerkers bij de frontoffice geven aan dat er volgens een vaste handelswijze wordt gewerkt. Voor de beroepbare rechten van de BRP zijn standaard formulieren opgesteld. Aan de hand van deze formulieren worden de verzoeken aangenomen. Er worden verschillende persoonsgegevens uitgevraagd bij elk verzoek. In onderstaand schema wordt overzichtelijk weergegeven wanneer welke persoonsgegevens worden uitgevraagd.

Verzoeken:	Soort persoonsgegevens:
Verzoek om inzage verwerkingsgegevens	Burgerservicenummer (hierna te noemen: 'BSN'), naam, geboorteplaats en –datum, adres en postcode, woonplaats, telefoonnummer, e-mailadres, handtekening en de verzoeker wordt aan de balie geïdentificeerd.
Verzoek om inzage persoonsgegevens	BSN, naam, geboorteplaats en –datum, adres en postcode, woonplaats, telefoonnummer, e-mailadres, handtekening, de verzoeker wordt aan de balie geïdentificeerd en de verzoeker geeft aan hoe hij of zij de persoonsgegevens in wil zien, de mogelijkheden zijn aan de balie of middels afschrift.
Verzoek om correctie	Naam, geboortedatum, adres, postcode en woonplaats, welke correcties / wijzigingen / aanvullingen, onderliggende stukken, handtekening en een kopie van het identiteitsbewijs.
Verzoek om geheimhouding	Middels DigiD kan dit verzoek worden ingediend. Er worden geen verdere gegevens uitgevraagd.
Bezwaar	Bezwaar kan vormloos worden ingediend, met inachtneming van de vormeisen zoals omschreven in de Algemene wet bestuursrecht. De algemene vormeisen zijn: naam, adres, dagtekening, omschrijving van het besluit waartegen bezwaar wordt ingediend en de gronden van bezwaar. ⁷⁸

Het is opvallend dat bij het verzoek tot inzage, van zowel verwerkingsgegevens als de persoonsgegevens, zeer veel gegevens worden uitgevraagd. Het telefoonnummer of e-mailadres van een burger lijkt in eerste instantie niet noodzakelijk om een verzoek tot inzage te beoordelen en uit te voeren. De vraag rijst of de uitgevraagde gegevens niet buitensporig zijn in verhouding tot de uitvoering van het verzoek.

§6.3 De inhoudelijke behandeling bij de backoffice

Bij de backoffice van de afdeling Burgerzaken worden alle verzoeken op basis van de BRP inhoudelijk behandeld. Bij de backoffice is een medewerker geobserveerd en geïnterviewd. Aan de hand van het interview en het protocol wordt meer duidelijk over de handelswijze met betrekking tot de beoordeling van de verzoeken. Onderstaand worden de verzoeken en de handelswijze doorgenomen. De citaten van de medewerker over de handelswijze zijn tussen aanhalingstekens aangegeven.

De verzoeken op basis van de BRP komen binnen bij de backoffice. *“De verzoeken komen altijd middels de formulieren binnen.”*⁷⁹ Aan de hand van het formulier kan het verzoek beoordeeld worden. Het verzoek wordt (gedeeltelijk) gehonoreerd en uitgevoerd of afgewezen. Over de vele persoonsgegevens die worden opgevraagd middels de standaard formulieren stelt de medewerker

⁷⁸ Artikel 6:5 van de Algemene wet bestuursrecht

⁷⁹ Bijlage 6.

van de backoffice het volgende: *“Ik heb dit niet allemaal nodig. Dit wordt waarschijnlijk gebruikt om dit in de BRP aan te vullen. We hebben een vrij veld in Key2Burgezaken. Hieraan zijn mensen makkelijker te vinden. In het zaakstelsel kunnen deze gegevens ook ingevuld worden. Voor het verzoek te behandelen heb je de gegevens niet nodig. Alleen voor administratieve doeleinden gebruiken we ze.”* Ook het BSN is niet nodig om het verzoek te behandelen. *“Ik kan mensen aan de hand van hun naam en adres ook vinden in het stelsel. Je hebt meerdere gegevens nodig om mensen te vinden, helemaal wanneer gegevens foutief zijn ingevuld. Een BSN is een middel om iemand te vinden maar het kan op meerdere manieren.”*

Tijdens de observatie zijn de rechten op inzage en correctie behandeld. De behandeling van het recht op inzage is vrij eenvoudig. De gevraagde gegevens worden verzameld en geprint. De geprinte gegevens worden gecontroleerd aan de hand van het verzoek en in een envelop gestopt waarnaar het verstuurd wordt.

Bij een verzoek op correctie wordt voornamelijk gekeken naar de brondocumenten die als onderbouwing dienen. Met brondocumenten duidt de medewerker op een officieel document zoals een akte. De burger levert brondocumenten aan om de correctie te onderbouwen. Gedurende de observatie werd een geboorteakte uit Polen en een trouwakte uit Turkije bestudeerd. De brondocumenten worden op echtheid gecontroleerd door het bestuderen van de echtheidskenmerken voordat het verzoek inhoudelijk wordt behandeld.⁸⁰ De meeste correcties die doorgevoerd worden, worden onderbouwd door buitenlandse brondocumenten. Het is daarom dus van belang dat de beoordeling van de buitenlandse brondocumenten op een juiste manier plaatsvindt. Als de correctie juist blijkt, worden de gegevens gewijzigd en ontvangt de burger hier een melding van.

Het recht op geheimhouding is niet gedurende de observatie aan bod gekomen. Dit verzoek vraagt niet om een intensief beoordelingsproces. Het verzoek komt digitaal binnen. Er wordt een aantekening in de basisregistratie gemaakt dat de gegevens in beginsel niet aan andere partijen verstrekt mogen worden. Vervolgens wordt een brief naar de burger gestuurd waarin bevestigd wordt dat de aantekening in de basisregistratie is opgenomen. Het recht op geheimhouding betekent echter niet dat de persoonsgegevens nooit aan andere partijen verstrekt worden. De medewerker zegt hier het volgende over:

“Er is een groep derde die deze gegevens altijd krijgen. Advocaten zijn de grootste groep hiervan. Komt er een verzoek binnen van de advocaat die deze informatie wil. Dan gaan wij de burger eerst benaderen.”

Met het benaderen van de burger wordt bedoeld dat er een voornemen van een besluit wordt toegezonden. In dit voornemen staat dat de gemeente Oosterhout van plan is de gegevens met de derde partij te delen. De burger kan hierop reageren. Wanneer de burger het niet eens is met de verstrekking, kan hij of zij dat gemotiveerd aangeven. Vervolgens zal er een beslissing moeten worden gemaakt over de verstrekking. De medewerker stelt het volgende over deze belangenafweging: *“We kijken naar de persoonlijke levenssfeer. Wanneer dit wordt geschaad mag je het verzoek afwijzen. Het verhaal is bij iedereen anders, dus moet je deze belangenafweging maken. In die brief die we versturen aan de burger, het voornemen, laat je weten dat we van plan zijn de gegevens te verstrekken en kunnen ze met een motivatie reageren. Negen van de tien keer krijgen we hier niet eens een reactie op.”* Twee weken nadat het voornemen is verstuurd, wordt het besluit genomen. De medewerker verklaart dat dit echter niet de gehele procedure is: *“Omdat ze hier ook weer het recht op bezwaar hebben doen we nog zes weken niks. Je moet mensen het termijn van bezwaar gunnen, geven.”*

⁸⁰ ‘wat zijn de echtheidskenmerken van het paspoort en de identiteitskaart’, *rijksoverheid* 27 april 2018, rijksoverheid.nl (zoek op: echtheidskenmerken).

Voor het laatste beroepbare recht, het recht op bezwaar, wordt met de afdeling Juridische Zaken samengewerkt. De burger kan een brief opstellen waarin wordt aangegeven tegen welk besluit hij of zij bezwaar maakt. Bezwaar kan ook ingesteld worden tegen een positief besluit, dit is opmerkelijk aangezien de wetgever enkel afwijzingen van een van de bovenstaand beroepbare rechten als besluit heeft gedefinieerd.⁸¹ De afdeling Juridische Zaken handelt het bezwaar af. Volgens de medewerker werkt de samenwerking als volgt: *“Zij beoordelen het verzoek. Ze halen hier voornamelijk de informatie vandaan en zij gieten het dan in een juridisch vat.”* De juridische afdeling overlegt met de backoffice. Er wordt besproken hoe het besluit tot stand is gekomen en welke belangenafweging is gemaakt en gemaakt moet worden. De samenwerking tussen beide afdelingen is intensief. Vervolgens wordt het besluit op bezwaar middels de fysieke post naar de burger terug gezonden. De medewerker stelt dat niet altijd tijdig een besluit wordt genomen. Dit heeft te maken met de werkdruk.

§6.4 Samenvatting en conclusie

De vraag die in dit hoofdstuk centraal staat luidt: *‘Hoe wordt voor de inwerkingtreding van de Algemene verordening gegevensbescherming omgegaan met de beroepbare rechten van de burger vanuit de Wet basisregistratie personen?’* Om deze vraag te beantwoorden zijn observaties en interviews gehouden bij de afdeling Burgerzaken. De beroepbare rechten van de BRP die onderzocht zijn, zijn het recht op inzage, correctie, geheimhouding en bezwaar.

Een verzoek om inzage of correctie wordt bij de frontoffice van de afdeling Burgerzaken ingediend. Het indienen gebeurt middels een formulier. In de formulieren voor inzage en correctie worden de volgende persoonsgegevens uitgevraagd: BSN, naam, geboorteplaats en –datum, adres en postcode, woonplaats, telefoonnummer, e-mailadres, handtekening, de verzoeker geeft aan hoe hij of zij de persoonsgegevens in wil zien en een kopie van het identiteitsbewijs wordt in sommige gevallen toegevoegd. Vervolgens wordt dit formulier doorgestuurd naar de backoffice van de afdeling Burgerzaken. Het besluit omtrent het verzoek wordt vervolgens via de post naar de burger gezonden. Over deze behandeling kan worden opgemerkt dat er te veel persoonsgegevens worden opgevraagd dan daadwerkelijk noodzakelijk is voor de behandeling van het verzoek. De medewerker bij de backoffice geeft aan dat veel persoonsgegevens als aanvullende informatie wordt gebruikt. De persoonsgegevens die worden opgevraagd worden per post naar de burger verzonden. Het recht op geheimhouding kan digitaal worden uitgeoefend. Er is een online platform gecreëerd waardoor de burger gemakkelijk een beroep kan doen op zijn of haar beroepbare recht. De gemeente Oosterhout kan hierop vervolgens eenvoudig reageren.

Het recht op bezwaar is vormvrij. De burger kan zelf kiezen hoe hij of zij gebruik wil maken van dit recht. Hierbij is te denken aan een brief versturen via (aangetekende) post of het gebruikmaken van het online contactformulier. Er wordt gesteld dat er te veel persoonsgegevens uitgevraagd worden middels de standaard formulieren. Dit zorgt voor een onnodige grote datastroom. Vervolgens wordt al deze informatie middels de post verzonden. De post is geen betrouwbare manier om de besluiten inclusief persoonsgegevens te versturen. Deze methode van verwerking kan het begin zijn van een groot aantal datalekken. Een positieve kanttekening die gemaakt kan worden is dat de problematiek omtrent de beroepbare rechten van de BRP vrij eenvoudig te herstellen zijn. De manier waarop het recht op geheimhouding wordt behandeld lijkt een ideaal platform. Het digitaliseren binnen een beveiligde applicatie zorgt voor waarborging. De vraag rijst waarom de ander drie rechten, inzage, correctie en bezwaar niet digitaal worden ingericht. Op korte termijn zal in ieder geval gekeken moeten worden naar de vragen die gesteld worden in de standaard formulieren bij het recht op inzage en correctie. Het aantal uitgevraagde persoonsgegevens kan zo al ingeperkt worden. Wanneer de gegevens middels aangetekende post worden verstuurd, wordt de kans op een datalek verkleind.

⁸¹ Artikel 2.60 juncto 3.24 van de Wet basisregistratie personen

Hoofdstuk 7: Het nieuwe bedrijfsproces

De beroepbare rechten van de burger op basis van de Avg zijn in hoofdstuk 5 besproken. In hoofdstuk 6 is de dagelijkse bedrijfsvoering binnen de gemeente Oosterhout besproken. In dit hoofdstuk wordt een nieuwe procedure besproken. De nieuwe procedure moet ervoor gaan zorgen dat de verzoeken op basis van de beroepbare rechten van de burger op een juiste manier worden beoordeeld door de gemeente Oosterhout. De vraag die centraal staat in dit hoofdstuk luidt: *‘Welke handelingen zijn van belang voor het waarborgen van de beroepbare rechten van de burgers op basis van de Algemene verordening gegevensbescherming in de dagelijkse bedrijfsvoering van de gemeente Oosterhout?’* De handelingen die van belang zijn zullen door middel van een proces worden uitgevoerd. Het proces is een primair proces, omdat alle activiteiten bijdragen aan het tot stand komen van een besluit. Om het primaire proces te beheersen worden drie elementen van het primaire proces besproken.

- Het eerste element: Er moet een duidelijke doelstelling zijn.

De verzoeken op basis van de beroepbare rechten van de burgers moeten middels een proces snel en effectief beoordeeld en inhoudelijke behandeld kunnen worden. Aan alle wettelijke vereisten van de Avg moet voldaan worden, maar dit mag niet ten koste gaan van de bedrijfsvoering.

- Het tweede element: De gestelde organisatiedoelen moeten uitvoerbaar zijn.

Dit betekent dat er voldoende capaciteit en kennis moet zijn om alle verzoeken te behandelen. Het proces omtrent het beoordelen van het verzoek kan in vijf stappen worden opgedeeld. De 5 stappen worden een voor een besproken in de volgende paragraaf.

- Het derde element: Het bedrijfsproces moet beïnvloed kunnen worden.

Het proces wordt beïnvloed door de vijf stappen van uitvoering.

§7.1 Het nieuwe bedrijfsproces in vijf stappen

Stap 1:

Om het de burger zo makkelijk mogelijk te maken om van zijn of haar beroepbare recht gebruik te maken, kan een verzoek digitaal worden ingediend. Op de website van de gemeente Oosterhout wordt aangegeven wat de Avg inhoudt. Er wordt aangegeven welke rechten de burger heeft, hoe de gemeente Oosterhout met deze rechten omgaat en hoe wordt voldaan aan de verantwoordingsplicht. Naast informatie over de Avg en de uitvoering hiervan, wordt dus de mogelijkheid aangeboden om een verzoek op een beroepbaar recht digitaal in te dienen. De burger kan inloggen met zijn of haar DigiD en vervolgens aangeven op welk recht een beroep wordt gedaan. Door het inloggen met DigiD wordt de identiteit van de burger vastgesteld en kan met zekerheid gesteld worden dat de burger zijn of haar eigen persoonsgegevens opvraagt. Naast het online platform kan een verzoek op een beroepbaar recht ook fysiek worden ingediend bij de frontoffice van de afdeling Burgerzaken. Er zal door de ambtenaar gecontroleerd worden of het verzoek betrekking heeft op de persoonsgegevens van de burger zelf. De formulieren die worden gebruikt om de verzoeken te behandelen zijn in het beroepsproduct te vinden.

Stap 2:

Wanneer het verzoek door de burger correct is ingevuld via de website of een fysiek formulier zal een beoordeling plaatsvinden door een ambtenaar van de afdeling Gegevensmanagement. (Het complete beoordelingsschema is terug te vinden in het beroepsproduct.) Als eerste moet gekeken worden of het verzoek betrekking heeft op de persoonsgegevens van de burger (1). Wanneer dit vaststaat moet gekeken worden op welke wettelijke basis het verzoek behandeld moet worden (2). De Avg is niet de enige wettelijke basis waarom een verzoek door de burger ingediend kan worden. Zoals eerder besproken kan op basis van de BRP en de Wob ook een verzoek tot inzage en correctie van (persoons)gegevens worden ingediend. Wanneer blijkt dat het verzoek op basis van een andere

grondslag dan de Avg is ingediend zal het verzoek moeten worden doorgestuurd naar de juiste afdeling. De desbetreffende afdeling zal het verzoek dan zelf afhandelen. Wanneer er geen andere grondslag gevonden kan worden voor het verzoek of het verzoek geen betrekking heeft op de persoonsgegevens van de burger, wordt het verzoek afgewezen. Aangezien het verzoek niet voldoet aan de formele eisen van de beroepbare rechten is de afwijzing geen besluit. De burger kan niet in bezwaar tegen deze beslissing.

Wanneer blijkt dat het verzoek betrekking heeft op de Avg zal gekeken moeten worden of het verzoek gehonoreerd kan worden. Het verzoek zal inhoudelijk beoordeeld moeten worden. De Europese wetgever heeft per beroepbaar recht een aantal eisen gesteld. Aan de wettelijke vereisten moet door de burger worden voldaan (3). Wanneer dit het geval is moet er nog gekeken worden of er geen uitzonderingsbepalingen van artikel 23 Avg van toepassing zijn. De gemeente Oosterhout moet kijken of er geen ander prevalerend belang is. Als het verzoek niet door de toetsing komt, wordt het verzoek afgewezen. De burger wordt hiervan schriftelijk op de hoogte gesteld door middel van een besluit. Wanneer er geen reden is het verzoek niet in te willigen na de inhoudelijke toetsing worden de persoonsgegevens verzameld binnen de gemeente Oosterhout(4).

Stap 3:

Middels het zaaksysteem worden de verzoeken doorgestuurd naar de afdelingen waar de persoonsgegevens zich bevinden. Een zaaksysteem is een compleet zaakgericht gemeente breed documentmanagementsysteem met archivering. Het zaaksysteem houdt bij wie wat heeft gedaan en worden alle handelingen opgeslagen en de documenten worden gelijk op de juiste plek gearhiveerd. Daarnaast kan ook aangegeven worden hoe lang bepaalde zaken / documenten bewaard moeten worden. In het zaaksysteem wordt aangegeven hoelang de medewerkers hebben om de gevraagde informatie te verzamelen en terug te sturen naar het team Gegevensmanagement. De afdelingen hoeven enkel de persoonsgegevens te verzamelen, verwijderen of wijzigen en doorsturen.

Stap 4:

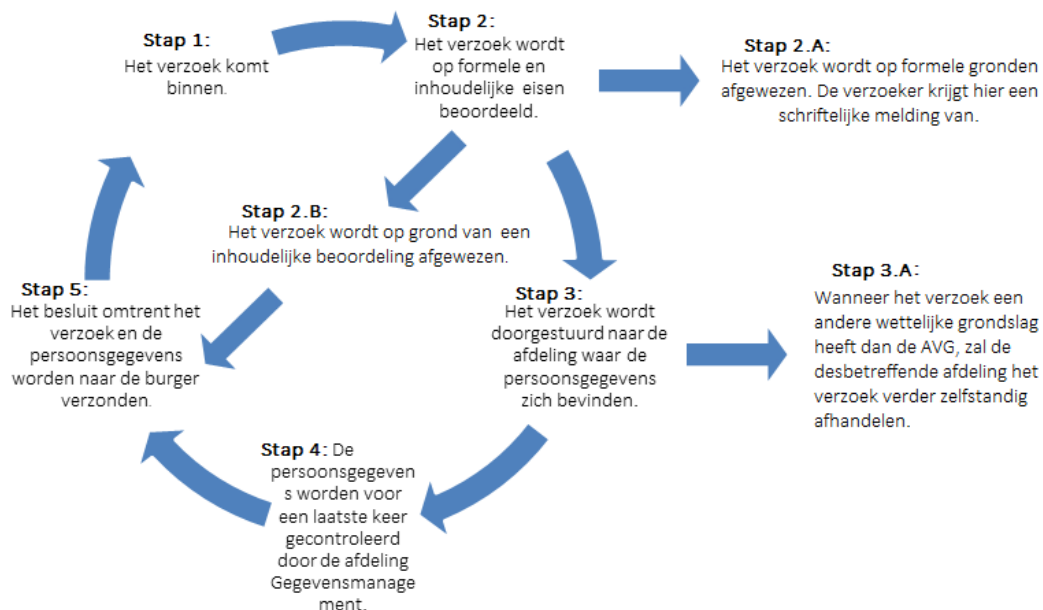
Wanneer de afdelingen de persoonsgegevens op hebben gestuurd naar het team Gegevensmanagement, zal er een laatste controle plaatsvinden. Er moet beoordeeld worden of: de juiste persoonsgegevens worden meegestuurd (1), of de belangen van andere burgers niet geraakt worden (2) en of andere verwerkers op de hoogte moeten worden gesteld van mogelijke wijzigingen omtrent de persoonsgegevens of de verwerking ervan (3). Wanneer deze laatste controle is uitgevoerd kan het besluit worden genomen. Het gehele beoordelingsschema is terug te vinden in het beroepsproduct.

Stap 5:

De beslissing wordt in de vorm van een besluit aan de burger overhandigd.⁸² Wanneer het verzoek digitaal is binnengekomen, kan het besluit in het postvak worden gezet inclusief de persoonsgegevens. Op deze manier hoeven er geen kosten gemaakt te worden voor het fysiek versturen van de persoonsgegevens. Wanneer het verzoek niet digitaal is ingediend, zal het besluit middels aangetekende post verstuurd worden of kan het besluit opgehaald worden bij het stadhuis. De burger geeft bij het indienen van het verzoek aan op welke manier hij of zij het besluit wil ontvangen. De burger kan tegen het besluit van de gemeente Oosterhout in bezwaar en beroep gaan.⁸³

⁸² Artikel 34 van de Uitvoeringswet algemene verordening gegevensbescherming

⁸³ Artikel 7:1 juncto 8:1 van de Algemene wet bestuursrecht

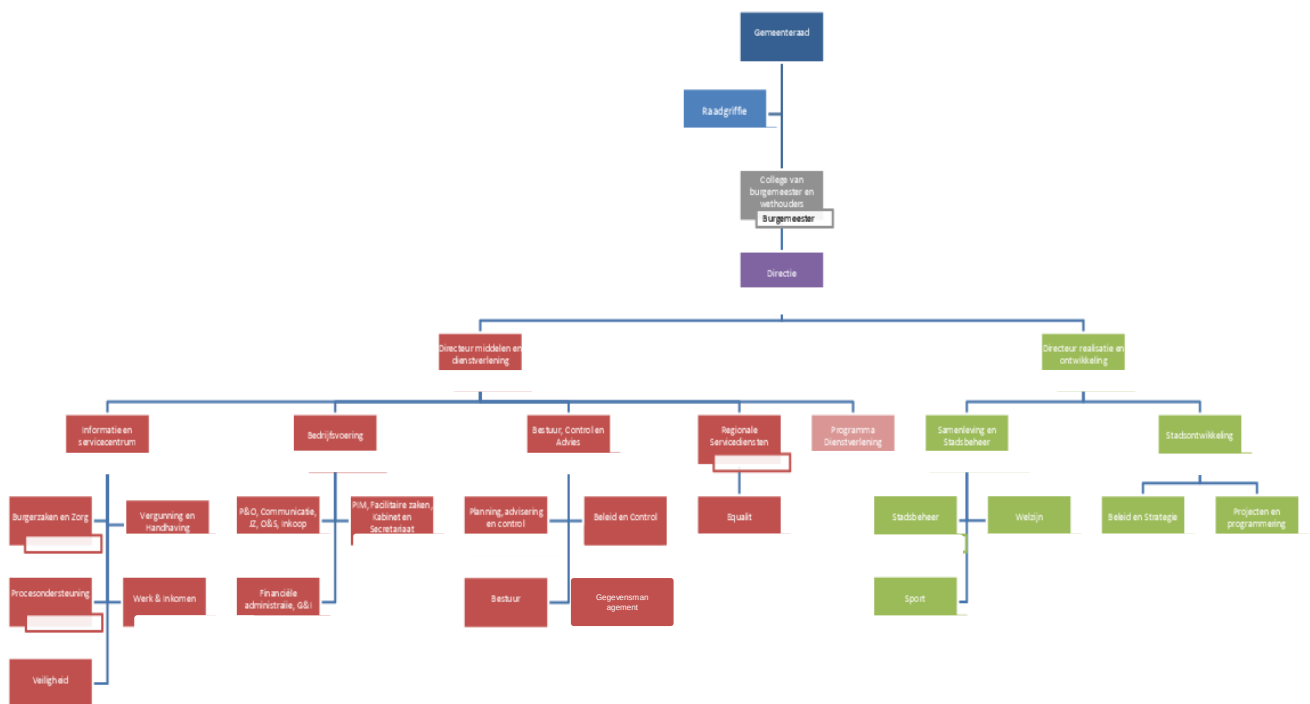


§7.2 De deelnemers van het nieuwe primaire proces

Bij het opzetten van een nieuw systeem is het van belang dat de juiste ambtenaren de juiste taken uitvoeren voor een zo efficiënt mogelijk proces. De toetsingsmomenten van stap 2 en 4 worden uitgevoerd door het team Gegevensmanagement. Op de andere afdelingen zullen de persoonsgegevens verzamelt, gewijzigd of verwijderd en vervolgens doorgestuurd moeten worden, zoals omschreven in stap 3. De taken omtrent de Avg voert de privacybeheerder van de afdeling uit. Elke afdeling binnen de gemeente Oosterhout is vanaf april 2018 verplicht een privacybeheerder aan te stellen. De privacybeheerder regelt voor de desbetreffende afdeling alle privacy rechtelijke aspecten. Hieronder vallen de verzoeken omtrent de beroepbare rechten van de burger, maar ook het uitvoeren van DPIA's op de gegevensverwerkingen. De gemeente Oosterhout is op te delen in de volgende afdelingen:

- Bestuur, Control & Advies;
- Informatie en Servicecentrum;
- Samenleving en Stadsbeheer;
- Regionale Servicediensten;
- Bedrijfsvoering; en
- Stadsontwikkeling.

Op al deze zes afdelingen is een privacybeheerder aangesteld. Voor sommige afdelingen zijn er twee of meer privacybeheerders aangesteld, omdat de taken op de afdeling ver uiteen lopen of er vallen meerdere clusters onder een afdeling.



§ 7.3 Samenvatting

Het hoofdstuk begon met de vraag: ‘Welke handelingen zijn van belang voor het waarborgen van de beroepbare rechten van de burgers op basis van de Algemene verordening gegevensbescherming in de dagelijkse bedrijfsvoering van de gemeente Oosterhout?’

De handelingen omtrent de beoordeling van het verzoek van de beroepbare rechten zijn in vijf stappen opgedeeld. Stap 1 is het verzoek aannemen. Het aannemen kan zowel digitaal als middels een formulier. Stap 2 is het beoordelen van het verzoek. De beoordeling is formeel en inhoudelijk. De formele beoordeling kijkt naar het feit of de burger wel de betrokkene is en of de wettelijke grondslag correct is. Tijdens de inhoudelijke beoordeling wordt gekeken naar de wettelijke eisen die de Avg stelt. Daarnaast wordt door de gemeente Oosterhout ook gekeken naar andere (prevalerende) belangen. Nadat de beoordeling is afgerond, wordt het verzoek naar de afdelingen gestuurd voor de uitvoering. Dit is stap 3. De uitvoering kan zijn het verzamelen, wijzigen of verwijderen van de persoonsgegevens. Wanneer de afdeling het verzoek heeft uitgevoerd wordt nogmaals gecontroleerd of het verzoek goed is uitgevoerd, er geen belangen van andere partijen worden geschaad of andere aspecten over het hoofd zijn gezien. Het tweede controle moment is stap 4. Als laatste stap, stap 5, wordt het besluit omtrent het verzoek naar de burger verzonden. De burger kan bij het indienen van het verzoek aangeven hoe hij of zij het besluit wenst te ontvangen.

Om de persoonsgegevens van de burgers te waarborgen zijn de toetsingsmomenten, zoals omschreven in stap 2 en 4, cruciaal. De stappen 2 en 4 zorgen dat er geen persoonsgegevens worden uitgegeven, verwijderd, doorgegeven of gewijzigd wanneer dit verzoek niet op een beroepbaar recht is gebaseerd. Zowel de burger die het verzoek indient als het verzoek zelf worden bekeken. De wettelijke vereisten en andere belangen worden bekeken. De stappen 2 en 4 zorgen ervoor dat er op een veilige manier met persoonsgegevens wordt omgegaan.

In het kader van een efficiënte afhandeling is stap 1 van belang. De verzoeken kunnen bij het Stadhuis ingeleverd te worden. Het verzoek kan online worden ingediend. Het besluit wordt middels een zelfde weg naar de burger teruggestuurd. Het gebruik maken van een digitaal platform maakt het voor zowel de burger als de ambtenaar makkelijker om aan de Avg te voldoen.

Hoofdstuk 8: De datalekprocedure van de gemeente Oosterhout

Het laatste onderdeel van de derde reeks deelvragen is de handelswijze rondom de datalekken binnen de gemeente Oosterhout in kaart brengen. De vraag die centraal staat in dit hoofdstuk luidt: *‘Wat is de huidige handelingswijze van de Gemeente Oosterhout bij het signaleren van een datalek?’* Om deze vraag te beantwoorden zal als eerste gekeken worden naar de datalekprocedure die de gemeente Oosterhout heeft opgesteld. Vervolgens wordt er aan de hand van een aantal casussen gekeken of ook daadwerkelijk volgens het protocol wordt gehandeld.

De gemeente Oosterhout heeft een datalekprocedure opgesteld. Deze procedure is terug te vinden in bijlage 9. In deze procedure wordt uitgelegd wat een datalek is. Daarnaast wordt vermeld dat een datalek bij de functionaris gegevensbescherming moet worden gemeld. Het maken van deze melding mag direct bij de functionaris gegevensbescherming of via de leidinggevende van de desbetreffende afdeling worden gemaakt. Wanneer de functionaris gegevensbescherming op de hoogte is gesteld, wordt het datalek ook doorgegeven aan het college van burgemeester en wethouders. Het onderzoek omtrent het datalek wordt direct na de constatering gestart. De functionaris gegevensbescherming, de informatiebeveiligingscoördinator en de privacybeheerder van de desbetreffende afdeling komen bij elkaar. Dit onderzoeksteam kijkt naar: de aard van het beveiligingsincident, de mogelijke oorzaak, of er sprake is van niet-nakoming of een tekortkoming in de beveiligingsprocedure en of er sprake is van verwijtbaar handelen. De nakoming heeft te maken met een correcte uitvoering van de beveiligingsprocedure. Een tekortkoming van de beveiligingsprocedure houdt in dat procedure niet toereikend is. De procedure is dan wel goed uitgevoerd, maar de procedure zelf zorgt voor onvoldoende bescherming. Het verwijtbaar handelen houdt in dat onachtzaam gehandeld wordt.⁸⁴

Wanneer deze vier aspecten in kaart zijn gebracht, wordt door de functionaris gegevensbescherming een verslag gemaakt over het datalek. De plaats van het datalek wordt hierin vernoemd. Hierbij is te denken aan de afdeling of zelfs welke medewerker betrokken is bij het datalek. In het verslag wordt ook benoemd op welke persoonsgegevens het datalek betrekking heeft. Het soort beveiligingsincident wordt ook in kaart gebracht en de (categorie) burgers van wie de persoonsgegevens zijn. Ook worden de maatregelen beschreven die genomen zijn nadat het onderzoeksteam op de hoogte werd gebracht van het datalek. Deze maatregelen bewerkstelligen het oplossen van het datalek, de schade te beperken die is ontstaan door het datalek en bieden voldoende veiligheid om dergelijke datalekken in de toekomst te voorkomen. Naast het opstellen van een verslag van het datalek, wordt ook gekeken naar de meldingsplicht. Wanneer de persoonlijke levenssfeer van de burger wordt geraakt, wordt een melding gemaakt bij de burger zelf. Wanneer het datalek gevolgen heeft voor de verwerking van de persoonsgegevens, wordt een melding gemaakt bij de Autoriteit Persoonsgegevens.

§8.1 Datalekken in de praktijk

In de bovenstaande paragrafen van dit hoofdstuk wordt het datalekprotocol van de gemeente Oosterhout besproken. Aan de hand van twee casussen zal gekeken worden hoe wordt gehandeld door de gemeente Oosterhout.

In december 2017 heeft een datalek plaatsgevonden bij de gemeente Oosterhout. Een medewerker (hierna te noemen: ‘medewerker X’) van de gemeente Oosterhout kreeg een e-mailbericht in de inbox van het programma Outlook. In dit e-mailbericht stonden inloggegevens die bestemd waren voor een andere nieuwe medewerker (hierna te noemen: ‘medewerker Z’). De medewerker X kon de: naam, adres, salarisgegevens, mailbox en burgerlijke staat van medewerker Z inzien en wijzigen. Het e-mailbericht was door de afdeling P&O (lees: personeelszaken) verstuurd. Nadat het datalek was gemeld door medewerker X is nader onderzoek ingesteld naar de handelswijze van P&O. Uit verschillende interviews is naar voren gekomen dat het (nieuwe) inboekproces bij P&O nog niet goed

⁸⁴ Kamerstukken II 2013/14, 33 662, nr. 16, p. 1.

beveiligd was. Wanneer een nieuwe medewerker wordt aangenomen, moet er een account gemaakt worden voor de nieuwe medewerker. Dit doet de subafdeling van P&O genaamd de Salarisadministratie handmatig in workforce. Workforce is een salarisadministratie applicatie waarin alle medewerkers van de gemeente Oosterhout staan. Voor het aanmaken van een account heeft de subafdeling Salarisadministratie een e-mailadres nodig. De subafdeling Salarisadministratie weet niet welke e-mailadressen al gebruikt worden door medewerkers. Salarisadministratie maakt het e-mailadres door de eerste letter van de voornaam, de achternaam en de naam van de gemeente toe te voegen. De inloggegevens van medewerker Z zijn naar medewerker X gestuurd, omdat het e-mailadres al in gebruik was. De medewerkers X en Z hadden dezelfde voorletter en achternaam. Drie dagen nadat het datalek geconstateerd was, werd de functionaris gegevensbescherming op de hoogte gesteld. De functionaris gegevensbescherming heeft dezelfde dag nog interviews afgenomen met de medewerkers van P&O en medewerker X. Medewerker X heeft de bewijzen van het datalek (printscreen en inloggegevens) gedeeld. Door de functionaris gegevensbescherming is besloten dat het niet waarschijnlijk is dat de inbreuk een risico vormt voor de rechten en vrijheden van medewerker Z. Om deze reden is er geen noodzaak om het datalek te melden bij de Autoriteit Persoonsgegevens. De medewerker Z is zes dagen nadat het datalek was geconstateerd geïnformeerd. De functionaris gegevensbescherming heeft medewerker Z laten zien tot welke gegevens medewerker X inzicht had en uitgelegd hoe de afweging heeft plaatsgevonden om dit datalek niet te melden bij de Autoriteit Persoonsgegevens. Er zijn maatregelen genomen om soortgelijke datalekken in de toekomst tegen te gaan. De medewerkers van Salarisadministratie werken bij het aanmaken van een e-mailadres en account voor de nieuwe medewerker samen met andere medewerkers van P&O. De andere medewerkers kunnen in het systeem wel zien welke e-mailadressen al in gebruik zijn.

Het tweede datalek:

Begin oktober 2017 zijn computers gestolen die zich binnen een pand van de gemeente Oosterhout bevonden. Op deze computers stonden persoonsgegevens. De persoonsgegevens hadden betrekking op: adressen van gemeente Oosterhout, kopieën van de pinbonnetjes en gedeeltelijke bankrekeningnummers. Het datalek is de volgende dag opgemerkt en gemeld bij de Autoriteit Persoonsgegevens. De burger van wie de persoonsgegevens afkomstig zijn, zijn niet op de hoogte gesteld. De functionaris gegevensbescherming heeft deze afweging gemaakt, omdat het onwaarschijnlijk is dat de burger ongunstige gevolgen ervaart in de persoonlijke levenssfeer naar aanleiding van het datalek. De computers bevatten niet voldoende persoonsgegevens om zeer nadelige effecten voor de burger te bewerkstelligen. Er zijn geen maatregelen genomen om een soortgelijk datalek in de toekomst te voorkomen.

§8.2 Samenvatting en conclusie

Dit hoofdstuk begon met de vraag: *‘Wat is de huidige handelingswijze van de Gemeente Oosterhout bij het signaleren van een datalek?’* Aan de hand van de casussen en het datalekprotocol kan de handelingswijze van de gemeente Oosterhout worden opgemaakt. Volgens het datalekprotocol moet het datalek zo spoedig mogelijk gemeld worden bij de functionaris gegevensbescherming of de leidinggevende van de melder. Bij de eerste casus zaten 3 dagen (72 uur) tussen de constatering van het datalek en de melding aan de functionaris gegevensbescherming. Het duurde 6 dagen (144 uur) voordat de nieuwe medewerker op de hoogte werd gesteld van het datalek. Hoewel voor het melden aan de betrokkene geen termijn van 72 uur is gesteld, lijkt het een onnodig lang termijn. De nieuwe medewerker had eerder op de hoogte gesteld kunnen worden. In beide casussen onderzoekt de gemeente Oosterhout de datalekken grondig en neemt, waar nodig, maatregelen om dergelijke datalekken in de toekomst te voorkomen. De aard en oorzaak van het lek worden vastgesteld. Met de medewerkers wordt het lek besproken om op deze manier maatregelen te kunnen nemen. De gemeente Oosterhout handelt volgens haar eigen datalekprotocol.

Hoofdstuk 9: Conclusies en aanbevelingen

Het onderzoek is uitgevoerd en alle deelvragen zijn beantwoord. In dit hoofdstuk zal de laatste vraag, de centrale vraag, beantwoord worden. De centrale vraag luidt: *“Aan welke juridische voorwaarden moet de gemeente Oosterhout voldoen om haar verwerkingsprocessen van persoonsgegevens van de burgers in overeenstemming met de Algemene verordening gegevensbescherming te laten lopen?”*

§9.1 Conclusies

De gemeente Oosterhout voert een groot aantal verwerkingsprocessen met betrekking tot persoonsgegevens uit. Gedurende dit onderzoek zijn er vier verwerkingsprocessen onder de loep genomen. Deze vier processen zijn:

- openbaring van persoonsgegevens op basis van de Wob;
- het uitvoeren van DPIA's;
- de rechten van betrokkenen uitvoeren; en
- de datalekprocedure.

Bij het eerste verwerkingsproces, het openbaar maken van stukken waarin persoonsgegevens worden vermeld op basis van de Wob, geeft de Avg de verwerkingsverantwoordelijke vrij veel speelruimte. De Avg maakt het mogelijk persoonsgegevens te verwerken, en dus ook te openbaren, op basis van een wettelijke grondslag. Artikel 2, 3 en 8 van de Wob bieden die wettelijke grondslag. Zolang het Wob-verzoek betrekking heeft op een bestuurlijke aangelegenheid, waar binnen een bestuursorgaan al snel sprake van is, worden persoonsgegevens geopenbaard op verzoek van de burger. Eenieder kan dus stukken met een bestuurlijk karakter waarin persoonsgegevens worden weergegeven inzien. Een voorbeeld hiervan is een bezwaarschrift. Een bezwaarschrift is opgesteld door een burger. Hierin wordt iemands mening, adres, naam en handtekening weergegeven.

Artikel 10 van de Wob geeft wel aan dat er een belangenafweging gemaakt moet worden wanneer er bij de openbaring van bestuursrechtelijke stukken de persoonlijke levenssfeer van een burger wordt geraakt. Jurisprudentie zorgt ervoor dat tijdens de belangenafweging wordt gekeken naar het maatschappelijk belang van het verzoek. Ook het doel van het instellen van een Wob-verzoek wordt meegenomen bij de belangenafweging. De gemeente Oosterhout geeft een duidelijke invulling aan de belangenafweging van artikel 10 van de Wob. De eerbiediging van de persoonlijke levenssfeer prevaleert in bijna alle gevallen. De gemeente Oosterhout zal door haar eigen invulling van deze belangenafweging niet snel persoonsgegevens van haar burgers openbaren. De juridische voorwaarden van de Avg en de Wob worden in dit verwerkingsproces nageleefd.

Het tweede verwerkingsproces is het uitvoeren van DPIA's. Het uitvoeren van de DPIA's is een verplichting die de gemeente Oosterhout is opgelegd vanuit de Avg. Door de uitvoering wordt dus al voldaan aan de juridische voorwaarden van de Avg. Over de inhoud van NOREA in samenhang met juridische verplichtingen valt wel het een en ander op te merken. NOREA stelt niet verplicht om een systematische beschrijving van het proces weer te geven, hoewel dit wel een verplichting is vanuit de Avg. Daarnaast wordt ook niet gekeken naar de uitvoering van de gedragscode. Aan niet alle juridische voorwaarden van de Avg wordt dus voldaan binnen NOREA. Daarnaast wordt aan de gehele verantwoordingsplicht nog niet voldaan. De verwerkingsovereenkomsten moeten nog opgesteld worden. De gemeente Oosterhout is druk bezig met alle verwerkers een overeenkomst te sluiten, maar dit proces kan nog enige tijd kosten. De rol van de functionaris gegevensbescherming kan anders worden ingedeeld. De functionaris gegevensbescherming is momenteel bezig met het aanpassen van de verwerkingsprocessen. Wanneer de gemeente Oosterhout zover is dat het aangepaste beleid gecontroleerd kan worden, controleert de functionaris gegevensbescherming feitelijk haar eigen werk. Dit zorgt voor een onbetrouwbare controle.

Het derde verwerkingsproces is het uitvoeren van de rechten van betrokkenen. De gemeente Oosterhout informeert de burger over het feit dat er gebruik kan worden gemaakt van de rechten. Aan de informatieplicht van artikel 12 Avg wordt dan ook voldaan. De plicht tot transparant werken komt gedeeltelijk tot uitvoering door het verwerkingsregister dat te vinden is op de website van de gemeente Oosterhout. Er kan nog niet geconstateerd worden of aan de meldplicht wordt voldaan. Hierover kan pas een oordeel worden gevormd na 25 mei 2018. De gemeente Oosterhout zal de burger op de hoogte moeten stellen wanneer nieuwe persoonsgegevens worden verwerkt. Wanneer deze melding wordt gemaakt bij de burger, voldoet de gemeente aan de meldingsplicht, mits overige formaliteiten in acht worden genomen.

De beroepbare rechten zullen ook uitgevoerd moeten worden binnen de gemeente Oosterhout. De verzoeken op basis van de Wbp zijn niet tot nauwelijks door de gemeente Oosterhout behandeld. Er is dus geen basis waarop verder gebouwd kan worden. De afdeling Burgerzaken beoordeelt de verzoeken op basis van de BRP. Er is echter niet voldoende kennis en capaciteit om ook de afhandeling van de verzoeken op basis van de beroepbare rechten van de Avg bij de afdeling Burgerzaken onder te brengen. De werkdruk zal verdeeld moeten worden. Uit het praktijkonderzoek bij de afdeling Burgerzaken is gebleken dat de digitale mogelijkheden te weinig worden benut. Het digitaal indienen van een verzoek zorgt voor meer rust bij de frontoffice van de afdeling Burgerzaken. Daarnaast is het eenvoudiger de juiste informatie, persoonsgegevens, bij de afdelingen op te vragen. Aangezien de burger al zijn persoonsgegevens op mag vragen zal meer samenwerking met de afdelingen noodzakelijk zijn. De gemeente Oosterhout voldoet niet aan de juridische voorwaarden die de Avg stelt voor de beroepbare rechten. Voor het inhoudelijk beoordelen van de verzoeken moeten processen worden opgesteld. Daarnaast moet het voor de burger makkelijk gemaakt worden om gebruik te maken van deze rechten.

Het vierde en laatste verwerkingsproces dat binnen de reikwijdte van dit onderzoek valt, is het verwerkingsproces rondom de datalekken. De Avg stelt een aantal wettelijke vereisten wanneer een datalek is geconstateerd. Hieronder valt de meldplicht bij de Autoriteit Persoonsgegevens en / of de betrokkene(n). Daarnaast moeten maatregelen genomen worden om dergelijke incidenten in de toekomst te voorkomen. Om aan de juridische voorwaarden te voldoen heeft de gemeente Oosterhout een datalekprotocol opgesteld. Door middel van het protocol worden de meldingen bij constatering bij de functionaris gegevensbescherming, of leidinggevende, gemeld. De functionaris gegevensbescherming kan het datalek vervolgens beoordelen, een eventuele melding maken, maatregelen nemen en een onderzoek starten. De gemeente Oosterhout hoeft geen veranderingen door te voeren. Het datalekprotocol voldoet aan de juridische voorwaarden.

Uit het eerste datalek blijkt dat de functionaris gegevensbescherming effectief heeft gehandeld nadat de melding was gemaakt. Er is dezelfde dag nog een onderzoek ingesteld naar het datalek. De betrokken medewerkers zijn gehoord en er zijn maatregelen genomen om dergelijke problematiek in de toekomst te voorkomen. De melding aan betrokkene, de nieuwe medewerker, had eerder plaats kunnen vinden. Het besproken datalek, is een beveiligingsincident binnen de organisatie zelf. Wanneer het datalek ervoor had gezorgd dat de gegevens van de medewerker voor het publiek toegankelijk werden, had de betrokkene onmiddellijk op de hoogte gesteld moeten worden. De inbreuk op de persoonlijke levenssfeer was dan vele malen groter geweest. Dat er een afweging wordt gemaakt hoe groot de kans is dat de betrokkene wordt geraakt in zijn of haar persoonlijke levenssfeer is ook terug te zien bij het tweede datalek.

Bij het tweede datalek is geen melding bij de Autoriteit Persoonsgegevens noch de betrokkenen gemaakt, omdat de persoonsgegevens zeer moeilijk herleidbaar waren. De gemeente Oosterhout handelt volgens haar eigen datalekprotocol. De belangenafwegingen worden zorgvuldig gemaakt en onderzoeken onmiddellijk ingesteld.

§9.2 Aanbevelingen

Aan de verantwoordingsplicht wordt nog niet geheel voldaan. De gemeente Oosterhout zal met alle verwerkers een verwerkingsovereenkomst op moeten stellen. De gemeente Oosterhout is momenteel druk bezig om aan deze verplichting te voldoen.

De rol van de functionaris gegevensbescherming moet een meer toezichthoudend karakter krijgen. De privacybeheerders hebben een privacy-expert nodig met wie gesproken kan worden over de implementatie van de Avg. Momenteel is de functionaris gegevensbescherming deze expert. Dit zorgt er echter wel voor dat het onafhankelijke en onbevooroordeelde karakter van de functionaris gegevensbescherming wordt beïnvloed. Wanneer de advisering door een andere privacy-expert uitgevoerd wordt, zorgt dat ervoor dat de onafhankelijke controlerende positie van de functionaris gegevensbescherming niet in gevaar komt. De gemeente Oosterhout zal een nieuwe medewerker aan moeten nemen. Het laatste aspect van de verantwoordingsplicht is het uitvoeren van DPIA's

De DPIA's kunnen worden uitgevoerd middels NOREA. Aan NOREA kunnen stappen worden toegevoegd om het beter aan te laten sluiten bij de dagelijkse bedrijfsvoering van de gemeente Oosterhout. Als de volgende stappen worden toegevoegd aan NOREA wordt zowel aangesloten bij de wettelijke verplichtingen als de dagelijkse bedrijfsvoering binnen de gemeente Oosterhout:

Stap 1.0 Beschrijf de verwerkingsketen van het verwerkingsproces.

Stap 3.2.1 Is het noodzakelijk een verwerkingsovereenkomst met de externe partijen op te stellen?

Stap 3.2.2 (Bij 'Ja' op vraag 3.2.1) Is er een verwerkingsovereenkomst opgesteld en ondertekenend met de externe partijen die voldoet aan alle wettelijke verplichtingen?

Stap 3.2.3 (Bij 'Ja' op vraag 3.2.2) Komt het beleid en de handelswijze van beide partijen overeen met de afspraken die gemaakt zijn in de verwerkingsovereenkomst?

Stap 9.0 Is er beleid of een gedragscode opgesteld omtrent de verwerking?

Stap 9.1 (Bij 'Ja' op vraag 9.0) Voldoet de gedragscode of het beleid aan de Avg?

Stap 9.2 (Bij 'Ja' op vraag 9.1) Wordt de gedragscode of het beleid nageleefd?

De gemeente Oosterhout heeft het nieuwe systeem voor de beroepbare rechten van de burger nog niet in de dagelijkse bedrijfsvoering opgenomen. De burger kan momenteel nog geen verzoek op basis van een beroepbaar recht indienen bij de gemeente Oosterhout. De gemeente Oosterhout is momenteel bezig een nieuw systeem hiervoor in te richten. Meer informatie hierover is te vinden in het beroepsproduct.

Hoofdstuk 10: Literatuurlijst

§10.1 Literatuur

Artikelen

Bastiaans, NJB 2018, p.1-3

Steven Bastiaans, 'De inwerkingtreding van de AVG', NJB 2018/61, P.1-3.

Bontje, NJB 2018/51, p.1-5

N.N. Bontje, 'Uitvoeringswet AVG', NJB 2018/51, p.1-5.

De Vries & Meijer, Gst. 2017, p. 1-8

mr. dr. H.H. de Vries en mr. S.A.M. Meijer, 'Privacy en gemeenten: de Algemene Verordening Gegevensbescherming', Gst. 2017/132, p.1-8.

Dujardin, NTB 2017/33, p.1-13

M.E.M. Dujardin, 'De actieve openbaarmaking van sancties door toezichthouders en de Wet open overheid', NTB 2017/33, p.1-13.

Hijmans, NJB 2018, p.1-9

Hijmans, 'De AVG en de UAVG', NJB 2018/356, p.1-9.

Klus, Computerrecht 2018, p.1-2

M.P. Klus, 'Artikel 29 Werkgroep: conceptopinie over geautomatiseerde besluitvorming en profilering', Computerrecht 2018/26, p.1-2.

Pietermaat & Bontje, NTB 2016, p.1-14

E.C. Pietermaat en N.N. Bontje, 'Openbaarheid en behoorlijkheid', NTB 2016/9, p.1-14.

Schermer & Blankestijn, ArbeidsRecht 2018 p.10-17

S. Schermer en S.R. Blankestijn, 'De rol van de ondernemingsraad bij de implementatie van de Algemene Verordening inzake Gegevensbescherming', Arbeidsrecht 2018/15, p. 10-17.

Van de Bunt & Strijbos, NJB 2018, p.2-10

T. van de Bunt en A. Strijbos, 'De bewerkersovereenkomst onder de AVG', NJB 2018/357, p.2-10.

Van Schaik & Abassi, Bb 2017, p.1-3

Mr. R.E. van Schaik en mr. I. Abassi, 'De verplichte aanstelling van een privacy-duizendpoot: de data protection officer', Bb2017/95, p.1-3.

Van der Sloot, NTM/NJCM-bull 2016, p.1-12

B. van der Sloot, 'Kronike privacy en gegevensbescherming', NTM/NJCM-bull 2016, p.1-12.

Van der Sluis, GST. 2017, p.1-13

mr. dr. C.N. van der Sluis, 'Openbaarheid van overheidsinformatie en bescherming van de privacy', GST. 2017/131, p.1-13.

Van der Sluis, Gst. 2016/144, p.1-13

mr. dr. C.N. van der Sluis, 'De wet open overheid in de gemeentelijke praktijk; besluitvorming bij passieve en actieve openbaarmaking (deel II)', Gst.2016/144, p.1.-13.

Van der Veen, Gst. 2018, p.1

Prof. mr. G.A. van der Veen, 'Naming and shaming van Wob-misbruikers', Gst. 2018/34, p.1.

Boeken

A. Engelfriet P. Kager & L. Chew-Meij, De Algemene Verordening Gegevensbescherming. Artikelgewijs commentaar, ICTRECHT, 2017.

J. Berkvens, S. Vinken, S. Wolters, S. Wiegerinck, Checklist privacy: privacybeleid in 30 checklists, Berghauser Pont Publishing eerste druk, december 2016.

J. Marcus en N. van Dam, Organisatie en management, Groningen/ Houten: Noordhof uitgevers zevende druk 2012.

Brieven

Autoriteit Persoonsgegevens, Toetsingsmodel gegevensbeschermingseffectbeoordeling Rijksdienst, 6 juni 2017, Minister van Binnenlandse Zaken en Koninklijke relaties.

Autoriteit persoonsgegevens, Actieve publicatie van persoonsgegevens door gemeenten, 13 oktober 2017, Vereniging van Nederlandse Gemeenten.

§ 10.2 Elektronische bronnen

'Algemeenverbindendvoorschrift', noorlandjuristen 2 april 2018, noorlandjuristen.nl (zoek op: *bestuursrecht*).

'De minister voor Wonen en Rijksdienst', autoriteitpersoonsgegevens 18 juli 2016, Autoriteitpersoonsgegevens.nl (zoek op *gemeente*).

'In tien stappen voorbereid op de AVG', autoriteitpersoonsgegevens december 2017, Autoriteitpersoonsgegevens.nl (zoek op *voorbereidingen AVG*).

'Norea de beroepsorganisatie van IT-Auditors', norea 5 april 2018, norea.nl (zoek op *norea*).

'register van verwerking', gemeenteeoosterhout 20 mei 2018, gemeenteeoosterhout.nl (zoek op: *rechten*).

'Vereniging van Nederlandse gemeenten', autoriteitpersoonsgegevens 13 oktober 2017, Autoriteitpersoonsgegevens.nl (zoek op: *gemeenten*).

§10.3 Jurisprudentie

RvS 3 februari 2010, ECLI:NL:RVS:2010:BL1831.

RvS 25 juli 2012, ECLI:NL:RVS:2012:BX2593.

RvS 28 augustus 2013, ECLI:NL:RVS:2013:910.

RvS 18 februari 2015, ECLI:NL:RVS:2015:426.

RvS 17 juni 2015, ECLI:NL:RVS:2015:1903.

RvS 1 juli 2015, ECLI:NL:RVS:2015:2060.

RvS 22 februari 2017, ECLI:NL:RVS:2017:498.

RvS 2 augustus 2017, ECLI:NL:RVS:2017:2086.

EHRM 16 december 1992, ECLI:NL:XX:1992:AD1800, NJ 1993/400 (Niemietz tegen Duitsland).
EHRM 16 februari 2000, no. 27798/95 (Aman t. Zwitserland).
EHRM 28 januari 2003, nr. 44647/98 (Peck tegen het Verenigd Koninkrijk).

[§10.4 Wet- en regelgeving](#)

[Richtlijnen](#)

Autoriteit Persoonsgegevens, ‘De meldplicht datalekken in de Wet bescherming persoonsgegevens (Wbp)’, 8 december 2015.

CBP Richtsnoeren, ‘Actieve openbaarmaking en eerbiediging van de persoonlijke levenssfeer, College bescherming persoonsgegevens’, 13 augustus 2009.

Richtlijn inzake het recht op gegevensoverdraagbaarheid, groep gegevensbescherming artikel 29, 16/nl wp 242 rev.01, 5 april 2017.

Richtlijn voor gegevensbeschermingseffectbeoordelingen en bepalingen of een verwerking “waarschijnlijk een hoog risico inhoudt” in de zin van de verordening 2016/679, groep gegevensbescherming artikel 29, 17/nl wp 248 rev.01, 4 oktober 2017.

[Parlementaire stukken](#)

Kamerstukken II 1993/ 94, 23700, nr. 3.
Kamerstukken II 2017/18,34851, nr.2.
Kamerstukken II 2013/14, 33 662, nr. 16.

[Verdragen](#)

Europees verdrag voor de Rechten van de Mens
Verdrag betreffende de werking van de Europese Unie

[Wetten](#)

Algemene verordening gegevensbescherming
Algemene wet bestuursrecht
Burgerlijk wetboek
Gemeentewet
Grondwet
Uitvoeringswet Algemene verordening gegevensbescherming (concept)
Wet basisregistratie personen
Wet bescherming persoonsgegevens
Wet openbaarheid van bestuur

JE HOEFT NIET ALLES TE WETEN

Een praktijkgericht juridisch onderzoek naar de verwerkingsprocessen van de persoonsgegevens van de burger, in het kader van de inwerkingtreding van de Algemene verordening gegevensbescherming, binnen de gemeente Oosterhout.