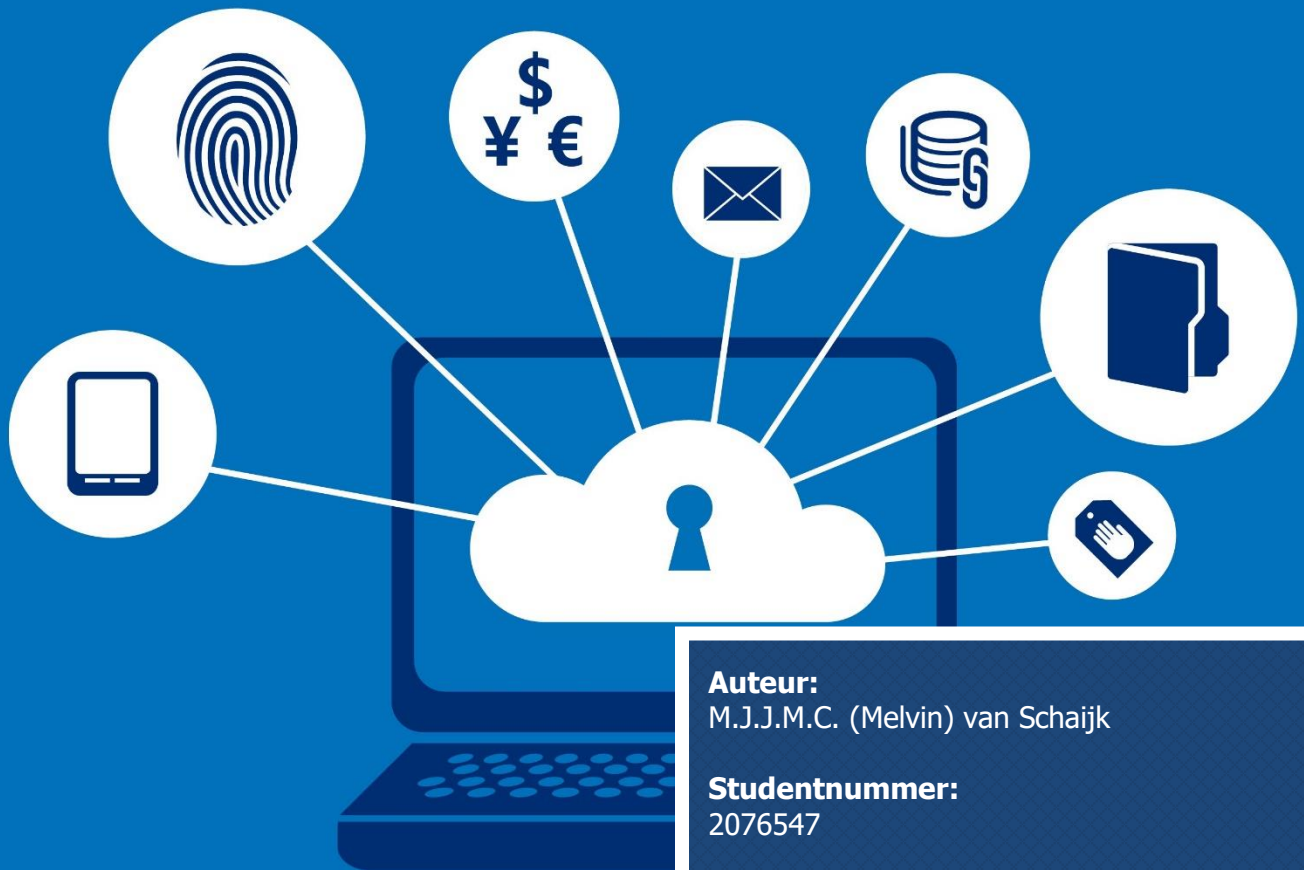


GEGEVENSVERWERKING OP ZIJN BEST

Een praktijkgericht juridisch onderzoek naar welke gevolgen de recente wijzigingen van de Wet bescherming persoonsgegevens (Wbp) en de aanstaande Algemene verordening gegevensbescherming (AVG) hebben voor de gegevensverwerkingen binnen de gemeente Best en het Privacyreglement gemeente Best.

**Auteur:**

M.J.J.M.C. (Melvin) van Schaijk

Studentnummer:

2076547

Opdrachtgever:

Gemeente Best

Afstudeermentor:

Mevrouw drs. M.W.C.C. (Marion) van Rooij

Afstudeerdocenten:

Mevrouw mr. M.M. (Marije) Knapen

Mevrouw mr. M.M.J. (Maria) van den Haspel

Stageperiode:

6 februari 2017 t/m 12 mei 2017

Best, 29 mei 2017

GEGEVENSVERWERKING

OP ZIJN BEST

Een praktijkgericht juridisch onderzoek naar welke gevolgen de recente wijzigingen van de Wet bescherming persoonsgegevens (Wbp) en de aanstaande Algemene verordening gegevensbescherming (AVG) hebben voor de gegevensverwerkingen binnen de gemeente Best en het Privacyreglement gemeente Best.

Auteur:

M.J.J.M.C. (Melvin) van Schaijk

Studentnummer:

2076547

Opdrachtgever:

Gemeente Best

Afstudeermentor:

Mevrouw drs. M.W.C.C. (Marion) van Rooij

Afstudeerdocenten:

Mevrouw mr. M.M. (Marije) Knapen

Mevrouw mr. M.M.J. (Maria) van den Haspel

Stageperiode:

6 februari 2017 t/m 12 mei 2017

Best, 29 mei 2017

VOORWOORD

Voor u ligt het onderzoeksrapport “Gegevensverwerking op zijn Best” dat is geschreven in opdracht van de gemeente Best. Het onderzoeksrapport is geschreven in het kader van mijn afstudeerstage van de opleiding HBO-Rechten aan de Juridische Hogeschool Avans-Fontys in Tilburg / 's-Hertogenbosch.

Voordat u verder gaat met lezen, wil ik een aantal personen bedanken. Op de eerste plaats mijn afstudeermentor Marion van Rooij (senior juridisch adviseur gemeente Best) voor haar enthousiaste begeleiding. Daarnaast wil ik mijn eerste afstudeerdocent Marije Knapen bedanken voor haar goede begeleiding met betrekking tot het doen van praktijkgericht juridisch onderzoek en het geven van feedback.

Het onderzoeksrapport heb ik met veel plezier geschreven. Ik vond het zeer leerzaam en interessant om dit onderzoek te verrichten. Ik wil u veel plezier wensen bij het lezen van mijn afstudeerscriptie.

Melvin van Schaijk

Best, mei 2017.

INHOUDSOPGAVE

Samenvatting

Lijst van afkortingen

1.	Inleiding	1
1.1	Probleembeschrijving	1
1.2	Centrale vraag en deelvragen	2
1.3	Doelstelling	3
1.4	Onderzoeksmethodiek	3
1.5	Leeswijzer	5
2.	Het huidige juridisch kader	6
2.1	Wet bescherming persoonsgegevens	6
2.1.1	<i>Reikwijdte</i>	6
2.1.2	<i>Begrippen</i>	7
2.1.3	<i>Algemeen kader</i>	7
2.1.4	<i>Bewaartermijn en beveiliging</i>	12
2.1.5	<i>Meldingsplicht verwerken persoonsgegevens</i>	13
2.1.6	<i>Rechten van de betrokkene</i>	13
2.1.7	<i>Rechtsbescherming</i>	14
2.1.8	<i>Toezicht en sancties</i>	15
2.2	Wet meldplicht datalekken	16
2.2.1	<i>Definitie datalek</i>	16
2.2.2	<i>Meldingsplicht</i>	17
2.2.3	<i>Sancties</i>	18
3.	De algemene verordening gegevensbescherming	19
3.1	Doelstelling	19
3.1.1	<i>Begrip persoonsgegevens</i>	19
3.1.2	<i>Begrip verwerken</i>	19
3.2	Beginselen	19
3.2.1	<i>Beginselen van rechtmatigheid, behoorlijkheid en transparantie</i>	19
3.2.2	<i>Beginsel van doelbinding</i>	20
3.2.3	<i>Beginsel van minimale gegevensverwerking</i>	20
3.3	Functionaris gegevensbescherming	21
3.3.1.	<i>Eisen</i>	21
3.3.2.	<i>Takenpakket</i>	21
3.3.3.	<i>Positie</i>	22
3.4.	Rechten van betrokkene	22
3.4.1	<i>Recht op inzage</i>	22
3.4.2	<i>Recht op rectificatie</i>	22
3.4.3	<i>Recht op gegevenswissing</i>	23
3.4.4	<i>Recht op beperking</i>	23
3.4.5	<i>Recht op dataportabiliteit</i>	23
3.5	Verschillen tussen de Wbp en AVG	24
4.	Gegevensverwerkingen binnen de gemeente Best	27
4.1	Organisatie	27
4.2	Medewerkers die zich bezighouden met gegevensverwerkingen	27
4.3	Gegevensverwerkingen	28
4.3.1	<i>Overzicht gegevensverwerkingen</i>	28
4.3.2	<i>Gegevensverwerking uitgelicht</i>	30

4.4	Beveiliging	32
4.5	Privacyreglement	34
4.6	Datalekken	34
5.	De huidige werkwijze en het Privacyreglement gemeente Best getoetst aan de Wbp & AVG	35
5.1	Huidige werkwijze	35
5.2	Privacyreglement	37
6.	Conclusies en aanbevelingen	40
6.1	Awareness	40
6.2	Functionaris voor de gegevensbescherming (FG)	40
6.3	Register- en documentatieplicht	41
6.4	Privacy impact analyse (PIA)	42
6.5	Meldplicht datalekken	42
6.6	Informatieplicht	43
6.7	Privacy by Design & Privacy by Default	43
6.8	Privacyreglement gemeente Best	44
	Literatuurlijst	45
	Bijlagen (apart document)	

SAMENVATTING

De wet- en regelgeving die ervoor zorgt dat bedrijven en organisaties persoonsgegevens op een rechtmatige manier moeten verwerken is volop in beweging. Sinds 2016 geldt de meldplicht datalekken. Kort samengevat houdt de meldplicht in dat bedrijven en organisaties binnen 72 uur een melding moeten doen bij de Autoriteit Persoonsgegevens (AP) zodra zich een ernstig datalek heeft voorgedaan. Indien de meldplicht niet wordt nagekomen kan de AP boetes opleggen die kunnen oplopen tot maximaal € 820.000,-. Voorts is met ingang van 25 mei 2018 de Algemene verordening gegevensbescherming (AVG) van toepassing. Vanaf 25 mei 2018 moeten bedrijven en organisaties voldoen aan de AVG en vervalt de Wet bescherming persoonsgegevens (Wbp). Door de komst van de AVG worden de rechten van betrokkenen verstrekt en uitgebreid, krijgen organisaties meer verplichtingen en krijgt de AP (als toezichthoudende autoriteit) een stevigere positie.

Het probleem van de gemeente Best komt erop neer dat onvoldoende duidelijk is wat de recente wijzigingen van de Wbp en de aanstaande AVG betekenen voor de ruim 100 gegevensverwerkingen die plaatsvinden binnen de gemeente Best en het Privacyreglement gemeente Best. De centrale vraag van het onderzoek luidt: *“Welke aanbevelingen kunnen gedaan worden om de huidige werkwijze met betrekking tot de verwerking van persoonsgegevens en het Privacyreglement gemeente Best zo aan te passen dat de werkwijze en het privacyreglement juridisch juist zijn gelet op de recente wijzigingen van de Wet bescherming persoonsgegevens (Wbp) en de aanstaande Algemene verordening gegevensbescherming (AVG)?”*. Om een antwoord op de centrale vraag te kunnen geven is gebruik gemaakt van verschillende onderzoeksmethoden. Voor het onderzoek van het recht zijn rechtsbronnen, literatuur en documenten geraadpleegd. Er is gebruik gemaakt van een rechtsbronnen- en literatuuronderzoek. Daar waar gebruik is gemaakt van bestaand materiaal is gebruik gemaakt van een inhoudsanalyse. Voor wat betreft het praktijkgericht deel van het onderzoek is gekozen voor een kwalitatief onderzoek. Om de praktijk te onderzoeken zijn semigestructureerde interviews gehouden, is geobserveerd en zijn documenten (beleidsstukken, werkinstructies e.d.) geraadpleegd.

Naar aanleiding van het onderzoek zijn samenvattend de volgende aanbevelingen gedaan. Voor wat betreft het beveiligingsbewustzijn van de medewerkers van de gemeente Best is aanbevolen actief door te gaan met het verhogen van het beveiligingsbewustzijn. Voor wat betreft de functionaris voor de gegevensbescherming (die de gemeente Best vanaf mei 2018 verplicht moet hebben) is aanbevolen om deze eerder dan mei 2018 aan te nemen. Voorts is aanbevolen om het overzicht gegevensverwerkingen uitvoerig te controleren op fouten en om in het overzicht gegevensverwerkingen een beschrijving te zetten van de genomen technische en organisatorische maatregelen. Daar waar uit het onderzoek is gebleken dat bepaalde gegevensverwerkingen die plaatsvinden binnen de gemeente Best een hoog privacyrisico opleveren, is aanbevolen te starten met het uitvoeren van “privacy impact assessments”. Voor wat betreft de meldplicht datalekken is aanbevolen om alle datalekken te registreren in een logboek en de datalekken te blijven melden bij de AP om hoge boetes te voorkomen. Om te voldoen aan de informatieplicht is geadviseerd om bij elke gegevensverwerking uit het overzicht gegevensverwerkingen te inventariseren hoe betrokkenen het beste geïnformeerd kunnen worden. Om te voldoen aan de beginselen van “Privacy by Design” en “Privacy by Default” is aanbevolen de medewerkers van de gemeente Best die zich bezighouden met het ontwikkelen van programma’s, websites en applicaties door middel van een vergadering op de hoogte te brengen van het beginsel van “Privacy by Design” en te controleren of in standaardformulieren niet gevraagd wordt om onnodige persoonsgegevens (bijvoorbeeld BSN-nummers). Tot slot is aanbevolen het huidige privacyreglement in te trekken en een nieuw privacyreglement op te stellen, omdat uit het onderzoek is gebleken dat het privacyreglement verouderd is.

LIJST VAN AFKORTINGEN

AP	Autoriteit Persoonsgegevens
APV	Algemene plaatselijke verordening
AVG	Algemene verordening gegevensbescherming
Awb	Algemene wet bestuursrecht
BIG	Baseline Informatiebeveiliging Gemeenten
BW	Burgerlijk wetboek
CBP	College Bescherming Persoonsgegevens
EVRM	Europees Verdrag voor de Rechten van de Mens
FG	Functionaris Gegevensbescherming
HvJ EU	Hof van Justitie van de Europese Unie
jo.	Juncto
KING	Kwaliteitsinstituut Nederlandse Gemeenten
KvK	Kamer van Koophandel
MvT	Memorie van toelichting
OM	Openbaar ministerie
PIA	Privacy impact assessment
VNG	Vereniging van Nederlandse Gemeenten
Wbp	Wet bescherming persoonsgegevens
Who	Wet hergebruik van overheidsinformatie
Wmd	Wet meldplicht datalekken
Wob	Wet Openbaarheid van Bestuur

HOOFDSTUK 1:

INLEIDING

In dit hoofdstuk komt eerst het probleem van de opdrachtgever (de gemeente Best) aan bod. Voorts worden de centrale vraag en de deelvragen beschreven. De methode van onderzoek staat per deelvraag geformuleerd. Het onderhavige hoofdstuk eindigt met een leeswijzer.

§ 1.1 Probleembeschrijving

Op grond van artikel 8 EVRM en artikel 10 Grondwet heeft iedereen in Nederland recht op eerbiediging van zijn persoonlijke levenssfeer (familie- en gezinsleven). Samengevat komt dit erop neer dat iedereen recht heeft op privacy. Artikel 10 Grondwet betreft sinds de herziening van de Grondwet in 1983 een klassiek grondrecht.¹ Dit houdt in dat de staat ervoor moet zorgen dat het recht op privacy zoveel mogelijk gewaarborgd moet worden. Privacy kan onderverdeeld worden in relationele privacy, lichamelijke privacy, territoriale privacy, communicatieve privacy, medische privacy en informationele privacy.² De vastlegging en verwerking van persoonsgegevens valt onder de informationele privacy.³ Het recht op privacy en gegevensbescherming zijn in een zekere zin met elkaar verweven. Het betreft overlappende gebieden. Het recht op privacy wordt immers gewaarborgd indien gegevens op een rechtmatige manier verwerkt worden.

De regels omtrent de verwerking van persoonsgegevens heeft de formele wetgever voornamelijk neergelegd in de Wet bescherming persoonsgegevens (Wbp). Deze wet is sinds 2001 van kracht en betreft de implementatie van richtlijn 95/46/EG.⁴ In 2016 heeft een belangrijke wijziging plaatsgevonden in de Wbp. Vanaf 2016 geldt namelijk de meldplicht datalekken. De meldplicht datalekken houdt in dat organisaties, waaronder de gemeente Best, direct (binnen 72 uur) een melding moeten doen bij de Autoriteit Persoonsgegevens (AP) zodra zij een (ernstig) datalek hebben.⁵ In 2016 hadden veel gemeenten te maken met datalekken van persoonlijke gegevens van burgers, want bijna tweederde van de gemeenten hebben in 2016 een datalek gemeld.⁶ Gemeenten, waaronder de gemeente Best, dienen dan ook maatregelen te treffen om datalekken in de toekomst te voorkomen.

Verder is op 25 mei 2016 de Algemene verordening gegevensbescherming (AVG) vastgesteld. In artikel 99 lid 2 AVG staat dat de AVG van toepassing is met ingang van 25 mei 2018.⁷ In 2018 vervalt de Wbp dan ook en moet de verwerking van persoonsgegevens voldoen aan de AVG.⁸ De wet- en regelgeving die ervoor zorgt dat bedrijven en organisaties persoonsgegevens op een rechtmatige manier moeten verwerken is dan ook volop in beweging.

Het probleem komt erop neer dat de medewerkers van de gemeente Best die zich bezighouden met het implementeren van de veranderingen op het gebied van gegevenswerking vooralsnog onvoldoende inzichtelijk hebben wat de recente wijzigingen van de Wbp en de komst van de AVG betekenen voor de gegevensverwerkingen die

¹ *Kamerstukken II* 1997/98, 25892, 3, p. 7 (MvT).

² Berkvens & Prins 2007, p. 8.

³ König & Karssenberg 2015, p. 8.

⁴ Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.

⁵ Autoriteit Persoonsgegevens, 'Beleidsregels voor toepassing van artikel 34a Wbp', p. 4.

⁶ L. Lonkhuyzen, 'Datalekken bij gemeenten; 'het is een beetje een zootje'', *NRC* 27 januari 2017.

⁷ Artikel 99 lid 2 AVG.

⁸ 'Internationale privacywetgeving', www.autoriteitpersoonsgegevens.nl (zoek op *Internationale privacywetgeving*), <Over Privacy, Wetten, Internationale privacywetgeving>.

plaatsvinden binnen de gemeente Best. Door de aanstaande AVG worden de privacyrechten van betrokkenen versterkt en uitgebreid.⁹ Een paar voorbeelden van nieuwe rechten zijn het recht op vergetelheid (ook wel het recht om vergeten te worden genoemd) en het recht op beperking.¹⁰ Voorts krijgen organisaties, waaronder de gemeente Best, meer verplichtingen waaraan voldaan moet worden.¹¹ Belangrijke verplichtingen zijn bijvoorbeeld het aanstellen van een functionaris voor de gegevensbescherming (FG) en het bijhouden van een register waarin alle verwerkingen staan beschreven (register- en documentatieplicht). De gemeente Best heeft behoefte aan een overzicht van de belangrijkste wijzigingen die betrekking hebben op de gegevensverwerkingen die plaatsvinden binnen de gemeente Best. Het is dan ook de bedoeling om een onderzoeksrapport te ontwikkelen waarbij de belangrijkste recente en aanstaande wijzigingen op het gebied van gegevensverwerking worden geanalyseerd. De medewerkers van de gemeente Best die zich bezighouden met de gegevensverwerkingen die plaatsvinden binnen de gemeente kunnen het onderzoeksrapport raadplegen indien zij van informatie voorzien willen worden over de recente en aanstaande wijzigingen.

Vrijwel zeker staat vast dat er binnen de gemeente Best organisatorische wijzigingen moeten plaatsvinden. Onderzocht moet worden welke wijzigingen dat precies zijn. In ieder geval moet er een FG worden aangesteld. De vraag rijst waar de FG aan moet voldoen (functie-eisen), wat het takenpakket van de FG is en wie de FG moet gaan worden voor de gemeente Best. Dit moet onderzocht worden. Voorts moet worden onderzocht of het Privacyreglement gemeente Best, dat openbaar gepubliceerd is op de website van de gemeente Best, nog juridisch juist is gelet op de recente wijzigingen van de Wbp en de aanstaande AVG.¹² Door middel van conclusies en aanbevelingen moet worden aangegeven welke wijzigingen noodzakelijk zijn om het privacyreglement juridisch juist te maken.

§ 1.2 Centrale vraag en deelvragen

Hieronder staat de centrale vraag beschreven. De centrale vraag wordt in het laatste hoofdstuk van het onderzoeksrapport (conclusies en aanbevelingen) beantwoord.

- Welke aanbevelingen kunnen gedaan worden om de huidige werkwijze met betrekking tot de verwerking van persoonsgegevens en het Privacyreglement gemeente Best zo aan te passen dat de werkwijze en het privacyreglement juridisch juist zijn gelet op de recente wijzigingen van de Wet bescherming persoonsgegevens (Wbp) en de aanstaande Algemene verordening gegevensbescherming (AVG)?

Hieronder staan de deelvragen beschreven. De antwoorden op de deelvragen vormen samen een antwoord op de centrale vraag.

1. Wat is het huidige juridisch kader voor het verwerken van persoonsgegevens gelet op de Wbp?
2. Wat betekent de AVG voor het verwerken van persoonsgegevens?
3. Wat is de huidige werkwijze van de gemeente Best met betrekking tot het verwerken van persoonsgegevens?

⁹ 'Algemene verordening gegevensbescherming', www.autoriteitpersoonsgegevens.nl (zoek op AVG), <Onderwerpen, Europese privacywetgeving, Algemene verordening gegevensbescherming>.

¹⁰ Artikel 17 jo. Artikel 18 AVG.

¹¹ 'Algemene verordening gegevensbescherming', www.autoriteitpersoonsgegevens.nl (zoek op AVG), <Onderwerpen, Europese privacywetgeving, Algemene verordening gegevensbescherming>.

¹² Privacyreglement gemeente Best van 25 april 2005, www.gemeentebest.nl (zoek op *Privacyreglement*), <Bestuur & organisatie, Beleid en regelgeving>.

4. Welke gevolgen heeft de nieuwe AVG voor de huidige werkwijze van de gemeente Best met betrekking tot het verwerken van persoonsgegevens en het Privacyreglement gemeente Best?

§ 1.3 Doelstelling

Op uiterlijk 28 mei 2017 om 12:00 uur wordt aan Marion van Rooij, senior juridisch adviseur gemeente Best, een onderzoeksrapport afgeleverd voor de gemeente Best, met daarin een advies betreffende de gegevensverwerkingen binnen de gemeente Best en het Privacyreglement gemeente Best.

De medewerkers van de gemeente Best die zich bezighouden met de gegevensverwerkingen binnen de gemeente Best kunnen het rapport raadplegen indien zij van informatie voorzien willen worden over de recente en aanstaande wijzigingen op het gebied van gegevensverwerking. Voorts kunnen de medewerkers van de gemeente Best die zich bezighouden met de gegevensverwerkingen binnen de gemeente Best de aanbevelingen uit het onderzoeksrapport gebruiken om de huidige werkwijze met betrekking tot de verwerking van persoonsgegevens en het Privacyreglement gemeente Best zo aan te passen dat de werkwijze en het privacyreglement juridisch juist zijn.

Het interne kennisdoel betreft adviseren. De huidige werkwijze wordt in kaart gebracht en vervolgens worden verbeterpunten voorgesteld om de werkwijze aan te passen gelet op de recente wijzigingen van de Wbp en de aanstaande AVG. Ook wordt het Privacyreglement gemeente Best beschreven en worden verbeterpunten voorgesteld.

§ 1.4 Onderzoeksmethodiek

Het onderhavige onderzoek betreft een praktijkgericht juridisch onderzoek. Een praktijkgericht juridisch onderzoek kent twee sporen: recht en praktijk.¹³ De eerste en tweede deelvraag hebben betrekking op het recht. De derde deelvraag heeft betrekking op de praktijk. De vierde deelvraag heeft betrekking op zowel het recht als de praktijk. Bij het onderzoek van de praktijk kan er gekozen worden tussen een kwantitatief en kwalitatief onderzoek. Om de praktijk te onderzoeken is gebruik gemaakt van een kwalitatief onderzoek. De nadruk voor wat betreft het onderzoek van de praktijk is namelijk gelegd op het beschrijven van de huidige werkwijze met betrekking tot het verwerken van persoonsgegevens en de toets of de werkwijze nog juridisch juist is gelet op de recente wijzigingen van de Wbp en de aanstaande AVG. Cijfermatige gegevens, die gebruikt worden bij een kwantitatief onderzoek, zijn niet gebruikt.

Voor alle bronnen die gebruikt zijn geldt dat deze gecontroleerd zijn op betrouwbaarheid en validiteit. Bij iedere bron die is gebruikt is de vraag gesteld of er redenen, eigenschappen of omstandigheden bestaan die een andere conclusie kunnen rechtvaardigen.¹⁴ Bronnen die niet aangemerkt konden worden als betrouwbaar zijn niet gebruikt in het onderzoeksrapport. Om de betrouwbaarheid van het rapport te waarborgen, is het onderzoeksrapport tussentijds beoordeeld door Marion van Rooij (senior juridisch adviseur gemeente Best). Haar expertise op het gebied van privacy en gegevensverwerking heeft geholpen bij het tot stand brengen van een volledig en betrouwbaar onderzoeksrapport.

Deelvraag 1: *Wat is het huidige juridisch kader voor het verwerken van persoonsgegevens gelet op de Wbp?*

De eerste deelvraag heeft betrekking op het onderzoek van het recht. Om de centrale vraag te beantwoorden was het noodzakelijk om het huidige juridisch kader te beschrijven. De

¹³ Van Schaaijk 2015 p. 31.

¹⁴ Van Schaaijk 2015 p. 216.

belangrijkste bronnen voor het onderzoek van het recht zijn rechtsbronnen, literatuur en documenten.¹⁵ Om een antwoord te krijgen op de eerste deelvraag is dan ook gebruik gemaakt van een rechtsbronnen- en literatuuronderzoek. De Wbp was de belangrijkste wet die geanalyseerd moest worden, omdat in de Wbp de belangrijkste regels voor het verwerken van persoonsgegevens in Nederland staan.¹⁶ Ook de meldplicht datalekken staat in de Wbp.¹⁷ Het bestuderen van de boeken “Wet bescherming persoonsgegevens in Europees perspectief” van H.R. Kranenburg & L.F.M. Verhey en “Privacyregulering in theorie en praktijk” van J.M.A. Berkmans en J.E.J. Prins heeft geholpen om de bepalingen die staan in de Wbp te begrijpen en toe te passen in het onderzoeksrapport. Voorts zijn kamerstukken geraadpleegd om achter de achterliggende bedoeling van de wetgever te komen. Er is gebruik gemaakt van bestaand materiaal en daarom is gebruik gemaakt van een inhoudsanalyse.¹⁸

Deelvraag 2: Wat betekent de AVG voor het verwerken van persoonsgegevens?

Naast de eerste deelvraag heeft ook de tweede deelvraag betrekking op het onderzoek van het recht. Wederom is een rechtsbronnen- en literatuuronderzoek verricht. De gemeente Best wilde uitgebreid geïnformeerd worden over de AVG. De AVG komt dan ook uitgebreid aan bod in het onderzoeksrapport. De AVG is als rechtsbron geraadpleegd. Deze moest geanalyseerd worden. Om de reden dat de AVG nieuw is, was er weinig literatuur over de AVG beschikbaar die geraadpleegd kon worden. Voornamelijk artikelen in vaktijdschriften en publicaties op websites (bijvoorbeeld: www.privacycompany.nl, www.autoriteitpersoonsgegevens.nl, www.ictrecht.nl en www.vng.nl) hebben geholpen bij het analyseren van de bepalingen die staan in de AVG. Wederom is gebruik gemaakt van bestaand materiaal en is gebruik gemaakt van een inhoudsanalyse.

Deelvraag 3: Wat is de huidige werkwijze van de gemeente Best met betrekking tot het verwerken van persoonsgegevens?

Deelvraag drie heeft betrekking op het onderzoek van de praktijk. Om een antwoord te krijgen op de derde deelvraag zijn semigestructureerde interviews gehouden. Een semigestructureerde interview is een interview waarbij vooraf een vragenlijst wordt gemaakt, maar ook ruimte wordt gelaten voor de inbreng van de geïnterviewde. Belangrijke/essentiële inbrengen zijn hierdoor alsnog in het onderzoeksrapport aan de orde gekomen, waardoor de volledigheid is gewaarborgd. Om antwoord te krijgen op deze deelvraag zijn de volgende mensen geïnterviewd: Marion van Rooij (senior juridisch adviseur gemeente Best), Frans Swiers (senior adviseur informatie- en automatiseringsmanagement) en Rik Verheul (informatiebeveiligingsfunctionaris). Deze personen zijn werkzaam voor de gemeente Best en konden de meeste informatie verstrekken over de huidige werkwijze met betrekking tot het verwerken van persoonsgegevens. Verder zijn documenten geraadpleegd die zowel openbaar als niet openbaar beschikbaar zijn. Met openbare documenten worden documenten bedoeld die iedereen kan raadplegen (bijvoorbeeld via de website van de gemeente Best). Met niet openbare documenten worden documenten bedoeld die alleen beschikbaar zijn voor de medewerkers van de gemeente Best (bijvoorbeeld handleidingen en/of werkinstructies). Verder is gebruik gemaakt van de methode observatie.

Om een goed beeld te geven hoe de gemeente Best persoonsgegevens verwerkt staat in hoofdstuk vier uitgebreid beschreven hoe de gemeente Best persoonsgegevens verwerkt

¹⁵ Van Schaaijk 2015, p. 122.

¹⁶ 'Wetten', www.autoriteitpersoonsgegevens.nl (zoek op *Wetten*), <Over privacy, Wetten>.

¹⁷ Artikel 34a Wbp.

¹⁸ Van Schaaijk 2015, p. 103.

bij het behandelen van een aanvraag van een evenementenvergunning. Er is, in overleg met de opdrachtgever, gekozen voor deze verwerking omdat het verstrekken van een evenementenvergunning een kerntaak is van de gemeente waarbij veel verschillende partijen zijn betrokken.

Deelvraag 4: Welke gevolgen heeft de nieuwe AVG voor de huidige werkwijze van de gemeente Best met betrekking tot het verwerken van persoonsgegevens en het Privacyreglement gemeente Best?

Het antwoord op deze deelvraag is gegeven door het onderzoek van het recht en de onderzoek van de praktijk aan elkaar te koppelen. Er is beschreven op welke manier de werkwijze met betrekking tot het verwerken van persoonsgegevens van de gemeente Best aangepast moet worden zodat deze werkwijze juridisch juist is gelet op de recente wijzigingen van de Wbp en de aanstaande AVG. Voorts is het privacyreglement van de gemeente Best beschreven. Er is getoetst of de artikelen die staan in het privacyreglement nog juridisch juist zijn gelet op de recente wijzigingen van de Wbp en de aanstaande AVG. Er zijn voorstellen gedaan om het privacyreglement te verbeteren.

§ 1.5 Leeswijzer

Het onderhavige hoofdstuk betreft de inleiding. In hoofdstuk twee van dit onderzoeksrapport wordt het huidige juridisch kader op grond van de Wbp beschreven. In het hoofdstuk daarna (hoofdstuk drie) komt de AVG uitgebreid aan bod. In hoofdstuk vier wordt de huidige werkwijze van de gemeente Best met betrekking tot het verwerken van persoonsgegevens beschreven. In het vijfde hoofdstuk is beschreven of de huidige werkwijze met betrekking tot het verwerken van persoonsgegevens en het Privacyreglement gemeente Best voldoen aan de Wbp en de aanstaande AVG. In hoofdstuk zes, tevens het laatste hoofdstuk, staan de conclusies en aanbevelingen. De aanbevelingen geven een antwoord op de centrale vraag.

HOOFDSTUK 2: HET HUIDIGE JURIDISCH KADER

In dit hoofdstuk staat het huidige juridisch kader omtrent de verwerking van persoonsgegevens beschreven. Eerst wordt de Wbp beschreven. Daarna komt de Wmd aan bod. Dit hoofdstuk geeft een antwoord op de eerste deelvraag: “Wat is het huidige juridisch kader voor het verwerken van persoonsgegevens gelet op de Wbp?”.

§ 2.1 Wet bescherming persoonsgegevens

De Wbp is de belangrijkste wet die regels geeft voor het verwerken van persoonsgegevens.¹⁹ De Wbp is sinds 2001 van kracht en betreft de implementatie van richtlijn 95/46/EG.²⁰ Hieronder wordt de Wbp in vogelvucht beschreven.

§ 2.1.1 Reikwijdte

De Wbp heeft betrekking op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede de niet geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om in een bestand te worden opgenomen.²¹ Met geautomatiseerde verwerking wordt bedoeld de verwerking waarbij gebruik wordt gemaakt van middelen en methoden van geautomatiseerde gegevensverwerking.²² Er is bijvoorbeeld sprake van geautomatiseerde verwerking indien gebruik wordt gemaakt van een computer. Van een gedeeltelijke geautomatiseerde verwerking is sprake indien zowel gebruik wordt gemaakt van middelen en methoden van geautomatiseerde gegevensverwerking als andere middelen.²³ Indien persoonsgegevens gedeeltelijk geautomatiseerd en gedeeltelijk handmatig verwerkt worden is sprake van een gedeeltelijke geautomatiseerde verwerking.²⁴ Niet geautomatiseerde verwerking betreft de handmatige verwerking van persoonsgegevens.²⁵

Uitzonderingen

In bepaalde situaties is de Wbp niet van toepassing. De Wbp is niet van toepassing indien de persoonsgegevens verwerkt worden ten behoeve van activiteiten met uitsluitend persoonlijke of huishoudelijke doeleinden.²⁶ Hiermee worden ook lijstjes van beroepsbeoefenaren met gegevens van personen met wie zij regelmatig contact onderhouden bedoeld.²⁷ Voorts is de Wbp niet van toepassing indien een bijzondere wet van toepassing is die een uitputtende regeling bevat ter bescherming van persoonsgegevens.²⁸ De Wbp is niet van toepassing op de verwerking van persoonsgegevens:

- door of ten behoeve van de inlichtingen- en veiligheidsdiensten, bedoeld in de Wet op de inlichtingen- en veiligheidsdiensten 2002;
- ten behoeve van de uitvoering van de politietaak, bedoeld in de artikelen 3 en 4, eerste lid, van de Politiewet 2012;
- die is geregeld bij of krachtens de Wet basisregistratie personen;

¹⁹ 'Wet bescherming persoonsgegevens', www.autoriteitpersoonsgegevens.nl (zoek op *Wet bescherming persoonsgegevens*), <Over privacy, Wetten, Wet bescherming persoonsgegevens>.

²⁰ Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.

²¹ Artikel 2 lid 1 Wbp.

²² *Kamerstukken II* 1997/98, 25892, nr. 3, p. 69 (MvT).

²³ *Kamerstukken II* 1997/98, 25892, nr. 3, p. 69 (MvT).

²⁴ Kranenburg & Verhey 2011, p. 59.

²⁵ Kranenburg & Verhey 2011, p. 59.

²⁶ Artikel 2 lid 2 aanhef en onder a Wbp.

²⁷ *Kamerstukken II* 1997/98, 25892, nr. 3, p. 70 (MvT).

²⁸ Kranenburg & Verhey 2011, p. 71.

- ten behoeve van de uitvoering van de Wet justitiële en strafvorderlijke gegevens en
- ten behoeve van de uitvoering van de Kieswet.²⁹

Een laatste uitzondering is in bepaalde gevallen van toepassing op de krijgsmacht en journalisten.³⁰ Hier wordt, gelet op de relevantie, verder niet op ingegaan.

§ 2.1.2 Begrippen

Om de reikwijdte van de Wbp te begrijpen is het van belang om te weten wat de Wbp verstaat onder bepaalde begrippen (bijvoorbeeld wat de Wbp verstaat onder de begrippen “persoonsgegevens” en “verwerken”). In artikel 1 Wbp staan verschillende begrippen gedefinieerd. Een overzicht van deze begrippen, alsmede de daarbij behorende definities, is hieronder te vinden in tabel 2.1.

TABEL 2.1: EEN AANTAL BELANGRIJKE BEGRIPPEN UIT DE WBP³¹	
Persoonsgegevens (artikel 1 aanhef en onder a Wbp)	<i>Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.</i>
Verwerken (artikel 1 aanhef en onder b Wbp)	<i>Elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.</i>
Bestand (artikel 1 aanhef en onder c Wbp)	<i>Elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen.</i>
Verantwoordelijke (artikel 1 aanhef en onder d Wbp)	<i>De natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of te zamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.</i>
Bewerker (artikel 1 aanhef en onder e Wbp)	<i>Degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.</i>
Betrokkene (artikel 1 aanhef en onder f Wbp)	<i>Degene op wie een persoonsgegeven betrekking heeft.</i>

§ 2.1.3 Algemeen kader

Indien de Wbp op de verwerking van toepassing is, moet de verwerking voldoen aan verschillende eisen. De voorwaarden voor de rechtmatigheid van de verwerking van persoonsgegevens staan in hoofdstuk 2 Wbp.³² Achtereenvolgens worden de voorwaarden hieronder beschreven.

²⁹ Artikel 2 lid 2 aanhef en onder b t/m f Wbp.

³⁰ Artikel 2 lid 3 Wbp jo. artikel 3 Wbp.

³¹ Artikel 1 Wbp.

³² Artikel 6-24 Wbp.

Behoorlijke en zorgvuldige verwerking

Persoonsgegevens moeten in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt worden.³³ In de Europese privacyrichtlijn (richtlijn 95/46/EG) wordt gesproken van “processed fairly” en “lawfully”. Gelet op het feit dat het begrip “eerlijk” geen juridische betekenis heeft in het Nederlandse recht, wordt in Nederland gesproken van “behoorlijk en “zorgvuldig”.³⁴ Van een behoorlijke en zorgvuldige verwerking is sprake indien de betrokkene van het bestaan van de verwerking op de hoogte is of kan zijn. Verder moet de betrokkene ingelicht worden over de omstandigheden waaronder de gegevens worden verkregen.³⁵

Doelbinding

Voordat persoonsgegevens verwerkt mogen worden moet er een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel bestaan.³⁶ Dit betekent dat er eerst een doel geformuleerd moet worden voordat persoonsgegevens verzameld mogen worden.³⁷ Het verzamelen van persoonsgegevens voor een doel dat mogelijk in de toekomst van belang kan zijn is dan ook niet toegestaan. Verder mag het doel tijdens het verzamelproces niet veranderen.³⁸ Persoonsgegevens mogen slechts voor een gerechtvaardigd doel worden verwerkt. Kort gezegd komt dit erop neer dat de gegevensverwerking gebaseerd moet worden op één van de zes grondslagen die limitatief staan opgesomd in artikel 8 Wbp.³⁹

Rechtmatigheid

In artikel 8 Wbp staan zes gronden beschreven op basis waarvan persoonsgegevens verwerkt mogen worden. Indien een bepaalde gegevensverwerking niet gebaseerd kan worden op ten minste één van de verwerkingsgronden uit artikel 8 Wbp is de gegevensverwerking niet rechtmatig. In tabel 2.2 staat een overzicht van alle verwerkingsgronden die staan opgesomd in artikel 8 Wbp.

TABEL 2.2: GRONDEN DIE EEN GEGEVENSVERWERKING RECHTVAARDIGEN⁴⁰	
Ondubbelzinnige toestemming van een betrokkene	In artikel 1 aanhef en onder i Wbp wordt onder “toestemming van een betrokkene” verstaan: elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem betreffende persoonsgegevens worden verwerkt. Ondubbelzinnig houdt in dat de verantwoordelijke geen twijfel mag hebben over de toestemming van de betrokkene. ⁴¹
Noodzakelijk uitvoering overeenkomst	De verwerking van persoonsgegevens is toelaatbaar indien deze noodzakelijk is om contractuele verplichtingen na te komen. ⁴² Het is dan wel van belang dat de betrokkene een partij is.
Noodzakelijk nakomen wettelijke verplichting	De verantwoordelijke is gerechtigd gegevens te verwerken indien dit noodzakelijk is om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is. ⁴³ Kort gezegd

³³ Artikel 6 Wbp.

³⁴ Kranenborg & Verhey 2011, p. 81.

³⁵ Overweging 38 van Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.

³⁶ Artikel 7 Wbp.

³⁷ Kamerstukken II 1997/98, 25892, nr. 3, p. 79 (MvT).

³⁸ Kamerstukken II 1997/98, 25892, nr. 3, p. 79 (MvT).

³⁹ Kamerstukken II 1997/98, 25892, nr. 3, p. 80 (MvT).

⁴⁰ Artikel 8 Wbp.

⁴¹ Sauerwein & Linnemann 2002, p. 21.

⁴² Kamerstukken II 1997/98, 25892, nr. 3, p. 80 (MvT).

⁴³ Artikel 8 onder c Wbp.

	komt het erop neer dat de verwerking gebaseerd moet zijn op een verplichting die bij of krachtens een algemeen verbindend voorschrift wordt opgelegd. ⁴⁴ Voorts dient de verantwoordelijke belast te zijn met de uitvoering van deze wettelijke verplichting. ⁴⁵ Een voorbeeld is de verplichting van bestuursorganen die op grond van de Wet openbaarheid van bestuur (Wob) verplicht zijn openbare gegevens te verstrekken. Hier kunnen ook persoonsgegevens tussen zitten. ⁴⁶
Noodzakelijk ter vrijwaring van een vitaal belang	De verwerking van persoonsgegevens is toelaatbaar indien er een dringende medische noodzaak aanwezig is en de toestemming van een betrokkene redelijkerwijs niet afgewacht kan worden. ⁴⁷ Kortom: het moet gaan om een zaak van leven of dood. ⁴⁸
Noodzakelijk vervulling van een publiekrechtelijke taak	Bestuursorganen mogen persoonsgegevens verwerken indien zij dit nodig achten voor de vervulling van een publiekrechtelijke taak. ⁴⁹
Noodzakelijk behartiging van het gerechtvaardigde belang	Indien de verwerking noodzakelijk is voor de behartiging van een gerechtvaardigd belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt is de verwerking rechtmatig, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, doorslaggevend zijn. ⁵⁰

Bijzondere gegevens

Voor bijzondere persoonsgegevens kent de Wbp een aangescherpt regime.⁵¹ In de Wbp staat dat gegevens die informatie verschaffen over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven en lidmaatschap van een vakbond aangemerkt moeten worden als bijzondere persoonsgegevens.⁵² Ook strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag kunnen worden aangemerkt als bijzondere gegevens.⁵³ Een voorbeeld van een opgelegd verbod naar aanleiding van onrechtmatig of hinderlijk gedrag is een straatverbod.⁵⁴ Het verwerken van bijzondere persoonsgegevens is, behoudens bepaalde uitzonderingen die staan in paragraaf 2 van hoofdstuk 2 Wbp, verboden.⁵⁵ Er kan een onderscheid worden gemaakt tussen algemene uitzonderingen en specifieke uitzonderingen.

⁴⁴ Kranenborg & Verhey 2011, p. 86.

⁴⁵ *Kamerstukken II* 1997/98, 25892, nr. 3, p. 82 (MvT).

⁴⁶ Kranenborg & Verhey 2011, p. 86.

⁴⁷ Kranenborg & Verhey 2011, p. 87.

⁴⁸ *Kamerstukken II* 1997/98, 25892, nr. 3, p. 84 (MvT).

⁴⁹ Kranenborg & Verhey 2011, p. 87.

⁵⁰ *Kamerstukken II* 1997/98, 25892, nr. 3, p. 86 (MvT).

⁵¹ Berkvens & Prins 2007, p. 36.

⁵² Artikel 16 Wbp.

⁵³ Artikel 16 Wbp.

⁵⁴ Sauerwein & Linnemann 2002, p. 47.

⁵⁵ Artikel 16-24 Wbp.

Algemene uitzonderingen

De volgende algemene uitzonderingen heffen het verbod om bijzondere persoonsgegevens te verwerken op:

- de betrokkene heeft uitdrukkelijk toestemming gegeven;
- de betrokkene heeft de gegevens zelf openbaar gemaakt;
- de verwerking is noodzakelijk voor de vaststelling, de uitoefening of de verdediging van een recht in een gerechtelijke procedure;
- de verwerking is noodzakelijk ter verdediging van de vitale belangen van de betrokkene of van een derde en het vragen van uitdrukkelijke toestemming is niet mogelijk;
- de verwerking is noodzakelijk ter voldoening aan een volkenrechtelijke verplichting;
- de wet of de AP geeft met het oog op een zwaarwegend algemeen belang een ontheffing of
- de gegevens worden verwerkt door de AP of de ombudsman.⁵⁶

Specifieke uitzonderingen

De specifieke uitzonderingen die het verbod om bijzondere persoonsgegevens te verwerken opheffen staan in artikel 17 t/m 22 Wbp. De specifieke uitzonderingen staan hieronder in vogelvucht beschreven.

*Godsdienst of levensovertuiging*⁵⁷

Het verbod om persoonsgegevens over iemands godsdienst of levensovertuiging te verwerken geldt niet voor kerkgenootschappen, instellingen op godsdienstige of levensbeschouwelijke grondslag (bijvoorbeeld onderwijsinstellingen) of andere instellingen voor zover de verwerking noodzakelijk is met het oog op de geestelijke verzorging van de betrokkene (bijvoorbeeld geestelijke zorg die plaatsvindt in een ziekenhuis). Wel geldt een verbod om de onderhavige persoonsgegevens te verstrekken aan derden, tenzij de betrokkene hiervoor toestemming heeft gegeven.⁵⁸

*Ras*⁵⁹

De verwerking van persoonsgegevens over iemands ras is slechts in zeer uitzonderlijke gevallen toegestaan.⁶⁰ Gegevens over iemands ras mogen slechts verwerkt worden wanneer dit wordt gedaan voor identificatiedoeleinden (bijvoorbeeld de met foto's voorziene identiteitspasjes die door een werkgever aan zijn werknemer worden verstrekt⁶¹) of in het kader van een voorkeursbeleid voor bepaalde etnische of culturele minderheidsgroeperingen.⁶² Indien de persoonsgegevens over iemands ras worden verwerkt in het kader van een voorkeursbeleid voor bepaalde etnische of culturele minderheidsgroeperingen moet wel worden voldaan aan aanvullende voorwaarden die staan opgesomd in artikel 18 Wbp.⁶³

*Politieke gezindheid*⁶⁴

Het verbod om persoonsgegevens te verwerken over iemands politieke gezindheid geldt in bepaalde gevallen niet indien de verwerking gebeurt door instellingen op politieke grondslag of met het oog op de vervulling van functies in bestuursorganen

⁵⁶ Artikel 23 lid 1 aanhef en onder a t/m g Wbp.

⁵⁷ Artikel 17 Wbp.

⁵⁸ artikel 17 lid 3 Wbp.

⁵⁹ Artikel 18 Wbp.

⁶⁰ *Kamerstukken II* 1997/98, 25892, nr. 3, p. 104 (MvT).

⁶¹ Kranenburg & Verhey 2011, p. 106.

⁶² Artikel 18 aanhef en onder a en b Wbp.

⁶³ Kranenburg & Verhey 2011, p. 106.

⁶⁴ Artikel 19 Wbp.

en adviescolleges.⁶⁵ Bij instellingen op politieke grondslag kan gedacht worden aan politieke partijen en de wetenschappelijke bureaus en vormingsorganisaties die daarmee verbonden zijn.⁶⁶

Lidmaatschap vakbond⁶⁷

De persoonsgegevens over iemands lidmaatschap van een vakbond mogen door de betreffende vakbond of de vakcentrale waarvan die bond een onderdeel vormt verwerkt worden. De verwerking dient wel noodzakelijk te zijn voor de doelstelling van de vakbond of de vakcentrale waarvan die bond een onderdeel vormt.⁶⁸ Ook bij deze uitzondering geldt een verbod om de onderhavige persoonsgegevens te verstrekken aan derden, tenzij de betrokkene hiervoor toestemming heeft gegeven.⁶⁹

Gezondheid⁷⁰

Gegevens over iemands gezondheid mogen alleen verwerkt worden door ziekenhuizen, instellingen voor maatschappelijke dienstverlening, verzekeraars, speciale scholen, reclasseringsinstellingen, de raad voor de kinderbescherming, (gezins-)voogdij instellingen en bestuursorganen of uitvoeringsinstellingen die bepaalde sociaalezekerheidswetten uitvoeren.⁷¹ In beginsel mogen gegevens over iemands gezondheid alleen verwerkt worden door personen die een geheimhoudingsplicht hebben uit hoofde van ambt, beroep of wettelijk voorschrift (bijvoorbeeld: advocaten, politieambtenaren of artsen en psychologen).⁷² Heerst er op de verantwoordelijke geen geheimhoudingsplicht uit hoofde van ambt, beroep of wettelijk voorschrift? Dan legt de Wbp een geheimhoudingsplicht op.⁷³ Het begrip “gezondheid” moet ruim worden geïnterpreteerd. Het omvat niet alleen de gegevens die in het kader van een medisch onderzoek of een medische behandeling door een arts worden verwerkt, maar alle gegevens die de geestelijke of lichamelijke gezondheid van een persoon betreffen.⁷⁴

Strafrechtelijke gegevens⁷⁵

Het verbod om strafrechtelijke gegevens te verwerken geldt niet voor organisaties die krachtens de wet zijn belast met de toepassing van het strafrecht of verantwoordelijken die de strafrechtelijke persoonsgegevens hebben verkregen krachtens de Wet politiegegevens of de Wet justitiële en strafvorderlijke gegevens.⁷⁶ Gedacht kan worden aan de politie of het OM. Het verbod om strafrechtelijke gegevens te verwerken is voorts niet van toepassing indien de verantwoordelijke de gegevens voor zichzelf verwerkt ter beoordeling van een verzoek van de betrokkene om een beslissing over hem te nemen of aan hem een prestatie te leveren of ter bescherming van zijn belangen voor zover het gaat om strafbare feiten die zijn of naar verwachting zullen worden gepleegd jegens hem of jegens personen die in dienst van de verantwoordelijke zijn.⁷⁷ Indien de verantwoordelijke strafrechtelijke

⁶⁵ Kranenborg & Verhey 2011, p. 107.

⁶⁶ *Kamerstukken II* 1997/98, 25892, nr. 3, p. 106 (MvT).

⁶⁷ Artikel 20 Wbp.

⁶⁸ Kranenborg & Verhey 2011, p. 108.

⁶⁹ Artikel 20 lid 2 Wbp.

⁷⁰ Artikel 21 Wbp.

⁷¹ Sauerwein & Linnemann 2002, p. 49.

⁷² Artikel 21 lid 2 Wbp.

⁷³ Artikel 21 lid 2 Wbp.

⁷⁴ Kranenborg & Verhey 2011, p. 109.

⁷⁵ Artikel 22 Wbp.

⁷⁶ Artikel 22 lid 1 Wbp.

⁷⁷ Artikel 22 lid 2 aanhef en onder a en b Wbp.

gegevens verwerkt over zijn personeel moet de ondernemingsraad bij de verwerking betrokken worden. Verder mogen strafrechtelijke gegevens in bepaalde gevallen verwerkt worden door derden (bijvoorbeeld beveiligingsorganisaties en recherchebureaus). Hier wordt, gelet op de relevantie, verder niet op ingegaan. Strafrechtelijke gegevens mogen ook verwerkt worden door publiekrechtelijke samenwerkingsverbanden van verantwoordelijken of groepen van verantwoordelijken indien de verwerking noodzakelijk is voor de uitvoering van de taak van deze verantwoordelijken of groepen van verantwoordelijken.⁷⁸ Het verbod om strafrechtelijke gegevens te verwerken is van overeenkomstige toepassing op persoonsgegevens betreffende een door de rechter opgelegd verbod naar aanleiding van onrechtmatig of hinderlijk gedrag.⁷⁹

*Identificatienummer (BSN)*⁸⁰

Een identificatienummer is volgens de AP een bijzonder persoonsgegeven.⁸¹ Een BSN-nummer mag in beginsel alleen door overheidsorganisaties verwerkt worden indien dat nodig is voor hun publieke taak. Organisaties buiten de overheid mogen een BSN-nummer slechts verwerken als dit in een wet is bepaald.⁸²

§ 2.1.4 Bewaartermijn en beveiliging

Persoonsgegevens mogen niet langer bewaard worden dan noodzakelijk is voor de verwezenlijking van de doeleinden waarvoor de persoonsgegevens zijn verzameld.⁸³ Indien persoonsgegevens bewaard worden voor historische, statistische of wetenschappelijke doeleinden, mogen persoonsgegevens langer bewaard worden. Dit mag alleen als de verantwoordelijke de nodige voorzieningen heeft getroffen die ervoor zorgen dat de persoonsgegevens uitsluitend voor deze specifieke doeleinden worden gebruikt.⁸⁴ De Wbp noemt geen concrete bewaartermijnen voor persoonsgegevens. Bewaartermijnen kunnen wel in andere wetten staan (bijvoorbeeld in belastingwetgeving).⁸⁵

Op grond van de Wbp moet de verantwoordelijke passende technische en organisatorische maatregelen nemen om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking.⁸⁶ Er is sprake van een onrechtmatige verwerking indien persoonsgegevens onbevoegd worden ingezien, worden gewijzigd en/of worden verstrekt.⁸⁷ Met 'passende' technische maatregelen wordt bedoeld dat de beveiliging in overeenstemming moet zijn met de stand van de techniek. De stand van de techniek is tijdsgebonden.⁸⁸ De verantwoordelijke moet zich, gelet op de komst van nieuwe technieken, steeds opnieuw de vraag stellen of de beveiliging nog voldoet. Het begrip 'passend' impliceert voorts een proportionaliteitstoets: er moet evenredigheid bestaan tussen de privacyrisico's die de verwerking en de aard van de te beschermen gegevens met zich

⁷⁸ Artikel 22 lid 6 Wbp.

⁷⁹ Artikel 22 lid 7 Wbp.

⁸⁰ Artikel 24 Wbp.

⁸¹ 'Burgerservicenummer (BSN)', www.autoriteitpersoonsgegevens.nl (zoek op *Burgerservicenummer*), <Onderwerpen, Identificatie, Burgerservicenummer (BSN)>.

⁸² "Welke organisaties mogen mijn burgerservicenummer (BSN) gebruiken?", www.rijksoverheid.nl (zoek op *Welke organisaties mogen mijn burgerservicenummer (BSN) gebruiken?*), <Onderwerpen, Persoonsgegevens, Vragen en antwoorden over Persoonsgegevens>.

⁸³ Artikel 10 lid 1 Wbp.

⁸⁴ Artikel 10 lid 2 Wbp.

⁸⁵ 'Bewaren van persoonsgegevens', www.autoriteitpersoonsgegevens.nl (zoek op *Bewaren van persoonsgegevens*), <Over privacy, Persoonsgegevens, Bewaren van persoonsgegevens>.

⁸⁶ Artikel 13 Wbp.

⁸⁷ *Kamerstukken II 1997/98*, 25892, nr. 3, p. 98 (MvT).

⁸⁸ *Kamerstukken II 1997/98*, 25892, nr. 3, p. 99 (MvT).

brengen enerzijds en de getroffen beveiligingsmaatregelen anderzijds.⁸⁹ Kortom: hoe gevoeliger de gegevens zijn, hoe beter de gegevens beveiligd moeten worden.

§ 2.1.5 Meldingsplicht verwerken persoonsgegevens

De verantwoordelijke is op grond van de Wbp in bepaalde gevallen verplicht om de verwerking van persoonsgegevens te melden bij de AP of, indien het bedrijf of de organisatie een FG in dienst heeft, de FG.⁹⁰ Niet alle verwerkingen hoeven gemeld te worden. De meldingsplicht is niet van toepassing op:

- openbare registers die bij wet zijn ingesteld (bijvoorbeeld het handelsregister);
- wettelijk verplichte verstrekkingen van persoonsgegevens aan bestuursorganen en
- verwerkingen die in het Vrijstellingsbesluit Wbp (VWbp) staan beschreven.⁹¹

Alle meldingen die zijn gedaan staan in het meldingenregister van de AP.⁹²

§ 2.1.6 Rechten van de betrokkene

In hoofdstuk 6 Wbp staan de rechten van betrokkenen beschreven. De belangrijkste rechten staan in tabel 2.3 uitgewerkt. Een toelichting op deze rechten volgt daarna.

TABEL 2.3: RECHTEN VAN BETROKKENEN	
Recht op kennisneming	Artikel 35 Wbp
Recht op correctie (verbetering, aanvulling verwijdering of afscherming)	Artikel 36 Wbp
Recht op verzet	Artikel 40 en artikel 41 Wbp

Recht op kennisneming⁹³

Het recht op kennisneming biedt de mogelijkheid aan een betrokkene om de verantwoordelijke te vragen of en welke persoonsgegevens over hem verwerkt worden. Het Hof van Justitie van de Europese Unie (HvJ EU) heeft bepaald dat wanneer een dergelijk verzoek wordt gedaan de verantwoordelijke een volledig overzicht van de gegevens moet verstrekken. De betrokkene moet in staat zijn om aan de hand van het overzicht kennis te nemen van de gegevens en moet kunnen controleren of de gegevens juist zijn en in overeenstemming met de richtlijn 95/46/EG zijn verwerkt.⁹⁴ Het gebruik van het recht op kennisneming kan misbruik van bevoegdheid opleveren (artikel 3:13 BW).⁹⁵ Het gerechtshof Amsterdam overwoog in de zaak Dexia Bank Nederland NV als volgt: *"In de wetsgeschiedenis van de Wbp zijn geen aanknopingspunten te vinden voor de gedachte dat de onderhavige bevoegdheid niet zou kunnen worden misbruikt. Het recht van de betrokkene op inzage wordt weliswaar verondersteld, maar deze veronderstelling zal hebben te wijken voor feiten en omstandigheden waaruit volgt dat de onderhavige bevoegdheid wordt misbruikt in de zin van art. 3:13 BW. De onderhavige bevoegdheid kan dus worden misbruikt."*⁹⁶ In artikel 3:13 BW staat dat degene aan wie een bevoegdheid toekomt deze bevoegdheid niet kan inroepen indien sprake is van misbruik. Artikel 3:13 BW is ook van toepassing buiten het vermogensrecht, voor zover de aard van de rechtsbetrekking zich daartegen niet verzet.⁹⁷

⁸⁹ Kranenborg & Verhey 2011, p. 99.

⁹⁰ Artikel 27 Wbp.

⁹¹ 'Melden verwerking persoonsgegevens', www.autoriteitpersoonsgegevens.nl (zoek op *Melden verwerking persoonsgegevens*), <Melden, Melden verwerking persoonsgegevens>.

⁹² www.collegebeschermingpersoonsgegevens.nl/asp/orsearch.asp.

⁹³ Artikel 35 Wbp.

⁹⁴ HvJ EU 17 juli 2014, C-141/12 en C-372/12 (Y.S. en M. en S.).

⁹⁵ Zwenne & Webbink, *Privacy & Informatie* 2006, p. 1-8.

⁹⁶ Hof Amsterdam 10 november 2005, ECLI:NL:GHAMS:2005:AU8223.

⁹⁷ Artikel 3:15 BW.

Recht op correctie (verbetering, aanvulling, verwijdering of afscherming)⁹⁸

Iedereen die het recht op kennisneming toekomt, heeft tevens het recht op correctie. Indien een betrokkene van mening is dat de persoonsgegevens feitelijk onjuist zijn of voor het doel van de verwerking onvolledig of niet ter zake dienend zijn dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt, kan de betrokkene de verantwoordelijke verzoeken om deze gegevens te verbeteren, aan te vullen, te verwijderen of af te schermen.⁹⁹ De verantwoordelijke moet binnen vier weken na ontvangst van het verzoek schriftelijk reageren. Indien de verantwoordelijke besluit het verzoek af te wijzen, moet de verantwoordelijke de afwijzing goed motiveren.¹⁰⁰

Recht van verzet¹⁰¹

Indien de gegevens verwerkt worden voor de vervulling van een publiekrechtelijke taak (artikel 8 onder e Wbp) of voor de behartiging van het gerechtvaardigd belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt (artikel 8 onder f Wbp), kan de betrokkene bij de verantwoordelijke verzet aantekenen in verband met bijzondere persoonlijke omstandigheden.¹⁰² ¹⁰³ Het aantekenen van verzet is vormvrij.¹⁰⁴ Dat wil zeggen dat een betrokkene op iedere wijze verzet kan aantekenen.

§ 2.1.7 Rechtsbescherming

In hoofdstuk 8 Wbp staat de rechtsbescherming beschreven. Een betrokkene kan naar de rechter, de AP of een andere instantie verzoeken het geschil te beslechten of schadevergoeding vorderen bij de verantwoordelijke (zie tabel 2.4).

TABEL 2.4: RECHTSBESCHERMING WBP	
Naar de rechter	Artikel 45 en artikel 46 Wbp
De AP of een andere instantie verzoeken het geschil te beslechten	Artikel 47 Wbp
Schadevergoeding vorderen bij de verantwoordelijke	Artikel 49 en artikel 50 WBP

Naar de rechter

Indien een bestuursorgaan als verantwoordelijke optreedt, is de bestuursrechter bevoegd. In andere gevallen kan de betrokkene naar de civiele rechter.¹⁰⁵

Bestuursrechter

Beslissingen die verband houden met het recht op kennisneming (artikel 35 Wbp), het recht op correctie (artikel 36 Wbp) en het recht van verzet (artikel 40 en 41 Wbp) zijn besluiten in de zin van de Awb.¹⁰⁶ Hierdoor is het instellen van beroep bij de bestuursrechter, nadat een bezwaarprocedure is doorlopen, mogelijk.¹⁰⁷ ¹⁰⁸ Bezwaar en beroep staat niet alleen voor een betrokkene open, maar voor alle belanghebbenden in de zin van artikel 1:2 Awb. In artikel 1:2 Awb staat het volgende: *“Onder een belanghebbende wordt verstaan: degene wiens belang rechtstreeks bij*

⁹⁸ Artikel 36 lid 1 Wbp.

⁹⁹ Berkvens & Prins 2007, p. 42.

¹⁰⁰ Artikel 36 lid 2 Wbp.

¹⁰¹ Artikel 40 jo. artikel 41 Wbp.

¹⁰² Artikel 40 lid 1 Wbp.

¹⁰³ Berkvens & Prins 2007, p. 43.

¹⁰⁴ *Kamerstukken II* 1997/98, 25892, nr. 3, p. 164 (MvT).

¹⁰⁵ Kranenborg & Verhey 2011, p. 142.

¹⁰⁶ Artikel 45 Wbp.

¹⁰⁷ Kranenborg & Verhey 2011, p.143.

¹⁰⁸ Artikel 1:3 jo. 7:1 en 8:1 Awb.

een besluit is betrokken.”. Verder is het ook mogelijk om bezwaar of beroep aan te tekenen tegen een schriftelijke weigering een besluit te nemen en het niet tijdig nemen van een besluit (artikel 6:2 Awb).¹⁰⁹

Civiele rechter

Indien de verantwoordelijke geen bestuursorgaan is, kan de betrokkene naar de civiele rechter stappen.¹¹⁰ Dit moet gedaan worden door een verzoekschrift in te dienen. Dit moet gebeuren binnen zes weken na ontvangst van het antwoord van de verantwoordelijke. Indien de verantwoordelijke niet binnen de gestelde termijn heeft geantwoord, moet het verzoekschrift worden ingediend binnen zes weken na afloop van die termijn.

AP of een andere instantie verzoeken om het geschil te beslechten¹¹¹

De belanghebbende heeft de mogelijkheid om – binnen de termijn waarbinnen beroep kan worden ingesteld – de AP te verzoeken te bemiddelen bij het geschil. De belanghebbende kan de AP ook verzoeken te adviseren in zijn geschil. Indien de belanghebbende de AP verzoekt te bemiddelen wordt de beroepstermijn opgeschort. Dit betekent dat een belanghebbende ook na de poging tot geschillenbeslechting beroep kan instellen. Op de website van de AP staat dat de AP niet alle verzoeken om klachtbehandeling of bemiddeling kan aannemen. De AP kijkt naar de ernst van de overtreding en naar hoeveel mensen hierdoor geraakt worden.¹¹²

Schadevergoeding vorderen bij de verantwoordelijke¹¹³

Indien de verantwoordelijke heeft gehandeld in strijd met de Wbp en een belanghebbende hierdoor schade lijdt of dreigt te lijden, kan de betrokkene de schade verhalen op de verantwoordelijke. Voor nadeel dat niet in vermogensschade bestaat, heeft de benadeelde recht op een naar billijkheid vast te stellen schadevergoeding.¹¹⁴ Indien een belanghebbende schade lijdt of dreigt te lijden kan de rechter de verantwoordelijke een verbod van bepaald gedrag opleggen en bevelen maatregelen te treffen tot herstel van de gevolgen van dat gedrag.¹¹⁵

§ 2.1.8 Toezicht en sancties

In hoofdstuk 9 Wbp is het toezicht geregeld. In hoofdstuk 9 Wbp staat dat toezicht wordt gehouden door het College bescherming persoonsgegevens (CBP). In het maatschappelijk verkeer wordt het CBP aangeduid als de Autoriteit Persoonsgegevens (AP).¹¹⁶

De AP kan zelf, maar ook op verzoek van een belanghebbende, onderzoek doen naar of een bepaalde gegevensverwerking niet in strijd is met de Wbp.¹¹⁷ De AP moet voorlopige bevindingen uit het onderzoek delen met de verantwoordelijke. De verantwoordelijke moet de gelegenheid geboden worden om te reageren.¹¹⁸ Indien het onderzoek is ingesteld naar aanleiding van een verzoek van de belanghebbende, moet de belanghebbende in kennis worden gesteld van de bevindingen van de AP.¹¹⁹

¹⁰⁹ Kranenborg & Verhey 2011, p. 144.

¹¹⁰ Artikel 46 Wbp.

¹¹¹ Artikel 47 Wbp.

¹¹² 'Taken en bevoegdheden', www.autoriteitpersoonsgegevens.nl (zoek op *Taken en bevoegdheden*), <Over privacy, Het werk van de Autoriteit Persoonsgegevens>.

¹¹³ Artikel 49 jo. artikel 50 Wbp.

¹¹⁴ Artikel 49 lid 2 Wbp.

¹¹⁵ Artikel 50 lid 1 Wbp.

¹¹⁶ Artikel 51 lid 4 Wbp.

¹¹⁷ Artikel 60 lid 1 Wbp.

¹¹⁸ Artikel 60 lid 2 Wbp.

¹¹⁹ Artikel 60 lid 3 Wbp.

Toezichthouders van de AP (buitengewone leden van de AP, ambtenaren van het secretariaat van de AP, alsmede de bij besluit van de AP aangewezen personen¹²⁰), moeten worden beschouwd als toezichthouder in de zin van artikel 5:11 Awb.¹²¹ Ingevolge artikel 5:11 Awb wordt onder een toezichthouder verstaan: een persoon, bij of krachtens wettelijk voorschrift belast met het houden van toezicht op de naleving van het bepaalde bij of krachtens enig wettelijk voorschrift. Omdat toezichthouders van de AP beschouwd moeten worden als toezichthouder in de zin van artikel 5:11 Awb, kunnen de toezichthouders van de AP gebruik maken van de in de Awb vastgelegde bevoegdheden voor toezichthouders. Iedereen is verplicht om aan een toezichthouder medewerking te verlenen (medewerkingsplicht).¹²²

In hoofdstuk 10 Wbp staan de sancties die de AP kan opleggen beschreven. De AP is bevoegd een last onder bestuursdwang op te leggen.¹²³ Daarnaast kan de AP een bestuurlijke boete opleggen van ten hoogste het bedrag van de geldboete van de vierde categorie van artikel 23 lid 4 Wetboek van Strafrecht (momenteel € 820.000 of tien procent van de jaaromzet). In de Boetebeleidsregels Autoriteit Persoonsgegevens 2016 staat beschreven in welke gevallen de AP een boete kan opleggen en hoe hoog deze boetes zijn.

§2.2 Wet meldplicht datalekken

Sinds 1 januari 2016 is de meldplicht datalekken van kracht. Op grond van deze meldplicht moeten bedrijven en organisaties, waaronder gemeenten, direct (binnen 72 uur) een melding doen bij de AP zodra zij een ernstig datalek hebben. De meldplicht datalekken staat in hoofdstuk 5 Wbp beschreven. De Wet meldplicht datalekken (Wmd) is dan ook een onderdeel van de Wbp. In het eerste kwartaal van 2017 zijn er ruim 2300 datalekken gemeld aan de AP.¹²⁴ In deze paragraaf wordt de meldplicht datalekken in vogelvlucht beschreven.

§ 2.2.1 Definitie datalek

In de wet staat geen heldere definitie van het begrip “datalek”. In artikel 34a Wbp wordt gesproken van een “inbreuk op de beveiliging, bedoeld in artikel 13 Wbp”. Zoals eerder beschreven in dit hoofdstuk (zie paragraaf 2.1.4 van dit onderzoeksrapport) moeten bedrijven en organisaties technische en organisatorische maatregelen nemen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking.¹²⁵ Indien zich een beveiligingsincident heeft voorgedaan waarbij persoonsgegevens verloren zijn gegaan of onrechtmatige verwerking niet is uit te sluiten, is sprake van een datalek.

Om te bepalen of een bepaalde gebeurtenis kan worden aangemerkt als een datalek, heeft de AP het onderstaand stappenplan gemaakt (zie figuur 2.1 op de volgende pagina).¹²⁶

¹²⁰ Artikel 61 lid 1 Wbp.

¹²¹ Kranenburg & Verhey 2011, p. 154.

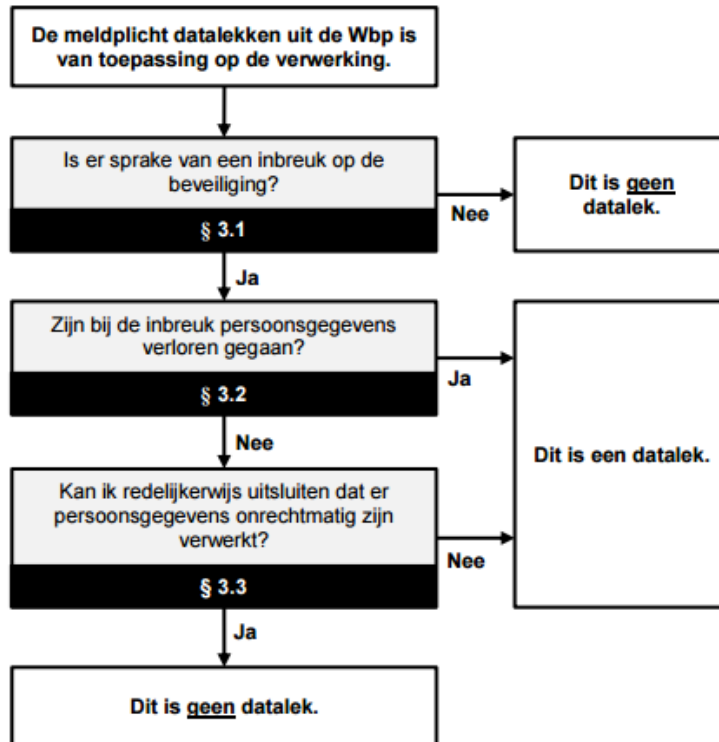
¹²² Artikel 5:20 lid 1 Awb.

¹²³ Artikel 65 Wbp.

¹²⁴ 'Overzichten meldingen datalekken', www.autoriteitpersoonsgegevens.nl (zoek op *Datalekken eerste kwartaal 2017*), <Onderwerpen, Beveiliging, Meldplicht datalekken, Overzichten meldingen datalekken>.

¹²⁵ Artikel 13 Wbp.

¹²⁶ Autoriteit Persoonsgegevens, 'Beleidsregels voor toepassing van artikel 34a Wbp', p. 19.



Figuur 2.1: stappenplan AP: 'Wat is een datalek?'.

Voorbeelden

Voorbeelden van mogelijke datalekken zijn een hackaanval, een slordige omgang met een wachtwoord of het verlies van een laptop of (onbeveiligde) USB-stick.¹²⁷

§ 2.2.2 Meldingsplicht

Niet alle datalekken hoeven gemeld te worden bij de AP. Alleen indien het datalek leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens moet het datalek gemeld worden.¹²⁸ Indien het datalek waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene, moet het datalek ook gemeld worden aan de betrokkene.

Indien de gelekte persoonsgegevens van gevoelige aard zijn is een melding in beginsel noodzakelijk. Gevoelige persoonsgegevens zijn in ieder geval:

- bijzondere persoonsgegevens in de zin van artikel 16 Wbp;
- gegevens over de financiële of economische situatie van de betrokkene;
- gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene;
- gebruikersnamen, wachtwoorden en andere inloggegevens en
- gegevens die misbruikt kunnen worden voor (identiteits)fraude.¹²⁹

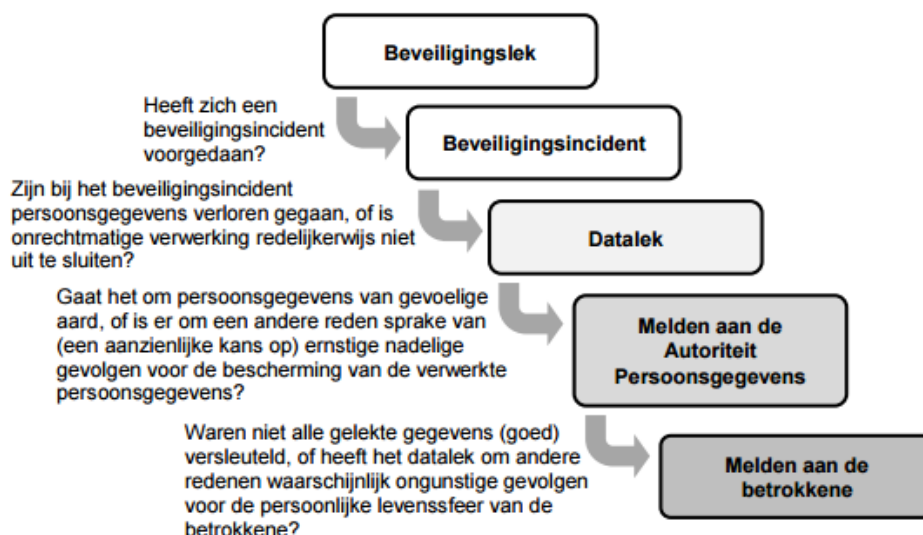
De AP heeft het onderstaand stappenplan (zie figuur 2.2 op de volgende pagina) gemaakt die bedrijven en organisaties kunnen gebruiken bij de beoordeling of een datalek gemeld moet worden.¹³⁰

¹²⁷ Bloemen-Patberg, *ELSA Magazine* 2012, p. 4-9.

¹²⁸ Artikel 34a lid 1 Wbp.

¹²⁹ Autoriteit Persoonsgegevens, 'Beleidsregels voor toepassing van artikel 34a Wbp', p. 5.

¹³⁰ Autoriteit Persoonsgegevens, 'Beleidsregels voor toepassing van artikel 34a Wbp', p. 4.



Figuur 2.2: stappenplan AP: 'Wanneer moet een datalek gemeld worden?'.

2.2.3. Sancties

Indien de meldplicht datalekken wordt overtreden kan de AP een bestuurlijke boete opleggen van ten hoogste € 820.000,-.¹³¹ De boete kan verhoogd worden tot ten hoogste tien procent van de jaaromzet.¹³² Voordat een boete wordt opgelegd zal de AP een bindende aanwijzing (een soort waarschuwing) opleggen, tenzij de overtreding opzettelijk is gepleegd of sprake is van ernstige verwijtbare nalatigheid.¹³³ De AP houdt bij het opleggen van de boete rekening met alle omstandigheden van het geval.¹³⁴

¹³¹ Artikel 66 lid 2 Wbp.

¹³² Artikel 66 lid 2 Wbp jo. artikel 23 lid 7 WvSr.

¹³³ Artikel 66 lid 3 en 4 Wbp.

¹³⁴ Autoriteit Persoonsgegevens, 'Beleidsregels voor toepassing van artikel 34a Wbp', p. 7.

HOOFDSTUK 3: DE ALGEMENE VERORDENING GEGEVENSBESCHERMING (AVG)

Op 25 mei 2016 werd de AVG vastgesteld. In de AVG staat dat de verordening met ingang van 25 mei 2018 van toepassing is.¹³⁵ In 2018 vervalt de Wbp dan ook en moet de verwerking van persoonsgegevens voldoen aan de AVG.¹³⁶ In dit hoofdstuk wordt de AVG in vogelvlucht beschreven. Het hoofdstuk wordt afgesloten met de belangrijkste verschillen tussen de Wbp en de AVG. Het onderhavige hoofdstuk geeft antwoord op de volgende deelvraag: “Wat betekent de AVG voor het verwerken van persoonsgegevens?”.

§ 3.1 Doelstelling

Het primair doel van de AVG is regels vaststellen over de bescherming van natuurlijke personen in verband met de *verwerking van persoonsgegevens* en betreffende het vrije verkeer van persoonsgegevens.¹³⁷ De vraag die direct opkomt is wat de AVG verstaat onder de begrippen “verwerken” en “persoonsgegevens”. Het antwoord op deze vraag is te vinden in artikel 4 AVG. In artikel 4 AVG staan begrippen gedefinieerd.

§ 3.1.1 Begrip persoonsgegevens

Het begrip “persoonsgegevens” wordt in de AVG als volgt gedefinieerd: “*Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identifier zoals een naam, een identificatienummer, locatiegegevens, een online identifier of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.*”¹³⁸ Hieruit volgt dat een naam, foto, BSN-nummer, e-mailadres of een vingerafdruk van een persoon concrete voorbeelden zijn van persoonsgegevens in de zin van de AVG.¹³⁹

§ 3.1.2 Begrip verwerken

In de AVG staat het begrip “verwerken” als volgt gedefinieerd: “*Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.*”¹⁴⁰ Hieruit volgt dat het begrip “verwerken” ruim is geformuleerd. Vrijwel alle soorten handelingen die te bedenken zijn, zijn verwerkingen in de zin van de AVG.

§ 3.2 Beginselen

In hoofdstuk 2 AVG staan verschillende beginselen beschreven. In deze paragraaf komen deze beginselen aan bod.

§ 3.2.1 Beginselen van rechtmatigheid, behoorlijkheid en transparantie

Persoonsgegevens moeten verwerkt worden op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is.¹⁴¹ Op grond van de AVG is de

¹³⁵ Artikel 99 lid 2 AVG.

¹³⁶ Uitvoeringswet Algemene verordening gegevensbescherming.

¹³⁷ Artikel 1 AVG.

¹³⁸ Artikel 4 onder 1 AVG.

¹³⁹ 'Verwerken van persoonsgegevens', www.europadecentraal.nl (zoek op *Verwerken van persoonsgegevens*), <Onderwerpen, Informatiemaatschappij, Privacy: de Algemene Verordening Gegevensbescherming, Verwerken van persoonsgegevens>.

¹⁴⁰ Artikel 4 onder 2 AVG.

¹⁴¹ Artikel 5 lid 1 aanhef en onder a AVG.

verwerking van persoonsgegevens gerechtvaardigd indien ten minste aan één van de volgende voorwaarden wordt voldaan:

- de betrokkene heeft toestemming voor de verwerking gegeven;
- de verwerking is noodzakelijk voor de uitvoering van een overeenkomst;
- de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting;
- de verwerking is noodzakelijk om vitale belangen te beschermen;
- de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen of
- de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde (deze voorwaarde geldt niet voor overheidsinstanties in het kader van de uitoefening van hun publieke taken).¹⁴²

Het transparantiebeginsel houdt in dat een bedrijf of organisatie aan de betrokkene moet meedelen dat zijn gegevens verwerkt worden. Daarbij moet het bedrijf of de organisatie vermelden hoelang de gegevens bewaard worden en met welk doel de gegevens verwerkt worden.¹⁴³

§ 3.2.2 Beginsel van doelbinding

Een verantwoordelijke bedrijf of organisatie mag persoonsgegevens slechts verzamelen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden.¹⁴⁴ Het beginsel van doelbinding uit de AVG is vrijwel gelijk aan het beginsel van doelbinding uit de Wbp.¹⁴⁵ Kort gezegd komt het beginsel van doelbinding erop neer dat voor elke verwerking van persoonsgegevens eerst een doel moet worden bepaald. Gegevens mogen slechts voor dit doel verwerkt worden (zie voor meer informatie ook paragraaf 2.1 van dit onderzoeksrapport).

§ 3.2.3 Beginsel van minimale gegevensverwerking

In de AVG staat dat persoonsgegevens slechts verwerkt mogen worden voor zover noodzakelijk is.¹⁴⁶ Kort gezegd komt het beginsel van minimale gegevensverwerking erop neer dat een verantwoordelijke ervoor moet zorgen dat de verwerking tot een minimum moet worden beperkt. Alleen de noodzakelijke gegevens mogen verwerkt worden. Het beginsel van minimale gegevensverwerking hangt samen met de beginselen van “Privacy by Design” en “Privacy by Default” (zie tabel 3.1).

TABEL 3.1: PRIVACY BY DESIGN EN PRIVACY BY DEFAULT	
Privacy by Design (artikel 25 AVG)	Houdt in dat een bedrijf of organisatie al tijdens het ontwikkelen van producten en diensten, bijvoorbeeld bij het ontwikkelen van informatiesystemen, in een vroegtijdig stadium aan de slag gaat met privacyverhogende maatregelen. Er moet rekening gehouden worden met dataminimalisatie (het verwerken van zo min mogelijk persoonsgegevens). ¹⁴⁷
Privacy by Default (artikel 25 AVG)	Houdt in dat een bedrijf of organisatie alleen persoonsgegevens mag verwerken die noodzakelijk zijn voor het beoogde doel. Standaardinstellingen van informatiesystemen (websites, applicaties,

¹⁴² Artikel 6 lid 1 aanhef en onder a t/m f AVG.

¹⁴³ Duthler & Biesheuvel 2013, p. 9.

¹⁴⁴ Artikel 5 aanhef en onder b AVG.

¹⁴⁵ Artikel 7 Wbp.

¹⁴⁶ Artikel 5 lid 1 aanhef en onder c AVG.

¹⁴⁷ 'Privacy by design', www.autoriteitpersoonsgegevens.nl (zoek op *Privacy by design*), <Zelf doen, Privacycheck, Privacy by design>.

etc.) moeten zo worden ingericht dat deze een zo klein mogelijke inbreuk op de privacy van de gebruikers bewerkstelligen.¹⁴⁸

§ 3.3 Functionaris voor de gegevensbescherming (FG)

Afdeling 4 AVG gaat over de FG. Overheidsinstanties, waaronder gemeenten, zijn op grond van de AVG verplicht een FG aan te wijzen.¹⁴⁹ Dit mag een medewerker van de desbetreffende instantie zijn, maar ook iemand van buitenaf. Overheidsinstanties mogen ervoor kiezen om samen één FG voor meerdere instanties aan te wijzen.¹⁵⁰ Dit kan bijvoorbeeld aantrekkelijk zijn voor kleinere gemeenten die met elkaar samenwerken.

§ 3.3.1 Eisen¹⁵¹

De AVG stelt als voorwaarde dat de FG wordt aangewezen op grond van zijn professionele kwaliteiten en deskundigheid. Kortom: de FG moet voldoende kennis en kunde hebben om te functioneren als FG. De FG moet een expert zijn op het gebied van privacywetgeving, kennis hebben van de organisatie, de processen die binnen de organisatie plaatsvinden, informatiebeveiliging en ICT. Louter een juridische achtergrond hebben is onvoldoende.

§ 3.3.2 Takenpakket

De belangrijkste taken van de FG staan in de AVG.¹⁵² In de AVG staat dat de FG een tweedelige kerntaak heeft, namelijk enerzijds het informeren en adviseren van de verwerkingsverantwoordelijke of de verwerker en anderzijds toezien op de naleving van de AVG.¹⁵³ Een FG die functioneert voor een gemeente heeft volgens het Kwaliteitsinstituut Nederlandse Gemeenten (KING) en de Vereniging Nederlandse Gemeenten (VNG) de volgende taken:

- het informeren en adviseren van de gemeente en de verwerkers die namens de gemeente persoonsgegevens verwerken;
- het toezien op naleving van de AVG en andere EU wet- en regelgeving of nationale bepalingen omtrent gegevensbescherming;
- het toezien op naleving van het gemeentelijke beleid of de verwerker met betrekking tot de bescherming van persoonsgegevens;
- het toezien op toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het bij de verwerking betrokken personeel en de betreffende audits;
- het geven van advies met betrekking tot de privacy impact assessment (PIA) en het toezien of de uitvoering daarvan in overeenstemming is met de AVG;
- het samenwerken met de AP en
- het optreden als contactpunt voor de AP.¹⁵⁴

In de 'Handreiking: Rol en taken Functionaris Gegevensbescherming' van het KING en de VNG staan de bovenstaande taken van de FG nader uitgewerkt en toegelicht.

¹⁴⁸ S.R. Wiegerinck, 'Blogserie Europese privacyverordening, aflevering 3: privacy by design, privacy by default, beveiliging en inbreuken hierop' (*geraadpleegd op 20 maart 2017 via www.banning.nl*).

¹⁴⁹ Artikel 37 lid 1 onder a AVG.

¹⁵⁰ Artikel 37 lid 3 AVG.

¹⁵¹ 'Functionaris voor de gegevensbescherming', www.autoriteitpersoonsgegevens.nl (zoek op *Functionaris voor de gegevensbescherming*), <Zelf doen, Functionaris voor de gegevensbescherming>.

¹⁵² Artikel 39 AVG.

¹⁵³ Artikel 39 lid 1 aanhef en onder a en b AVG.

¹⁵⁴ KING/VNG, 'Handreiking: Rol en taken Functionaris Gegevensbescherming', p. 2.

§ 3.3.3 Positie

Op grond van de AVG moet de FG naar behoren en tijdig betrokken worden bij alle aangelegenheden die betrekking hebben op de bescherming van persoonsgegevens.¹⁵⁵ Hieruit volgt een soort medewerkingsplicht voor de verwerkingsverantwoordelijke. De verwerkingsverantwoordelijke en de verwerker moeten de FG toegang verschaffen tot persoonsgegevens en verwerkingsactiviteiten, middelen beschikbaar stellen voor het vervullen van zijn taken en ervoor zorgen dat zijn deskundigheid in stand blijft (een opleidingsverplichting).¹⁵⁶ Indien de FG meerdere taken of plichten voor de organisatie vervult is het aan de verwerkingsverantwoordelijke of verwerker om ervoor te zorgen dat deze taken of plichten niet leiden tot belangenconflicten.¹⁵⁷

De AP heeft de onderstaande richtsnoeren opgesteld die organisaties en bedrijven kunnen gebruiken om ervoor te zorgen dat de FG tijdig wordt betrokken bij de aangelegenheden die betrekking hebben op de bescherming van persoonsgegevens:

- De FG wordt regelmatig uitgenodigd om aan vergaderingen van het hoger management en het middenmanagement deel te nemen.
- Er wordt aangeraden de FG uit te nodigen wanneer beslissingen met gevolgen voor gegevensbescherming worden genomen. Alle relevante informatie dient tijdig aan de functionaris voor gegevensbescherming doorgegeven te worden om hem of haar in staat te stellen passend advies te geven.
- De FG dient onmiddellijk geraadpleegd te worden indien zich een datalek of ander incident heeft voorgedaan.¹⁵⁸

Volgens de AP dient aan de mening van de FG altijd een passende waarde gehecht te worden. Bij geschillen raadt WP29 (Artikel 29-werkgroep) aan om vast te leggen waarom het advies van de FG niet gevolgd is.¹⁵⁹

§ 3.4 Rechten van betrokkene

Betrokkenen hebben op grond van de AVG verschillende rechten. Het recht op inzage, rectificatie, vergetelheid, beperking en dataportabiliteit zijn de belangrijkste rechten. In deze paragraaf worden deze rechten beschreven.

§ 3.4.1 Recht op inzage¹⁶⁰

Een betrokkene heeft het recht om persoonsgegevens die over hem worden verzameld in te zien. Op die manier kan de betrokkene controleren of de persoonsgegevens op een rechtmatige manier verwerkt worden.¹⁶¹ De betrokkene heeft tevens het recht op inzage van de verwerkingsdoeleinden en de bewaartermijnen.

§ 3.4.2 Recht op rectificatie¹⁶²

Het recht op rectificatie houdt in dat een betrokkene de verwerkingsverantwoordelijke kan verzoeken om onjuiste persoonsgegevens onverwijld te verbeteren.

¹⁵⁵ Artikel 38 lid 1 AVG.

¹⁵⁶ Artikel 38 lid 2 AVG.

¹⁵⁷ Artikel 38 lid 6 AVG.

¹⁵⁸ Autoriteit Persoonsgegevens, 'Richtlijnen voor functionarissen voor de gegevensbescherming (FG's)', p. 12.

¹⁵⁹ De Artikel 29-werkgroep is een onafhankelijk advies- en overlegorgaan van Europese privacytoezichthouders.

¹⁶⁰ Artikel 15 AVG.

¹⁶¹ Overweging 63 AVG.

¹⁶² Artikel 16 AVG.

§ 3.4.3 Recht op gegevenswissing

Het recht op gegevenswissing (ook wel “recht om vergeten te worden” genoemd) is nieuw en vloeit voort uit het Costeja-arrest.¹⁶³ Het recht op gegevenswissing op grond van de AVG komt erop neer dat gegevens van een betrokkene verwijderd moeten worden indien:

- de verwerking niet langer noodzakelijk is voor de doeleinden waarvoor de persoonsgegevens zijn verzameld of anderszins zijn verwerkt;
- de betrokkene zijn toestemming intrekt waarop de verwerking is gebaseerd en er geen andere rechtsgrond is voor de verwerking van de persoonsgegevens;
- de betrokkene bezwaar maakt tegen de verwerking en er geen dwingende gerechtvaardigde gronden voor de verwerking aanwezig zijn;
- de persoonsgegevens onrechtmatig zijn verwerkt;
- er voldaan moet worden aan een wettelijke verplichting op grond van het Unierecht of het nationaal recht of
- de persoonsgegevens verzameld zijn in het kader van een aanbod van diensten van de informatiemaatschappij als bedoeld in artikel 8 lid 1 AVG.¹⁶⁴

Indien de verantwoordelijke de persoonsgegevens heeft gedeeld met anderen, is de verantwoordelijke verplicht deze derden op de hoogte te stellen van het verzoek van de betrokkene. De verantwoordelijke moet hierbij het verzoek doen om iedere koppeling, kopie of reproductie naar/van de persoonsgegevens waarop het verzoek betrekking heeft te verwijderen.¹⁶⁵

Het bovenstaande is niet van toepassing indien de verwerking nodig is:

- voor het uitoefenen van het recht op vrijheid van meningsuiting en informatie;
- voor het nakomen van een in het Unierecht of het lidstatelijke recht neergelegde wettelijke verwerkingsverplichting die op de verwerkingsverantwoordelijke rust;
- voor het vervullen van een taak van algemeen belang of het uitoefenen van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend;
- om redenen van algemeen belang op het gebied van volksgezondheid;
- met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden en
- voor de instelling, uitoefening of onderbouwing van een rechtsvordering.¹⁶⁶

§ 3.4.4 Recht op beperking¹⁶⁷

Het recht op beperking houdt in dat de betrokkene het recht heeft om de verwerking van gegevens op te schorten. Dit kan de betrokkene bijvoorbeeld doen indien hij van mening is dat zijn gegevens onjuist zijn of onrechtmatig worden verwerkt. Indien de verwerking is opgeschort mogen de gegevens slechts nog met toestemming van de betrokkene worden verwerkt.¹⁶⁸ Indien de verwerkingsverantwoordelijke het recht op beperking wil opheffen, moet de verwerkingsverantwoordelijke eerst de betrokkene op de hoogte brengen.¹⁶⁹

§ 3.4.5 Recht op dataportabiliteit¹⁷⁰

De betrokkene heeft het recht op dataportabiliteit (ook wel het recht op overdraagbaarheid van gegevens genoemd). Het recht op dataportabiliteit houdt in dat de betrokkene het recht heeft de gegevens die hij aan een verantwoordelijke heeft verstrekt te ontvangen. Dit moet

¹⁶³ HvJ EU 13 mei 2014, C-131/12, ECLI:EU:C:2014:317.

¹⁶⁴ Artikel 17 lid 1 AVG.

¹⁶⁵ Duthler & Biesheuvel 2013, p. 22.

¹⁶⁶ Artikel 17 lid 3 AVG.

¹⁶⁷ Artikel 18 AVG.

¹⁶⁸ Artikel 18 lid 2 AVG.

¹⁶⁹ Artikel 18 lid 3 AVG.

¹⁷⁰ Artikel 20 AVG.

gebeuren in een gestructureerde, gangbare en machineleesbare vorm. De betrokkene heeft het recht om de verkregen gegevens aan een andere verantwoordelijke over te dragen zonder daarbij gehinderd te worden door de verantwoordelijke aan wie de persoonsgegevens in eerste instantie waren verstrekt. Door het recht op dataportabiliteit heeft de betrokkene meer controle over zijn persoonsgegevens.¹⁷¹ De AP heeft voor wat betreft het recht op dataportabiliteit richtlijnen gepubliceerd voor verwerkingsverantwoordelijken.¹⁷²

§ 3.5 Verschillen tussen de Wbp en AVG

Hieronder staan de belangrijkste verschillen tussen de Wbp en de AVG puntsgewijs beschreven.

- Begrippen

In de Wbp wordt gesproken van “verantwoordelijke” en “bewerker”. In de AVG worden de begrippen “verantwoordelijke” en “bewerker” vervangen door respectievelijk “verwerkingsverantwoordelijke” en “verwerker”.¹⁷³

In de Wbp wordt het begrip “toestemming” als volgt gedefinieerd: *“elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem betreffende persoonsgegevens worden verwerkt”*.¹⁷⁴ In de AVG wordt het begrip “toestemming” anders gedefinieerd, namelijk als volgt: *“elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt”*.¹⁷⁵ Op grond van de AVG moet toestemming “ondubbelzinnig” gegeven worden door een verklaring of een duidelijke actieve handeling van de betrokkene. Een stilzwijgende of impliciete toestemming is door de komst van de AVG niet meer voldoende.

- Accountability

De AVG gaat uit van het ‘accountability principe’. Bedrijven en organisaties moeten op grond van het ‘accountability principe’ kunnen aantonen dat zij voldoen aan de wettelijke vereisten.¹⁷⁶ Bedrijven en organisaties krijgen een documentatieplicht en moeten in bepaalde gevallen een privacy impact assessment (ook wel Data protection impact assessment of een gegevensbeschermingseffectbeoordeling genoemd) uitvoeren.

Documentatieplicht

Gegevensverwerkingen die plaatsvinden binnen bedrijven en organisaties moeten op grond van de Wbp gemeld worden aan de AP.¹⁷⁷ Deze verplichting staat niet in de AVG. De verplichting om gegevensverwerkingen te melden aan de AP wordt vervangen door de register- en documentatieplicht. De register- en documentatieplicht houdt in dat bedrijven en organisaties een overzicht bij moeten houden van alle gegevensverwerkingen die plaatsvinden binnen het bedrijf of de organisatie. De volgende informatie moet per verwerking in het overzicht geregistreerd worden:

- de gegevens over de verantwoordelijke (indien aanwezig medeverantwoordelijke);
- het doel van de verwerking;

¹⁷¹ De IT-jurist bv, ‘Het recht op overdraagbaarheid van gegevens’, 20 februari 2017 (geraadpleegd op 10 april 2017 via www.it-jurist.nl).

¹⁷² Autoriteit Persoonsgegevens, ‘Richtlijnen voor het recht op dataportabiliteit’.

¹⁷³ Zwenne & Mommers, *Tijdschrift voor Compliance* 2016, p. 182-189.

¹⁷⁴ Artikel 1 aanhef en onder i Wbp.

¹⁷⁵ Artikel 4 aanhef en onder 11 AVG.

¹⁷⁶ Zwenne & Mommers, *Tijdschrift voor Compliance* 2016, p. 182-189.

¹⁷⁷ Artikel 27 Wbp.

- de categorieën van persoonsgegevens die worden verwerkt door de verantwoordelijke;
- de bewaartermijnen;
- de ontvangers van de persoonsgegevens en
- een beschrijving van de genomen technische en organisatorische maatregelen.^{178 179}

De register- en documentatieplicht geldt niet voor bedrijven en organisaties die minder dan 250 personen in dienst hebben, tenzij het waarschijnlijk is dat verwerkingen een risico inhouden voor de rechten en vrijheden van de betrokkenen, verwerkingen niet incidenteel zijn of indien bijzondere gegevens als bedoeld in artikel 9 lid 1 AVG of gegevens in verband met strafrechtelijke veroordelingen en strafbare feiten als bedoeld in artikel 10 AVG worden verwerkt.¹⁸⁰

Privacy impact assessment (PIA)

De AVG verplicht bedrijven en organisaties een PIA uit te voeren indien het bedrijf of de organisatie:

- systematisch en uitvoerig persoonlijke aspecten evalueert, waaronder profilering;
- op grote schaal bijzondere persoonsgegevens verwerkt of
- op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied (bijvoorbeeld met cameratoezicht).¹⁸¹

Een PIA maakt op een systematische wijze inzichtelijk hoe groot de kans is dat de privacy van de betrokkene wordt geschaad, waar de risico's zitten en welke gevolgen daaraan voor de betrokkene verbonden zijn.¹⁸²

• Informatieplicht

Op grond van de Wbp moeten bedrijven en organisaties op grond van de informatieplicht de volgende informatie verstrekken aan de betrokkenen:

- de identiteit van de verantwoordelijke;
- de doeleinden van de verwerking en
- nadere informatie voor zover dat nodig is om een zorgvuldige verwerking te waarborgen.¹⁸³

De informatieplicht wordt door de komst van de AVG uitgebreid. Door de komst van de AVG is de verantwoordelijke onder andere verplicht om naast de bovenstaande informatie ook de volgende informatie te verstrekken aan de betrokkene:

- de contactgegevens van de FG;
- de rechtsgrond voor de verwerking;
- de bewaartermijn van de gegevens;
- de rechten van betrokkene;
- dat een eventueel gegeven toestemming altijd kan worden ingetrokken;
- dat een klacht bij de toezichthouder (in dit geval de AP) kan worden ingediend;
- of verstrekking van gegevens verplicht is en wat de gevolgen zijn indien de gegevens niet worden verstrekt en

¹⁷⁸ C. Arts, 'Het accountability principe onder de Algemene Verordening Gegevensbescherming', 23 augustus 2016 (geraadpleegd op 12 april 2017 via www.considerati.com).

¹⁷⁹ Artikel 30 lid 1 AVG.

¹⁸⁰ Artikel 30 lid 5 AVG.

¹⁸¹ 'Algemene verordening gegevensbescherming', www.autoriteitpersoonsgegevens.nl (zoek op *Algemene verordening gegevensbescherming*), <Onderwerpen, Europese privacywetgeving, Algemene verordening gegevensbescherming>.

¹⁸² König & Karssenbergh 2015, p. 9.

¹⁸³ Artikel 33 Wbp.

- de kern van de taak-/rolverdeling indien er meerdere partijen gezamenlijk verantwoordelijk zijn voor een verwerking.¹⁸⁴

- Rechten van betrokkenen

In de AVG zijn de rechten van betrokkenen (inzage-, correctie- en verwijderingsrecht) meer uitgewerkt en gedetailleerd.¹⁸⁵ De rechten van betrokkenen worden door de komst van de AVG verstrekt. Een nieuw recht voor betrokkene is het recht op gegevenswissing (zie ook paragraaf 3.4.3 van dit onderzoeksrapport). In de Wbp staat dat een betrokkene slechts een verzoek tot verwijdering van zijn gegevens kan doen wanneer de gegevens feitelijk onjuist zijn, voor het doel of de doeleinden van de verwerking onvolledig of niet ter zake dienend zijn dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt.¹⁸⁶ In de AVG kan het recht op gegevenswissing te allen tijde (dus ook wanneer geen sprake is van onjuiste of onvolledige gegevens) worden uitgeoefend. Het recht op beperking en het recht op dataportabiliteit zijn nieuwe rechten van betrokkenen die niet in de Wbp staan (zie paragraaf 3.4.4 en 3.4.5 van dit onderzoeksrapport).

- Functionaris voor gegevensbescherming (FG)

Bepaalde bedrijven en organisaties, waaronder overheidsinstanties, zijn op grond van de AVG verplicht om een FG aan te stellen. Op grond van de Wbp is het aanstellen van een FG vrijwillig. In paragraaf 3.3 van dit onderzoeksrapport wordt uitgebreid beschreven welke eisen er aan een FG worden gesteld, alsmede wat de positie en het takenpakket van de FG is.

- Meldplicht datalekken

In Nederland is sinds 1 januari 2016 de Wmd van kracht. Bedrijven en organisaties moeten datalekken (waarbij sprake is van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens) binnen 72 uur melden bij de AP. Nederland loopt hierdoor vooruit op de AVG, waarin een soortgelijke meldplicht staat. Er zitten nauwelijks verschillen tussen de huidige meldplicht uit de Wbp en de aanstaande meldplicht op grond van de AVG. Het belangrijkste verschil is de hoogte van de boete. Op grond van de Wbp kan de AP bij het overtreden van de meldplicht een boete van maximaal € 820.000,- opleggen. Op grond van de AVG kan de AP een boete van maximaal € 20.000.000,- of 4% van de jaarlijkse wereldwijde omzet opleggen. Voorts moeten bedrijven en organisaties op grond van de AVG alle datalekken die hebben plaatsgevonden documenteren (oftewel registreren in een logboek).¹⁸⁷

- Verhoging boetes

De boetes die de AP als toezichthoudende autoriteit kan opleggen worden door de komst van de AVG verhoogd. De hoogste boete die in de Wbp staat is € 820.000,- of tien procent van de jaaromzet.¹⁸⁸ De hoogste boete die in de AVG staat is € 20.000.000,- of vier procent van de wereldwijde jaaromzet.¹⁸⁹

¹⁸⁴ M. Jansen, 'De privacy-paradox: steeds meer informatie verstrekken, maar wel zo compact en simpel mogelijk alstublieft' (*geraadpleegd op 20 april 2017 via www.dirkzwagerieit.nl*).

¹⁸⁵ Zwenne & Mommers, *Tijdschrift voor Compliance* 2016, p. 182-189.

¹⁸⁶ Artikel 36 lid 1 Wbp.

¹⁸⁷ Artikel 33 lid 5 AVG.

¹⁸⁸ Artikel 66 lid 2 Wbp jo. artikel 23 WvSr.

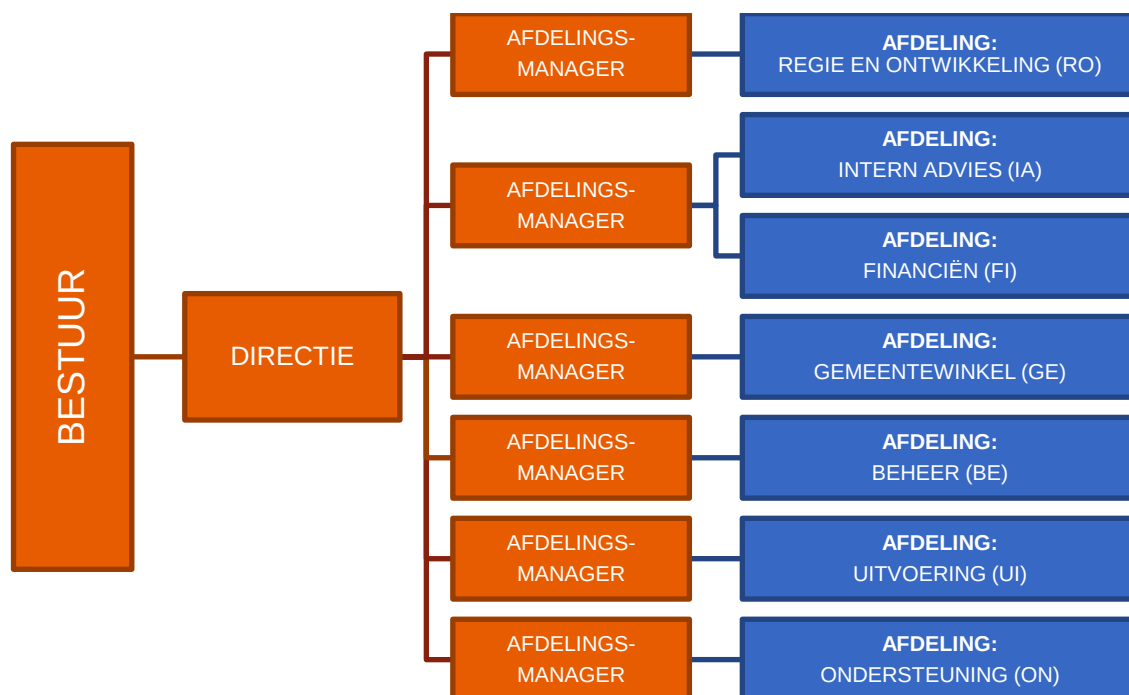
¹⁸⁹ Artikel 83 lid 5 AVG.

HOOFDSTUK 4: GEGEVENSVERWERKINGEN BINNEN DE GEMEENTE BEST

In dit hoofdstuk wordt eerst beschreven hoe de gemeente Best is georganiseerd. Daarna wordt beschreven op welke wijze de gemeente Best (persoons)gegevens verwerkt. Dit hoofdstuk geeft antwoord op de volgende deelvraag: “Wat is de huidige werkwijze van de gemeente Best met betrekking tot het verwerken van persoonsgegevens?”.

§ 4.1 Organisatie

Bij de gemeente Best zijn ongeveer 250 medewerkers werkzaam. Er zijn zeven afdelingen en een tweehoofdige directie. De afdelingen worden geleid door de afdelingsmanagers. Bepaalde afdelingen hebben een adjunct afdelingsmanager. Om een goed beeld te krijgen van de organisatie, is een organogram gemaakt (figuur 3.1). Een uitgebreidere organogram is opgenomen als bijlage (bijlage 1).



Figuur 3.1: organogram gemeente Best.

§ 4.2 Medewerkers die zich bezighouden met gegevensverwerkingen

De medewerkers die vanuit hun functie controleren of de verschillende gegevensverwerkingen binnen de gemeente Best voldoen aan de huidige wet- en regelgeving zijn Marion van Rooij, Frans Swiers en Rik Verheul. Marion van Rooij is privacyfunctionaris en senior juridisch adviseur van de gemeente Best. Frans Swiers is informatie- en automatiseringsmanager van de gemeente Best. Rik Verheul is informatiebeveiligingsfunctionaris van de gemeente Best. Er is – vooralsnog – geen FG werkzaam binnen de gemeente Best die is aangemeld bij de AP en onafhankelijk toezicht houdt of de gemeente Best voldoet aan de Wbp / AVG. Marion van Rooij voert wel taken uit die raakvlakken hebben met de werkzaamheden van een FG (bijvoorbeeld: medewerkers van de gemeente Best adviseren over wet- en regelgeving omtrent gegevensbescherming).

§ 4.3 Gegevensverwerkingen

Alle afdelingen van de gemeente Best verwerken verschillende persoonsgegevens. De afgelopen jaren zijn alle gegevensverwerkingen die plaatsvinden op de afdelingen in kaart gebracht. Dit is gedaan door Marion van Rooij en Adri van der Peet (specialist op het gebied van privacy en gegevensverwerking). Alle gegevensverwerkingen (ruim 100) staan geregistreerd in het overzicht gegevensverwerkingen. Het overzicht gegevensverwerkingen is terug te vinden in de bijlage (zie bijlage 2).

§ 4.3.1 Overzicht gegevensverwerkingen

De verschillende gegevensverwerkingen staan per afdeling beschreven. Dit is doelbewust gedaan, omdat elke afdeling een afdelingsmanager heeft die medeverantwoordelijk is voor de gegevensverwerkingen binnen zijn of haar afdeling. Een afdelingsmanager kan door het raadplegen van het overzicht gegevensverwerkingen snel zien welke gegevensverwerkingen plaatsvinden binnen zijn of haar afdeling. De eindverantwoordelijke voor alle gegevensverwerkingen is het college van burgemeester en wethouders van de gemeente Best of de burgemeester van de gemeente Best (zie bijlage 3 voor het interview met Marion van Rooij). Wie eindverantwoordelijk is, is afhankelijk van welk bestuursorgaan het bevoegd gezag is. Het verantwoordelijk / bevoegd bestuursorgaan voor de behandeling van een aanvraag van een bijstandsuitkering is bijvoorbeeld het college van burgemeester en wethouders, terwijl het verantwoordelijk bestuursorgaan voor de behandeling van een aanvraag van een evenementenvergunning de burgemeester is. Voorts wordt in het overzicht gegevensverwerkingen per gegevensverwerking het volgende beschreven:

- wie de contactpersoon is;
- wat het doel van de verwerking is;
- wie de betrokkenen zijn;
- welke persoonsgegevens verwerkt worden;
- wie de ontvangers van de persoonsgegevens zijn;
- of er een rechtmatige grondslag aanwezig is;
- of de verwerking gemeld moet worden bij de AP;
- wat het risicoklasse is;
- wat de bewaartermijn is;
- of de verwerking geautomatiseerd of handmatig plaatsvindt en
- eventueel met welke applicatie de persoonsgegevens verwerkt worden.

Contactpersoon

In het overzicht gegevensverwerkingen heeft de gemeente Best per gegevensverwerking geregistreerd wie de contactpersoon van een bepaalde gegevensverwerking is. De contactpersonen die in het overzicht gegevensverwerkingen beschreven staan zijn medewerkers van de gemeente Best. De contactpersonen zijn niet de verantwoordelijken (volgens de Wbp) of de verwerkingsverantwoordelijken (volgens de AVG).

Doel van de verwerking

De gemeente Best heeft in het overzicht gegevensverwerkingen per gegevensverwerking het doel van de verwerking omschreven. Dit heeft de gemeente Best gedaan omdat op grond van de Wbp en de aanstaande AVG eerst het doel van de verwerking omschreven moet worden voordat de persoonsgegevens verzameld en verwerkt mogen worden. Op grond van de Wbp en de AVG mogen persoonsgegevens slechts verzameld en verwerkt worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden.

Betrokkenen

In het overzicht gegevensverwerkingen heeft de gemeente Best per gegevensverwerkingen geregistreerd wie de betrokkenen zijn. De gemeente Best registreert de betrokkenen omdat de gemeente Best zich ervan bewust is dat persoonsgegevens transparant verwerkt

moeten worden. De gemeente Best probeert iedere betrokkene actief in te lichten over welke persoonsgegevens over hem of haar verwerkt worden en met welk doel de verwerking plaatsvindt.

Gegevens

De gemeente Best heeft in het overzicht gegevensverwerkingen per gegevensverwerking beschreven welke persoonsgegevens er verzameld worden. De meest voorkomende persoonsgegevens die de gemeente Best verwerkt zijn:

- NAW-gegevens (naam, adres en woonplaats);
- e-mailadressen;
- telefoonnummers
- geboortedatums;
- BSN-nummers;
- kopieën van identiteitsbewijzen;
- financiële persoonsgegevens (waaronder bankgegevens) en
- medische persoonsgegevens / gezondheidsinformatie.

De gemeente Best verwerkt bijzondere persoonsgegevens, namelijk BSN-nummers, kopieën van identiteitsbewijzen, gegevens over politieke voorkeur, strafrechtelijke gegevens en medische persoonsgegevens / gezondheidsinformatie. Voorts verwerkt de gemeente Best financiële gegevens. Financiële gegevens zijn gevoelige gegevens.¹⁹⁰

Ontvangers

In het overzicht gegevensverwerkingen heeft de gemeente Best per gegevensverwerking beschreven wie de persoonsgegevens allemaal ontvangen. De gemeente Best deelt persoonsgegevens met verschillende organisaties. De gemeente Best deelt bijvoorbeeld – afhankelijk van de gegevensverwerking – persoonsgegevens met de politie, brandweer, verzekeraars, de belastingdienst of andere gemeenten.

Rechtmatige grondslag

Persoonsgegevens mogen alleen verwerkt worden indien dit gebeurt op basis van een rechtmatige grondslag (zie ook paragraaf 2.1.3 van dit onderzoeksrapport). In het overzicht gegevensverwerkingen heeft de gemeente Best daarom bij iedere gegevensverwerking aangegeven wat de rechtmatige grondslag van de gegevensverwerking is. Vrijwel alle gegevensverwerkingen die plaatsvinden binnen de gemeente Best zijn noodzakelijk ter uitvoering van een wettelijke plicht en/of voor de goede vervulling van een publiekrechtelijke taak.

Meldingsplicht

In het overzicht gegevensverwerkingen heeft de gemeente Best per gegevensverwerking beschreven of de gegevensverwerking gemeld moet worden bij de AP. Gegevensverwerkingen moeten, behoudens bepaalde uitzonderingen die staan beschreven in het Vrijstellingsbesluit Wbp (VWbp), gemeld worden bij de AP. De gemeente Best heeft op dit moment 43 gegevensverwerkingen gemeld bij de AP.¹⁹¹ Met de komst van de AVG vervalt de meldingsplicht.

Risicoklasse

De gemeente Best heeft per gegevensverwerking beschreven wat het risicoklasse is. Een hoog risico houdt in dat er bij een inbreuk op de beveiliging ernstige gevolgen kunnen zijn

¹⁹⁰ 'Financiën', www.autoriteitpersoonsgegevens.nl (zoek op *Financiën*), <Onderwerpen, Financiën>

¹⁹¹ Meldingenregister Autoriteit Persoonsgegevens

<<https://www.collegebeschermingpersoonsgegevens.nl/asp/ORSearch.asp>>.

voor de betrokkenen. Indien sprake is van een hoog risico wordt extra zorgvuldigheid bij de verwerking verwacht.

Bewaartermijn

De gemeente Best is zich ervan bewust dat persoonsgegevens niet langer bewaard mogen worden dan noodzakelijk is voor het doel waarvoor de persoonsgegevens zijn verzameld. De gemeente Best heeft daarom in het overzicht gegevensverwerkingen per gegevensverwerking beschreven hoelang de persoonsgegevens bewaard mogen worden.

Applicatie

De gemeente Best heeft in het overzicht gegevensverwerkingen per gegevensverwerking beschreven in welke applicaties de persoonsgegevens eventueel geregistreerd worden. De gemeente Best maakt gebruik van veel verschillende applicaties (o.a. CiVision, Corsa, en Squit XO, maar ook Microsoft Word en Excel). Het is belangrijk om per gegevensverwerking te registreren in welke applicaties persoonsgegevens staan opgeslagen. Indien persoonsgegevens verwijderd moeten worden, bijvoorbeeld naar aanleiding van een verzoek tot verwijdering van een betrokkene, kan de gemeente Best het overzicht gegevensverwerkingen raadplegen om te zien in welke applicaties de gegevens staan geregistreerd. Hiermee voorkomt de gemeente Best dat persoonsgegevens per ongeluk in applicaties blijven staan die over het hoofd worden gezien.

§ 4.3.2 Gegevensverwerking uitgelicht

Om een extra goed beeld te geven hoe de gemeente Best persoonsgegevens verwerkt wordt hieronder een willekeurige gegevensverwerking uit het overzicht gegevensverwerkingen uitgebreid beschreven. De gegevensverwerking die hieronder is beschreven is samen met de opdrachtgever geselecteerd uit het overzicht gegevensverwerkingen. Gelet op de beperkte beschikbare tijd voor dit onderzoek is het niet gelukt om alle gegevensverwerkingen die plaatsvinden binnen de gemeente Best uitgebreid te beschrijven. Voor een compleet overzicht van alle gegevensverwerkingen die plaatsvinden binnen de gemeente Best wordt verwezen naar het overzicht gegevensverwerkingen (bijlage 2).

APV vergunningen en ontheffingen:

Op grond van de Algemene plaatselijke verordening 2010 APV van de gemeente Best (APV) moet voor bepaalde activiteiten een vergunning of ontheffing worden aangevraagd. In deze paragraaf wordt beschreven welke persoonsgegevens verwerkt worden bij het behandelen van een aanvraag van een evenementenvergunning. De aanvraag van een evenementenvergunning wordt behandeld door de afdeling Uitvoering (vakgroep Vergunningen). In een willekeurig dossier betreffende een aanvraag van een evenementenvergunning is gekeken welke persoonsgegevens in het dossier zitten.

Persoonsgegevens

Een evenementenvergunning kan zowel schriftelijk als digitaal worden aangevraagd via de website van de gemeente Best (www.gemeentebest.nl). De meeste evenementenvergunningen worden digitaal aangevraagd. De digitale aanvraag van een evenementenvergunning start met het inloggen op de website van de gemeente met DigiD. DigiD is een afkorting van Digitale Identiteit. Met DigiD kan iedereen inloggen op websites van de overheid en de zorg.¹⁹² Bij de aanvraag van een evenementenvergunning worden verschillende persoonsgegevens verwerkt. De volgende persoonsgegevens worden bij de aanvraag van een evenementenvergunning door de gemeente Best verwerkt:

- burgerservicenummer of KvK-nummer aanvrager;

¹⁹² 'Wat is DigiD', www.digid.nl (zoek op *Wat is DigiD?*), <Onderwerpen, Digitale overheid, Vraag en antwoord>.

- (bedrijfs)naam aanvrager;
- adres aanvrager;
- postcode aanvrager;
- woonplaats aanvrager;
- geboortedatum aanvrager;
- naam contactpersoon;
- BSN-nummer contactpersoon en
- mobiel nummer contactpersoon.

Indien ten behoeve van het evenement een ontheffing voor het verstrekken van zwak-alcoholhoudende drank nodig is op grond van artikel 35 Drank- en Horecawet (DHW), worden door de gemeente Best ook de volgende persoonsgegevens verwerkt bij de aanvraag:

- achternaam persoon drankvoorziening;
- voornaam persoon drankvoorziening;
- adres persoon drankvoorziening;
- postcode persoon drankvoorziening;
- woonplaats persoon drankvoorziening;
- geboortedatum persoon drankvoorziening en
- verklaring sociale hygiëne en een kopie van het identiteitsbewijs (leidinggevend).

Gelet op het voorgaande verwerkt de gemeente Best bij de aanvraag van een evenementenvergunning bijzondere persoonsgegevens, namelijk burgerservicenummers en kopieën van identiteitsbewijzen. Bijzondere gegevens zijn extra privacygevoelig en mogen niet zonder meer verwerkt worden. Er geldt namelijk, behoudens bepaalde uitzonderingen die staan in de Wbp, een verbod op het verwerken van bijzondere persoonsgegevens. In paragraaf 2.1.3 van dit onderzoeksrapport wordt hier uitgebreid aandacht aan besteed. De gemeente Best moet bij het verwerken van bijzondere persoonsgegevens extra beveiligingsmaatregelen treffen. Voor het beveiligen van persoonsgegevens geldt namelijk een proportionaliteitstoets; hoe gevoeliger de gegevens zijn, hoe beter de gegevens beveiligd moeten worden. Meer informatie over de beveiliging van persoonsgegevens staat in paragraaf 2.1.4 van dit onderzoeksrapport.

Doel

De persoonsgegevens die bij de behandeling van een aanvraag van een evenementenvergunning worden verzameld, worden verwerkt met het volgende doel: “Behandelen van aanvragen om evenementenvergunningen”. Dit doel staat in het overzicht gegevensverwerkingen beschreven.

Betrokkenen

Volgens het overzicht gegevensverwerkingen worden er slechts persoonsgegevens verwerkt die betrekking hebben op de aanvragers van de evenementenvergunning. Kortom: de aanvragers van de evenementenvergunning zijn de betrokkenen.

Ontvangers

De persoonsgegevens die worden verwerkt bij het behandelen van een aanvraag van een evenementenvergunning deelt de gemeente Best met verschillende organisaties en personen. Dit wordt voornamelijk gedaan om de veiligheid van evenementen te waarborgen. In het overzicht gegevensverwerkingen staat dat de persoonsgegevens gedeeld kunnen worden met de volgende organisaties en personen:

- de brandweer;
- de Geneeskundige Hulpverleningsorganisatie in de Regio (GHOR);
- politie en

- belanghebbenden.

Rechtmatige grondslag

Het verstrekken van evenementenvergunningen is een publiekrechtelijke taak die bij of krachtens de wet (in dit geval de APV) is opgedragen aan de burgemeester van de gemeente Best. De burgemeester is een bestuursorgaan. Op grond van artikel 8 aanhef en onder e Wbp mogen persoonsgegevens verwerkt worden indien de gegevensverwerking noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan. De burgemeester heeft bij de behandeling van de aanvraag van een evenementenvergunning verschillende persoonsgegevens nodig van de aanvrager(s). De verwerking van de persoonsgegevens bij het behandelen van een aanvraag van een evenementenvergunning vindt dan ook plaats op grond van artikel 8 aanhef en onder e Wbp. De onderhavige verwerking is immers noodzakelijk voor de goede vervulling van de publiekrechtelijke taak van de burgemeester van de gemeente Best.

Meldingsplicht

De verwerking van persoonsgegevens bij het behandelen van een aanvraag van een evenementenvergunning hoeft op grond van artikel 22 Vrijstellingsbesluit Wbp niet gemeld te worden bij de AP. De gemeente Best heeft de verwerking dan ook niet gemeld bij de AP.

Bewaartermijn

De persoonsgegevens die worden verzameld ten behoeve van het behandelen van een aanvraag van een evenementenvergunning worden op grond van artikel 22 lid 6 Vrijstellingsbesluit Wbp maximaal twee jaren bewaard. De persoonsgegevens worden daarna vernietigd. In artikel 22 lid 6 Vrijstellingsbesluit Wbp is het volgende bepaald: *“De persoonsgegevens worden verwijderd uiterlijk twee jaren nadat het betrokken verzoek om verlening van een vergunning, ontheffing of machtiging door de betrokkene is ingetrokken, de desbetreffende vergunning, ontheffing of machtiging is ingetrokken of de geldigheidsduur daarvan is verlopen, dan wel de desbetreffende verplichting tot melding is vervallen, tenzij de persoonsgegevens noodzakelijk zijn ter voldoening aan een wettelijke bewaarplicht.”*

Applicatie

De persoonsgegevens die worden verwerkt bij de aanvraag van een evenementenvergunning worden volgens het overzicht gegevensverwerkingen verwerkt in de applicatie Squit XO. Squit XO is een programma die door ruim 200 organisaties in Nederland wordt gebruikt voor het verlenen van vergunningen.¹⁹³ De persoonsgegevens die worden verwerkt bij de aanvraag van een evenementenvergunning vindt gelet op het voorgaande geautomatiseerd plaats. Er wordt immers gebruik gemaakt van een programma die is geïnstalleerd op een computer.

§ 4.4 Beveiliging

De informatiebeveiliging binnen de gemeente Best is gebaseerd op het Informatiebeveiligingsbeleid gemeente Best en Veldhoven. Het Informatiebeveiligingsbeleid gemeente Best en Veldhoven is gebaseerd op de Code voor Informatiebeveiliging (NEN/ISO 27002) en de Baseline Informatiebeveiliging Gemeenten (BIG). De BIG bestaat uit twee varianten: de Strategische Baseline en de Tactische Baseline.¹⁹⁴ De Strategische BIG is ontwikkeld voor alle werknemers binnen de gemeente, maar met name het college van burgemeester en wethouders en

¹⁹³ 'Squit Suite', www.roxit.nl (zoek op *Squit Suite*), <Producten, Squit Suite>.

¹⁹⁴ 'Strategische en tactische BIG', www.ibdgemeenten.nl (zoek op *Strategische en tactische BIG*), <BIG, Strategische en tactische BIG>.

gemeentesecretarissen.¹⁹⁵ De Tactische BIG is ontwikkeld voor alle werknemers binnen de gemeente, maar met name; informatiebeveiligingsfunctionarissen, lijnmanagers, beleidsmakers, personeelszaken, fysieke beveiliging, ICT-diensten en infrastructuur, applicatie- en systeemeigenaren, informatiebeveiligingsadviseurs en ICT-auditors en externe leveranciers.¹⁹⁶ De BIG is bedoeld om:

1. Gemeenten op een vergelijkbare manier efficiënt te laten werken met informatiebeveiliging.
2. Gemeenten een hulpmiddel te geven om aan alle eisen op het gebied van informatiebeveiliging te kunnen voldoen.
3. De auditlast bij gemeenten te verminderen.
4. Gemeenten een aantoonbaar betrouwbare partner te laten zijn.¹⁹⁷

Het Informatiebeveiligingsbeleid gemeente Best en Veldhoven is opgesteld met de volgende doelstelling: *“Dit informatiebeveiligingsbeleid (IB-beleid) is het kader voor passende technische en organisatorische maatregelen om gemeentelijke informatie te beschermen en te waarborgen, dat de gemeente voldoet aan relevante wet en regelgeving. Best en Veldhoven streven er naar om ‘in control’ te zijn en daarover op professionele wijze verantwoording af te leggen. In control betekent in dit verband dat de gemeente weet welke maatregelen genomen zijn en dat er een SMART-planning is van de maatregelen die nog niet genomen zijn en als laatste dat dit geheel verankerd is in de PDCA-cyclus”*.¹⁹⁸

In het Informatiebeveiligingsbeleid gemeente Best en Veldhoven staan onder andere de risico's met betrekking tot de beveiliging van persoonsgegevens beschreven. Voorts staan in het Informatiebeveiligingsbeleid gemeente Best en Veldhoven verschillende maatregelen beschreven die de beveiliging van persoonsgegevens bevorderen. Voorbeelden van deze maatregelen zijn:

- De medewerkers nemen passende technische en organisatorische maatregelen om gemeentelijke informatie te beveiligen tegen verlies of tegen enige vorm van onrechtmatig gebruik.
- Medewerkers die werken met vertrouwelijke of geheime informatie overleggen voorindiensttreding een Verklaring Omtrent het Gedrag (VOG). De VOG wordt indien nodig herhaald tijdens het dienstverband.
- Alle medewerkers (en voor zover van toepassing externe gebruikers van onze systemen) dienen training te krijgen in procedures die binnen de gemeente of afdeling gelden voor informatiebeveiliging. Deze training dient regelmatig te worden herhaald om het beveiligingsbewustzijn op peil te houden.
- Toegang tot niet-openbare gedeelten van gebouwen of beveiligingszones is alleen mogelijk na autorisatie daartoe.¹⁹⁹

Medewerkers van de gemeente Best worden regelmatig voorgelicht over gegevensbeveiliging. De medewerkers van de gemeente Best die zich bezighouden met het beveiligen van persoonsgegevens doen er alles aan om het beveiligingsbewustzijn van de medewerkers van de gemeente Best te verhogen. Dit wordt bijvoorbeeld gedaan door berichten over gegevensbescherming en beveiligingsbewustzijn te plaatsen op Intrabest (een startpagina die alleen toegankelijk is voor medewerkers van de gemeente Best) en informatieschermen die staan in diverse servicecorners. Een voorbeeld van zo'n bericht is

¹⁹⁵ 'Strategische en tactische BIG', www.ibdgemeenten.nl (zoek op *Strategische en tactische BIG*), <BIG, Strategische en tactische BIG>.

¹⁹⁶ 'Strategische en tactische BIG', www.ibdgemeenten.nl (zoek op *Strategische en tactische BIG*), <BIG, Strategische en tactische BIG>.

¹⁹⁷ KING/VNG, 'Strategische Baseline Informatiebeveiliging Nederlandse Gemeenten', p. 3.

¹⁹⁸ Gemeenten Best en Veldhoven, 'Informatiebeveiligingsbeleid Gemeenten Best en Veldhoven', p. 9.

¹⁹⁹ Gemeenten Best en Veldhoven, 'Informatiebeveiligingsbeleid Gemeenten Best en Veldhoven'.

opgenomen als bijlage (bijlage 6). Verder heeft de gemeente Best recent een “phishingtest” laten uitvoeren om erachter te komen of de medewerkers van de gemeente Best op de hoogte zijn van de gevaren van “phishing”. Door dit soort testen uit te voeren en de resultaten hiervan terug te koppelen hoopt de gemeente Best het beveiligingsbewustzijn van de medewerkers van de gemeente Best te verhogen.

Het beveiligen van persoonsgegevens betreft een continu proces (zie bijlage 5 voor het interview met Rik Verheul). Daar waar 100% veiligheid nooit te garanderen is, is de kans dat een inbreuk op de beveiliging plaatsvindt altijd aanwezig. Volgens Frans Swiers maakt een grote gemeente, bijvoorbeeld de gemeente Amsterdam, meer kans om getroffen te worden door een hackaanval dan een kleine gemeente (zoals de gemeente Best). Dit komt omdat grotere gemeenten veel meer gegevens verwerken dan kleine gemeenten.

§ 4.5 Privacyreglement

Op de verwerking van persoonsgegevens binnen de gemeente Best is het Privacyreglement gemeente Best van toepassing (zie bijlage 7). Het privacyreglement gemeente Best betreft een besluit van 25 april 2005 van het college van burgemeester en wethouders van de gemeente Best. Het privacyreglement gemeente Best is formeel nog van kracht en staat gepubliceerd op de website van de gemeente Best (www.gemeentebest.nl). In het volgende hoofdstuk wordt het privacyreglement uitgebreid beschreven. Om herhalingen te voorkomen wordt voor een verdere toelichting op het Privacyreglement gemeente Best verwezen naar het volgende hoofdstuk.

§ 4.6 Datalekken

In deze paragraaf staat beschreven hoe de gemeente Best omgaat met datalekken. De gemeente Best heeft sinds de komst van de Wmd in 2016 verschillende datalekken gehad. De medewerker die verantwoordelijk is voor het melden van datalekken is Marion van Rooij. Alle medewerkers van de gemeente Best zijn hiervan op de hoogte. Aan Marion van Rooij is gevraagd hoeveel datalekken hebben plaatsgevonden na de invoering van de Wmd. Volgens Marion van Rooij gaat het om vijf datalekken. De gemeente Best heeft een werkinstructie voor het afhandelen van datalekken. In de werkinstructie staat onder andere hoe een datalek afgehandeld moet worden, wanneer sprake is van een datalek en in welke gevallen het datalek gemeld moet worden bij de AP. De gemeente Best heeft geen logboek waarin alle datalekken worden geregistreerd, maar de gemeente Best registreert de datalekken wel in het online portaal “TOPdesk”. De gemeente Best is hierdoor in staat om alle datalekken die hebben plaatsgevonden snel te raadplegen. De gemeente Best is zich ervan bewust dat datalekken onverwijld (binnen 72 uur) gemeld moeten worden bij de AP.

Voorbeelden datalekken

Marion van Rooij heeft tijdens het interview (zie bijlage 3) twee voorbeelden gegeven van datalekken die recent hebben plaatsgevonden bij de gemeente Best. Deze twee datalekken heeft Marion van Rooij gemeld bij de AP.

Datalek 1

De sociaal rechercheur van de gemeente Best heeft een rapportage met gevoelige financiële (persoons)gegevens van de betrokkene gedeeld met een woningbouwcorporatie zonder toestemming van de betrokkene.

Datalek 2

Een medewerker van de afdeling Regie en Ontwikkeling heeft een Excel-bestand met verborgen persoonsgegevens (o.a. BSN-nummers) gedeeld met kinderopvangorganisaties.

HOOFDSTUK 5:

DE HUIDIGE WERKWIJZE EN HET PRIVACYREGLEMENT GETOETST AAN DE WBP & AVG

Dit hoofdstuk geeft antwoord op de volgende deelvraag: *“Welke gevolgen hebben de recente wijzigingen van de Wbp en de aanstaande AVG voor de huidige werkwijze van de gemeente Best met betrekking tot het verwerken van persoonsgegevens en het privacyreglement van de gemeente Best?”*.

§ 5.1 Huidige werkwijze

Er is getoetst of de huidige werkwijze van de gemeente Best met betrekking tot het verwerken van persoonsgegevens voldoet aan de Wbp en de aanstaande AVG.

Doelbinding

Op grond van de Wbp en AVG geldt het beginsel van doelbinding. De gemeente Best is zich ervan bewust dat voor elke gegevensverwerking een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel nodig is. De gemeente Best heeft voor alle gegevensverwerkingen die plaatsvinden binnen de gemeente Best een doel geregistreerd in het overzicht gegevensverwerkingen (zie bijlage 2). Het verdient de opmerking dat bepaalde doelen kort zijn geformuleerd. Het is raadzaam om deze doelen uitgebreider te formuleren. De grondslag “de behartiging van het gerechtvaardigde belang van de verantwoordelijke of een derde aan wie de gegevens worden verstrekt” vervalt met de komst van de AVG voor overheidsinstanties (zie paragraaf 3.2.1 van dit onderzoeksrapport). Vooralsnog zijn geen gegevensverwerkingen binnen de gemeente Best gebaseerd op deze grondslag.

Meldplicht gegevensverwerkingen

De gemeente Best heeft alle gegevensverwerkingen die gemeld moeten worden bij de AP gemeld (zie paragraaf 4.3.1 van dit onderzoeksrapport). De gemeente Best voldoet dan ook aan de meldplicht gegevensverwerkingen op grond van de Wbp. In mei 2018 wordt de meldplicht gegevensverwerkingen vervangen door de register- en documentatieplicht en hoeft de gemeente Best eventuele nieuwe gegevensverwerkingen niet meer te melden bij de AP.

Accountability

In hoofdstuk drie van dit onderzoeksrapport staat beschreven dat de AVG uitgaat van het ‘accountability principe’. Gelet hierop heeft de gemeente Best vanaf mei 2018 een register- en documentatieplicht. Op grond van de AVG is elke verwerkingsverantwoordelijke en verwerker vanaf mei 2018 verplicht een register bij te houden van alle verwerkingsactiviteiten die plaatsvinden binnen de organisatie (zie paragraaf 3.5. van dit onderzoeksrapport). De gemeente Best beschikt momenteel over een overzicht gegevensverwerkingen (zie bijlage 2). Dit overzicht kan als basis dienen voor het register dat op grond van de AVG opgesteld moeten worden. Het verdient de opmerking dat in het overzicht gegevensverwerkingen fouten kunnen zitten. Het overzicht gegevensverwerkingen is een paar jaar geleden gemaakt door Marion van Rooij en Adri van der Peet. Het overzicht gegevensverwerkingen is daarna een paar keer geüpdatet. Het kan zijn dat verwerkingen na verloop van tijd zijn aangepast en dat wijzigingen niet zijn doorgegeven aan de personen die het overzicht gegevensverwerkingen updaten. Zo worden bijvoorbeeld bij de behandeling van een aanvraag van een evenementenvergunning (zie paragraaf 4.3.2. van dit onderzoeksrapport) bijzondere persoonsgegevens verwerkt, terwijl dit niet staat in het overzicht gegevensverwerkingen.

Het is belangrijk dat het overzicht gegevensverwerkingen uitvoerig wordt gecontroleerd op fouten en dat deze fouten voor mei 2018 uit het overzicht worden gehaald.

Gelet op het ‘accountability principe’ is de gemeente Best op grond van de AVG voorts verplicht om PIA’s uit te voeren. Bepaalde gegevensverwerkingen die plaatsvinden binnen de gemeente Best (bijvoorbeeld de verwerking van persoonsgegevens in het kader van een BIBOB-toets) hebben namelijk een hoog privacyrisico. De gemeente Best heeft nog geen PIA’s uitgevoerd.

Privacy by Design en Privacy by Default

De beginselen van “Privacy by Design” en “Privacy by Default” (artikel 25 AVG) staan beschreven in paragraaf 3.2.3 van dit onderzoeksrapport. Op grond van het beginsel van Privacy by Design moet de gemeente Best al bij het ontwikkelen van informatiesystemen rekening houden met privacy en de bescherming van persoonsgegevens. Op grond van het beginsel van Privacy by Default moeten de standaardinstellingen van informatiesystemen (programma’s, websites, applicaties, e.d.) zo worden ingericht dat deze een zo klein mogelijke inbreuk op de privacy bewerkstelligen. In het digitaal aanvraagformulier voor een evenementenvergunning wordt gevraagd om een BSN-nummer van de aanvrager, terwijl de identiteit van de aanvrager door middel van DigiD al vastgesteld kan worden. Het vragen om het BSN-nummer is dan ook overbodig.

Functionaris voor de gegevensbescherming (FG)

In paragraaf 3.3. van dit onderzoeksrapport staat de FG uitgebreid beschreven. De gemeente Best heeft momenteel geen FG in dienst. De gemeente Best heeft budget vrijgemaakt om vanaf mei 2018 een FG in dienst te nemen. Het is raadzaam om de FG eerder dan mei 2018 in dienst te nemen, zodat de FG spoedig betrokken kan worden bij de voorbereidingen om de gemeente Best in mei 2018 “AVG-proof” te hebben.

Informatieplicht

Door de komst van de AVG wordt de informatieplicht van de gemeente Best uitgebreid (zie paragraaf 3.5 van dit onderzoeksrapport). De gemeente Best moet bij een gegevensverwerking aan de betrokkene o.a. aangeven wat het doel van de verwerking is, welke rechten de betrokkene heeft en hoelang de persoonsgegevens door de gemeente Best bewaard worden. Uit observatie is gebleken dat betrokkenen nauwelijks worden geïnformeerd over de gegevensverwerkingen die over hen plaatsvinden. De gemeente Best moet dan ook nadenken welke maatregelen genomen moeten worden om te voldoen aan de informatieplicht. In het laatste hoofdstuk (conclusies en aanbevelingen) wordt een aantal maatregelen aanbevolen die de gemeente Best kan nemen om in de toekomst te voldoen aan de informatieplicht.

Meldplicht datalekken

De gemeente Best heeft een werkinstructie voor het afhandelen van datalekken. De gemeente Best kan hierdoor snel handelen zodra zich een datalek voordoet. De gemeente Best houdt geen specifiek logboek bij van datalekken die hebben plaatsgevonden, maar registreert alle datalekken die hebben plaatsgevonden wel in het online portaal “TOPdesk”. De gemeente Best is hierdoor in staat om alle datalekken die hebben plaatsgevonden snel te raadplegen.

Gegevensbeschermingsbeleid

De gemeente Best is op grond van de AVG verplicht een gegevensbeschermingsbeleid op te stellen met maatregelen die laten zien dat de gemeente Best de AVG naleeft.²⁰⁰ De

²⁰⁰ Artikel 24 lid 2 AVG.

gemeente Best heeft onlangs een privacybeleid ontwikkeld die reeds is vastgesteld door het managementteam van de gemeente Best. Het privacybeleid moet nog worden vastgesteld door het college van burgemeester en wethouders van de gemeente Best en wordt daarom niet als bijlage toegevoegd. Voorts hanteert de gemeente Best een informatiebeveiligingsbeleid (zie paragraaf 4.4. van dit onderzoeksrapport). Gelet op het voorgaande voldoet de gemeente Best aan de verplichting om een gegevensbeschermingsbeleid op te stellen.

§ 5.2 Privacyreglement

In deze paragraaf wordt het Privacyreglement gemeente Best (zie bijlage 7) beschreven. Dit is een besluit van het college van burgemeester en wethouders van de gemeente Best (het college) van 25 april 2005. Het besluit is op 1 mei 2005 in werking getreden en is het gevolg van de Wbp en artikel 4 van de Verordening verwerking persoonsgegevens gemeente Best. De Verordening verwerking persoonsgegevens gemeente Best is bij besluit van 22 februari 2010 vervangen door de Verordening Gemeentelijke Basisregistratie Het Privacyreglement gemeente Best is nooit ingetrokken.

Hieronder staat per paragraaf beschreven of het Privacyreglement gemeente Best voldoet aan de huidige Wbp en de aanstaande AVG.

In paragraaf 1 Privacyreglement gemeente Best staan de algemene bepalingen van het Privacyreglement gemeente Best. Hierbij kunnen de volgende opmerkingen worden geplaatst:

- In artikel 1 Privacyreglement gemeente Best staan begrippen gedefinieerd. De begrippen die staan in het Privacyreglement gemeente Best zijn gelet op de Wbp juist gedefinieerd. Gelet op de AVG moeten de begrippen “bewerker” en “verantwoordelijke” opnieuw worden gedefinieerd. In de AVG worden deze begrippen vervangen door “verwerkingsverantwoordelijke” en “verwerker”. Het begrip “toestemming” staat niet gedefinieerd in artikel 1 Privacyreglement gemeente Best, maar wordt in het Privacyreglement gemeente Best wel gebruikt. Het verdient de opmerking dat het begrip “toestemming” in de AVG anders staat gedefinieerd als in de Wbp.
- In een aantal artikelen uit deze paragraaf (bijvoorbeeld artikel 2 en artikel 3 Privacyreglement gemeente Best) wordt verwezen naar bijlagen. Het verdient de opmerking dat de bijlagen bij het Privacyreglement gemeente Best verouderd zijn. De gemeente Best heeft sinds een aantal jaren een overzicht gegevensverwerkingen (zie bijlage 2). Aan de hand van dit overzicht kunnen de bijlagen geactualiseerd worden.
- In artikel 3 lid 3 Privacyreglement gemeente Best wordt verwezen naar de Verordening verwerking persoonsgegevens gemeente Best. Deze verordening is ingetrokken. Artikel 3 Privacyreglement gemeente Best verwijst dan ook naar een verordening die is ingetrokken.
- In artikel 3 lid 1 Privacyreglement gemeente Best staat dat de manager van een betreffende cluster beheerder is van de gemeentelijke persoonsverwerkingen op diens cluster. Het verdient de opmerking dat de gemeente Best niet meer werkt met clusters, maar met afdeling. Om verwarringen te voorkomen is het raadzaam om dit aan te passen.

Paragraaf 2 Privacyreglement gemeente Best gaat over doelbinding. Bij paragraaf 2 Privacyreglement gemeente Best kunnen de volgende opmerkingen worden geplaatst:

- In artikel 5 worden de rechtmatige grondslagen voor de verwerkingen beschreven. De rechtmatige grondslagen zijn volgens artikel 5 Privacyreglement gemeente Best:
 - *de goede vervulling van een publiekrechtelijke taak;*
 - *de wettelijke verplichting van de verantwoordelijke;*
 - *de uitvoering van met derden gesloten overeenkomsten;*

- de ondubbelzinnige toestemming van de betrokkene;
- de vrijwaring van een vitaal belang van betrokkene en
- de behartiging van het gerechtvaardigde belang van de verantwoordelijke of een derde aan wie de gegevens worden verstrekt.

Het verdient de opmerking dat in de AVG staat dat de grondslag “de behartiging van het gerechtvaardigde belang van de verantwoordelijke of een derde aan wie de gegevens worden verstrekt” niet geldt voor overheidsinstanties. Dit wordt ook bevestigd in de memorie van toelichting van de Uitvoeringswet Algemene verordening gegevensbescherming.

- In een aantal artikelen uit deze paragraaf (bijvoorbeeld artikel 6 en artikel 7 Privacyreglement gemeente Best) wordt verwezen naar bijlagen. Het verdient de opmerking dat de bijlagen bij het Privacyreglement gemeente Best verouderd zijn. De gemeente Best heeft sinds een aantal jaren een overzicht gegevensverwerkingen (zie bijlage 2). Aan de hand van dit overzicht kunnen de bijlagen geactualiseerd worden.

Bij paragraaf 3 Privacyreglement gemeente Best (rechtstreekse toegang tot en verstrekking van persoonsgegevens) kan de volgende opmerking worden geplaatst:

- In het tweede lid van artikel 12 Privacyreglement gemeente Best staat dat persoonsgegevens verwerkt mogen worden wanneer dat noodzakelijk is om een wettelijke verplichting na te komen waaraan de verantwoordelijke is onderworpen of indien de verwerking geschiedt met de ondubbelzinnige toestemming van de betrokkene. Het verdient de opmerking dat persoonsgegevens niet alleen verwerkt kunnen worden wanneer dat noodzakelijk is om een wettelijke verplichting na te komen of met ondubbelzinnige toestemming van de betrokkene. Persoonsgegevens mogen op grond van de Wbp en de AVG bijvoorbeeld ook verwerkt worden voor de goede vervulling van een publiekrechtelijke taak of voor de vrijwaring van een vitaal belang van de betrokkene (zie ook paragraaf 2.1.3 en 3.2.1 van dit onderzoeksrapport).

In paragraaf 4 Privacyreglement gemeente Best staan de plichten van de verantwoordelijke, beheerder en bewerker beschreven. Hierbij kan de volgende opmerking worden geplaatst:

- In artikel 16 Privacyreglement gemeente Best staat de informatieplicht beschreven. Artikel 16 Privacyreglement gemeente Best voldoet aan de Wbp, maar niet aan de AVG. Door de komst van de AVG wordt de informatieplicht van de gemeente Best namelijk uitgebreid (zie paragraaf 3.5 van dit onderzoeksrapport). De gemeente Best moet artikel 16 Privacyreglement, gelet op de uitbreiding van de informatieplicht, aanpassen.

In paragraaf 5 Privacyreglement gemeente Best staan de rechten van de betrokkene beschreven. Hierbij kunnen de volgende opmerkingen worden geplaatst:

- Het recht op beperking en het recht op dataportabiliteit (nieuwe rechten op grond van de AVG) staan niet beschreven in paragraaf 5 Privacyreglement gemeente Best (zie paragrafen 3.4.4 en 3.4.5 van dit onderzoeksrapport). Het is raadzaam om het recht op beperking en het recht op dataportabiliteit in deze paragraaf op te nemen.
- In artikel 17 lid 3 Privacyreglement gemeente Best staat dat de gemeente Best een FG in dienst heeft met een toezichthoudende functie. Dit is onjuist. De gemeente Best heeft momenteel geen FG in dienst die een toezichthoudende rol heeft. Marion van Rooij (privacyfunctionaris gemeente Best) houdt zich wel bezig met taken die normaal gesproken door een FG worden uitgevoerd, maar toezicht houden doet zij niet.
- In artikel 20 Privacyreglement gemeente Best wordt het recht op correctie (verbetering, aanvulling, verwijdering en/of afscherming) beschreven. Het recht op vergetelheid lijkt op het recht op verwijdering, maar is niet hetzelfde (zie paragraaf 3.4.3 en 3.5 van dit onderzoeksrapport). Het recht op vergetelheid staat in de AVG als een afzonderlijk recht beschreven. Het is dan ook raadzaam om het recht op vergetelheid in het Privacyreglement gemeente Best in een apart artikel op te nemen.

In paragraaf 6 Privacyreglement gemeente Best staat de rechtsbescherming en toezicht beschreven. Hierbij kan de volgende opmerking worden geplaatst:

- In artikel 22 Privacyreglement gemeente Best staat dat de verwerkingen worden gemeld bij de FG. In artikel 24 Privacyreglement staat dat de FG op grond van de Wbp bevoegd is toe te zien op de naleving van het Privacyreglement gemeente Best. Echter heeft de gemeente Best momenteel geen FG in dienst. Dit is ook de reden waarom de gemeente Best bepaalde gegevensverwerkingen heeft gemeld bij de AP (zie paragraaf 5.1 van dit onderzoeksrapport).

HOOFDSTUK 6: CONCLUSIES & AANBEVELINGEN

In dit hoofdstuk staan de conclusies en aanbevelingen beschreven. Het onderhavige hoofdstuk geeft antwoord op de centrale vraag: *“Welke aanbevelingen kunnen gedaan worden om de huidige werkwijze met betrekking tot de verwerking van persoonsgegevens en het Privacyreglement gemeente Best zo aan te passen dat de werkwijze en het privacyreglement juridisch juist zijn gelet op de recente wijzigingen van de Wbp en de aanstaande AVG?”*.

§ 6.1 Awareness

De volgende aanbevelingen kunnen gedaan worden voor wat betreft het privacy/ -beveiligingsbewustzijn van de medewerkers van de gemeente Best.

Conclusie(s)

De medewerkers van de gemeente Best die zich bezighouden met informatiebeveiliging doen er veel aan om het beveiligingsbewustzijn van de medewerkers van de gemeente Best te verhogen. Er worden regelmatig berichten over het beveiligen van persoonsgegevens verspreid via Intrabest en de informatieschermen die staan in diverse servicecorners. Voorts geven de personen die zich bezighouden met de gegevensverwerkingen die plaatsvinden binnen de gemeente Best regelmatig cursussen/informatiesessies op het gebied van privacy/ -beveiligingsbewustzijn aan de medewerkers van de gemeente Best. Tijdens de cursussen/informatiesessies krijgen de medewerkers van de gemeente Best tips over het beveiligen van (gevoelige) persoonsgegevens. Echter blijven veel medewerkers van de gemeente Best zich onvoldoende bewust van de risico's die ze lopen op het gebied van informatiebeveiliging. Uit observatie is gebleken dat medewerkers van de gemeente Best bij het verlaten van hun werkplekken hun computers aanlaten zonder deze te vergrendelen. Hierdoor is de kans aanwezig dat personen (bijvoorbeeld schoonmaakpersoneel of bezoekers) gegevens onbevoegd inzien. Verder heeft de gemeente Best onlangs een “phishingtest” laten uitvoeren. Hieruit kwam naar voren dat een derde van de groep medewerkers naar wie een phishingmail werd verzonden op de link in de phishingmail heeft geklikt. Hieruit kan de conclusie worden getrokken dat een grote groep medewerkers van de gemeente Best het lastig vindt om legitieme e-mails te onderscheiden van “phishingmails”.

Aanbeveling(en)

Daar waar veel medewerkers van de gemeente Best zich onvoldoende bewust zijn van de risico's die ze lopen op het gebied van informatiebeveiliging wordt aanbevolen actief door te gaan met het verhogen van het beveiligingsbewustzijn van de medewerkers van de gemeente Best. Dit kan de gemeente Best bijvoorbeeld doen door organisatiebrede cursussen op het gebied van privacy/ -beveiligingsbewustzijn te geven aan hun medewerkers. Om te illustreren hoe belangrijk het is om zorgvuldig om te gaan met persoonsgegevens, wordt aanbevolen de nieuwe cijfers van de AP waaruit blijkt dat het aantal meldingen van datalekken door gemeenten fors is toegenomen (331 incidenten in het eerste kwartaal van 2017, tegen 533 incidenten in het gehele jaar 2016) op Intrabest te plaatsen.

§ 6.2 Functionaris voor de gegevensbescherming (FG)

De volgende aanbevelingen kunnen gedaan worden voor wat betreft de FG.

Conclusie(s)

De gemeente Best is vanaf mei 2018 verplicht een FG aan te stellen. De FG heeft samengevat een tweedelige kerntaak, namelijk enerzijds het informeren en adviseren van de verwerkingsverantwoordelijke of verwerker en anderzijds toezien op de naleving van de AVG (zie voor een compleet overzicht van de taken paragraaf 3.3.2 van dit onderzoeksrapport). De FG moet snel in contact kunnen komen met de verwerkingsverantwoordelijke (het college van burgemeester en wethouders of de burgemeester). Dit is belangrijk gelet op de kerntaken (informeren, adviseren en toezicht houden) die de FG heeft.

De gemeente Best heeft momenteel geen FG in dienst. Marion van Rooij is privacyfunctionaris, maar houdt zich niet bezig met een toezichthoudende rol (een belangrijke taak van de FG). Marion van Rooij is ook niet aangemeld als FG bij de AP. De gemeente Best heeft momenteel niemand in dienst die de ambitie heeft om FG te worden. De gemeente Best moet hierdoor op zoek naar iemand buiten de organisatie. De gemeente Best heeft onlangs budget vrijgemaakt om vanaf mei 2018 een FG aan te stellen.

Aanbeveling(en)

Aanbevolen wordt om eerder dan mei 2018 een FG in dienst te nemen. Indien de FG een paar maanden eerder wordt aangenomen kan de FG 'feeling' krijgen met de organisatie en betrokken worden bij de voorbereidingen om de gemeente Best "AVG-proof" te maken. Gelet op het feit dat de FG snel in contact moet kunnen komen met de verwerkingsverantwoordelijke (het college van burgemeester en wethouders of de burgemeester) wordt aanbevolen om een stafafdeling onder de directie te creëren. De FG kan dan op deze afdeling worden geplaatst waardoor de FG een kort lijntje heeft met de afdelingsmanagers (medeverwerkingsverantwoordelijken) en het college van burgemeester en wethouders of de burgemeester (verwerkingsverantwoordelijke). Indien het niet mogelijk blijkt een stafafdeling te creëren wordt aanbevolen om de FG te plaatsen op de afdeling Intern Advies (vakgroep Juridische Zaken). Indien de FG op de vakgroep Juridische Zaken wordt geplaatst, kan de FG – bij twijfel over wet- en regelgeving omtrent privacy en gegevensverwerking – direct sparren met andere juristen (bijvoorbeeld met Marion van Rooij).

§ 6.3 Register- en documentatieplicht

De volgende aanbevelingen kunnen gedaan worden voor wat betreft de register- en documentatieplicht.

Conclusie(s)

Vanaf mei 2018 heeft de gemeente Best een register- en documentatieplicht. De gemeente Best moet op grond van de AVG alle gegevensverwerkingen die plaatsvinden binnen de gemeente Best registreren in een overzicht. In het overzicht moeten de gegevens over de verantwoordelijke, de verwerkingsdoeleinden, de categorieën van persoonsgegevens die worden verwerkt, de bewaartermijnen en de ontvangers van de persoonsgegevens worden geregistreerd. Voorts moet in het overzicht een beschrijving van de genomen technische en organisatorische maatregelen worden geregistreerd. De gemeente Best heeft momenteel al een overzicht waarin alle gegevensverwerkingen die plaatsvinden binnen de gemeente Best staan (zie bijlage 2). Dit overzicht is een aantal jaren geleden gemaakt. In het overzicht gegevensverwerkingen staan fouten die eruit gehaald moeten worden (bijvoorbeeld: in het overzicht gegevensverwerkingen wordt bij de verwerking "APV vergunningen en ontheffingen" niet gemeld dat er BSN-nummers verwerkt worden, terwijl dit wel gebeurt."

Aanbeveling(en)

Daar waar onvoldoende tijd beschikbaar was om tijdens het onderzoek ruim 100 gegevensverwerkingen te analyseren wordt aanbevolen alle gegevensverwerkingen uit het overzicht gegevensverwerkingen te controleren op fouten. Dit kan de gemeente Best het beste doen door alle contactpersonen die staan in het overzicht gegevensverwerkingen te benaderen met de vraag of de gegevens die bij een bepaalde gegevensverwerking staan (doel, betrokkenen, ontvangers, grondslag, etc.) juist zijn. Verder wordt aanbevolen om bij elke gegevensverwerking neer te zetten wie de verwerkingsverantwoordelijke is (de burgemeester of het college van burgemeester en wethouders). Voorts wordt aanbevolen om in het overzicht een beschrijving te zetten van de genomen technische en organisatorische maatregelen.

§ 6.4 Privacy impact analyse (PIA)

De volgende aanbevelingen kunnen gedaan worden voor wat betreft de PIA's.

Conclusie(s)

Uit het onderzoek is gebleken dat bepaalde gegevensverwerkingen die plaatsvinden binnen de gemeente Best een hoog privacyrisico opleveren (bij bepaalde gegevensverwerkingen worden op grote schaal bijzondere persoonsgegevens verwerkt). Op grond van de AVG is de gemeente Best dan ook verplicht om PIA's uit te voeren. Een PIA brengt de privacyrisico's van een bepaalde gegevensverwerking in kaart.

Aanbeveling(en)

Aanbevolen wordt om in kaart te brengen voor welke gegevensverwerkingen een PIA uitgevoerd moet worden en daar een prioritering aan te koppelen op grond van het privacyrisico. Aanbevolen wordt om zo snel mogelijk te starten met het uitvoeren van de PIA's. Daarbij wordt opgemerkt dat het verstandig is te starten met de gegevensverwerkingen die een hoog privacyrisico hebben.

§ 6.5 Meldplicht datalekken

De volgende aanbevelingen kunnen gedaan worden voor wat betreft de meldplicht datalekken.

Conclusie(s)

Sinds 2016 is de Wmd van kracht. De gemeente Best heeft sinds 2016 vijf datalekken gehad. De gemeente Best heeft drie datalekken gemeld bij de AP. Bij twee van de vijf datalekken was namelijk geen sprake van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens van de betrokkene. De gemeente Best heeft een werkwijze waarin staat hoe datalekken afgehandeld moeten worden. Hierdoor is de gemeente Best in staat snel te handelen zodra zich een datalek voordoet. De gemeente Best houdt geen specifiek logboek bij waarin de datalekken die hebben plaatsgevonden worden geregistreerd, maar registreert alle datalekken wel in het online portaal "TOPdesk". Hierdoor kan de gemeente Best snel zien welke datalekken hebben plaatsgevonden. De gemeente Best heeft voorts nog geen waarschuwing of boete ontvangen van de AP.

Aanbeveling(en)

Aanbevolen wordt om de datalekken (naast de meldingen die gedaan worden in het online portaal "TOPdesk") te registreren in een logboek. Indien de AP verzoekt om een overzicht van alle datalekken die hebben plaatsgevonden is de gemeente Best door het overleggen van het logboek in staat om snel aan het verzoek van de AP te voldoen. Aanbevolen wordt om toekomstige datalekken (waarbij sprake is van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens) binnen 72 uur te melden.

bij de AP. Indien wordt getwijfeld of een datalek wel of niet gemeld moet worden bij de AP wordt aanbevolen het datalek toch te melden. Indien later blijkt dat melden niet nodig was, kan de gemeente Best de melding eenvoudig intrekken.

§ 6.6 Informatieplicht

De volgende aanbevelingen kunnen gedaan worden voor wat betreft de informatieplicht.

Conclusie(s)

De informatieplicht wordt door de komst van de AVG fors uitgebreid. Naast de identiteit van de verantwoordelijke en de doeleinden van de verwerking, is de gemeente Best door de komst van de AVG ook verplicht de contactgegevens van de FG, de rechtsgrond van de verwerking, de bewaartermijn van de gegevens en de rechten van de betrokkene mede te delen aan de betrokkene. De gemeente Best is door de komst van de AVG voorts verplicht om aan de betrokkene te melden dat een eventueel gegeven toestemming kan worden ingetrokken, dat een klacht kan worden ingediend bij de toezichthouder, of de verstrekking van de gegevens verplicht is en wat de gevolgen zijn als de gegevens niet worden verstrekt en wat de kern van de taak-/rolverdeling is indien meerdere partijen gezamenlijk verantwoordelijk zijn voor een verwerking. Uit observatie is gebleken dat betrokkenen nauwelijks geïnformeerd worden. Op de website van de gemeente Best, aanvraagformulieren (voor bijvoorbeeld vergunningen, subsidies of uitkeringen) en ontvangstbevestigingen van brieven of e-mails die de gemeente Best ontvangt staat vrijwel geen informatie over hoe de gemeente Best persoonsgegevens verwerkt.

Aanbeveling(en)

Aanbevolen wordt om bij elke gegevensverwerking uit het overzicht gegevensverwerkingen te inventariseren hoe betrokkenen het beste geïnformeerd kunnen worden. Om te voldoen aan de informatieplicht op grond van de AVG kan de gemeente Best er bijvoorbeeld voor kiezen om bij het aanvraagformulier van een vergunning, subsidie of uitkering een bijlage te voegen waarin informatie over de gegevensverwerking staat. Voorts kan de gemeente Best ervoor kiezen om in hun ontvangstbevestiging van een brief of e-mail te verwijzen naar een pagina op de website van de gemeente Best waarop algemene informatie (bijvoorbeeld de contactgegevens van de FG en de rechten van de betrokkenen) over gegevensverwerkingen te vinden is.

§ 6.7 Privacy by Design & Privacy by Default

De volgende aanbevelingen kunnen gedaan worden voor wat betreft de beginselen van Privacy by Design en Privacy by Default.

Conclusie(s)

Op grond van deze beginselen moet de gemeente Best al bij het ontwikkelen van informatiesystemen rekening houden met privacy en de bescherming van persoonsgegevens (Privacy by Design) en moeten de standaardinstellingen van informatiesystemen (programma's, websites, applicaties, e.d.) zo worden ingericht dat deze een zo klein mogelijke inbreuk op de privacy bewerkstelligen (Privacy by Default). In het digitaal aanvraagformulier voor een evenementenvergunning wordt gevraagd om een BSN-nummer van de aanvrager, terwijl de identiteit van de aanvrager door middel van DigiD al vastgesteld wordt. Gelet hierop wordt niet voldaan aan het beginsel "Privacy by Default".

Aanbeveling(en)

Aanbevolen wordt om de medewerkers van de gemeente Best die zich bezighouden met het ontwikkelen van programma's, websites en applicaties door middel van het houden van een vergadering op de hoogte te brengen van het beginsel van Privacy by Design. Op die manier kunnen deze medewerkers al bij het ontwikkelen van systemen rekening houden

met de privacy van de betrokkenen en de bescherming van persoonsgegevens. Voorts wordt aanbevolen om te controleren of geen onnodige persoonsgegevens (bijvoorbeeld BSN-nummers) gevraagd worden in standaard (aanvraag)formulieren die klanten/cliënten van de gemeente Best moeten invullen.

§ 6.8 Privacyreglement gemeente Best

De volgende aanbevelingen kunnen gedaan worden voor wat betreft het Privacyreglement gemeente Best.

Conclusie(s)

Het Privacyreglement gemeente Best voldoet in grote lijnen aan de Wbp, maar niet aan de AVG. Er staat in het Privacyreglement niks over de meldplicht datalekken, terwijl de meldplicht datalekken sinds 2016 een belangrijke nieuwe verplichting is voor de gemeente Best. Voorts moet het Privacyreglement gemeente Best worden aangepast gelet op de informatieplicht die door de komst van de AVG wordt uitgebreid. In het Privacyreglement gemeente Best staat dat de gemeente Best een FG in dienst heeft, terwijl dit niet het geval is. Het recht op beperking, het recht op dataportabiliteit en het recht op vergetelheid staan niet beschreven in het Privacyreglement gemeente Best, terwijl dit op grond van de AVG nieuwe rechten van betrokkenen zijn. Verder verwijst het Privacyreglement gemeente Best naar een verordening die is ingetrokken en zijn de bijlagen bij het Privacyreglement gemeente Best verouderd.

Aanbeveling(en)

Uit het onderzoek is gebleken dat het Privacyreglement gemeente Best toe is aan vernieuwing. Aanbevolen wordt om het huidige privacyreglement in te trekken en – met het oog op de opmerkingen over het Privacyreglement gemeente Best in paragraaf 5.2 van dit onderzoeksrapport en de aanstaande AVG – een nieuw privacyreglement op te stellen (zie bijlage 8 voor een voorzet).

BRONNENLIJST

Boeken

Berkvens & Prins 2007

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

Duthler & Biesheuvel 2013

A.W. Duthler & A.J. Biesheuvel, *Het Europees Privacyrecht in beweging*, Deventer: Kluwer 2013.

Kranenburg & Verhey 2011

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

Van Schaaijk 2015

G.A.F.M. van Schaaijk, *Praktijkgericht juridisch onderzoek*, Den Haag: Boom Juridische Uitgevers 2015.

Handleidingen / Handboeken

König & Karssenberg 2015

König & Karssenberg, 'Privacy Impact Assessment (PIA); introductie, handreiking en vragenlijst', Amsterdam: NOREA 2015.

Sauerwein & Linnemann 2002

L.B. Sauerwein & J.J. Linnemann, 'Handleiding voor verwerkers van Persoonsgegevens (Wet bescherming persoonsgegevens)', Den Haag: Ministerie van Justitie 2002.

Tijdschriften / Blogs (digitaal)

Arts 2017

C. Arts, 'Het accountability principe onder de Algemene Verordening Gegevensbescherming', 23 augustus 2016 (*geraadpleegd op 12 april 2017 via www.considerati.com*).

Bloemen-Patberg, ELSA Magazine 2012

L.A. Bloemen-Patberg, 'Oei een lek bijvoorbeeld door een hack', Leiden: ELSA Magazine 2012, afl. 1.

Jansen 2017

M. Jansen, 'De privacy-paradox: steeds meer informatie verstrekken, maar wel zo compact en simpel mogelijk alstublieft' (*geraadpleegd op 20 april 2017 via www.dirkzwagerieit.nl*).

IT-jurist bv 2017

De IT-jurist bv, 'Het recht op overdraagbaarheid van gegevens', 20 februari 2017 (*geraadpleegd op 10 april 2017 via www.it-jurist.nl*).

Wiegerinck 2017

S.R. Wiegerinck, 'Blogserie Europese privacyverordening, aflevering 3: privacy by design, privacy by default, beveiliging en inbreuken hierop' (*geraadpleegd op 20 maart 2017 via www.banning.nl*).

Zwenne & Mommers, *Tijdschrift voor Compliance* 2016, p. 182-189.

G-J. Zwenne & L. Mommers, 'De tien belangrijkste veranderingen die de algemene verordening gegevensbescherming gaat brengen (in minder dan vijfduizend woorden)', *Tijdschrift voor Compliance*, 2016/4, p. 182-189.

Zwenne & Webbink, *Privacy & Informatie* 2006

G-J. Zwenne & J. Webbink, 'De winstverdubbelaar en de Wbp: over de reikwijdte en inhoud van het kennisnemingsrecht van artikel 35', *Privacy & Informatie* 2006/1.

Parlementaire stukken

Kamerstukken II 1997/98, 25892, 3 (MvT).

Jurisprudentie

Hof Amsterdam 10 november 2005, ECLI:NL:GHAMS:2005:AU8223.
HvJ EU 17 juli 2014, C-141/12 en C-372/12 (Y.S. en M. en S.).

Krantenartikelen

L. Lonkhuyzen, 'Datalekken bij gemeenten; 'het is een beetje een zootje' *NRC* 27 januari 2017.

Elektronische bronnen

www.autoriteitpersoonsgegevens.nl
www.banning.nl
www.considerati.com
www.digid.nl
www.dirkzwagerieit.nl
www.europadecentraal.nl
www.gemeentebest.nl
www.ibdgemeenten.nl
www.it-jurist.nl
www.rijksoverheid.nl
www.roxit.nl