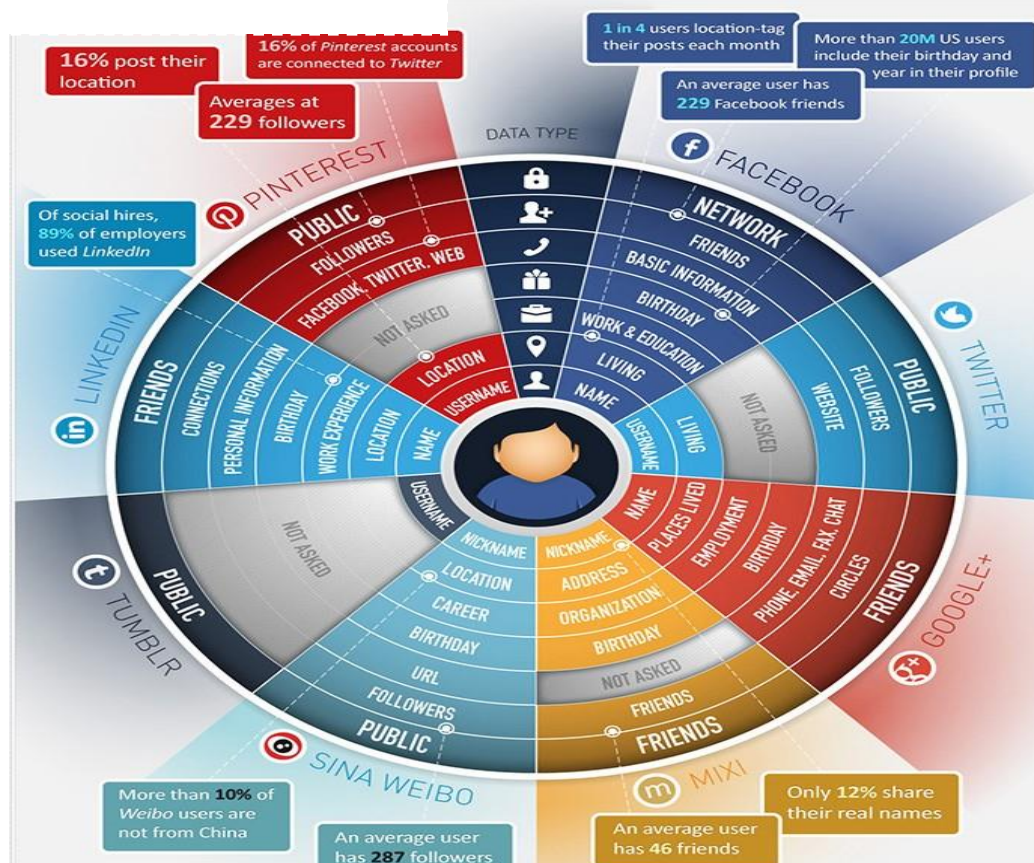


Een FYN persoonlijkheidsprofiel

*Een onderzoeksrapport voor FYN Software
over het gebruik van persoonsgegevens voor
profilering*



Kristina Samardzic

In opdracht van FYN Software

Oss, mei 2017

Een FYN persoonlijkheidsprofiel

*Een onderzoeksrapport voor FYN Software
over het gebruik van persoonsgegevens voor
profilering*

Student: Kristina Samardzic

Studentnummer: 2081413

Onderwijsinstelling: Juridische Hogeschool Avans-Fontys

Locatie: Tilburg

Afstudeerperiode: E3-E4 2016/2017

Afstudeerorganisatie: FYN Software

Afstudeermentor: dhr. E. Sanderse

Eerste afstudeerdocent: mw. C. van der Voort

Tweede afstudeerdocent: dhr. M. Kooij

Voorwoord

Geachte lezer,

Allereerst dank ik u met groot genoegen voor uw interesse in dit onderzoeksrapport en voor de tijd die u hierin steekt. Dit rapport heb ik opgesteld in de periode van februari 2017 tot en met mei 2017 in het kader van mijn afstuderen aan de opleiding HBO-Rechten van de Juridische Hogeschool Avans-Fontys te Tilburg.

Privacy is tegenwoordig een hot item. Na verschillende wijzigingen en aankondigingen van wetten en verdragen, en media-aandacht voor datalekken en privacyissues, wilde ik een afstudeeronderzoek doen naar een juridisch vraagstuk dat privacy gerelateerd is. Met veel plezier heb ik dan ook de afgelopen maanden aan dit rapport gewerkt.

Graag wil ik mijn dank en waardering uitspreken naar iedereen die mij heeft ondersteund tijdens dit onderzoeksproces. Allereerst wil ik de heer Edwin Sanderse, afstudeermentor, bedanken voor de tijd en energie die hij heeft gestoken in de begeleiding en ondersteuning op mijn stageplek. Ook bedank ik de heer Michiel Hazelhof, ICT-deskundige bij FYN Software, voor de tijd die hij heeft vrijgemaakt om het omnichannelsysteem uit te leggen. Als laatste bedank ik mevrouw Caro van der Voort, eerste afstudeerdocent, en de heer Mark Kooij, tweede afstudeerdocent, voor hun feedback en ondersteuning gedurende deze maanden.

Ik wens u veel leesplezier toe!

Kristina Samardzic

Oss, mei 2017

Inhoudsopgave

Voorwoord.....	
Samenvatting	
Lijst van afkortingen.....	
Hoofdstuk 1 Inleiding	8
1.1 Probleembeschrijving	8
1.2 Centrale vraag.....	9
1.3 Doelstelling	9
1.4 Deelvragen	10
1.5 Methoden, bronnen en verantwoording	10
1.6 Onderzoeksstrategie	11
1.7 Leeswijzer	11
Hoofdstuk 2 Juridisch kader	12
Inleiding.....	12
2.1 Wet bescherming persoonsgegevens	12
2.1.1 Toepassing Wet bescherming persoonsgegevens	12
2.1.1.1 Persoonsgegevens	12
2.1.1.2 Verwerken	13
2.1.1.3 Bestand	13
2.1.2 Rechtmatige gegevensverwerking	14
2.1.2.1 Zorgvuldigheidseis	14
2.1.2.2 Doeleinden	14
2.1.2.3 Rechtvaardigingsgronden	14
2.1.2.4 Doelbinding.....	15
2.1.2.5 Kwaliteit waarborgen	16
2.1.2.6 Beveiliging	16
2.1.2.7 Bewaartermijn.....	16
2.1.3 De actoren	16
2.1.3.1 Verantwoordelijke	16
2.1.3.2 Bewerker	17
2.1.3.3 Betrokkene	18
Het recht op kennisneming.....	18
Het recht van correctie	19
Het recht van verzet	19
Vrijwaring van geautomatiseerde, individuele besluitvorming	19
2.2 Algemene Verordening Gegevensbescherming	19
2.2.1 Rechtmatige gegevensverwerking onder de AVG	20
2.2.1.1 Transparantiebeginsel	20
2.2.1.2 Toestemming	20
2.2.1.3 Opslagbeperking	21
2.2.1.4 Nieuwe beveiligingsmaatregelen	21
2.2.2 De nieuwe rechten en plichten	22
2.2.2.1 Verwerkingsverantwoordelijke en verwerker	22
Registratieplicht	22
Privacy by design	22

Privacy by default.....	22
Privacy Impact Assessment	22
Uitgebreidere informatieplicht.....	24
Functionaris Gegevensbescherming	24
2.2.2.2 Nieuwe rechten van de betrokkene.....	25
Het recht op vergetelheid	25
Het recht van dataportabiliteit.....	25
2.3 Telecommunicatiewet.....	26
2.3.1 Tracking cookies.....	26
2.3.1.1 Tracking cookies: informatieplicht	26
2.3.1.2 Tracking cookies: toestemming.....	26
Hoofdstuk 3 De werkwijze van FYN.....	28
Inleiding.....	28
3.1 FYN dienstverlening.....	28
3.2 Omnichannelsysteem	29
3.2.1 Één database	29
3.2.2 Online dienstverlening	29
3.3 FYNE gegevensverwerking.....	30
3.3.1 Programma's voor de gegevensverwerking	30
3.3.2 Wijze van verzamelen.....	31
3.3.3 Huidige gegevensverwerking door FYN.....	32
3.3.4 Toekomstig gegevensverwerkingsproces: profilering.....	33
3.3.4.1 Verzamelen en verstrekken van persoonsgegevens	33
3.3.4.2 Algoritmes instellen	34
3.3.4.3 Anonimiseren en verwijderen van persoonlijkheidsprofielen.....	35
Hoofdstuk 4 De wet versus de praktijk.....	37
Inleiding.....	37
4.1 Toepasbaarheid juridisch kader	37
4.1.1 Soorten persoonsgegevens.....	37
4.1.2 Soorten verwerkingshandelingen.....	38
4.2 FYN: bewerker of verantwoordelijke?	39
4.3 FYNE profilering.....	39
4.3.1 Verstrekken van persoonsgegevens aan FYN	40
4.3.1.1 Verstrekking persoonsgegevens: verenigbaarheid	40
4.3.1.2 Verstrekking persoonsgegevens: rechtvaardigingsgrond.....	41
4.3.2 Rechtmatig profileren.....	42
4.3.2.1 Profilering: doel en grondslag	42
4.3.2.2 Alleen een kwalitatieve profilering.....	43
4.3.3 Marketing en profilering.....	44
Hoofdstuk 5 Conclusies en aanbevelingen.....	46
5.1 Conclusies en aanbevelingen Wbp en AVG.....	46
5.1.1 FYN als bewerker: conclusie	46
5.1.2 FYN als bewerker: aanbeveling	47
5.1.3 FYN als verantwoordelijke: conclusie	47
5.1.4 FYN als verantwoordelijke: aanbevelingen	47

Doeleinden formuleren	47
Rechtvaardigingsgrond voor het profileren	47
Bewaartermijn	47
Overeenkomst gegevensverstrekking	48
Profileren registreren.....	48
Beveiliging: privacy by design	48
PIA voorafgaand aan het profileren.....	49
Een Functionaris Gegevensbescherming benoemen	49
Mogelijkheid tot dataportabiliteit	49
5.2 Conclusies en aanbevelingen Tw.....	49
5.2.1 Cookies: conclusie.....	50
5.2.2 Cookies: aanbeveling	50
Literatuurlijst.....	51
Overige bronnen	52

Samenvatting

FYN Software is een IT-bedrijf. De kernactiviteit van FYN is het ontwikkelen van kassasoftware en -hardware voor retailers. Het belangrijkste product van FYN is het POS-softwareprogramma dat functioneert op basis van het omnichannelsysteem. Door middel van het omnichannelsysteem verzamelt de retailer klantgegevens van zijn klanten, de consumenten, via verschillende kanalen.

Uit het juridisch onderzoek is gebleken dat de verantwoordelijke de persoon is die de doeleinden formuleert en de middelen voor de gegevensverwerking aanwijst. De bewerker handelt conform de instructies van de verantwoordelijke en heeft geen inspraak bij het formuleren van de doeleinden en het aanwijzen van de middelen. Op basis van de huidige situatie is FYN aan te merken als bewerker en de retailer als verantwoordelijke. De retailer is immers degene die de persoonsgegevens verzamelt en de doeleinden formuleert. De retailers hebben twee doeleinden geformuleerd voor de gegevensverwerking: direct marketing en efficiëntie. FYN verwerkt de gegevens alleen op verzoek van en onder de instructies van de retailers.

FYN wil in de toekomst overgaan tot profileren. Door het opstellen van persoonlijkheidsprofielen kan FYN deze profielen omzetten in statistieken en deze tegen een vergoeding aan de leveranciers van de retailers verstrekken. De leverancier kan hierop zijn marketingstrategie aanpassen. Het is namelijk de bedoeling dat FYN namens de leverancier gerichte aanbiedingen stuurt aan de klanten van de retailers. Deze direct marketing zal wel geschieden in overleg met de retailer en uit diens naam en vanuit diens mailserver. De retailers zullen de persoonsgegevens van hun klanten hiertoe aan FYN verstrekken. Nu FYN de gegevens gaat verwerken voor andere doeleinden, zal FYN aangemerkt worden als een verantwoordelijke.

FYN zal voortaan als verantwoordelijke gehouden zijn om te voldoen aan de eisen die de wet stelt aan een rechtmatige gegevensverwerking. FYN zal het profileren als doeleinde moeten formuleren. Daarnaast moet FYN een programma ontwikkelen dat in staat is om de database te zijner tijd op te schonen. Op dit moment worden de gegevens immers oneindig in het systeem bewaard en dat is niet de bedoeling. FYN moet ook toestemming van de consumenten hebben voor het profileren. Bovendien zal FYN de plicht hebben om het profileren als een gegevensverwerkingsproces te registreren. Tevens is FYN voortaan gehouden om een geveenseffectbeoordeling te maken alvorens het overgaat tot het profileren en dient het een functionaris gegevensbescherming te benoemen. Ook moet FYN zorgen dat op correcte wijze toestemming gevraagd is voor het plaatsen van tracking cookies en dat de consument hierover is geïnformeerd. Dit type cookies zal namelijk voor het registreren van het klik- en surfgedrag ingezet worden.

FYN wordt niet als verantwoordelijke aangemerkt indien FYN mailings verstuurt voor de leveranciers. De retailers hebben zelf momenteel direct marketing als een doeleinde geformuleerd. Op dit moment verstuurt FYN mailings conform de eisen van de retailers aan de klanten van de retailers. Dit zal ook gebeuren wanneer de mailing aanbiedingen bevat van de producten van de leveranciers. De leveranciers zullen in overleg met de retailer aangeven waaraan de mailing moet voldoen. Vervolgens zal FYN een mailing conform deze wensen opstellen en deze uit de naam van en vanuit de mailserver van de retailer aan de consumenten sturen. Dit komt neer op hetgeen FYN op dit moment doet voor de retailer in de rol als bewerker.

Lijst van afkortingen

AVG:	Algemene Verordening Gegevensbescherming
AP:	Autoriteit Persoonsgegevens
Cbp:	College Bescherming Persoonsgegevens
FG:	Functionaris Gegevensbescherming
FYN:	FYN Software
Artikel 29-werkgroep:	Groep Gegevensbescherming artikel 29
HvJEU:	Hof van Justitie van de Europese Unie
MvT:	Memorie van toelichting
MKB:	midden- kleinbedrijf
POS:	Point of Sale
PET:	privacy enhancing technologies
PIA:	Privacy Impact Assessment
Tw:	Telecommunicatiewet
Wbp:	Wet bescherming persoonsgegevens

Hoofdstuk 1 Inleiding

1.1 Probleembeschrijving

FYN Software (FYN) is een IT-bedrijf dat gevestigd is in Oss. Het bedrijf is in 2009 opgericht door de heer Edwin Sanderse. FYN is van mening dat het zich ontwikkeld heeft als een vooraanstaand bedrijf op het gebied van IT-dienstverlening. Het bedrijf is van plan om verder te groeien en uit te breiden met vestigingen in het buitenland. FYN verleent IT-diensten aan retailers die aan te merken zijn als een midden- of kleinbedrijf (mkb). Dit onderzoek heeft betrekking op de retailers die opereren in de detailhandel (denk aan juwelierszaken en fietsenwinkels). Zij vormen tachtig procent van het klantenbestand van FYN. Onder retailer wordt in dit rapport dan ook verstaan: een bedrijf dat in een fysieke winkel en/of webshop goederen en/of diensten aanbiedt aan consumenten. Vanuit FYN was er geen behoefte om aandacht te besteden aan de overige twintig procent van de klanten, omdat deze groep niet uit vaste klanten bestaat.

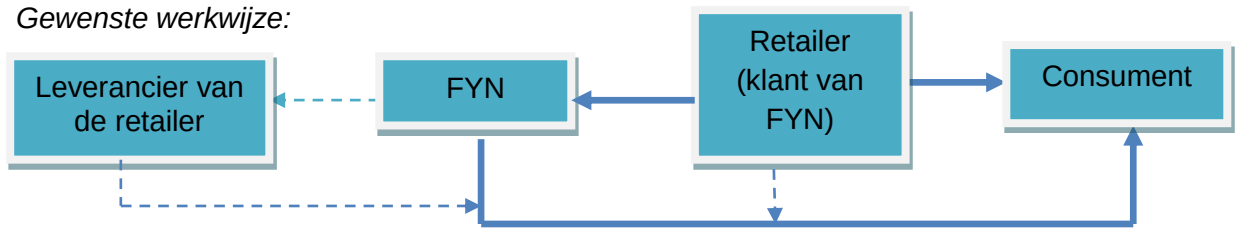
De dienstverlening van FYN bestaat uit het verkopen van het softwareprogramma Point of Sale (POS). Dit programma is door FYN ontwikkeld. FYN biedt de retailers ook na aankoop van de software ondersteuning op technisch gebied. De software functioneert op basis van het omnichannelsysteem. Dit systeem bevat alle winkelmanagementtools (kassasysteem, voorraadbeheer, webshop, inzicht in omzetcijfers, leverancier-integratie, direct mailings, klantbeheersysteem, en dergelijke). Deze winkelmanagementtools zijn aparte communicatiekanalen die data verzamelen. Het omnichannelsysteem zorgt ervoor dat de klant centraal staat en dat alle gegevens in één database worden verzameld.

Na het aanschaffen van de software blijven de retailers gebruikmaken van de IT-dienstverlening van FYN. Zoals aangegeven bestaat deze dienstverlening uit het ondersteunen van de retailer op technisch gebied. Hierbij kan gedacht worden aan een technisch probleem dat niet door de retailer zelf opgelost kan worden. FYN geeft zichzelf dan toegang tot het systeem en lost het probleem op. Wanneer FYN wordt verzocht om van afstand hulp te bieden, kan het zichzelf toegang geven tot de database. Hierdoor kan FYN bij het oplossen van het probleem de persoonsgegevens inzien die de retailer verzameld heeft. FYN ziet deze gegevens alleen in en gebruikt ze verder niet. De medewerkers van FYN beschikken echter over voldoende kennis om de gegevens op te slaan, te kopiëren en er andere handelingen mee te verrichten.

De verzamelde gegevens worden momenteel door de retailer onder andere gebruikt voor marketingdoeleinden. FYN zelf gebruikt de gegevens op geen enkele wijze en ziet deze alleen in wanneer de retailer bijvoorbeeld om technische ondersteuning verzoekt.

In de nabije toekomst wil FYN overgaan tot het profileren. FYN heeft mensen in dienst die voldoende kennis bezitten om de persoonsgegevens op een slimme manier te combineren en te analyseren. Op basis van deze combinaties en analyses kunnen persoonlijkheidsprofielen opgesteld worden. FYN wil daartoe de persoonsgegevens ontvangen die de retailers hebben verzameld. Deze profilering moet leiden tot het in kaart brengen van voorkeuren en interesses, waardoor namens de leveranciers van de retailers gerichte aanbiedingen verstuurd kunnen worden naar de klanten van de retailers. De leveranciers bepalen in overleg met de retailers de inhoud van de aanbiedingen. De direct marketing zal plaatsvinden uit naam van de retailers en vanuit de mailserver van de retailers. De leveranciers krijgen door de persoonlijkheidsprofielen een beeld van de trends in een bepaalde periode en van welke producten veel verkocht worden in een bepaald deel van het land. De profielen worden geanonimiseerd in de vorm van statistieken. FYN verstrekt deze statistieken aan de leveranciers: er is dan geen sprake meer van persoonsgegevens.

Gewenste werkwijze:



De regelgeving met betrekking tot de verwerking van persoonsgegevens wordt momenteel geregeld in de Wet bescherming persoonsgegevens (Wbp). Deze wet is een uitwerking van de Europese richtlijn bescherming persoonsgegevens (95/46/EG).¹ Echter, op 27 april 2016 heeft het Europees Parlement ingestemd met de Algemene Verordening Gegevensbescherming (EU) 2016/679 (AVG) van het Europees Parlement en de Raad.² Deze verordening is vanaf 25 mei 2018 van kracht. De AVG zal de Europese richtlijn bescherming persoonsgegevens (95/46/EG) vervangen en heeft ook tot gevolg dat de nationale privacywetten van de lidstaten vervallen.³

Het is voor FYN van groot belang om te weten of het op basis van de huidige en toekomstige wet- en regelgeving de klantdata (persoonsgegevens en het klik- en surfgedrag) die zijn verzameld door de retailers, mag gebruiken voor profilering om direct marketing ten behoeve van leveranciers mogelijk te maken. Er is op dit moment nog niets geregeld tussen FYN en de retailers.

Kortom, het kennisdoel van dit onderzoek is het opleveren van een oordeel met een bijbehorend advies aan FYN. In dit oordeel wordt beschreven in hoeverre FYN persoonsgegevens, die zijn verzameld door de retailers en betrekking hebben op de klanten van de retailers, mag gebruiken voor profilering om direct marketing ten behoeve van de leveranciers mogelijk te maken op basis van de huidige en toekomstige wet- en regelgeving. Vervolgens wordt naar aanleiding van het antwoord op deze vraag een advies gegeven, in de vorm van aanbevelingen, of er al dan niet gehandeld kan worden conform de gewenste werkwijze en onder welke voorwaarden dit eventueel kan.

1.2 Centrale vraag

In hoeverre mag FYN Software persoonsgegevens van de retailer die zijn verzameld door middel van het omnichannelsysteem verwerken voor het profileren ten behoeve van direct marketing voor de leveranciers in overeenstemming met de relevante regelgeving, waaronder de Wet bescherming persoonsgegevens en de Algemene Verordening Gegevensbescherming (EU) 2016/679 van het Europees Parlement en de Raad?

1.3 Doelstelling

Op uiterlijk 29 mei 2017 wordt dit onderzoeksrapport opgeleverd aan FYN Software te Oss. In dit rapport wordt een oordeel gegeven in hoeverre FYN Software persoonsgegevens van de klanten van de retailer uit het omnichannelsysteem mag verwerken voor profilering, om zo direct marketing ten behoeve van de leveranciers mogelijk te maken, op basis van de huidige en toekomstige wet- en regelgeving. Dit dient onderzocht te worden, omdat FYN op korte termijn tegen een vergoeding een nieuwe dienst wil gaan aanbieden aan de leveranciers van de retailers.

¹ 'Wet bescherming persoonsgegevens', *autoriteitpersoonsgegevens* z.j., autoriteitpersoonsgegevens.nl.

² Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG algemene verordening gegevensbescherming (*PbEU* 2016, L 119/1)

³ 'Internationale privacywetgeving', *autoriteitpersoonsgegevens* z.j., autoriteitpersoonsgegevens.nl.

1.4 Deelvragen

1. Welke regels stelt de Wbp ten aanzien van het verwerken van persoonsgegevens?
2. Welke wijzigingen brengt de AVG met zich mee ten aanzien van het verwerken van persoonsgegevens?
3. Op welke wijze wil FYN Software in de toekomst persoonsgegevens verwerken voor profilering om direct marketing ten behoeve van derden mogelijk te maken?
4. In hoeverre mag FYN Software persoonsgegevens verwerken voor profilering om over te kunnen gaan tot direct marketing voor derden op basis van de huidige en toekomstige wet- en regelgeving?

1.5 Methoden, bronnen en verantwoording

Deelvraag één en twee hebben een juridisch kader. Beide vragen hebben als kennisdoel om een beschrijving op te leveren van wat de wet voorschrijft voor de verwerking van persoonsgegevens. Onderzocht wordt wie als verantwoordelijke en bewerker wordt aangemerkt. Ook wordt gekeken naar de plichten die aan deze twee actoren worden opgelegd. Voor een rechtmatige gegevensverwerking zullen zij immers aan meerdere plichten moeten voldoen. Ook worden de rechten van de betrokkene besproken. De Wbp en de AVG kennen de betrokkene rechten toe om stappen te ondernemen tegen de verwerking van de hem betreffende persoonsgegevens. Tevens wordt gekeken naar de eisen die de Wbp momenteel stelt aan de verwerking van persoonsgegevens en of er een verandering optreedt in deze eisen zodra de AVG van kracht wordt. Vervolgens worden de regels behandeld die de wet stelt voor de gegevensverwerking ten behoeve van profilering. FYN gaat immers persoonlijkheidsprofielen opstellen ten behoeve van de leveranciers en voor hun marketingdoeleinden. De Wbp, de memorie van toelichting (MvT) en literatuur over de Wbp worden geraadpleegd. Daarnaast wordt de AVG bestudeerd en de literatuur die ingaat op de aankomende verordening. Ook worden artikelen bestudeerd van vakmensen uit de praktijk die kennis hebben van het privacyrecht en wordt jurisprudentie geraadpleegd. Om de eerste twee deelvragen te kunnen beantwoorden, dienen immers de Wbp, de AVG en stukken naar aanleiding van deze twee wetten bestudeerd te worden. Literatuur en artikelen van vakmensen dienen om meer duidelijkheid te verkrijgen over hetgeen in de wetten is bepaald. Ook wordt één artikel uit de Telecommunicatiewet (Tw) bestudeerd: het cookie-artikel. FYN gaat immers tracking cookies plaatsen om het klik- en surfgedrag van klanten te registreren. Tracking cookies zijn bestanden die op een computer geplaatst worden. Organisaties kunnen met deze cookies het surfgedrag van mensen volgen.⁴ Daarom is het van belang te weten welke regels de wet stelt voor het plaatsen van deze cookies. Het rechtsbronnen- en literatuuronderzoek wordt toegepast om de eerste twee deelvragen te beantwoorden. Bij het rechtsbronnen- en literatuuronderzoek wordt de inhoudsanalyse als methode gehanteerd.

Deelvraag drie heeft een praktisch kader. Het kennisdoel van de derde deelvraag is om een beschrijving op te leveren van de wijze waarop FYN gaat profileren. Er moet onderzocht worden hoe het omnichannelsysteem werkt, omdat dit systeem wordt gebruikt voor het verzamelen van persoonsgegevens. Ook wordt gekeken welke handelingen FYN nu verricht met betrekking tot de persoonsgegevens en welke rol FYN hierin vervult. Vervolgens wordt gekeken naar het profileren en hoe vorm wordt gegeven aan deze gegevensverwerking. De persoonlijkheidsprofielen zullen omgezet worden in statistieken om deze te verstrekken aan de leveranciers, die de statistieken gebruiken voor marketingdoeleinden. FYN zal de direct marketing uitvoeren uit naam van de retailer. Er wordt daarom ook aandacht besteed aan hoe precies vorm wordt gegeven aan deze direct marketing. Daarnaast komt aan bod hoe de gegevens worden verzameld en wie de

⁴ 'Cookies', *acm* z.j., *acm.nl*.

doeleinden en de middelen voor de gegevensverwerking vaststelt. Dit is van belang, aangezien er onderzocht dient te worden of FYN bewerker of verantwoordelijke is. Ter beantwoording van de derde deelvraag wordt het surveyonderzoek als onderzoeksstrategie gehanteerd. Er wordt een interview met open vragen afgenomen bij de heer Hazelhof en de heer Sanderse. Door het stellen van open vragen zijn de antwoorden op de vragen uitgebreider en daardoor wordt meer duidelijkheid verkregen over de werkwijze van FYN. Ook stellen open vragen de onderzoeker in de gelegenheid om door te vragen, mocht er iets onduidelijk zijn. De heer Hazelhof is ICT-expert en ontwikkelt software, waaronder de software die de klanten van FYN momenteel gebruiken. Het profileren zal in de toekomst plaatsvinden door een systeem dat de heer Hazelhof eveneens zal ontwikkelen. Daarom is hij de meest geschikte persoon om te interviewen over hoe het profileren precies zal plaatsvinden en om duidelijkheid te krijgen over de technische kant van dit proces. Naast de heer Hazelhof wordt ook de heer Sanderse geïnterviewd. Het interview met de heer Sanderse zal vooral op de commerciële kant gericht zijn. Het is immers van belang om te weten of de persoonlijkheidsprofielen ook op een andere commerciële wijze geëxploiteerd zullen worden.

Deelvraag vier heeft een praktisch en juridisch kader. Het kennisdoel van deze vraag is om een oordeel te geven over of de gewenste werkwijze toegestaan is op grond van de huidige en toekomstige wet- en regelgeving. De werkwijze wordt allereerst getoetst aan de regelgeving die besproken wordt in het juridisch kader. Ter beantwoording van deze deelvraag wordt het rechtsbronnen- en literatuuronderzoek gecombineerd met een surveyonderzoek. Immers, het surveyonderzoek dat uitgevoerd is ter beantwoording van deelvraag drie levert informatie op over de werkwijze. De werkwijze wordt vervolgens getoetst aan de hand van de theorie, die in kaart is gebracht met het rechtsbronnen- en literatuuronderzoek en behandeld wordt in deelvraag één en twee.

1.6 Onderzoeksstrategie

Het rechtsbronnen- en literatuuronderzoek wordt toegepast ter beantwoording van de juridische deelvragen. Het surveyonderzoek wordt toegepast bij het in kaart brengen van de praktijk. Bij de analyse tussen de wet en de praktijk worden deze twee strategieën gecombineerd. Bij het rechtsbronnen- en literatuuronderzoek wordt de inhoudsanalyse als methode gehanteerd. De wet, jurisprudentie en literatuur moeten geraadpleegd worden. Een surveyonderzoek dat bestaat uit een interview met open vragen wordt als methode toegepast om de derde deelvraag te beantwoorden.

1.7 Leeswijzer

Dit onderzoeksrapport bestaat uit vijf hoofdstukken. Het eerste hoofdstuk beschrijft de aanleiding van dit rapport. In het tweede hoofdstuk wordt het juridisch kader in kaart gebracht. Vervolgens wordt in hoofdstuk drie de praktijk behandeld. In hoofdstuk vier wordt een analyse gemaakt van de wet en de praktijk. Geanalyseerd wordt in hoeverre de praktijk in overeenstemming is met de relevante wet- en regelgeving. Als laatste worden in hoofdstuk vijf conclusies getrokken en aanbevelingen gegeven naar aanleiding van hetgeen is besproken in hoofdstuk twee tot en met vier.

Hoofdstuk 2 Juridisch kader

Inleiding

In dit hoofdstuk wordt het juridisch kader behandeld. De wetten die aan bod komen zijn de Wbp, de AVG en de Tw. Deze wetten worden behandeld omdat zij betrekking hebben op de verwerking van persoonsgegevens. Allereerst wordt stilgestaan bij de Wbp. Deze wet stelt momenteel de regels die gelden voor de verwerking van persoonsgegevens. Vervolgens wordt de AVG behandeld, omdat die de Wbp zal vervangen. Als laatste wordt ingegaan op de regels die de Tw stelt voor het plaatsen van cookies, omdat voor het registreren van het klik- en surfgedrag tracking cookies worden geplaatst.

2.1 Wet bescherming persoonsgegevens

De Wbp geeft regels die betrekking hebben op de verwerking van persoonsgegevens. In 1995 werd de Europese richtlijn bescherming persoonsgegevens (95/46/EG) van kracht. Deze richtlijn had onder andere tot doel om de nationale wetgeving van de lidstaten op het gebied van de bescherming van persoonsgegevens te harmoniseren.⁵ De richtlijn diende omgezet te worden naar nationaal recht. De Wet persoonsregistratie werd tweemaal geëvalueerd. Het bleek dat een herziening onvermijdelijk was en daarom werd de Wbp voorbereid.⁶ In deze paragraaf wordt ingegaan op de vraag wanneer de Wbp van toepassing is. Het is van belang om te weten of de Wbp van toepassing is voordat wordt overgegaan tot de toetsing ervan aan de praktijk. Vervolgens worden de eisen behandeld waaronder de gegevensverwerking als rechtmatig wordt aangemerkt. Een organisatie moet namelijk weten aan welke vereisten voldaan moet zijn om niet aangesproken te worden door de toezichthoudende autoriteit. Als laatste wordt gekeken naar de personen die betrokken zijn bij de gegevensverwerking: de verantwoordelijke, de bewerker en de betrokkene. De Wbp legt immers plichten op aan de bewerker en de verantwoordelijke en kent de betrokkene rechten toe.

2.1.1 Toepassing Wet bescherming persoonsgegevens

De Wbp is van toepassing zodra er sprake is van het geheel of gedeeltelijk geautomatiseerd verwerken van persoonsgegevens die eventueel in een bestand zijn opgenomen of daarin dienen te worden opgenomen.⁷ Hieruit wordt afgeleid dat er voldaan moet zijn aan drie vereisten. Er moet sprake zijn van gegevens die aan te merken zijn als persoonsgegevens. Deze dienen verwerkt te worden. Als laatste dient er sprake te zijn van een bestand, tenzij er sprake is van geautomatiseerde gegevensverwerking. Immers, als er sprake is van geautomatiseerde gegevensverwerking, is de Wbp automatisch van toepassing. In het geval van gedeeltelijk geautomatiseerde of niet-geautomatiseerde gegevensverwerking moet voldaan zijn aan het vereiste dat de persoonsgegevens in een bestand worden opgeslagen.

2.1.1.1 Persoonsgegevens

Er is sprake van een persoonsgegeven indien het gegeven te herleiden is naar een geïdentificeerde of identificeerbare natuurlijk persoon.⁸ Om te spreken van een persoonsgegeven worden twee eisen gesteld: het gegeven moet betrekking hebben op

⁵ 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 (*PbEG*, L 281/31-50), overweging 1

⁶ Kranenborg & Verhey 2011, p. 56.

⁷ Art. 2 lid 1 Wbp.

⁸ Art. 1 sub a Wbp.

een natuurlijk persoon en deze natuurlijke persoon moet identificeerbaar of al geïdentificeerd zijn.⁹

De wetgever legt het begrip ‘persoonsgegevens’ ruim uit. Zolang het gegeven betrekking heeft op informatie die gekoppeld kan worden aan een natuurlijk persoon, is er sprake van een persoonsgegeven. Om het gegeven te koppelen aan een natuurlijk persoon dient zijn identiteit vastgesteld te worden. De vaststelling van de identiteit moet geen onevenredige inspanning kosten.¹⁰ Bij de identiteitsvaststelling spelen de volgende twee factoren een rol: de aard van de gegevens en de mogelijkheden die de verantwoordelijke tot zijn beschikking heeft om identificatie mogelijk te maken.¹¹

Richtlijn (95/46/EG) definieert ‘identificeerbaar’ als volgt: *‘een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een of meer specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit’*.¹² Er zijn twee soorten identificeerbaarheid: directe en indirecte identificeerbaarheid. Gegevens die leiden tot directe identificeerbaarheid hebben als kenmerk dat de identiteit op een eenvoudige wijze vastgesteld kan worden, bijvoorbeeld een naam of een adres.¹³ Indirecte gegevens leiden alleen in combinatie met andere gegevens naar een persoon, denk bijvoorbeeld aan het koppelen van een IP-adres aan een natuurlijk persoon. Desondanks merkte het College Bescherming Persoonsgegevens (Cbp) een indirect gegeven aan als een persoonsgegeven. Het Cbp heet nu Autoriteit Persoonsgegevens (AP); de AP wordt ook als definitie gehanteerd in dit rapport. Volgens de AP is het voldoende dat er sprake is van een gegeven dat herleidbaar is naar een persoon om het te kunnen aanmerken als een persoonsgegeven.¹⁴

2.1.1.2 Verwerken

Het verwerken heeft betrekking op het gehele proces van gegevensverwerking. De Wbp definieert verwerken als volgt: *‘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’*.¹⁵ Onder het verwerken worden dus alle handelingen verstaan die worden verricht met betrekking tot persoonsgegevens. Deze handelingen kunnen zowel geautomatiseerd als niet-geautomatiseerd zijn. De bovengenoemde handelingen zijn niet-limitatief.

2.1.1.3 Bestand

Het gestructureerd geheel van de persoonsgegevens wordt aangemerkt als bestand. Dit gestructureerd geheel hoeft niet gecentraliseerd te zijn. Echter, het vereiste dat er sprake moet zijn van een gestructureerd geheel impliceert wel dat de gegevensverwerkingen onderling met elkaar moeten samenhangen.¹⁶ Het bestand moet toegankelijk zijn en betrekking hebben op personen.¹⁷

⁹ Kamerstukken II 1997/98, 25892, 3, p.46 (MvT).

¹⁰ Kranenburg & Verhey 2011, p. 61.

¹¹ Kamerstukken II 1997/98, 25892, 3, p.47 (MvT).

¹² Art. 2 sub a Richtlijn (95/46/EG).

¹³ Kamerstukken II 1997/98, 25892, 3, p.48 (MvT).

¹⁴ L. Meij, ‘BigDatamaandag deel 3: Persoonsgegevens en gegevensverwerking’, *ictrecht* 21 juli 2014, ictrecht.nl.

¹⁵ Art. 1 sub b Wbp.

¹⁶ Hooghiemstra & Nouwt 2016, p. 23.

¹⁷ Art. 1 sub c Wbp.

2.1.2 Rechtmatige gegevensverwerking

Zodra vastgesteld is dat de Wbp van toepassing is, moet worden gekeken of de verwerking rechtmatig plaatsvindt. De Wbp stelt de volgende eisen om te spreken van een rechtmatige gegevensverwerking: zorgvuldigheidseis, doeleinden, rechtvaardigingsgronden, doelbinding, kwaliteit waarborgen, beveiligingsmaatregelen treffen en bewaartermijn bepalen.¹⁸

2.1.2.1 Zorgvuldigheidseis

De zorgvuldigheidseis schrijft voor dat de verwerking van persoonsgegevens in overeenstemming met de wet dient te geschieden en dat de gegevens op een behoorlijke en zorgvuldige wijze verwerkt worden.¹⁹ De gegevensverwerking is als zorgvuldig aan te merken zodra voldaan is aan de overige vereisten. Deze overige vereisten worden hieronder toegelicht.

2.1.2.2 Doeleinden

Alvorens wordt overgegaan tot verwerking van persoonsgegevens moeten welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden geformuleerd worden.²⁰ Het vereiste van welbepaaldheid houdt in dat het doel niet vaag en ruim geformuleerd mag zijn: het doel moet in de toekomst een duidelijk kader bieden voor de vraag in hoeverre de verwerking van persoonsgegevens in een situatie daadwerkelijk nodig is.²¹ Het vereiste dat het doel 'uitdrukkelijk' moet zijn, betekent dat de verantwoordelijke het doel dient te hebben omschreven. Het rechtvaardigheidsvereiste houdt in dat de verwerking een wettelijke grondslag moet hebben. In de Wbp is een limitatieve opsomming opgenomen van rechtvaardigingsgronden. Deze worden nader besproken in paragraaf 2.1.2.3.

2.1.2.3 Rechtvaardigingsgronden

De Wbp geeft zes limitatieve rechtvaardigingsgronden.²² Elke gegevensverwerking dient minimaal op een van de rechtvaardigingsgronden gebaseerd te zijn. Is dit niet het geval, dan is de verwerking niet gerechtvaardigd en mag deze niet plaatsvinden.²³ De volgende rechtvaardigingsgronden worden niet behandeld: verwerking op grond van een wettelijke verplichting, verwerking ten behoeve van een vitaal belang en verwerking ter vervulling van een publiekrechtelijke taak door een bestuursorgaan. Deze kunnen immers nooit van toepassing zijn in het geval van profilering en direct marketing.

De eerste rechtvaardigingsgrond betreft de toestemming van de betrokkene.²⁴ Deze dient ondubbelzinnig te zijn.²⁵ In geval van twijfel dient de verantwoordelijke na te gaan of de betrokkene daadwerkelijk instemt met de verwerking.²⁶ Een beroep op deze grond kan uitgesloten worden wanneer er tussen de verantwoordelijke en de betrokkene een ongelijke machtsverhouding bestaat.²⁷

Daarnaast kan de gegevensverwerking gerechtvaardigd zijn wanneer deze noodzakelijk is voor het uitvoeren van een overeenkomst.²⁸ De betrokkene dient partij te zijn bij deze overeenkomst. Deze rechtvaardigingsgrond geldt ook in de precontractuele fase.²⁹

¹⁸ Kranenborg & Verhey 2011, p. 81.

¹⁹ Art. 6 Wbp.

²⁰ Art. 7 Wbp.

²¹ Hooghiemstra & Nouwt 2016, p. 49.

²² Art. 8 Wbp.

²³ Kranenborg & Verhey 2011, p. 83.

²⁴ Art. 8 sub a Wbp.

²⁵ *Kamerstukken II* 1997/98, 25892, 3, p.10 (MvT).

²⁶ Kranenborg & Verhey 2011, p. 85.

²⁷ Hooghiemstra & Nouwt 2016, p. 51.

²⁸ Art. 8 sub b Wbp.

²⁹ Hooghiemstra & Nouwt 2016, p. 52.

Als laatste wordt de rechtvaardigingsgrond besproken waarop de verantwoordelijke een beroep kan doen indien hij van mening is dat de verwerking noodzakelijk is ten behoeve van de behartiging van zijn gerechtvaardigd belang.³⁰ Het belang van de betrokkene prevaleert in dit geval niet boven het belang van de verantwoordelijke. Deze rechtvaardigingsgrond is een restbepaling in vergelijking met de overige gronden. In de overige rechtvaardigingsgronden wordt telkens een specifiek doel genoemd. Bij deze rechtvaardigingsgrond is geen specifiek doel geformuleerd, alleen het aanwezig zijn van een gerechtvaardigd belang wordt genoemd. Er wordt echter niet aangegeven wat een gerechtvaardigd belang is. Een gerechtvaardigd belang wordt onder andere aanwezig geacht als de gegevensverwerking noodzakelijk is voor de bedrijfsactiviteiten van de verantwoordelijke.³¹ Naast het feit dat er een gerechtvaardigd belang aanwezig moet zijn, moet deze ook prevaleren boven het belang van de betrokkene. Deze belangenafweging dient de verantwoordelijke te maken. De belangenafweging dient ertoe om de persoonlijke levenssfeer van de betrokkene te beschermen. Indien de bescherming van de persoonlijke levenssfeer van de betrokkene prevaleert, moet afgezien worden van de gegevensverwerking. Bij de afweging wordt gekeken naar verschillende zaken. De aard van de gegevens en de genomen beveiligingsmaatregelen spelen een rol.³² Ook moet beoordeeld worden of het doel van de gegevensverwerking niet gediend kan worden op een andere wijze die minder ingrijpend is en minder nadelige gevolgen met zich meebrengt voor de betrokkene (subsidiariteitsbeginsel). Als laatste moet bezien worden of de inbreuk op de belangen van de betrokkene niet onevenredig is in verhouding met het doel van de gegevensverwerking (proportionaliteitsbeginsel).³³

2.1.2.4 Doelbinding

Persoonsgegevens mogen niet worden verwerkt op een wijze die onverenigbaar is met de oorspronkelijke doeleinden waarvoor de gegevens zijn verkregen.³⁴ Gegevens mogen dus wel voor andere doeleinden worden gebruikt, mits deze niet onverenigbaar zijn met de oorspronkelijke doeleinden.³⁵ De verantwoordelijke moet beoordelen of het gebruik onverenigbaar is. De wet geeft een niet-limitatieve opsomming van omstandigheden waarmee rekening gehouden moet worden bij deze beoordeling.³⁶ Allereerst moet gekeken worden wat de verwantschap is tussen het oorspronkelijke doel en het doel waarvoor de gegevens op dat moment gebruikt zullen worden.³⁷ Nadat aandacht besteed is aan de verwantschap tussen de verschillende doelen, moet ook rekening gehouden worden met de aard van de gegevens.³⁸ Bij gebruik van gevoelige gegevens is de kans kleiner dat de gegevensverwerking verenigbaar wordt geacht met het oorspronkelijke doel.³⁹ Tevens moet aandacht besteed worden aan de gevolgen van de verstrekking.⁴⁰ Zodra de verstrekking gevolgen heeft voor de bescherming van de persoonlijke levenssfeer van de betrokkene, moet afgewogen worden welk belang prevaleert. De verantwoordelijke zal deze belangenafweging moeten maken. Daarnaast moet de wijze van verkrijging worden beoordeeld.⁴¹ Als laatste moet gekeken worden naar de waarborgen die getroffen zijn ter beveiliging van de persoonsgegevens. Deze getroffen

³⁰ Art. 8 sub f Wbp.

³¹ Hooghiemstra & Nouwt 2016, p. 53.

³² Hooghiemstra & Nouwt 2016, p. 53.

³³ *Kamerstukken II* 1997/98, 25892, 3, p.87 (MvT).

³⁴ Art. 9 Wbp.

³⁵ *Kamerstukken II* 1997/98, 25892, 3, p.79 (MvT).

³⁶ Art. 9 lid 2 Wbp.

³⁷ Art. 9 lid 2 sub a Wbp.

³⁸ Art. 9 lid 2 sub b Wbp.

³⁹ Hooghiemstra & Nouwt 2016, p. 67.

⁴⁰ Art. 9 lid 2 sub c Wbp.

⁴¹ Art. 9 lid 2 sub d Wbp.

waarborgen moeten de persoonsgegevens een voldoende beschermingsniveau bieden tijdens en na de verstrekking.⁴²

2.1.2.5 Kwaliteit waarborgen

De gegevens mogen worden verwerkt voor zover zij toereikend, ter zake dienend en niet bovenmatig zijn, gelet op de doeleinden waarvoor ze verzameld zijn en worden verwerkt.⁴³ De eis dat de gegevens ‘toereikend’ dienen te zijn, houdt in dat de gegevens voldoende informatie moeten verschaffen over het doel van de verwerking.⁴⁴ De voorwaarden dat de gegevens ‘ter zake dienend’ en niet ‘bovenmatig’ zijn, hangen nauw met elkaar samen. Deze twee eisen zijn in principe een uitwerking van het proportionaliteitsvereiste: de gegevensverwerking mag niet verder gaan dan noodzakelijk is om de gestelde doeleinden te realiseren.⁴⁵

2.1.2.6 Beveiliging

De verantwoordelijke dient passende technische en organisatorische maatregelen te nemen om te waarborgen dat de gegevensverwerking op een zorgvuldige wijze geschiedt.⁴⁶ Bij de beoordeling of de maatregelen passend zijn, dient aandacht besteed te worden aan de stand van de techniek en het proportionaliteitsvereiste. De maatregelen dienen in overeenstemming te zijn met de stand van de techniek.⁴⁷ Ook moet er proportionaliteit zijn tussen de beveiligingsmaatregelen en de aard van de gegevens. Hoe gevoeliger de gegevens, hoe strenger de gestelde beveiligingseisen zijn.⁴⁸ Het komt erop neer dat de genomen beveiligingsmaatregelen in overeenstemming moeten zijn met de stand van de techniek en dat gekeken wordt naar de aard van de gegevens en de risico's die de gegevensverwerking met zich meebrengt.

2.1.2.7 Bewaartermijn

De persoonsgegevens mogen bewaard worden zolang dit noodzakelijk is om de doeleinden te verwezenlijken waarvoor de gegevens in eerste instantie zijn verzameld.⁴⁹ De verantwoordelijke zal dus moeten beoordelen of het noodzakelijk is om de gegevens nog te bewaren ten behoeve van zijn doeleinden.

2.1.3 De actoren

In deze paragraaf wordt aandacht besteed aan de volgende drie actoren: verantwoordelijke, bewerker en betrokkene. Deze zijn immers betrokken bij de gegevensverwerking. In de voorgaande paragraaf zijn de eisen van een rechtmatige gegevensverwerking besproken. Naast deze eisen worden er ook plichten opgelegd aan de verantwoordelijke en de bewerker en worden rechten aan de betrokkene toegekend. Voor een rechtmatige gegevensverwerking moet ook aan deze rechten en plichten aandacht worden besteed.

2.1.3.1 Verantwoordelijke

De verantwoordelijke, die zowel een natuurlijk persoon als een rechtspersoon kan zijn, is degene die het doel van de gegevensverwerking vaststelt en de middelen ten behoeve van de verwerking aanwijst.⁵⁰ Meestal ligt de bepaling van de doeleinden en het aanwijzen van de middelen in één hand. Is dit niet het geval, dan wordt gesproken van gezamenlijke verantwoordelijkheid.⁵¹ De verantwoordelijke heeft een aantal

⁴² Art. 9 lid 2 sub e Wbp.

⁴³ Art. 11 Wbp.

⁴⁴ Kranenborg & Verhey 2011, p. 97.

⁴⁵ Kranenborg & Verhey 2011, p. 98.

⁴⁶ Art. 13 Wbp.

⁴⁷ *Kamerstukken II* 1997/98, 25892, 3, p.98 (MvT).

⁴⁸ *Kamerstukken II* 1997/98, 25892, 3, p.99 (MvT).

⁴⁹ Art. 10 lid 1 Wbp.

⁵⁰ Art. 1 sub d Wbp.

⁵¹ *Kamerstukken II* 1997/98, 25892, 3, p.55 (MvT).

verplichtingen. De eisen voor een rechtmatige verwerking die in paragraaf 2.1.2 zijn besproken, zijn plichten van de verantwoordelijke. Naast deze verwerkingseisen legt de Wbp ook de volgende plichten op aan de verantwoordelijke:

- De verantwoordelijke heeft een informatieplicht jegens de betrokkene.⁵² Deze plicht is een tegenhanger van het recht tot kennisneming van de betrokkene.⁵³
De Wbp verplicht de verantwoordelijke zijn identiteit en de doeleinden mede te delen.⁵⁴ Daarnaast is er een algemene plicht opgenomen: de verantwoordelijke is gehouden om nadere informatie te verstrekken indien hij van oordeel is dat dit noodzakelijk is gelet op de aard van de gegevens en de omstandigheden waaronder deze zijn verkregen.⁵⁵ Er wordt niet aangegeven waaruit deze extra informatieoverdracht moet bestaan.
- De verantwoordelijke heeft een meldplicht. Deze plicht houdt in dat de verantwoordelijke het aan de AP moet melden zodra hij gegevens verwerkt.⁵⁶
- De verantwoordelijke moet een datalek melden bij de AP.⁵⁷

2.1.3.2 Bewerker

De bewerker is degene aan wie de verantwoordelijke de verwerking van de persoonsgegevens uitbesteedt. Deze persoon is hiërarchisch niet ondergeschikt aan de verantwoordelijke: de bewerker is een persoon buiten de organisatie.⁵⁸

De verantwoordelijke is degene die het doel van de gegevensverwerking vaststelt en middelen daarvoor aanwijst. Een bewerker heeft hier in beginsel geen zeggenschap over en dient de instructies van de verantwoordelijke op te volgen. In beginsel, want de bewerker heeft wel een inbreng bij het vaststellen van de middelen op het gebied van technische en organisatorische vragen.⁵⁹ Bij het vaststellen van middelen buiten het technische en organisatorische gedeelte heeft de bewerker geen zeggenschap. Het gaat dan om vragen zoals 'Voor welke duur worden de gegevens bewaard?', 'Wie heeft toegang tot de gegevens?', enzovoort. De verantwoordelijke moet deze vragen bij het vaststellen van de middelen beantwoorden.⁶⁰ De wet stelt het verplicht dat de verantwoordelijke en de bewerker een bewerkersovereenkomst sluiten.⁶¹

De Wbp legt de bewerker de volgende verplichtingen op:

- De bewerker mag alleen overgaan tot het verwerken van persoonsgegevens als de verantwoordelijke hiertoe opdracht geeft.⁶²
- De bewerker is verplicht schade te betalen aan de betrokkene als deze schade ondervindt door de verwerkingshandelingen, tenzij de bewerker kan aantonen dat de schade niet aan hem kan worden toegerekend.⁶³
- De bewerker heeft een geheimhoudingsplicht.⁶⁴

⁵² Art. 33 jo. 34 Wbp.

⁵³ Kranenborg & Verhey 2011, p. 120.

⁵⁴ Art. 33 lid 2 jo. art. 34 lid 2 Wbp.

⁵⁵ Art. 33 lid 3 jo. art. 34 lid 3 Wbp.

⁵⁶ Art. 27 t/m 30 Wbp.

⁵⁷ Art. 34a Wbp.

⁵⁸ Art. 1 sub e Wbp.

⁵⁹ Opinie van de Groep Gegevensbescherming Artikel 29 nr. 1 van 2010, p.16.

⁶⁰ Opinie van de Groep Gegevensbescherming Artikel 29 nr. 1 van 2010, p.17.

⁶¹ Art. 14 lid 2 Wbp.

⁶² Art. 12 lid 1 Wbp.

⁶³ Sauerwein & Linnemann 2002, p. 44.

⁶⁴ Art. 12 lid 2 Wbp.

2.1.3.3 Betrokkene

De gegevensverwerking heeft op de betrokkene betrekking.⁶⁵ De betrokkene heeft de volgende rechten: het recht op kennisneming, het recht van correctie, het recht van verzet en het recht om zich te vrijwaren van geautomatiseerde, individuele besluitvorming.⁶⁶

HET RECHT OP KENNISNEMING

De betrokkene heeft het recht om de verantwoordelijke te verzoeken hem mede te delen of er persoonsgegevens worden verwerkt die op hem betrekking hebben.⁶⁷ De betrokkene moet in de gelegenheid worden gesteld kennis te nemen van het feit of zijn persoonsgegevens worden verwerkt en moet de mogelijkheid hebben dit in rechte aan te vechten.⁶⁸

HET RECHT VAN CORRECTIE

Op grond van het recht van correctie heeft de betrokkene de mogelijkheid om de verantwoordelijke te verzoeken de hem betreffende persoonsgegevens te verbeteren, aan te vullen, te verwijderen of af te schermen. Dit recht kan door de betrokkene alleen worden uitgeoefend indien de gegevens onjuist, onvolledig of niet ter zake dienend zijn voor het doel waarvoor ze worden verwerkt.⁶⁹

HET RECHT VAN VERZET

De betrokkene heeft twee grondslagen in de Wbp om zich te beroepen op zijn recht van verzet. Ten eerste bestaat de mogelijkheid om verzet aan te tekenen tegen het verwerken van persoonsgegevens op de grondslag dat dit geschiedt ten behoeve van de vervulling van een publiekrechtelijke taak of voor de behartiging van het gerechtvaardigd belang van de verantwoordelijke.⁷⁰ Ten tweede heeft de betrokkene het recht om verzet aan te tekenen tegen de gegevensverwerking ten behoeve van direct marketing.⁷¹

VRIJWARING VAN GEAUTOMATISEERDE, INDIVIDUELE BESLUITVORMING

Een betrokkene kan niet worden onderworpen aan een besluit dat tot stand is gekomen door middel van een geautomatiseerde gegevensverwerking.⁷² De achterliggende gedachte van dit artikel is om de persoonlijke levenssfeer van de betrokkene te beschermen. Immers, het besluit dat genomen wordt door middel van geautomatiseerde verwerking is bedoeld om inzicht te krijgen in bepaalde persoonlijkheidsaspecten. Dergelijke beslissingen mogen niet genomen worden zonder menselijke tussenkomst.⁷³

2.2 Algemene Verordening Gegevensbescherming

Zoals blijkt uit paragraaf 2.1 is de verwerking van persoonsgegevens geregeld in de Wbp. De Wbp vervalt per 25 mei 2018 en wordt vervangen door de AVG. De AVG is een verordening die van toepassing is, zodra er sprake is van het geheel of gedeeltelijk geautomatiseerd verwerken van persoonsgegevens die eventueel in een bestand zijn opgenomen of daarin opgenomen dienen te worden.⁷⁴ In het geval van geautomatiseerde gegevensverwerking is de AVG direct van toepassing.⁷⁵ De AVG gaat meteen doorwerken in de lidstaten: er is geen wet nodig om de regels van de AVG te implementeren in de nationale rechtstelsels van de lidstaten.⁷⁶ In deze paragraaf wordt

⁶⁵ Art. 1 sub f Wbp.

⁶⁶ Kranenborg & Verhey 2011, p. 125.

⁶⁷ Art. 35 lid 1 Wbp.

⁶⁸ Hooghiemstra & Nouwt 2016, p. 174.

⁶⁹ Art. 36 lid 1 Wbp.

⁷⁰ Art. 40 lid 1 jo. art. 8 sub e en sub f Wbp.

⁷¹ Art. 41 lid 1 Wbp.

⁷² Art. 42 lid 1 Wbp.

⁷³ Hooghiemstra & Nouwt 2016, p. 207.

⁷⁴ Art. 2 lid 1 AVG.

⁷⁵ Berkvens & Jakimowicz 2016, p. 14.

⁷⁶ F.Salverda, 'Algemene Verordening Gegevensbescherming treedt in werking op 25 mei 2016', *europadecentraal* 17 mei 2016, europadecentraal.nl.

stilgestaan bij de wijzigingen die de AVG met zich meebrengt. Allereerst wordt gekeken naar de gewijzigde eisen die gesteld worden aan de verwerking van persoonsgegevens. Ook wordt gekeken naar de wijzigingen in de plichten van de verantwoordelijke en de bewerker en de nieuwe rechten die worden toegekend aan de betrokkene. Het is van belang om te weten welke wijzigingen de AVG met zich meebrengt, omdat de Wbp over minder dan een jaar vervalt en vervangen wordt door de AVG.

2.2.1 Rechtmatige gegevensverwerking onder de AVG

In deze paragraaf wordt gekeken naar de gewijzigde eisen aan een rechtmatige gegevensverwerking die de AVG stelt. De AVG bevat onder andere een verandering bij de zorgvuldigheidseis. Dit vereiste kent voortaan een extra aspect: het transparantiebeginsel. De grondslagen die de gegevensverwerking rechtvaardigen, zijn hetzelfde gebleven ten opzichte van de Wbp. Er is echter een aanvullend artikel opgenomen waarin eisen worden gesteld aan de toestemming van de betrokkene. Ook is in de AVG een nieuwe eis geïntroduceerd: de eis van de opslagbeperking. Als laatste worden de nieuwe beveiligingseisen besproken: de AVG gaat strengere beveiligingseisen stellen aan de bescherming van persoonsgegevens.

2.2.1.1 Transparantiebeginsel

De verwerking van persoonsgegevens dient altijd transparant te zijn. Dit geldt ook onder de huidige wetgeving. Maar in tegenstelling tot de Wbp noemt de AVG dit vereiste expliciet. In paragraaf 2.1.2.1 is de zorgvuldigheidseis besproken. In de AVG is de zorgvuldigheidseis als volgt gedefinieerd: *‘Persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is’*.⁷⁷ De AVG schrijft uitdrukkelijk een extra eis voor, namelijk transparantie. Het vereiste dat de gegevensverwerking transparant dient te geschieden, houdt in dat de betrokkene op een eenvoudige, toegankelijke en begrijpelijke manier geïnformeerd moet worden over de gegevensverwerking. De communicatie dient eenvoudig plaats te vinden: er moet duidelijke en eenvoudige taal gebruikt worden. Er moet informatie verstrekt worden over de doeleinden van de gegevensverwerking en de identiteit van de verantwoordelijke.⁷⁸

2.2.1.2 Toestemming

In paragraaf 2.1.2.3 zijn de rechtvaardigingsgronden uit de Wbp behandeld. Deze zijn exact overgenomen in de AVG.⁷⁹ De eerste rechtvaardigingsgrond is het verkrijgen van toestemming van de betrokkene.⁸⁰ De Wbp stelt alleen dat de toestemming ondubbelzinnig moet zijn. De AVG daarentegen heeft een artikel gewijd aan de vereisten waaraan deze ondubbelzinnige toestemming moet voldoen.⁸¹

Als de gegevensverwerking op toestemming berust, is de verantwoordelijke gehouden om aan te tonen dat de betrokkene daadwerkelijk zijn toestemming heeft gegeven voor de gegevensverwerking.⁸² De toestemming moet bestaan uit een duidelijke, actieve handeling. Ook moet de toestemming vrij, specifiek en ondubbelzinnig zijn. Een schriftelijke, mondelinge of een elektronische verklaring (bijvoorbeeld het aanvinken van een vakje op de website) zijn onder andere duidelijke, actieve handelingen die een vrije, specifieke en ondubbelzinnige toestemming tot stand brengen. Stilzwijgen of een al aangevinkt vakje worden niet aangemerkt als een actieve handeling en daardoor is er geen sprake van een geldige toestemming.⁸³ Toestemming moet gegeven worden voor elk doeleinde. Indien er meerdere doeleinden ten grondslag liggen aan de gegevensverwerking, moet de verantwoordelijke toestemming hebben voor elk van deze

⁷⁷ Art. 5 lid 1 sub a AVG.

⁷⁸ Berkvens & Jakimowicz 2016, p. 29.

⁷⁹ Art. 6 lid 1 sub a t/m f AVG.

⁸⁰ Art. 6 lid 1 sub a AVG.

⁸¹ Art. 7 AVG.

⁸² Art. 7 lid 1 AVG.

⁸³ Berkvens & Jakimowicz 2016, p. 40.

doeleinden. Toestemming wordt niet als een geldige rechtvaardigingsgrond aangemerkt zodra er een ongelijke verhouding is tussen de verantwoordelijke en de betrokkene.⁸⁴ De betrokkene kan te allen tijde zijn toestemming intrekken zonder opgave van redenen.⁸⁵ Een ingetrokken toestemming laat de gegevensverwerking voortgaand aan deze intrekking onverlet.⁸⁶

Voor profileren zal op grond van de AVG toestemming gevraagd moeten worden.⁸⁷ Organisaties mogen in de toekomst mensen niet onderwerpen aan geautomatiseerde besluitvorming, waaronder ook profilering valt, als deze rechtsgevolgen met zich meebrengt voor de betrokkene of het profileren de betrokkene in aanmerkelijke mate treft.⁸⁸ Als voorbeelden van rechtsgevolgen worden gegeven: het afwijzen van een sollicitatie of een kredietaanvraag. Wat de wetgever bedoelt onder 'anderszins in aanmerkelijke mate' is nog niet duidelijk. Niet-verregaande profilering, zoals bijvoorbeeld direct marketing nadat een persoon vaak heeft gezocht op een bepaald product, gaat waarschijnlijk niet onder de toestemmingsplicht vallen. Voor zwaardere profileringsmiddelen, denk hierbij aan het inzetten van een Data Management Platform (DMP), zal toestemming vereist zijn. Een DMP is vergelijkbaar met een database waarin data uit verschillende kanalen worden verzameld en worden opgeslagen in een centrale database. Organisaties worden hierdoor in staat gesteld om gericht te adverteren.⁸⁹

2.2.1.3 Opslagbeperking

Een nieuwe eis die de AVG introduceert is de eis van opslagbeperking. Deze verplichting houdt in dat de verantwoordelijke er bij de gegevensverwerking voor moet zorg dragen dat de persoonsgegevens in een zodanige vorm worden bewaard dat de betrokkene niet langer is te identificeren dan voor de doeleinden waarvoor de gegevens worden verwerkt.⁹⁰ Deze verplichting ligt in het verlengde van de eis dat de gegevens toereikend en ter zake dienend zijn en niet verder verwerkt mogen worden dan noodzakelijk is.⁹¹

2.2.1.4 Nieuwe beveiligingsmaatregelen

De AVG schrijft net als de Wbp voor dat de beveiliging conform de stand van de techniek moet zijn. In tegenstelling tot de Wbp noemt de AVG beveiligingsmaatregelen die getroffen moeten worden. Allereerst verplicht de AVG dat pseudonimisering en versleuteling van persoonsgegevens plaatsvindt.⁹² Daarnaast is de verantwoordelijke gehouden om de verwerkingssystemen en diensten kwalitatief in te richten. Deze kwalitatieve inrichting moet ervoor zorgen dat de verwerkingssystemen en diensten de verwerking van persoonsgegevens garanderen op basis van vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht.⁹³ Ook moet het verwerkingssysteem in staat zijn om snel toegang tot de persoonsgegevens te verkrijgen bij een technisch of fysiek incident.⁹⁴ Dit vereiste houdt in dat het systeem zodanig moet zijn ingericht dat de persoonsgegevens bij

⁸⁴ Berkvens & Jakimowicz 2016, p. 41.

⁸⁵ Art. 7 lid 3 AVG.

⁸⁶ Art. 7 lid 3 AVG.

⁸⁷ Art. 22 lid 1 sub c AVG.

⁸⁸ Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG algemene verordening gegevensbescherming (PbEU 2016, L 119/1), overweging 71

⁸⁹ N. Kamalzadeh, 'Geautomatiseerde besluitvorming & profilering: wat zijn de eisen?', *considerati* 10 april 2017, considerati.com.

⁹⁰ Art. 5 lid 1 sub e AVG.

⁹¹ Berkvens & Jakimowicz 2016, p. 30.

⁹² Art. 32 lid 1 sub a AVG.

⁹³ Art. 32 lid 1 sub b AVG.

⁹⁴ Art. 32 lid 1 sub c AVG.

een incident niet verloren gaan of moeilijk raadpleegbaar worden.⁹⁵ Als laatste moet de verantwoordelijke een procedure opstellen waarmee hij kan beoordelen of de technische en organisatorische maatregelen doeltreffend zijn.⁹⁶ Deze procedure moet de verantwoordelijke als beleid vastleggen.⁹⁷

2.2.2 De nieuwe rechten en plichten

De betrokkene krijgt onder de AVG twee nieuwe rechten toegekend: het recht van vergetelheid en het recht van dataportabiliteit. Naast het toekennen van rechten aan de betrokkene brengt de AVG ook meer plichten voor de verantwoordelijke en bewerker met zich mee.

2.2.2.1 Verwerkingsverantwoordelijke en verwerker

Op grond van de AVG zal de terminologie veranderen. De Wbp noemt degene die het doel en de middelen vaststelt de verantwoordelijke. Onder de AVG zal deze persoon 'verwerkingsverantwoordelijke' genoemd worden. De bewerker zal als verwerker worden gedefinieerd in de AVG. In dit rapport worden de huidige definities gehanteerd: verantwoordelijke en bewerker. In paragraaf 2.1.3.1 en 2.1.3.2 zijn de verplichtingen die de Wbp oplegt aan de verantwoordelijke en de bewerker behandeld. Deze gelden nog steeds op grond van de AVG. Echter, de AVG heeft meer verplichtingen gecreëerd voor deze twee actoren. De plichten van deze twee actoren worden gezamenlijk behandeld, omdat enkele plichten van de verantwoordelijke voortaan ook aan de bewerker worden opgelegd.

REGISTRATIEPLICHT

De verantwoordelijke is voortaan gehouden om een register bij te houden van zijn verwerkingsactiviteiten.⁹⁸ In dit register moeten de naam van de verantwoordelijke en zijn contactgegevens zijn vermeld. Tevens moeten de doeleinden van de gegevensverwerking benoemd worden en moet een beschrijving zijn gegeven van de soort persoonsgegevens en van de betrokkenen waarop de gegevens betrekking hebben. Ook moeten de ontvangers aan wie de persoonsgegevens worden verstrekt, benoemd worden en indien van toepassing ook de maatregelen die zijn genomen bij verstrekking aan een derde land. Als laatste moeten de termijnen aangegeven worden waarbinnen de gegevens worden gewist en moet er een beschrijving zijn gegeven van de technische en organisatorische beveiligingsmaatregelen.⁹⁹ De toezichthoudende autoriteiten hebben het recht om het register op te vragen en de verantwoordelijke is gehouden hieraan gehoor te geven.¹⁰⁰ Onder de AVG heeft niet elke verantwoordelijke deze verplichting. Indien het een onderneming betreft met minder dan 250 werknemers, is deze onderneming niet verplicht om een register van verwerkingsactiviteiten bij te houden. Deze uitzondering geldt echter niet als de verwerking een risico vormt voor de rechten en vrijheden van de betrokkene of zodra er bijzondere gegevens worden verwerkt.¹⁰¹ De AVG merkt op dat het gebruik van nieuwe technologieën een aanwijzing is dat de verwerking van persoonsgegevens een hoog risico met zich meebrengt.¹⁰² Omnichannel wordt als voorbeeld gegeven van een nieuwe technologie.¹⁰³

⁹⁵ Engelfriet, Meij & Kager 2017, p. 139.

⁹⁶ Art. 32 lid 1 sub d AVG jo. art. 5 lid 2 AVG.

⁹⁷ Engelfriet, Meij & Kager 2017, p. 140.

⁹⁸ Art. 30 lid 1 AVG.

⁹⁹ Art. 30 lid 1 sub a t/m g AVG.

¹⁰⁰ Art. 30 lid 4 AVG.

¹⁰¹ Art. 30 lid 5 AVG.

¹⁰² Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG algemene verordening gegevensbescherming (PbEU 2016, L 119/1), overweging 91

¹⁰³ M. Blijham, 'Maak werk van omnichannel', *retailwatching* 4 november 2014, retailwatching.nl.

De AVG legt de registratieplicht ook op aan de bewerker.¹⁰⁴ Ook dient de bewerker gehoor te geven aan het verzoek van de toezichthoudende autoriteit: hij moet desgevraagd het register ter beschikking stellen.¹⁰⁵

PRIVACY BY DESIGN

Tevens moet de verantwoordelijke op grond van de AVG meer technische en organisatorische maatregelen nemen ter bescherming van de persoonlijke levenssfeer van de betrokkene. Privacy by design dient de standaard te worden bij elke gegevensverwerking. Privacy by design is met name van toepassing bij de ontwikkeling van nieuwe producten of diensten.¹⁰⁶ Door privacy by design toe te passen, wordt voorafgaand aan de gegevensverwerking aandacht besteed aan de bescherming van de rechten en vrijheden van de betrokkene.¹⁰⁷ Deze aandacht moet uitmonden in privacyverhogende maatregelen, ofwel privacy enhancing technologies (PET).¹⁰⁸ Daarnaast houdt privacy by design in dat de verantwoordelijke ervoor zorg draagt dat er zo min mogelijk gegevens verwerkt worden – ook wel dataminimalisatie genoemd – bij het verwezenlijken van de doeleinden.¹⁰⁹

PRIVACY BY DEFAULT

Privacy by default hangt nauw samen met privacy by design.¹¹⁰ Waar het bij privacy by design draait om het nemen van maatregelen voorafgaand aan de verwerking, draait het er bij privacy by default om dat de systeeminstellingen maximale privacyveiligheid bieden.¹¹¹ Bij privacy by default verstrekken de gebruikers van een product of dienst zelf hun persoonsgegevens. Privacy by default legt organisaties de plicht op om de media waarop hun gebruikers hun persoonsgegevens verstrekken en delen op de privacyvriendelijkste stand te zetten.¹¹² Gedacht kan worden aan bijvoorbeeld wachtwoorden, virusscanners, privacyvriendelijke algemene voorwaarden, enzovoort.¹¹³

Hierboven is besproken dat de verantwoordelijke moet voldoen aan het beginsel van privacy by design en privacy by default. De beoordeling of voldaan is aan deze twee beginselen is overgelaten aan de bewerker. Deze moet beoordelen of er voldoende technische en organisatorische maatregelen genomen zijn met inachtneming van het doel en de omvang van de gegevensverwerking.¹¹⁴ Naast het beoordelen of deze maatregelen voldoende zijn, moet de bewerker voortaan zelf dergelijke maatregelen nemen.¹¹⁵ Volgens de AVG mag de verantwoordelijke immers alleen een bewerker inschakelen die voldoende technische en organisatorische maatregelen heeft genomen.¹¹⁶

PRIVACY IMPACT ASSESSMENT

Ook zal de verantwoordelijke onder de AVG gehouden zijn om in bepaalde gevallen een Privacy Impact Assessment (PIA) uit te voeren. Een PIA is een gegevenseffectbeoordeling. Bij deze beoordeling wordt gekeken naar de privacyrisico's waaraan de betrokkene wordt blootgesteld door de gegevensverwerking en wat de

¹⁰⁴ Art. 30 lid 2 AVG.

¹⁰⁵ Art. 30 lid 4 AVG.

¹⁰⁶ D. The, 'Privacy by Default: wat houdt het in en welke impact kan het hebben op een organisatie?', *privacycompany* 6 december 2016, [privacycompany.eu](https://www.privacycompany.eu).

¹⁰⁷ Art. 25 lid 1 AVG.

¹⁰⁸ 'Privacy by design', *autoriteitpersoonsgegevens* z.j., autoriteitpersoonsgegevens.nl.

¹⁰⁹ 'Privacy by design', *autoriteitpersoonsgegevens* z.j., autoriteitpersoonsgegevens.nl.

¹¹⁰ Art. 25 lid 1 AVG.

¹¹¹ 'Privacy by Default', *justitia* z.j., justitia.nl.

¹¹² D. The, 'Privacy by Default: wat houdt het in en welke impact kan het hebben op een organisatie?', *privacycompany* 6 december 2016, [privacycompany.eu](https://www.privacycompany.eu).

¹¹³ 'Privacy by Default', *justitia* z.j., justitia.nl.

¹¹⁴ 'De Algemene Verordening Gegevensbescherming', *home.kpmg* 1 juli 2016, home.kpmg.be.

¹¹⁵ Art. 32 lid 1 AVG.

¹¹⁶ Art. 28 lid 1 AVG.

gevolgen zijn van deze privacyrisico's. De beoordeling draagt ook bij aan het vermijden of verminderen van privacyrisico's.¹¹⁷ Indien uit de PIA blijkt dat de verwerking hoge privacyrisico's met zich meebrengt, is de verantwoordelijke gehouden om passende maatregelen te treffen om ervoor te zorgen dat de persoonlijke levenssfeer van de betrokkene alsnog gewaarborgd blijft ondanks de geconstateerde risico's.¹¹⁸ Een PIA moet onder andere uitgevoerd worden zodra de verwerking hoge privacyrisico's met zich meebrengt gelet op de aard, de omvang, de context en de doeleinden van de gegevensverwerking.¹¹⁹ De vraag die rijst naar aanleiding van deze formulering is wanneer een gegevensverwerking, gelet op de aard, omvang, context en doeleinden, aanzienlijke privacyrisico's met zich meebrengt. Om tegemoet te komen aan deze onzekerheid, verplicht de AVG de nationale toezichthoudende autoriteiten om een lijst op te stellen met situaties waarbij een PIA overeenkomstig deze algemene grond verplicht is.¹²⁰

Daarnaast schrijft de AVG in drie gevallen een PIA verplicht voor. Ten eerste is een PIA verplicht indien de persoonsgegevens van een persoon gebruikt worden om een besluit te nemen en dit besluit rechtsgevolgen met zich meebrengt voor de betrokkene. Het besluit moet gebaseerd zijn op een analyse van de persoonlijke aspecten van de natuurlijke persoon, waarbij de analyse tot stand is gekomen door middel van onder andere profilering.¹²¹ Ten tweede is een PIA verplicht wanneer er op grote schaal bijzondere persoonsgegevens verwerkt worden.¹²² Ten derde is een PIA verplicht als er sprake is van stelselmatig en grootschalig cameratoezicht in openbare ruimten.¹²³

Aan de PIA worden eisen gesteld.¹²⁴ De verantwoordelijke dient een beschrijving op te leveren van de verwerkingsdoeleinden en een systematische beschrijving van de beoogde verwerkingen. Bij het opstellen van deze beschrijvingen dienen ook de eventuele gerechtvaardigde belangen van de verantwoordelijke opgenomen te worden die door de verwerking worden behartigd.¹²⁵ Daarnaast is de verantwoordelijke gehouden de noodzaak en de evenredigheid van de verwerking te vermelden in relatie tot de geformuleerde doeleinden.¹²⁶ Net zoals bij de beoordeling of het gerechtvaardigd belang van de verantwoordelijke prevaleert boven dat van de betrokkene, dient de verantwoordelijke bij een PIA ook rekening te houden met de rechten en vrijheden van de betrokkene. De verantwoordelijke moet immers de risico's beoordelen die de gegevensverwerking met zich meebrengt voor de rechten en vrijheden van de betrokkene.¹²⁷ Als laatste moet de verantwoordelijke een beschrijving opleveren van de beoogde maatregelen om de risico's voor de rechten en vrijheden van de betrokkene te beperken.¹²⁸ Bij het uitvoeren van een PIA is de verantwoordelijke verplicht om advies in te winnen bij de functionaris gegevensbescherming (FG).¹²⁹ Indien uit de PIA blijkt dat de gegevensverwerking een hoog risico met zich meebrengt voor de rechten en vrijheden van de betrokkene, is de verantwoordelijke gehouden om de toezichthoudende autoriteit te raadplegen voorafgaand aan de verwerking.¹³⁰

¹¹⁷ P. Lammerts, 'Privacy Impact Assessment', *ensie* 20 juli 2016, ensie.nl.

¹¹⁸ Berkvens & Jakimowicz 2016, p. 92.

¹¹⁹ Art. 35 lid 1 AVG.

¹²⁰ Art. 35 lid 4 AVG.

¹²¹ Art. 35 lid 3 sub a AVG.

¹²² Art. 35 lid 3 sub b AVG.

¹²³ Art. 35 lid 3 sub c AVG.

¹²⁴ Art. 35 lid 7 AVG.

¹²⁵ Art. 35 lid 7 sub a AVG.

¹²⁶ Art. 35 lid 7 sub b AVG.

¹²⁷ Art. 35 lid 7 sub c AVG.

¹²⁸ Art. 35 lid 7 sub d AVG.

¹²⁹ Art. 35 lid 2 AVG.

¹³⁰ Art. 36 lid 1 AVG.

UITGEBREIDERE INFORMATIEPLICHT

De verantwoordelijke heeft onder de Wbp een informatieplicht ten aanzien van de betrokkene. Deze informatieplicht is onder de AVG uitgebreider. De verantwoordelijke moet zijn identiteit bekendmaken. Ook moet hij de contactgegevens van de FG vermelden. Tevens moet hij aangeven wat de verwerkingsdoeleinden zijn. Daarnaast moet het belang (indien de verwerking gebaseerd is op het gerechtvaardigd belang van de verantwoordelijke) worden aangegeven. Als de verantwoordelijke de persoonsgegevens verstrekt, moet hij vermelden wie de ontvangers zijn. Als laatste moet de verantwoordelijke aangeven of hij de intentie heeft om de persoonsgegevens te verstrekken aan een derde land.¹³¹

FUNCTIONARIS GEGEVENS BESCHERMING

De AVG verplicht organisaties in drie situaties om een FG aan te stellen. Als gegevens verwerkt worden door een overheidsinstantie of -orgaan is het verplicht om een FG aan te stellen.¹³² Daarnaast moet een FG aangewezen worden als een organisatie voor de gegevensverwerking op regelmatige basis en op grote schaal overgaat tot observatie van de betrokkenen.¹³³ Als laatste is het verplicht om een FG aan te wijzen indien er bijzondere persoonsgegevens worden verwerkt.¹³⁴ Desondanks staat het organisaties vrij om een FG aan te wijzen wanneer dit niet wettelijk verplicht is.¹³⁵

De bewerker zal in de drie verplichte situaties die hierboven zijn besproken ook verplicht zijn om een FG aan te wijzen. Indien zich geen van deze situaties voordoet, is de bewerker vrij om op vrijwillige basis een FG aan te wijzen.¹³⁶

De tweede situatie kan de vraag oproepen wanneer gesproken kan worden van een observatie op grote schaal en op regelmatige basis. De Groep gegevensbescherming artikel 29 (Artikel 29-werkgroep) geeft daar meer duidelijkheid over. Bij de vraag wanneer sprake is van observatie op grote schaal kan gelet worden op vier factoren. Allereerst is het aantal betrokkenen dat wordt geobserveerd van belang. Daarnaast moet gelet worden op de hoeveelheid gegevens die wordt verwerkt en de duur van deze verwerking. Als laatste is de geografische reikwijdte van belang.¹³⁷

‘Regelmatige en stelselmatige observatie’ wordt niet gedefinieerd in de AVG. Daarentegen wordt in de AVG wel gesproken over het ‘monitoren van het gedrag van betrokkenen’. Als voorbeeld voor het monitoren van het gedrag van betrokkenen wordt in de AVG gegeven: het gebruik van het surfgedrag van personen bij het profileren.¹³⁸ Dit is dan ook een van de voorbeelden die de Artikel 29-werkgroep geeft voor het regelmatig en stelselmatig observeren.¹³⁹

Een FG vervult een belangrijke rol. Indien door de organisatie een FG is aangewezen, is de organisatie gehouden om voorafgaand aan een PIA advies in te winnen bij de FG.¹⁴⁰ Naast het desgevraagd verstrekken van advies over de PIA dient de FG ook toezicht uit te oefenen op de uitvoering van de PIA.¹⁴¹ De FG geeft advies of er een PIA uitgevoerd

¹³¹ Art. 13 lid 1 jo. art. 14 lid 1 AVG.

¹³² Art. 37 lid 1 sub a AVG.

¹³³ Art. 37 lid 1 sub b AVG.

¹³⁴ Art. 37 lid 1 sub c AVG.

¹³⁵ Art. 37 lid 4 AVG.

¹³⁶ Art. 37 lid 1 AVG.

¹³⁷ Richtlijnen voor functionarissen voor de gegevensbescherming (FG's) van de Artikel- 29 Werkgroep, p.6.

¹³⁸ Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG algemene verordening gegevensbescherming (PbEU 2016, L 119/1), overweging 24

¹³⁹ Richtlijnen voor functionarissen voor de gegevensbescherming (FG's) van de Artikel- 29 Werkgroep, p.7.

¹⁴⁰ Art. 35 lid 2 jo. art. 39 lid 1 sub c AVG.

¹⁴¹ Art. 39 lid 1 sub c AVG.

moet worden, op welke manier deze PIA het beste kan plaatsvinden, of de PIA door een intern of extern persoon moet worden uitgevoerd en welke waarborgen er gesteld moeten worden bij de PIA. Tot slot beoordeelt de FG of de PIA goed is uitgevoerd en of de resultaten aantonen dat er voldaan is aan de AVG. Het advies van de FG is niet bindend. Als wordt afgeweken van het advies, is de verantwoordelijke gehouden om de beweegredenen hiervoor schriftelijk te verklaren in de documentatie van de PIA.¹⁴²

In paragraaf 2.2.1.4 zijn de nieuwe beveiligingsmaatregelen behandeld die de AVG voorschrijft. De AVG verplicht onder andere dat er een procedure, die is vastgelegd in een beleid, wordt opgesteld, om te beoordelen of de maatregelen technisch en organisatorisch doeltreffend zijn. Bij het opstellen van dit beleid moet de FG zijn betrokken.¹⁴³

2.2.2.2 Nieuwe rechten van de betrokkene

De rechten van de betrokkene uit de Wbp (paragraaf 2.1.3.3) komen aan de betrokkene ook toe op grond van de AVG. De AVG kent de betrokkene daarnaast twee nieuwe rechten toe: het recht op vergetelheid en het recht op dataportabiliteit.

HET RECHT OP VERGETELHEID

De betrokkene heeft het recht om de verantwoordelijke te verzoeken zijn persoonsgegevens te wissen zonder opgaaf van redenen: het recht op vergetelheid.¹⁴⁴ Dit recht werd in het Google/Agencia Española-arrest geïntroduceerd door het Hof van Justitie van de Europese Unie (HvJEU). Het HvJEU heeft in het genoemde arrest bepaald dat dit recht ook geldt onder de huidige Richtlijn 95/46/EG.¹⁴⁵ Dit recht komt aan de betrokkene toe wanneer zijn persoonsgegevens niet langer bewaard hoeven te blijven voor de doeleinden waarvoor zij zijn verzameld dan wel verwerkt.¹⁴⁶ Ook heeft de betrokkene dit recht wanneer hij zijn toestemming voor de verwerking intrekt.¹⁴⁷ Tevens kan dit recht uitgeoefend worden als de betrokkene bezwaar maakt tegen de gegevensverwerking en de verantwoordelijke geen prevalerende, gerechtvaardigde gronden kan aanvoeren.¹⁴⁸ Daarnaast komt de betrokkene dit recht toe indien zijn persoonsgegevens onrechtmatig zijn verwerkt.¹⁴⁹ Als laatste komt dit recht de betrokkene toe wanneer de gegevens zijn verzameld ten behoeve van diensten van informatiemaatschappijen of als de verwerking in strijd zou zijn met een nationale of Europese rechtsregel.¹⁵⁰

HET RECHT VAN DATAPORTABILITEIT

Daarnaast heeft de betrokkene onder de AVG het recht van dataportabiliteit toegekend gekregen.¹⁵¹ Dit recht houdt in dat de betrokkene de verantwoordelijke kan verzoeken om de hem betreffende persoonsgegevens op een machineleesbaar en interoperabel formaat te verkrijgen, waarbij de gegevens gestructureerd zijn.¹⁵² Om een beroep te doen op dit recht, dient de gegevensverwerking te berusten op een toestemming van de betrokkene of plaats te vinden uit hoofde van een overeenkomst.¹⁵³ Daarnaast moet de gegevensverwerking geautomatiseerd zijn.¹⁵⁴ Doordat dit recht aan de betrokkene is toegekend, wordt met dit recht ook impliciet een plicht opgelegd aan de verantwoordelijke.

¹⁴² Richtlijnen voor functionarissen voor de gegevensbescherming (FG's) van de Artikel- 29 Werkgroep, p.17.

¹⁴³ Engelfriet, Meij & Kager 2017, p. 140.

¹⁴⁴ Art. 17 lid 1 AVG.

¹⁴⁵ HvJ EU 13 mei 2014, C-131/12, ECLI:EU:C:2014:317 (Google/Agencia Española).

¹⁴⁶ Art. 17 lid 1 sub a AVG.

¹⁴⁷ Art. 17 lid 1 sub b AVG.

¹⁴⁸ Art. 17 lid 1 sub c AVG.

¹⁴⁹ Art. 17 lid 1 sub d AVG.

¹⁵⁰ Art. 17 lid 1 sub e en sub f AVG.

¹⁵¹ Art. 20 lid 1 AVG.

¹⁵² Berkvens & Jakimowicz 2016, p. 65.

¹⁵³ Art. 20 lid 1 sub a AVG.

¹⁵⁴ Art. 20 lid 1 sub b AVG.

Deze dient nu immers interoperabele formaten te ontwikkelen om gegevensoverdraagbaarheid mogelijk te maken.¹⁵⁵

2.3 Telecommunicatiewet

In deze paragraaf wordt stilgestaan bij het cookie-artikel. Tracking cookies worden ingezet om op internet het klik- en surfgedrag van personen te volgen om vervolgens te kunnen profileren.¹⁵⁶ Nu tracking cookies van belang zijn voor het profileren, is het noodzakelijk om te weten welke eisen de wet stelt aan het plaatsen van deze cookies.

2.3.1 Tracking cookies

Er zijn drie soorten cookies: analytische, functionele en tracking cookies. Voor het plaatsen van analytische en functionele cookies hoeft geen toestemming gevraagd te worden.¹⁵⁷ Voor het plaatsen van tracking cookies stelt de Tw twee voorwaarden: degene die deze cookies plaatst heeft een informatieplicht en dient toestemming te hebben van de betrokkene.

2.3.1.1 Tracking cookies: informatieplicht

De verantwoordelijke heeft een informatieplicht jegens de betrokkene bij het plaatsen van tracking cookies.¹⁵⁸ In de MvT van de cookiewet wordt verwezen naar opinie 2/2010 van de Artikel 29-werkgroep. De Artikel 29-werkgroep heeft in de desbetreffende opinie aangegeven waaruit deze informatieoverdracht moet bestaan. De betrokkene moet geïnformeerd worden over degene die de cookies plaatst en vervolgens beschikking krijgt over de verzamelde gegevens. Ook moet de betrokkene erop gewezen worden dat de geplaatste cookies tot doel hebben om een profiel op te stellen van hem, op basis van zijn surfgedrag op de website. Om dit profiel op te stellen, worden persoonsgegevens van de betrokkene verzameld. De betrokkene moet weten welke persoonsgegevens dit precies zijn. Als laatste moet de betrokkene geïnformeerd worden of de opgestelde profielen worden gebruikt voor het sturen van gerichte aanbiedingen.¹⁵⁹ De verstrekte informatie moet duidelijk, zichtbaar en niet misleidend zijn.¹⁶⁰

2.3.1.2 Tracking cookies: toestemming

Als tweede eis wordt gesteld dat de betrokkene toestemming moet verlenen voor het plaatsen van tracking cookies.¹⁶¹ In de Tw wordt voor de definitie van 'toestemming' verwezen naar de Wbp.¹⁶² De Wbp eist dat de toestemming ondubbelzinnig is. Volgens de Tw dient in beginsel de toestemming voor het plaatsen van cookies niet ondubbelzinnig te zijn.¹⁶³ De Wbp is immers van toepassing op het verwerken van persoonsgegevens. Echter, in de Tw is bepaald dat bij tracking cookies wordt vermoed dat er sprake is van het verwerken van persoonsgegevens. Als gevolg van dit vermoeden dient de toestemming ondubbelzinnig te zijn.¹⁶⁴

Om te voorkomen dat er twijfel rijst over de wilsuiting van de betrokkene, dient de toestemming afgeleid te worden uit een handeling. Met andere woorden: het uitblijven van

¹⁵⁵ Berkvens & Jakimowicz 2016, p. 65.

¹⁵⁶ Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG algemene verordening gegevensbescherming (PbEU 2016, L 119/1), overweging 30

¹⁵⁷ 'Cookies', acm z.j., acm.nl.

¹⁵⁸ Art. 11.7a lid 1 sub a Tw.

¹⁵⁹ Opinie van Groep Gegevensbescherming Artikel 29 nr. 2 van 2010, p.24.

¹⁶⁰ Kamerstukken II 2013/14, 33902, 3, p.13 (MvT).

¹⁶¹ Art. 11.7a lid 1 sub b Tw.

¹⁶² Kamerstukken II 2013/14, 33902, 3, p.13 (MvT).

¹⁶³ Kamerstukken II 2013/14, 33902, 3, p.14 (MvT).

¹⁶⁴ Art. 11.7a lid 4 Tw.

een handeling kan niet aangemerkt worden als een toestemming.¹⁶⁵ Het aanklikken van een button waarmee toestemming wordt gegeven voor het plaatsen van tracking cookies, wordt aangemerkt als een ondubbelzinnige toestemming. Het is een misverstand dat de toestemming bij het plaatsen van tracking cookies pas geacht wordt aanwezig te zijn na het aanklikken van een button waarmee toestemming wordt verleend. Het geven van toestemming voor het plaatsen van tracking cookies kan ook worden aangenomen zodra de websitebezoeker andere onderdelen van de website raadpleegt. De websitebezoeker dient echter, zodra hij op de desbetreffende website komt, duidelijk en volledig geïnformeerd te zijn alvorens hij doorsurft. Wordt de websitebezoeker bij het eerste bezoek niet volledig en duidelijk geïnformeerd over het gebruik van tracking cookies en blijft hij doorsurfen op de website, dan kan hieruit geen toestemming worden afgeleid.¹⁶⁶

Resumerend is duidelijk geworden onder welke voorwaarden persoonsgegevens verwerkt mogen worden onder de Wbp en in de toekomst onder de AVG. De Wbp zal in mei 2018 vervangen worden door de AVG. Dit brengt veel wijzigingen met zich mee. Uit de besproken wijzigingen valt af te leiden dat de AVG meer plichten zal opleggen aan de verantwoordelijke en de bewerker en dat er striktere regels gesteld zullen worden aan de verwerking van persoonsgegevens. Daarbij krijgt de betrokkene twee nieuwe rechten toegekend. Als laatste is een blik geworpen op de Tw die regels geeft voor het gebruik van cookies. In het volgende hoofdstuk wordt de praktijk in kaart gebracht.

¹⁶⁵ *Kamerstukken II 2013/14, 33902, 3, p.13 (MvT).*

¹⁶⁶ *Kamerstukken II 2013/14, 33902, 3, p.14 (MvT).*

Hoofdstuk 3 De werkwijze van FYN

Inleiding

In dit hoofdstuk wordt de praktijk in kaart gebracht. Allereerst wordt kort stilgestaan bij de dienstverlening die FYN biedt. Vervolgens wordt het omnichannelsysteem besproken. Het is van belang om te weten hoe dit systeem functioneert, omdat er duidelijkheid dient te bestaan over hoe de persoonsgegevens door middel van dit systeem verzameld worden. Vervolgens wordt besproken voor welke doeleinden de gegevens momenteel worden verzameld, welke handelingen FYN nu precies verricht met betrekking tot de verzamelde persoonsgegevens en welke programma's FYN gebruikt voor de verwerking van persoonsgegevens. Het is van belang om dit in kaart te brengen, omdat in het volgende hoofdstuk getoetst wordt of de verwerking van persoonsgegevens rechtmatig plaatsvindt. Naderhand wordt specifiek aandacht besteed aan het profileren voor marketingdoeleinden. De persoonlijkheidsprofielen zullen immers in de vorm van statistieken aan de leveranciers van de retailers worden verstrekt voor marketingdoeleinden. Ten behoeve van dit hoofdstuk zijn de heer Hazelhof (bijlage I) en de heer Sanderse (bijlage II) geïnterviewd.

3.1 FYN dienstverlening

FYN verleent IT-diensten. In deze paragraaf wordt besproken waaruit de dienstverlening van FYN bestaat en aan wie deze diensten worden verleend.

FYN verleent onder andere IT-diensten aan retailers. FYN richt zich voornamelijk op de kleinere winkelketens. Deze kunnen aangemerkt worden als een middelgroot of klein bedrijf en zijn gevestigd in Nederland en België. De kernactiviteiten van FYN bestaan uit het ontwikkelen van kassasoftware: het Point of Sale (POS)-softwareprogramma. FYN verkoopt het POS-softwareprogramma aan de retailers. Naderhand blijft FYN de retailers ondersteunen op technisch gebied en zorgt FYN voor het installatieonderhoud en het netwerkbeheer van het systeem. Bij de POS-software zijn ook een tablet, kiosk en narrowcasting inbegrepen.

Narrowcasting is bedoeld om klanten, voordat zij de goederen of genoten diensten afrekenen, alsnog te verleiden om meer aankopen te doen. Dit gebeurt door het plaatsen van kleine schermen bij de kassa waarop aanbiedingen worden weergegeven, met de bedoeling de consument te prikkelen meer aan te schaffen. De kiosk is een bestelzuil die klanten zelf kunnen bedienen. De klant kan zonder tussenkomst van personeel bestellingen plaatsen en deze vervolgens een paar dagen later kan ophalen. De tablet is een mobiel kassasysteem. Een normaal kassasysteem zit vast aan de kassabalie, maar door deze tablet is het mogelijk om met de klant de winkel door te lopen en producten te scannen zonder gebruik te hoeven maken van de kassabalie.

Naast het ontwikkelen en verkopen van de POS-software en het verzorgen van installatieonderhoud en netwerkbeheer, ontwikkelt FYN ook hardware. Deze hardware bestaat uit handscanners en bonprinters, als aanvulling op het POS-softwarepakket. Dit betekent dat FYN alles levert wat een retailer nodig heeft om een winkel draaiende te kunnen houden, van software tot hardware.

Tot slot levert FYN ook e-mailhosting aan de retailers. De retailers versturen mailings met aanbiedingen aan hun eigen klanten. Deze mailings worden door FYN opgesteld en vervolgens verstuurd naar de klanten van de retailer.

FYN heeft momenteel geen enkele overeenkomst met de retailers afgesloten. Aan de relatie tussen FYN en de retailers ligt ook geen bewerkersovereenkomst ten grondslag. Er

is slechts sprake van een mondelinge koopovereenkomst. Het enige wat op schrift is gesteld, is de factuur die FYN aan de retailers stuurt nadat deze klant zijn geworden en gebruik gaan maken van de diensten van FYN.

3.2 Omnichannelsysteem

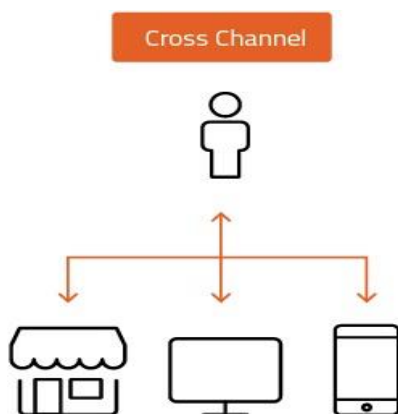
In deze paragraaf wordt het omnichannelsysteem besproken waarmee FYN werkt. Het POS-softwareprogramma is een uitwerking van dit systeem. Er wordt beschreven hoe dit systeem werkt en hoe het ervoor zorgt dat de gegevens worden verzameld.

Het omnichannelsysteem zorgt ervoor dat er data wordt verzameld. Het systeem is immers een overkoepelend geheel voor alle media waaruit de gegevens worden verzameld. Deze verschillende media zijn bijvoorbeeld het klik- en surfgedrag, social media, geregistreerde aankopen in de winkel, ingelogde klanten op het webportaal, gegevens die zijn geregistreerd door het gebruik van de tablets en kiosken, etcetera. Het omnichannelsysteem is een naam voor alle genoemde kanalen, omdat door het gebruik van dit systeem de data uit alle verschillende kanalen die gekoppeld zijn aan de database, worden verzameld en opgeslagen in één database. De manier waarop dit systeem door FYN wordt gebruikt kent twee voordelen. Ten eerste wordt bij het omnichannelsysteem alles in één database opgeslagen. De afbeelding hiernaast (FYN Software, z.j.) illustreert dit. Dit lijkt niet uniek te zijn, omdat in de maatschappij de gedachte heerst dat het overgrote deel van de commerciële bedrijven een dergelijk systeem gebruikt om big data te verzamelen. Deze gedachte klopt echter niet. Een tweede voordeel van dit systeem is dat FYN in staat is om diensten online aan te bieden.



3.2.1 Één database

Concurrerende IT-bedrijven geven op hun websites een verkeerde weergave van de werkwijze die zij hanteren. Daardoor lijkt het alsof zij ook één database hebben, dat alle data in deze database terechtkomen en alles vanuit één dashboard wordt bestuurd. Achter de schermen werken zij echter met de zogenoemde 'eilanden'. Bij dit 'eilandensysteem' worden gegevens in verschillende databases verzameld. Zo is er sprake van een database die gegevens verzamelt via social media, een andere database verzamelt gegevens die geregistreerd worden door middel van het klik- en surfgedrag, de derde database slaat gegevens op die geregistreerd zijn bij verkoop, enzovoort. Het 'eilandensysteem' is vergelijkbaar met het cross-channelsysteem. Zie de afbeelding (FYN Software, z.j.) hiernaast ter illustratie.



De concurrenten koppelen de gegevens in de databases achteraf, waardoor het lijkt alsof alle gegevens in één database worden opgeslagen. FYN heeft de POS-software daarentegen zo ontwikkeld dat het daadwerkelijk mogelijk wordt dat de data die uit verschillende kanalen verzameld worden in één database terechtkomen, zonder dat achteraf koppeling van de verzamelde data nodig is.

3.2.2 Online dienstverlening

Een tweede voordeel van het omnichannelsysteem van FYN is, dat FYN zijn diensten online aanbiedt. Als er een technisch probleem is, kunnen de medewerkers van FYN

daardoor achter de schermen in het systeem om het probleem op te lossen. Hierdoor lopen klanten minder risico dat de verzamelde data verloren gaan. De werkwijze van de concurrenten brengt meer risico's met zich mee, omdat zij service op locatie bieden. Doordat FYN de diensten online aanbiedt, is de kans nihil dat data verloren gaan. Er is immers sprake van één databaseserver, die alle gegevens online opslaat. Naast de server heeft FYN ook een replicatie ontwikkeld. Deze dient ertoe om kopieën te maken van de hoofdservers. Mocht er iets gebeuren met de hoofdservers, dan zijn de data niet verloren, aangezien de replicatie alles heeft opgeslagen. Tot slot worden er back-ups gemaakt. Op de back-ups wordt in uitzonderlijke situaties teruggevallen. Bij een back-up gaan enige data verloren, omdat een back-up om de zoveel tijd wordt gemaakt. Deze back-up dienen de werknemers bij FYN telkens zelf op te vragen en op te slaan. De concurrenten van FYN laten hun klant echter een hoofdservers aanschaffen. Deze wordt in het pand van de klant zelf geplaatst. Als dit pand wordt overvallen waarbij de hoofdservers wordt ontvreemd, of als er sprake is van blikseminslag en stroomuitval, zijn alle data verloren. Dit risico ontstaat door de werkwijze van de concurrenten van FYN. FYN vermijdt dit risico, doordat het beheer en onderhoud van het omnichannelsysteem online plaatsvindt.

3.3 FYNE gegevensverwerking

In deze paragraaf wordt de gegevensverwerking in kaart gebracht. Allereerst worden de programma's besproken die FYN gebruikt bij diverse handelingen met betrekking tot de persoonsgegevens. Vervolgens wordt gekeken hoe de persoonsgegevens worden verzameld. Ook wordt besproken wie inzage heeft in deze gegevens en welke handelingen FYN verricht met betrekking tot de verzamelde persoonsgegevens. Als laatste wordt bekeken hoe het profileren zal plaatsvinden.

3.3.1 Programma's voor de gegevensverwerking

FYN gebruikt de volgende vijf programma's voor het verwerken van persoonsgegevens: Connect, Toolkit, PhpMyAdmin, Notepad++ en het POS-softwareprogramma. Connect, Toolkit en POS-software heeft FYN zelf ontwikkeld. De overige twee programma's zijn door derden ontwikkeld.

Connect is een programma dat FYN vaak gebruikt, met name om mailings te sturen ten behoeve van de retailers. Zoals gezegd blijft FYN de retailers na aanschaf van het softwarepakket ondersteunen en IT-diensten bieden. Het versturen van mailings hoort bij deze dienstverlening. FYN heeft Connect zelf ontwikkeld en daardoor kan dit programma contact maken met de database van de retailer. In deze database zijn immers alle klantdata verzameld en deze data zijn nodig voor de direct mailing. Zodra de retailer de eisen waaraan de mailing moet voldoen heeft doorgegeven aan FYN, voert een van de medewerkers die toegang heeft tot het systeem de desbetreffende criteria in. Connect verwerkt deze criteria, haalt de data uit de database en verstuurt de mailing aan de klanten van de retailer.

Toolkit wordt ook gebruikt om gegevens te verwerken. Met dit programma worden de gegevens van de retailers (de klanten van FYN) zelf verwerkt. Het programma wordt gebruikt zodra FYN een nieuwe klant heeft geworven. Voor deze klant moet met het Toolkit-programma een database worden aangemaakt. Ook wordt het programma gebruikt voor handelingen die FYN verricht met betrekking tot de verzamelde persoonsgegevens, bijvoorbeeld het wijzigen van door de retailer fout ingevoerde persoonsgegevens. Als de retailer constateert dat hij de gegevens van een grote hoeveelheid klanten verkeerd heeft ingevoerd, verbetert FYN deze fouten achter de schermen. Hierbij wordt in het programma Toolkit aangegeven wat de fout precies is en waardoor de fout vervangen moet worden. Het programma voert de opdracht vervolgens uit en brengt de wijzigingen aan in de persoonsgegevens.

PhPMyAdmin is een tool om de databasestructuur in te zien. Hiermee is het mogelijk om alles in te zien wat door de retailers in de database is opgeslagen. Dit programma gebruikt FYN wanneer er een technisch probleem is dat op afstand moet worden opgelost. Om te achterhalen waar het probleem zich bevindt, moet FYN immers toegang hebben tot de database.

Notepad++ is vergelijkbaar met het gewone kladblok Notepad. Notepad++ is een geavanceerde versie die alleen door ICT'ers wordt gebruikt. Het programma wordt in beginsel niet gebruikt voor gegevensverwerking, maar alleen om een kleine hoeveelheid data uit het programma PhPMyAdmin te converteren.

Tot slot wordt het POS-softwareprogramma gebruikt voor gegevensverwerking. De POS-software is de 'voorkant' van de database. Deze software slaat de persoonsgegevens op die de retailers uit verschillende kanalen verzamelen.

3.3.2 Wijze van verzamelen

De persoonsgegevens kunnen door de retailer en door zijn klant (de consument) in de database ingevoerd worden. Ten eerste kunnen de retailers zelf de persoonsgegevens registreren, bij het voltooien van een transactie. De persoonsgegevens worden dan ter plekke ingevuld en opgeslagen in de database. De volgende vijf persoonsgegevens worden bij een transactie opgeslagen: de naam, het adres, de woonplaats, het telefoonnummer en het e-mailadres.

Ten tweede kunnen de consumenten zelf de persoonsgegevens in de database opslaan. Elke retailer heeft zijn eigen website. Consumenten kunnen daarop een eigen account aanmaken en inloggegevens krijgen. Zij loggen vervolgens in op het klantenportaal om bijvoorbeeld hun bestelstatus in te zien of om producten te bestellen. Bij het bestellen van producten worden de persoonsgegevens door de consumenten zelf ingevuld. De gegevens die de consumenten zelf invullen komen in dezelfde database terecht als de overige data. De website is immers een onderdeel van het softwarepakket dat door FYN wordt aangeboden aan de retailers. Als consumenten op de website inloggen en persoonsgegevens achterlaten, dan loggen zij in feite in op de database en registreert de database de persoonsgegevens ook op de server.

De verzamelde persoonsgegevens worden oneindig in het omnichannelsysteem bewaard: als data eenmaal opgeslagen zijn in de database, blijven ze oneindig beschikbaar. De verzamelde data kunnen momenteel alleen door de retailers zelf worden verwijderd. FYN heeft geen softwareprogramma ontwikkeld dat in staat is om de database te zijner tijd op te schonen. In de toekomst wil FYN een dergelijk programma wel ontwikkelen, met name omdat een potentiële klant hier vraag naar heeft.

De retailers hebben voor de gegevensverwerking twee doeleinden geformuleerd. Ten eerste worden de gegevens verzameld voor direct marketing. De direct marketing bestaat uit het versturen van mailings aan consumenten. De retailer geeft aan waar de inhoud van de mailing aan moet voldoen. De medewerkers van FYN verschaffen zich vervolgens met toestemming van de retailer toegang tot het systeem en stellen een mailing op volgens de criteria van de retailer. De mailing wordt dan verstuurd vanuit de mailserver van de retailer.

Voor de gegevensverwerking ten behoeve van direct marketing vragen de retailers expliciet toestemming aan de consumenten. De retailers kunnen, afhankelijk van de situatie, op twee manieren toestemming krijgen voor het genereren van persoonsgegevens voor dit doeleinde. Allereerst kan de consument zich via het webportaal registreren en daarmee inloggegevens krijgen. Bij deze registratie is er een hokje dat aangevinkt moet worden. Met het aanvinken van het hokje wordt

toestemming gegeven om de persoonsgegevens te gebruiken voor marketingdoeleinden.

Wanneer er aankopen worden gedaan in de winkel en de retailer de persoonsgegevens noteert om de transactie te voltooien, verschijnt er een pop-up op zijn scherm. Deze pop-up waarschuwt de retailer dat hij de klant moet vragen of de retailer de persoonsgegevens van zijn klant mag verwerken voor direct marketing. Als de retailer toestemming heeft gekregen, vinkt hij het hokje op zijn scherm aan en wordt in de database geregistreerd dat deze klant benaderd wil worden met gerichte aanbiedingen.

De klanten die niet benaderd willen worden met aanbiedingen staan in het systeem geregistreerd. Deze klanten hebben dan het hokje op de webshop niet aangevinkt of hebben in de winkel geen toestemming aan de retailer gegeven. Wanneer er een mailing naar de consumenten uitgaat, worden de consumenten die hiertegen bezwaar hebben door het programma Connect automatisch uitgefilterd.

Ten tweede is het doel van de retailer dat de gegevensverwerking geschiedt ten behoeve van efficiëntie. Het is voor de retailer van belang dat hij voor zijn eigen boekhouding een overzicht heeft van de transacties. Behalve voor deze twee doeleinden worden de data niet voor overige doeleinden gebruikt. Ook de middelen worden door de retailers vastgesteld. FYN heeft alleen inspraak bij het aanwijzen van middelen op technisch en organisatorisch gebied.

3.3.3 Huidige gegevensverwerking door FYN

De retailer heeft toegang tot en inzage in de verzamelde persoonsgegevens. Naast de retailer hebben vier medewerkers van FYN toegang tot de persoonsgegevens. De heer Hazelhof, de heer Jansen, de heer Vos en de heer Kruining hebben indien nodig toegang tot de database. De heer Hazelhof en de heer Jansen zijn beiden softwaredevelopers: zij ontwikkelen en programmeren software. De heer Vos en de heer Kruining zijn full-stack-developers. Zij moeten in staat zijn om een applicatie van begin tot eind te ontwikkelen: een database inrichten, de back-end programmeren en de front-end maken. De medewerkers van FYN verschaffen zichzelf niet zomaar toegang tot het systeem. Dit gebeurt alleen op verzoek van de retailer, wanneer er sprake is van bijvoorbeeld een technisch probleem dat op afstand wordt opgelost door een van de vier medewerkers.

Bij het verrichten van handelingen met betrekking tot persoonsgegevens door FYN kunnen de onderstaande stappen worden onderscheiden:

1. De persoonsgegevens worden in de database opgeslagen.

Zoals in paragraaf 3.3.2 is besproken, kunnen de persoonsgegevens door twee actoren in de database worden ingevoerd. Ten eerste door de retailer bij een verkooptransactie en ten tweede door de consument via het klantenportaal.

2. De retailer geeft toestemming aan FYN om bepaalde handelingen met betrekking tot de persoonsgegevens te verrichten.

Bij het verhelpen van problemen verrichten de medewerkers van FYN verschillende handelingen. Een handeling is het aanbrengen van wijzigingen in de persoonsgegevens. Het komt vaak voor dat de retailers bij een grote hoeveelheid consumenten de gegevens verkeerd noteren, bijvoorbeeld telkens een nul vergeten bij het registreren van het telefoonnummer. De retailer kan dan FYN verzoeken om deze fout te herstellen door overal waar een nul ontbreekt deze toe te voegen.

Daarnaast raadpleegt FYN de persoonsgegevens wanneer een direct mailing handmatig moet worden verstuurd. Als Connect (het programma waarmee direct mailings worden verstuurd) niet goed functioneert vanwege een technische storing, moeten de medewerkers van FYN de mailing handmatig versturen. Hiertoe moeten zij de persoonsgegevens raadplegen van de consumenten die deze mailing krijgen.

De laatste handeling is dat FYN de persoonsgegevens bewaart voor de retailers. In feite doet FYN dit niet zelf, maar vindt dit automatisch plaats door het POS-softwareprogramma. FYN heeft in dit programma echter wel algoritmes ingevoerd om dit te kunnen bewerkstelligen.

3.FYN verricht de handelingen waartoe de retailer opdracht heeft gegeven.

Bij het verrichten van de opgedragen handelingen worden de persoonsgegevens in beginsel niet uit de database gehaald, met uitzondering van de situatie waar de retailer opdracht heeft gegeven tot het sturen van een mailing. Bij het bewaren en het wijzigen van verkeerd ingevoerde persoonsgegevens blijven de gegevens in de database.

4.Als FYN de opgedragen handeling heeft verricht, wordt dit genoteerd in de database.

Als er bijvoorbeeld een direct mailing is uitgegaan naar de consumenten van de retailer, dan slaat FYN in de database van de retailer op dat er een direct mailing verstuurd is.

Deze handelingen van FYN zijn volledig geautomatiseerd. Er wordt daarbij gebruikgemaakt van de gegevensverwerkingsprogramma's die in paragraaf 3.3.1 zijn besproken.

3.3.4 Toekomstig gegevensverwerkingsproces: profilering

In de toekomst wil FYN, naast de huidige handelingen die het verricht op verzoek van de retailer, op eigen initiatief gaan profileren. Het profileren zal geschieden ten behoeve van de leveranciers van de retailers. De bedoeling is dat de opgestelde persoonlijkheidsprofielen omgezet worden in statistieken en dat deze tegen een vergoeding aan de leveranciers worden verstrekt.

Het profileringsproces zal als een nieuw gegevensverwerkingsproces aangemerkt worden. Dit proces zal bestaan uit de volgende vijf fasen: verzamelen van persoonsgegevens, verstrekking van persoonsgegevens, algoritmes instellen, persoonlijkheidsprofielen anonimiseren en als laatste de persoonlijkheidsprofielen verwijderen.

De consumenten hebben geen toestemming voor het profileren gegeven. Profileren heeft tot op heden niet plaatsgevonden, noch door FYN, noch door de retailer. Ook is het profileren geen doeleinde van de retailer voor de huidige gegevensverwerking.

3.3.4.1 Verzamelen en verstrekken van persoonsgegevens

De gegevens worden verzameld in de database van de retailer. De retailers zullen de persoonsgegevens aan FYN moeten verstrekken. FYN zal de gegevens die het van de retailers ontvangen heeft in zijn eigen database opslaan. Het verstrekken zal erop neerkomen dat FYN met toestemming van de retailer zichzelf toegang verschaft tot de database van de retailer. Deze database is een klein blokje dat onderdeel uitmaakt van een groter geheel: de hele database. Het grotere geheel, de hele database, bestaat uit meerdere blokjes. Elk blokje is een kleinere database die toebehoort aan een retailer. Een van deze blokjes zal aan FYN toebehoren. FYN zal in dit blokje de ontvangen persoonsgegevens opslaan voor het profileren. Nu het gaat om één en dezelfde

database, geldt voor FYN ook wat geldt voor de retailers: de gegevens blijven oneindig raadpleegbaar. FYN heeft immers geen programma ontwikkeld dat de database te zijner tijd kan opschonen.

FYN is zich ervan bewust dat de retailers uiteraard een vergoeding willen ontvangen voor het verstrekken van de persoonsgegevens. Daarom heeft FYN als optie om de leveranciers tien cent te laten betalen per e-mailadres dat gebruikt wordt voor het sturen van gerichte aanbiedingen. Van deze tien cent zal dan vijf cent worden afgestaan aan de retailer. Dit staat echter nog niet vast, het is een mogelijk verdienmodel.

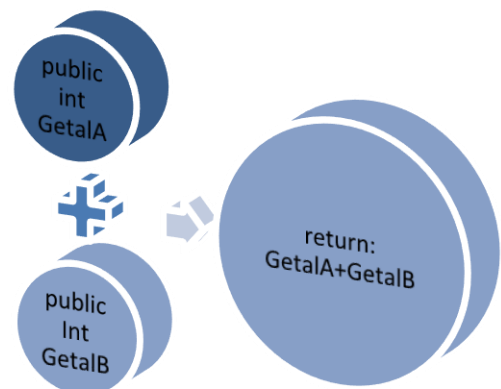
Om te kunnen profileren, zijn verschillende persoonsgegevens nodig. Het omnichannelsysteem verzamelt data uit verschillende kanalen (paragraaf 3.2). FYN wil allereerst het klik- en surfgedrag van de klanten van de retailers volgen. Hiermee kan bijvoorbeeld worden ingezien welke consument een bepaald product heeft bekeken en hoe vaak op het desbetreffende product in het algemeen wordt gezocht. Daarnaast wil FYN de naam, de adresgegevens en het e-mailadres van de consumenten hebben. Het klik- en surfgedrag zal immers gekoppeld moeten worden aan natuurlijke personen en daarvoor zijn de naam, het e-mailadres en het woonadres nodig.

Om het klik- en surfgedrag te kunnen registreren, is het noodzakelijk om cookies te plaatsen. Bij het leveren van de POS-software wordt er door FYN ook een website voor de retailers gemaakt. FYN heeft bij het inrichten van deze websites cookies geplaatst. Het gaat om analytische, functionele en tracking cookies. De consument wordt bij bezoek aan de website geïnformeerd over de cookies en er wordt om toestemming verzocht voor het plaatsen van de cookies. Bij het geven van de toestemming moet op de knop 'accepteren' worden geklikt. Pas daarna worden er cookies geplaatst en wordt het klik- en surfgedrag van de consument geregistreerd. Als een consument geen toestemming geeft voor het plaatsen van de cookies, blijft het voor hem wel mogelijk om overige onderdelen van de website te raadplegen. Voor het registreren van het klik- en surfgedrag zal gebruikgemaakt worden van tracking cookies. Momenteel wordt het klik- en surfgedrag echter geanonimiseerd ontvangen: zo is de software door FYN geprogrammeerd. In de toekomst moeten deze data niet-geanonimiseerd binnenkomen, waardoor deze gekoppeld kunnen worden aan natuurlijke personen.

3.3.4.2 Algoritmes instellen

Zodra de persoonsgegevens zijn verzameld door de retailer en deze zijn verstrekt aan FYN, moeten er persoonlijkheidsprofielen opgesteld worden. Vanaf deze fase zullen er handelingen door FYN verricht worden. FYN zal voor het opstellen van persoonlijkheidsprofielen gebruikmaken van algoritmes. De algoritmes die ingezet zullen worden, zal FYN zelf ontwikkelen en programmeren in de verschillende programma's die gebruikt worden voor de verwerking van persoonsgegevens (paragraaf 3.3.1).

Algoritmes werken met functies (zie de afbeelding hiernaast ter illustratie). Er zijn diverse functies die ingezet kunnen worden. Neem de afbeelding hiernaast als voorbeeld. In de desbetreffende functie worden het getal A en het getal B ingevuld. Het algoritme berekent deze getallen en dan krijg je als uitkomst $\text{GetalA} + \text{GetalB}$. Dit is een voorbeeld van een algoritme. Bij algoritmes draait het in de kern om in- en uitvoer. Er wordt iets in het systeem ingevoerd en door het inzetten van verschillende functies – in dit geval optellen – komt er een uitkomst uit.



Door het inzetten van de algoritmes worden persoonlijkheidsprofielen opgesteld. Hierbij kan de invoer bestaan uit de persoonsgegevens van een persoon, zijn klik- en surfgedrag op de website, het aantal webviews op social media, zijn aankoopgedrag, etcetera. Het inzetten van algoritmes op de gegevens uit de database leidt tot een uitkomst: een persoonlijkheidsprofiel.

Bij het verwerken van de persoonsgegevens neemt FYN beveiligingsmaatregelen, zowel nu als bij de toekomstige profilering. De volgende beveiligingsmaatregelen zijn geïntegreerd in de vijf programma's die FYN gebruikt voor de gegevensverwerking: tweestapsverificatie, gelimiteerde toegang, toegang vanaf één IP-adres, pseudonimisering, encryptie, hashing en salting. De tweestapsverificatie is een tweeledige inlogstructuur: om toegang te verkrijgen tot de verwerkingsprogramma's dienen twee beveiligingslagen gepasseerd te worden door inlogcodes in te voeren. Daarnaast kunnen alleen de vier programmeurs die genoemd zijn in paragraaf 3.3.3 met deze tweestapsverificatie toegang krijgen tot de database. Toegang tot de gegevensverwerkingsprogramma's is alleen mogelijk vanaf het IP-adres van FYN. Het versleutelen van persoonsgegevens met een algoritme – een pseudoniem – is aan te merken als pseudonimisering van persoonsgegevens. De persoonsgegevens worden dan vervangen door dit pseudoniem. Om de oorspronkelijke gegevens te achterhalen, zijn naderhand aanvullende gegevens nodig. Encryptie is het versleutelen van persoonsgegevens. De versleuteling vindt plaats door van de persoonsgegevens een onbruikbare brij te maken. Deze versleuteling kan naderhand echter wel gedecodeerd worden. Daarvoor is een sleutel vereist. Hashing is een vorm van pseudonimisering. Bij hashing wordt de kans geminimaliseerd dat twee verschillende invoerwaarden dezelfde uitkomst geven. Salting vindt plaats door het afleiden van een sleutel in de cryptografie. Deze beveiligingsmaatregelen worden bij de huidige gegevensverwerking – het verrichten van de opgedragen handelingen door de retailer – gehanteerd en worden ook ingezet zodra er wordt overgegaan tot het profileren. De heer Hazelhof heeft als ICT-expert aangegeven dat deze beveiligingsmaatregelen conform de stand van de techniek zijn.

3.3.4.3 Anonimiseren en verwijderen van persoonlijkheidsprofielen

De bedoeling is dat FYN op basis van de persoonlijkheidsprofielen statistieken opstelt, om deze vervolgens te verstrekken aan de leveranciers van de retailers. De leveranciers kunnen door middel van deze statistieken zien wat de trends zijn. Deze trends kunnen seizoensgebonden zijn (bijvoorbeeld rond Valentijn worden vaak sieraden van Pandora verkocht) of locatiegebonden zijn (bijvoorbeeld in een gemeente met oudere inwoners worden veel elektrische fietsen verkocht). Door inzicht in deze trends kunnen de leveranciers hun aanbod op de trends aanpassen en inspelen op de behoeften van de consumenten.

FYN wil graag winst halen uit deze werkwijze. FYN beschikt immers over de klantdata die de retailer heeft verstrekt en bezit de kennis om deze data op een zodanige wijze te analyseren en te combineren door middel van algoritmes, dat er persoonlijkheidsprofielen mee kunnen worden opgesteld.

Zodra de statistieken zijn verstrekt en de leveranciers hun marketingstrategie hierop hebben aangepast, wil FYN overgaan tot direct marketing ten behoeve van deze leveranciers. De direct marketing zal echter wel geschieden onder de naam van de retailer. Dat komt neer op het volgende: Batavus gaat een nieuw fietsmodel op de markt brengen en dit tegen een scherpe prijs aanbieden. Batavus bepaalt vervolgens in overleg met de retailer waaraan de inhoud van de mailing moet voldoen. FYN stelt overeenkomstig de gestelde eisen de mailing op. Vervolgens wordt de mailing verstuurd aan de consumenten onder de naam van de retailers en vanuit de mailserver van de retailers, in dit voorbeeld de fietsenwinkels. De retailer zal hiervoor zijn toestemming moeten geven. Bepaalde retailers hebben met hun leveranciers al afspraken gemaakt over deze wijze van direct marketing.

FYN heeft niet de behoefte om de persoonlijkheidsprofielen te gebruiken voor eigen marketingdoeleinden. De producten en diensten die FYN levert, zijn immers alleen geschikt voor retailers en groothandelaren. Daarnaast levert FYN geen losse onderdelen zoals bijvoorbeeld een beveiligingsprogramma. Bij FYN dient het gehele professionele softwarepakket afgenomen te worden en dat is niet geschikt voor consumenten.

De retailer zal evenals de leverancier de persoonlijkheidsprofielen niet kunnen inzien: hij verzamelt alleen de klantdata. Hij bezit zelf niet de kennis om de verzamelde data te koppelen door middel van algoritmes om er persoonlijkheidsprofielen mee op te stellen. De retailer is slechts in staat om bijvoorbeeld op te vragen hoe vaak op een bepaald product is gezocht. Hij krijgt dan alleen statistische gegevens te zien. Echter, de geanonimiseerde persoonlijkheidsprofielen, die uiteindelijk statistieken zullen zijn, worden ook aan de retailers verstrekt. Zij kunnen dan ook hun aanbod aanpassen. Het verstrekken van deze statistieken zal niet inbegrepen zijn in de standaarddienstverlening van FYN. FYN biedt momenteel iets vergelijkbaars aan, namelijk benchmarking. Dit houdt in dat de retailers zichzelf kunnen vergelijken met andere retailers. Er worden gemiddelden genomen van verschillende zaken, zoals verkoopcijfers, omzet, etcetera. Deze gemiddelden stelt FYN op door gebruik te maken van de data van hun eigen klanten, de retailers. De retailers kunnen dan zien in hoeverre hun eigen resultaten overeenkomen met deze gemiddelden.

Als de persoonlijkheidsprofielen zijn opgesteld, worden deze door FYN verwijderd. De heer Hazelhof noemt 'verwijderen' niet een geschikte definiëring. Bij het opstellen van de persoonlijkheidsprofielen wordt zoals besproken in paragraaf 3.3.4.2 gebruikgemaakt van algoritmes. Het algoritme is een code waarin elke keer andere data ingevoerd kunnen worden. Daardoor is er elke keer een andere uitkomst. Zodra de algoritmes deze data hebben geanalyseerd en er persoonlijkheidsprofielen zijn opgesteld, is de taak voltooid. De code van het algoritme onthoudt niet wat er is ingevoerd. Kortom, er hoeven geen handelingen verricht te worden om de persoonlijkheidsprofielen te verwijderen. De code van het algoritme onthoudt de ingevoerde data niet en de persoonlijkheidsprofielen worden door FYN geanonimiseerd: de profielen zijn uiteindelijk alleen door FYN in te zien.

Geconstateerd is dat het omnichannelsysteem een grote hoeveelheid data verzamelt. Er komen namelijk data uit verschillende kanalen binnen in een database waar de retailer en vier medewerkers van FYN toegang tot hebben. Momenteel doet FYN niets met de door de retailer verzamelde persoonsgegevens. Gebleken is echter dat FYN de intentie heeft om over te gaan tot profileren. Dit profileren is niet als een doeleinde door de retailers geformuleerd en zal aangemerkt worden als een nieuw gegevensverwerkingsproces. Aangezien het profileren niet als doeleinde is geformuleerd, wordt in het volgende hoofdstuk gezien welke gevolgen dit met zich meebrengt voor FYN.

Hoofdstuk 4 De wet versus de praktijk

Inleiding

In dit hoofdstuk wordt getoetst in hoeverre de praktijk in overeenstemming is met de wet- en regelgeving. Voordat wordt gekeken of de wijze van verwerking van persoonsgegevens in overeenstemming is met de wet- en regelgeving, is het noodzakelijk om te toetsen of de Wbp en AVG van toepassing zijn. Vervolgens wordt gezien hoe FYN aangemerkt kan worden: als bewerker of als verantwoordelijke. De plichten van de bewerker en verantwoordelijke zijn immers verschillend. Bovendien wordt gekeken of voldaan is aan de informatieplicht en of op correcte wijze toestemming is verkregen voor het plaatsen van tracking cookies. Als laatste wordt getoetst onder welke voorwaarden FYN de persoonsgegevens van de retailers mag ontvangen en of de gewenste wijze van gegevensverwerking, het profileren, in overeenstemming is met de wet- en regelgeving.

4.1 Toepasbaarheid juridisch kader

In deze paragraaf wordt getoetst of de Wbp en de AVG van toepassing zijn. De toetsing geschiedt aan de hand van de volgende criteria: persoonsgegevens en verwerken. Het criterium 'bestand' verdient geen nadere aandacht, aangezien er bij FYN sprake is van geautomatiseerde gegevensverwerking. De AVG en de Wbp zijn immers van toepassing zodra er sprake is van geautomatiseerde verwerking van persoonsgegevens.¹⁶⁷

4.1.1 Soorten persoonsgegevens

De retailers zullen de volgende gegevens aan FYN verstrekken ten behoeve van de profilering: de naam, het e-mailadres, het woonadres en het geregistreerde klik- en surfgedrag. De eerste drie gegevens die door de retailers worden verzameld, hebben betrekking op natuurlijke personen. Daarnaast zijn deze personen al geïdentificeerd. Het zijn immers klanten van de retailers: zij voeren de persoonsgegevens van hun klanten in het systeem in bij een verkooptransactie of de klanten laten hun persoonsgegevens zelf achter bij het inloggen op het klantenportaal op de website. Nu er sprake is van gegevens die betrekking hebben op een natuurlijk persoon en deze personen geïdentificeerd zijn, is voldaan aan het vereiste om te spreken van een persoonsgegeven.¹⁶⁸ Weliswaar kunnen deze persoonsgegevens versleuteld worden (door middel van pseudonimisering en encryptie), maar het is ook mogelijk om de versleuteling te decoderen door gebruik te maken van aanvullende gegevens, om zo de gegevens alsnog te kunnen koppelen aan een natuurlijk persoon. De AVG bepaalt dan ook dat gepseudonimiseerde gegevens die met gebruik van aanvullende gegevens kunnen worden herleid tot een natuurlijk persoon, aangemerkt worden als persoonsgegevens.¹⁶⁹

Het klik- en surfgedrag zal door middel van tracking cookies geregistreerd worden en niet-geanonimiseerd binnenkomen in de database. De vraag is in hoeverre het klik- en surfgedrag aangemerkt kan worden als een persoonsgegeven. Zowel de AVG als de Wbp spreken van een gegeven dat herleidbaar is naar een identificeerbare of geïdentificeerde persoon. FYN heeft medewerkers in dienst die de nodige kennis bezitten om het klik- en surfgedrag te koppelen aan een natuurlijk persoon om zo te achterhalen wie nu precies op een bepaald product zoekt, welke bestellingen deze persoon heeft geplaatst, etcetera. Er is dan sprake van een indirect gegeven: het is immers nodig dat het klik- en surfgedrag met overige gegevens gekoppeld moet worden om te leiden tot een natuurlijk persoon.

¹⁶⁷ Art. 2 lid 1 Wbp jo. art. 2 lid 1 AVG.

¹⁶⁸ Art. 1 sub a Wbp jo. art. 4 lid 1 AVG.

¹⁶⁹ Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG algemene verordening gegevensbescherming (PbEU 2016, L 119/1), overweging 24

Desondanks is het aan te merken als een persoonsgegeven, want de AP is van mening dat het voldoende is dat het gegeven herleidbaar is naar een persoon om het te kunnen aanmerken als een persoonsgegeven.¹⁷⁰ Echter, in de AVG is expliciet aangegeven dat persoonsgegevens die verzameld zijn door middel van online identificatoren aangemerkt worden als een persoonsgegeven.¹⁷¹ Tracking cookies worden volgens de AVG aangemerkt als een online identifier.¹⁷² Het komt erop neer dat het klik- en surfgedrag zowel onder de Wbp als onder de AVG als een persoonsgegeven aangemerkt kan worden.

4.1.2 Soorten verwerkingshandelingen

De definitie 'verwerking van persoonsgegevens' blijft in de AVG hetzelfde als in de Wbp. Beide wetten noemen enkele voorbeelden van wanneer handelingen met betrekking tot persoonsgegevens aangemerkt worden als een verwerking van persoonsgegevens.¹⁷³

Op dit moment worden de volgende verwerkingshandelingen verricht met betrekking tot de persoonsgegevens: verzamelen, raadplegen, wijzigen en bewaren. Zowel de retailer als FYN zelf verrichten verwerkingshandelingen. Raadplegen, wijzigen en bewaren van persoonsgegevens wordt door FYN uitgevoerd op verzoek van de retailers. Deze handelingen zijn volledig geautomatiseerd: er wordt gebruikgemaakt van speciaal hiervoor ontwikkelde programma's die in hoofdstuk drie paragraaf 3.3.1 zijn besproken. Nu er sprake is van het geautomatiseerd verwerken van persoonsgegevens worden de gegevens niet opgeslagen in een bestand en zal dit ook niet gebeuren. Dit vereiste verdient dan ook geen nader aandacht.

Zodra FYN gaat profileren zal er ook sprake zijn van het combineren van persoonsgegevens. Voor het opstellen van persoonlijkheidsprofielen is het immers noodzakelijk om diverse persoonsgegevens met elkaar op een zodanige wijze te combineren dat trends voorspelt kunnen worden voor leveranciers en deze hun marketingstrategie daarop kunnen aanpassen. Het combineren wordt volgens de Wbp en de AVG ook aangemerkt als een verwerking van persoonsgegevens.¹⁷⁴ Onder de AVG wordt het profileren daarnaast expliciet aangemerkt als een vorm van gegevensverwerking.¹⁷⁵

De verwerkingshandeling die de retailers verrichten, is het verzamelen van persoonsgegevens. Bij het uitoefenen van zijn onderneming verkoopt de retailer producten of verleent hij diensten. Bij het aanbieden van producten en het verlenen van diensten worden persoonsgegevens van de consumenten geregistreerd. Deze registratie geschiedt door de retailer. De retailer maakt gebruik van de POS-software ten behoeve van zijn bedrijfsuitoefening. Doordat de retailer van deze software gebruikmaakt en deze software ervoor zorgt dat data uit verschillende kanalen wordt verzameld, is de retailer de persoon die de persoonsgegevens van zijn klanten (de consumenten) verzamelt. FYN verzamelt geen persoonsgegevens van de consumenten. Omdat de retailers de persoonsgegevens verzamelen, formuleren zij de doeleinden voor de gegevensverwerking.

Met inachtneming van hetgeen in deze paragraaf besproken is, kan geconcludeerd worden dat de Wbp en de AVG van toepassing zijn. Er is immers sprake van een geautomatiseerde verwerking van persoonsgegevens.

¹⁷⁰ L. Meij, 'BigData maandag deel 3: Persoonsgegevens en gegevensverwerking', *ictrecht* 21 juli 2014, ictrecht.nl.

¹⁷¹ Art. 4 lid 1 AVG.

¹⁷² Berkvens & Jakimowicz 2016, p. 24.

¹⁷³ Art. 1 sub b Wbp jo. art. 4 lid 2 AVG.

¹⁷⁴ Art. 2 lid 1 sub b Wbp jo. art. 4 lid 2 AVG.

¹⁷⁵ Art. 4 lid 4 AVG.

4.2 FYN: bewerker of verantwoordelijke?

Nu vast is komen te staan dat de Wbp en de AVG van toepassing zijn, moet gekeken worden of FYN aangemerkt kan worden als verantwoordelijke of bewerker. FYN verricht met betrekking tot de persoonsgegevens de volgende handelingen: raadplegen, wijzigen en bewaren. Deze handelingen worden alleen verricht op verzoek van de retailer zelf (hoofdstuk drie paragraaf 3.3.3).

De retailers hebben twee doeleinden geformuleerd voor de huidige gegevensverwerking: direct marketing en efficiëntie. Ook de middelen voor de gegevensverwerking worden in beginsel door de retailers aangewezen. In beginsel, want FYN heeft wel inspraak bij het aanwijzen van de middelen op technisch en organisatorisch gebied. De medewerkers van FYN bezitten de kennis om de middelen op technisch en organisatorisch gebied aan te wijzen. Dit betekent niet dat FYN door dit gegeven meteen als een verantwoordelijke aangemerkt kan worden. Voor zover FYN zich bij het aanwijzen van de middelen niet buiten het technische en organisatorische gedeelte begeeft – en dat doet FYN niet – is FYN niet aan te merken als een verantwoordelijke.¹⁷⁶ Op basis van de huidige situatie is FYN aan te merken als een bewerker. FYN wijst immers, buiten het technische en organisatorische gedeelte om, geen middelen aan voor de gegevensverwerking en stelt ook niet de doeleinden vast.¹⁷⁷ Dit wordt gedaan door de retailers. Bovendien verwerkt FYN de persoonsgegevens alleen op verzoek van de retailer, ofwel op diens instructies. Ook is FYN een persoon buiten de organisatie van de retailer en is FYN hiërarchisch niet ondergeschikt aan een van de retailers.¹⁷⁸ De wet schrijft voor dat er aan de relatie tussen de verantwoordelijke en de bewerker een bewerkersovereenkomst ten grondslag moet liggen om zekerheid te hebben over de relatie.¹⁷⁹ FYN handelt nu in strijd met de wet: aan de relatie tussen FYN en de retailer ligt immers geen enkele overeenkomst ten grondslag. Het enige wat op schrift gesteld is tussen deze twee partijen is een factuur die FYN naar aanleiding van een bestelling aan de retailer stuurt. Afspraken over de verwerking van persoonsgegevens zijn niet gemaakt.

Nu geconstateerd is dat FYN op dit moment aan te merken is als bewerker, is FYN niet gehouden om te voldoen aan de eisen die de wet stelt aan een rechtmatige gegevensverwerking. Deze moeten door de retailer worden nageleefd. De retailer is immers op dit moment aan te merken als verantwoordelijke. Toch betekent dit niet dat FYN als bewerker geen verplichtingen heeft. FYN moet voldoen aan de plichten die de Wbp en de AVG aan de bewerker opleggen (hoofdstuk twee paragraaf 2.1.3.2 en paragraaf 2.2.2.1).

Echter, FYN wil in de nabije toekomst overgaan tot het profileren op eigen initiatief. Profileren is een doeleinde dat niet door de retailers is geformuleerd. Voortaan zal FYN voor dit doeleinde aangemerkt worden als verantwoordelijke. De verantwoordelijke is immers degene die de doeleinden van de gegevensverwerking formuleert. Nu FYN voor het profileren aangemerkt zal worden als verantwoordelijke, moet FYN voldoen aan de eisen die gesteld worden aan een rechtmatige gegevensverwerking en moet het de plichten naleven die de Wbp en de AVG opleggen aan een verantwoordelijke.

4.3 FYNE profilering

In deze paragraaf wordt allereerst besproken of FYN de persoonsgegevens mag ontvangen van de retailer ten behoeve van profilering. Vervolgens wordt gekeken of profileren voor marketingdoeleinden door FYN als rechtmatig is aan te merken.

¹⁷⁶ Opinie van de Groep Gegevensbescherming Artikel 29 nr. 1 van 2010, p. 17.

¹⁷⁷ Art. 1 sub d Wbp.

¹⁷⁸ Art. 1 sub e Wbp.

¹⁷⁹ Art. 14 lid 2 Wbp jo. art. 28 lid 3 AVG.

4.3.1 Verstrekken van persoonsgegevens aan FYN

Persoonsgegevens kunnen op twee manieren worden verkregen. De eerste mogelijkheid is dat deze door een organisatie zelf worden verzameld. Een andere optie is het verkrijgen van gegevens die door een andere organisatie zijn verzameld. Het verstrekken van persoonsgegevens wordt aangemerkt als een gegevensverwerking.¹⁸⁰

De eigenaar van de persoonsgegevens is juridisch gezien de betrokkene.¹⁸¹ De gegevens hebben immers betrekking op hem. De verantwoordelijke is degene die deze gegevens verzamelt voor uitdrukkelijk omschreven doeleinden. In overeenstemming met deze doeleinden kan de verantwoordelijke de verzamelde persoonsgegevens verwerken.

Eenieder heeft het recht op eerbiediging en bescherming van zijn persoonlijke levenssfeer.¹⁸² Het verstrekken van persoonsgegevens kan een inbreuk maken op dit grondrecht. Daarom mag het verstrekken van persoonsgegevens aan een ander alleen plaatsvinden als dit bij de wet is bepaald.¹⁸³ Onder de Wbp en AVG mogen persoonsgegevens verstrekt worden als er een rechtvaardigingsgrond aanwezig is en het verenigbaar is met het oorspronkelijke doel.¹⁸⁴

4.3.1.1 Verstrekking persoonsgegevens: verenigbaarheid

Om te beoordelen of het verstrekken van persoonsgegevens rechtmatig is, wordt gekeken naar verschillende factoren. Allereerst moet gekeken worden naar de verwantschap tussen de oorspronkelijke doeleinden en de nieuwe doeleinden.¹⁸⁵ In 1998 heeft de Registratiekamer geoordeeld of er in het geval van verstrekking van persoonsgegevens voor marketingdoeleinden sprake is van verenigbaar gebruik.¹⁸⁶ In casu was er sprake van een verzekeringsmaatschappij met concernverhoudingen. De persoon in kwestie was verzekerd bij het ziekenfonds – de moedermaatschappij – en had ook een aanvullende verzekering afgesloten bij een dochtermaatschappij. De verzekerde werd met een mailing benaderd over een aanvullende uitvaartverzekering door de dochtermaatschappij. De Registratiekamer oordeelde dat de situatie vanuit twee perspectieven bezien kan worden: er is sprake van gegevensverstrekking tussen twee concernonderdelen of de dochtermaatschappij treedt als bewerker op en krijgt de gegevens in de rol als bewerker aangeleverd.

Bezien vanuit het eerste perspectief oordeelde de Registratiekamer dat het verstrekken van de persoonsgegevens gerechtvaardigd was. Het gebruik was beperkt gebleven tot niet-privacygevoelige gegevens, namelijk de NAW-gegevens (naam, adres, woonplaats) van de verzekerden. Daarnaast oordeelde de Registratiekamer dat het aanbieden van aanverwante producten of diensten door een onderdeel van het concern – waar in casu sprake van was – gebruikelijk is.

Vanuit het perspectief dat de dochtermaatschappij als bewerker optreedt, heeft de Registratiekamer in het nadeel van de verzekeringsconcern geoordeeld. De Registratiekamer is van oordeel dat als het ziekenfonds in de rol als bewerker beschikking kreeg over de persoonsgegevens en deze ging gebruiken voor eigen doeleinden – in dit geval direct marketing – er sprake is van ongerechtvaardigd gebruik.

Uit de bovenstaande overwegingen van de Registratiekamer kan de conclusie getrokken worden dat de bewerker de persoonsgegevens niet voor eigen doeleinden mag gaan gebruiken. Hij moet handelen conform de instructies van de verantwoordelijke.

¹⁸⁰ Art. 1 sub b Wbp.

¹⁸¹ A. van der Heijden, 'De Wet bescherming persoonsgegevens', *flynth* 16 september 2016, flynth.nl.

¹⁸² Art. 10 lid 1 Gw.

¹⁸³ Art. 10 lid 2 Gw.

¹⁸⁴ Art. 9 lid 2 Wbp jo. art. 6 lid 4 AVG.

¹⁸⁵ Art. 9 lid 1 sub a Wbp jo. art. 6 lid 4 sub a AVG.

¹⁸⁶ Cbp 16 januari 1998, 97.V.906.

Daarentegen kan een ontvanger niet zijnde een bewerker de gegevens wel gebruiken voor eigen doeleinden voor zover deze verenigbaar zijn met de oorspronkelijke doeleinden, waaronder dus ook direct marketing.

Hieruit volgt dat FYN in de rol als bewerker de gegevens die het aangeleverd krijgt niet mag gebruiken voor eigen doeleinden: het profileren. Echter, indien FYN met de retailers een overeenkomst sluit om de persoonsgegevens voor andere doeleinden te ontvangen, zou FYN de persoonsgegevens wel voor het profileren kunnen gebruiken. Het oorspronkelijke doeleinde van de gegevensverwerking (direct marketing) is immers nauw verbonden met het nieuwe doel (profilering). Veel bedrijven gebruiken persoonlijkheidsprofielen om hun marketingstrategie beter te kunnen afstemmen op de consument en om zo gericht te kunnen adverteren.

Ook moet rekening worden gehouden met de aard van de gegevens en de gevolgen van de verstrekking.¹⁸⁷ Hoe gevoeliger de aard van de gegevens is, hoe kleiner de kans is dat de verstrekking van de persoonsgegevens verenigbaar is met de oorspronkelijke doeleinden. FYN wil voor het profileren de volgende gegevens ontvangen van de retailers: de naam, het woonadres, het e-mailadres en het geregistreerde klik- en surfgedrag. De naam, het woonadres en het e-mailadres zijn voor de hand liggende gegevens. Het klik- en surfgedrag daarentegen is door de AP aangemerkt als gegeven van gevoelige aard.¹⁸⁸

Daarnaast is de wijze van verkrijging van belang.¹⁸⁹ Als aan de relatie tussen de retailer en FYN een overeenkomst ten grondslag ligt die bedingen behelst ter bescherming van de rechten van de betrokkene, zal de wijze van verkrijgen niet snel als onrechtvaardig aangemerkt worden. Ook moeten passende waarborgen gesteld worden.¹⁹⁰ FYN neemt voor de huidige gegevensverwerking en ook in geval van profilering voldoende technische en organisatorische maatregelen die overeenstemmen met de huidige stand van de techniek. Dit heeft de heer Hazelhof, een expert op het gebied van ICT, aangegeven. Daarnaast worden encryptie en pseudonimisering toegepast ter bescherming van de persoonsgegevens. Dit is een beveiligingsmaatregel die de AVG expliciet voorschrijft. Er is echter nog geen beleid ontwikkeld dat de beveiligingsmaatregelen toetst op hun technische en organisatorische doeltreffendheid. Dit wordt onder de AVG wel verplicht gesteld. Zodra de AVG van kracht is, kan daardoor niet meer worden aangenomen dat aan alle vereisten is voldaan die gesteld worden aan de beveiliging van de persoonsgegevens.

4.3.1.2 Verstrekking persoonsgegevens: rechtvaardigingsgrond

Er moet ook een rechtvaardigingsgrond aanwezig zijn die de verstrekking van persoonsgegevens aan FYN rechtvaardigt. Een rechtvaardigingsgrond waarop een beroep gedaan kan worden is de toestemming van de betrokkene.¹⁹¹ Daarnaast is het gerechtvaardigd belang van de verantwoordelijke of van een derde een rechtvaardigingsgrond waarop een beroep gedaan kan worden.¹⁹² Als de retailer kan aanvoeren dat het verstrekken van persoonsgegevens noodzakelijk is om zijn gerechtvaardigd belang of dat van FYN te behartigen, en dit belang prevaleert boven het belang van de betrokkene, is deze grond eventueel ook een optie.¹⁹³ Het bedrijfsbelang wordt aangemerkt als een gerechtvaardigd belang.¹⁹⁴ Bij het beoordelen welk belang prevaleert, wordt gekeken naar verschillende zaken. Allereerst is de aard van de gegevens van belang. Hierboven is beargumenteerd dat de naam, het woonadres en het

¹⁸⁷ Art. 9 lid 2 sub b Wbp jo. art. 6 lid 4 sub c AVG.

¹⁸⁸ W. Heck, 'Zomaar ons online surfgedrag volgen kan nu echt niet meer', *nrc* 14 mei 2014, nrc.nl.

¹⁸⁹ Art. 9 lid 2 sub d Wbp jo. art. 6 lid 4 sub b AVG.

¹⁹⁰ Art. 9 lid 2 sub e Wbp jo. art. 6 lid 4 sub e AVG.

¹⁹¹ Art. 8 sub a Wbp jo. art. 6 lid 1 sub a AVG.

¹⁹² Art. 8 sub f Wbp jo. art. 6 lid 1 sub f AVG.

¹⁹³ 'Verstrekken van persoonsgegevens', *autoriteitpersoonsgegevens* z.j., autoriteitpersoonsgegevens.nl.

¹⁹⁴ Hooghiemstra & Nouwt 2016, p. 53.

e-mailadres voor de hand liggende gegevens zijn. Het klik- en surfgedrag is daarentegen wel gevoelig van aard. Ook is beargumenteerd dat de huidige beveiligingsmaatregelen conform de stand van de techniek zijn. Echter, de huidige maatregelen zijn niet voldoende zodra de AVG van kracht is: er moet op dat moment ook een beleid worden ontwikkeld dat de beveiligingsmaatregelen toetst op hun technische en organisatorische doeltreffendheid. Kijkend naar het subsidiariteitsvereiste kan het doel van FYN niet op een andere wijze gediend worden.¹⁹⁵ FYN verzamelt immers zelf geen persoonsgegevens, met uitzondering van die van haar eigen klanten (de retailers). Deze zijn echter niet interessant voor de leveranciers. Lettend op het proportionaliteitsvereiste is de gegevensverstrekking niet onevenredig in verhouding met het doel van de gegevensverwerking.¹⁹⁶ De gegevens worden immers al gebruikt voor marketingdoeleinden van de retailers. Nu de persoonlijkheidsprofielen tot doel hebben om de leveranciers van statistieken te voorzien om gericht te kunnen adverteren, kan aangenomen worden dat de verstrekking van de gegevens voor het profileren niet onevenredig is met het huidige doel, direct marketing.

4.3.2 Rechtmatig profileren

In de Wbp is geen artikel expliciet gewijd aan profilering. Er is slechts een artikel gewijd aan het recht om niet te worden onderworpen aan een besluit dat tot stand is gekomen door middel van geautomatiseerde besluitvorming.¹⁹⁷ Ook is in de Wbp geen wetsartikel opgenomen dat expliciet aan de betrokkene het recht geeft verzet aan te tekenen tegen profilering. Dit in tegenstelling tot de AVG. Wel is het recht van verzet tegen profilering impliciet opgenomen in het algemene verzetsartikel. De betrokkene heeft het recht om verzet aan te tekenen zodra zijn persoonsgegevens worden gebruikt ten behoeve van direct marketing.¹⁹⁸ Dit recht van verzet heeft volgens de AP niet alleen betrekking op direct marketing, maar ook op profileren.¹⁹⁹ De AP heeft bepaald dat het recht van verzet betrekking heeft op alle fasen van de gegevensverwerking. Bij het profileren worden allerlei data die betrekking hebben op een persoon met elkaar in verband gebracht, om zo de persoonlijke interesses en voorkeuren in kaart te brengen. Het in verband brengen van data die betrekking hebben op een persoon wordt volgens de Wbp aangemerkt als een verwerking van persoonsgegevens.²⁰⁰ De AVG daarentegen kenmerkt profileren expliciet als een vorm van gegevensverwerking.²⁰¹ Nu zowel de AVG als de Wbp profileren als gegevensverwerking karakteriseren, moet voldaan zijn aan de eisen die gesteld worden aan een rechtmatige gegevensverwerking.

4.3.2.1 Profilering: doel en grondslag

FYN zal als verantwoordelijke gehouden zijn om doeleinden te formuleren. Het doeleinde van FYN zal 'profilering' worden. Dit doeleinde dient gerechtvaardigd te zijn. De Wbp en AVG noemen zes limitatieve rechtvaardigingsgronden.²⁰² In beginsel kan profileren gerechtvaardigd worden door een beroep op de volgende twee gronden: toestemming hebben van de betrokkene of aanvoeren dat er sprake is van een gerechtvaardigd belang.

De voorwaarden waaronder het profileren door FYN zal plaatsvinden, hebben tot gevolg dat er expliciet toestemming gevraagd moet worden.²⁰³ De AVG schrijft immers voor dat er toestemming is vereist als het profileren de betrokkene in aanmerkelijke mate treft. Het inzetten van een DMP werd als voorbeeld gegeven van een situatie waarin de betrokkene

¹⁹⁵ Kamerstukken II 1997/98, 25892, 3, p.87 (MvT).

¹⁹⁶ Kamerstukken II 1997/98, 25892, 3, p.87 (MvT).

¹⁹⁷ Art. 42 lid 1 Wbp.

¹⁹⁸ Art. 41 lid 1 Wbp.

¹⁹⁹ 'Artikel 41 lid 1 Wbp', *autoriteitpersoonsgegevens z.j.*, autoriteitpersoonsgegevens.nl.

²⁰⁰ Art. 1 sub b Wbp.

²⁰¹ Art. 4 lid 4 AVG.

²⁰² Art. 8 Wbp jo. art. 6 AVG.

²⁰³ Art. 8 sub a Wbp jo. art. 6 lid 1 sub a AVG.

in het geval van profilering in aanmerkelijke mate wordt getroffen (hoofdstuk twee paragraaf 2.2.1.2). De wijze van profileren en de middelen die FYN hiervoor inzet, zijn aan te merken als een DMP. Besproken is immers dat een DMP vergelijkbaar is met een database en dat er in deze database data uit verschillende kanalen worden verzameld en opgeslagen.²⁰⁴ Het omnichannelsysteem van FYN werkt ook op deze manier. Het omnichannelsysteem verzamelt data door middel van verschillende media: social media, surf- en klikgedrag, geregistreerde data bij verkoop, etcetera. Dit systeem kan daarmee als een DMP worden aangemerkt. Aangezien dit systeem gebruikt zal worden voor het verzamelen van data ten behoeve van profilering, is toestemming vereist en kan geen beroep gedaan worden op het gerechtvaardigd belang.

Er zal niet alleen voor het profileren toestemming gevraagd moeten worden. Ook voor het plaatsen van tracking cookies is toestemming vereist. Momenteel plaatst FYN ten behoeve van de retailer verschillende soorten cookies: analytische, functionele en tracking cookies. Voor het plaatsen van tracking cookies heeft de verantwoordelijke een informatieplicht en er dient toestemming gevraagd te worden aan de consumenten.²⁰⁵ Nu het de webshop van de retailer betreft en het klik- en surfgedrag via zijn webshop, en dus door hem, wordt verzameld, geldt de informatieplicht en het toestemmingsvereiste voor de retailers. De retailer moet de consument om toestemming vragen voor het plaatsen van tracking cookies. Momenteel wordt aan deze plicht voldaan. De consumenten krijgen, zodra zij de webshop bezoeken, een balk te zien met de mededeling dat er cookies geplaatst worden en dienen hiervoor toestemming te geven. Deze toestemming wordt gegeven door het aanklikken van de button 'accepteren'. Dit wordt volgens de MvT aangemerkt als een actieve handeling. Pas vanaf het moment dat op deze button is geklikt, wordt het klik- en surfgedrag geregistreerd. Wordt de button niet aangeklikt, dan wordt het internetgedrag niet geregistreerd.²⁰⁶

Ook moet de retailer de consument informeren over wie er beschikking krijgt over het geregistreerde klik- en surfgedrag. Hierover wordt momenteel geen informatie verschaft: het internetgedrag wordt immers geanonimiseerd ontvangen. Nu FYN het klik- en surfgedrag wil gebruiken voor het profileren, zal de retailer de consument hierover moeten informeren. Daarnaast zal de retailer, naast de plicht om informatie te geven over wie het geregistreerde surfgedrag inziet, ook gehouden zijn om de consument erop te wijzen dat de verzamelde data gebruikt worden ten behoeve van profilering. Tot slot wil FYN het klik- en surfgedrag gebruiken om persoonlijkheidsprofielen op te stellen om vervolgens gerichte aanbiedingen te versturen aan de consumenten ten behoeve van de leveranciers. Dit zal onder de naam van de retailer geschieden en dus zal de retailer ook gehouden zijn om de consument erover te informeren dat de profielen gebruikt worden voor het sturen van gerichte aanbiedingen.²⁰⁷

4.3.2.2 Alleen een kwalitatieve profilering

FYN heeft momenteel geen intentie om de ontvangen gegevens voor andere doeleinden dan voor profilering te gebruiken. Uit het interview met de heer Sanderse bleek dat FYN de gegevens eventueel in de toekomst voor analyses zou kunnen gebruiken. Dit zijn echter gedachtespinsels en geen concrete plannen. Er is geen intentie om van het

²⁰⁴ N. Kamalzadeh, 'Geautomatiseerde besluitvorming & profilering: wat zijn de eisen?', *considerati* 10 april 2017, considerati.com.

²⁰⁵ Art. 11.7a lid 1 Tw.

²⁰⁶ *Kamerstukken II* 2013/14, 33902, 3, p.14 (MvT).

²⁰⁷ *Opinie van Groep Gegevensbescherming Artikel 29 nr. 2 van 2010*, p.24.

doeleinde 'profilering' af te wijken en daarmee wordt voldaan aan het vereiste van doelbinding.²⁰⁸

Ook wordt de kwaliteit van de gegevensverwerking door FYN gewaarborgd. De gegevensverwerking zal immers niet verder gaan dan noodzakelijk is om het gestelde doeleinde, het opstellen van persoonlijkheidsprofielen, te realiseren.²⁰⁹ Zodra de noodzakelijke persoonsgegevens in de algoritmes zijn ingevoerd en de persoonlijkheidsprofielen zijn opgesteld door inzet van deze algoritmes, worden de persoonlijkheidsprofielen omgezet in anonieme statistieken en daarna verwijderd. De algoritmes zijn ontwikkelde codes, waarbij het gaat om in- en uitvoer. Zodra er gegevens zijn ingevoerd en er op basis van deze invoer resultaten uitkomen, 'vergeet' de code van het algoritme wat er is ingevoerd.

Bij het verwerken van persoonsgegevens moeten voldoende technische en organisatorische maatregelen genomen worden die in overeenstemming zijn met de stand van de techniek.²¹⁰ De AVG noemt expliciet vier maatregelen die genomen moeten worden.²¹¹ Gebleken is dat FYN de persoonsgegevens pseudonimiseert en versleutelt. Ook is de database in het geval van een fysiek of technisch incident snel raadpleegbaar en is de kans dat de persoonsgegevens verloren gaan nihil. FYN heeft namelijk een hoofdservers die alle data uit de databases van de retailer online opslaat. Mocht er iets met deze server gebeuren, dan kan FYN altijd terugvallen op de replicatie. Deze maakt kopieën van hetgeen de hoofdservers heeft opgeslagen. In uitzonderlijke gevallen is het nog mogelijk om op back-ups terug te vallen. Er zijn dus drie mogelijkheden om de persoonsgegevens alsnog op te halen bij een fysiek of technisch incident in het systeem. De heer Hazelhof heeft daarnaast aangegeven dat de overige beveiligingsmaatregelen (hoofdstuk drie paragraaf 3.3.4.2) conform de stand van de techniek zijn. Echter, op grond van de AVG zal FYN gehouden zijn om een beleid op te stellen. Dit beleid moet een procedure zijn waarmee FYN in staat is om te beoordelen of de beveiligingsmaatregelen zowel op technisch als organisatorisch gebied doeltreffend zijn. Op dit moment heeft FYN een dergelijk beleid niet.

Tot slot wordt de bewaartermijn besproken. Zowel de AVG als de Wbp stellen geen tijdsgrens aan het bewaren van persoonsgegevens. De code van het algoritme slaat de ingevoerde persoonsgegevens niet op. Deze worden automatisch 'verwijderd' nadat de persoonlijkheidsprofielen zijn opgesteld. FYN zal de ontvangen persoonsgegevens wel opslaan in zijn eigen database. Tot op heden heeft FYN geen programma ontwikkeld dat in staat is om de verzamelde persoonsgegevens te zijner tijd uit de database te verwijderen. Zodra persoonsgegevens in de database zijn opgeslagen, blijven ze oneindig raadpleegbaar. Dit betekent dat hoewel de code van het algoritme de gegevens niet onthoudt, deze wel in de database raadpleegbaar blijven en na het verstrekken aan FYN ook altijd in de database van FYN ingezien kunnen worden. Ondanks dat de wet geen specifieke bewaartermijn stelt voor het opslaan van persoonsgegevens, is het niet de bedoeling dat bedrijven de verzamelde gegevens nooit verwijderen. Het is immers de bedoeling van de wetgever geweest dat organisaties zelf beoordelen hoelang zij de persoonsgegevens nodig hebben voor het verwezenlijken van hun doeleinden. Na het verwezenlijken van de gestelde doeleinden dienen de gegevens verwijderd te worden.²¹²

4.3.3 Marketing en profilering

Het doel is dat de persoonlijkheidsprofielen omgezet worden in statistieken om deze vervolgens voor marketingdoeleinden te verstrekken aan de leveranciers van de retailers.

²⁰⁸ Art. 9 lid 1 Wbp jo. art. 5 lid 1 sub b AVG.

²⁰⁹ Art. 11 Wbp jo. art. 5 lid 1 sub c AVG.

²¹⁰ Art. 13 Wbp jo. art. 32 lid 1 AVG.

²¹¹ Art. 32 lid 1 sub a t/m d AVG.

²¹² Art. 10 lid 1 Wbp jo. art. 5 lid 1 sub e AVG.

Deze direct marketing zal geschieden onder de naam van de retailer en vanuit diens mailserver. De retailer zal na overleg met zijn leverancier aangeven aan welke eisen de mailing moet voldoen en aan welke consumenten deze gestuurd moet worden. Tijdens het interview met de heer Hazelhof is gebleken dat bepaalde retailers al dergelijke afspraken hebben gemaakt met hun eigen leveranciers. Deze vorm van hosting verleent FYN momenteel ook als onderdeel van de dienstverlening voor zijn eigen klanten.

Direct marketing voor de leveranciers zal geschieden onder de naam van de retailer, waardoor ook diens doel wordt gediend: hij maakt daarmee ook reclame voor de producten die hij aanbiedt in zijn fysieke winkel of webshop. FYN wordt daardoor voor deze gegevensverwerking niet aangemerkt als verantwoordelijke.

Nu de retailer voor de direct marketing, ook indien deze geschiedt voor de leverancier, als verantwoordelijke blijft aan te merken, dient de retailer voor dit gedeelte van de gegevensverwerking te voldoen aan de eisen die de wet stelt aan een rechtmatige verwerking van persoonsgegevens. FYN zal voor dit gedeelte aangemerkt worden als bewerker en op instructie van de retailer en de leverancier de mailing versturen aan de consumenten.

Met inachtneming van het bovenstaande kan geconcludeerd worden dat FYN als verantwoordelijke is aan te merken zodra er wordt geprofileerd. Ook zal FYN enkele afspraken moeten maken met de retailers om te bewerkstelligen dat overgegaan kan worden tot het profileren. In het volgende hoofdstuk worden er conclusies getrokken en aanbevelingen gegeven naar aanleiding van hetgeen is onderzocht in dit hoofdstuk en in de voorgaande hoofdstukken.

Hoofdstuk 5 Conclusies en aanbevelingen

In opdracht van FYN is onderzocht in hoeverre FYN mag profileren voor marketingdoeleinden ten behoeve van de leveranciers van de retailers.

De centrale vraag in dit onderzoek luidde als volgt:

In hoeverre mag FYN Software persoonsgegevens van de retailer die zijn verzameld door middel van het omnichannelsysteem verwerken voor het profileren ten behoeve van direct marketing voor de leveranciers in overeenstemming met de relevante regelgeving waaronder de Wet bescherming persoonsgegevens en de Algemene Verordening Gegevensbescherming (EU) 2016/679 van het Europees Parlement en de Raad?

Hieronder worden naar aanleiding van deze centrale vraag conclusies getrokken en aanbevelingen gegeven.

5.1 Conclusies en aanbevelingen Wbp en AVG

De Wbp en de AVG zijn van toepassing. Deze twee wetten zijn van toepassing zodra er sprake is van het geautomatiseerd verwerken van persoonsgegevens. De naam, het e-mailadres en het woonadres zijn volgens de Wbp en de AVG aan te merken als een persoonsgegeven, omdat zij betrekking hebben op natuurlijke personen. Daarnaast zijn de personen, in dit geval consumenten (de klanten van de retailers), geïdentificeerd. Ook is geconstateerd dat het klik- en surfgedrag aan te merken is als persoonsgegeven. Het betreft weliswaar een indirect gegeven omdat het gekoppeld moet worden aan een natuurlijk persoon, maar het AP merkt op dat een indirect gegeven ook aan te merken is als een persoonsgegeven, zolang het te herleiden is naar een natuurlijk persoon. Het klik- en surfgedrag wordt daarnaast in de AVG expliciet aangemerkt als een persoonsgegeven. Het is door middel van online identificatoren (tracking cookies) verzameld en daardoor is het volgens de AVG een persoonsgegeven.

Ook is er sprake van het verwerken van persoonsgegevens. De volgende handelingen worden door FYN verricht in de rol als bewerker: bewaren, raadplegen en wijzigen. Deze handelingen zijn aan te merken als verwerkingshandelingen. De verwerking van persoonsgegevens vindt geautomatiseerd plaats. Profileren is onder de Wbp aan te merken als een gegevensverwerking, omdat er gegevens worden gecombineerd. Onder de AVG wordt profileren expliciet als gegevensverwerking aangemerkt. Nu er sprake is van een geautomatiseerde verwerking van persoonsgegevens zijn de Wbp en de AVG van toepassing.

5.1.1 FYN als bewerker: conclusie

FYN is op dit moment aan te merken als bewerker. FYN verricht momenteel bepaalde handelingen op verzoek en onder de instructies van de retailers. De retailers verzamelen de gegevens, formuleren de doeleinden en wijzen de middelen aan. FYN heeft alleen inspraak bij het aanwijzen van middelen op technisch en organisatorisch gebied. FYN houdt zich niet bezig met het aanwijzen van middelen buiten het organisatorische en technische gedeelte om. Zolang FYN zich daarmee niet bezighoudt, is FYN niet aan te merken als een verantwoordelijke. Ook is FYN een persoon buiten de organisatie van de retailer en daarmee niet hiërarchisch ondergeschikt aan de retailer. Nu FYN hiërarchisch niet ondergeschikt is aan de retailer, alleen onder de instructies van de retailer handelt, de doeleinden niet formuleert en zich niet bezighoudt met het aanwijzen van de middelen buiten het technische en organisatorische gedeelte om, is FYN aan te merken als bewerker. De retailer is momenteel aan te merken als verantwoordelijke. Hij wijst immers de middelen voor de gegevensverwerking aan en formuleert de doeleinden. De retailers hebben twee doeleinden geformuleerd: direct marketing en efficiëntie.

5.1.2 FYN als bewerker: aanbeveling

De wet stelt het verplicht dat er een bewerkersovereenkomst ten grondslag ligt aan de relatie tussen de bewerker en de verantwoordelijke. Momenteel heeft FYN geen bewerkersovereenkomst gesloten met de retailers. Aanbevolen wordt dan ook dat FYN dit zo spoedig mogelijk zal doen nu het wettelijk verplicht is gesteld. Voor meer informatie over bewerkersovereenkomsten wordt verwezen naar de scriptie van studente L. Wigboldus.

5.1.3 FYN als verantwoordelijke: conclusie

De retailers hebben profileren niet als doeleinde van de huidige gegevensverwerking geformuleerd. Profileren wordt daarmee aangemerkt als een nieuw doel. Nu FYN wil profileren en niet de retailer zelf, zal FYN voor dit doeleinde aangemerkt worden als verantwoordelijke. De verantwoordelijke is immers degene die de doeleinden van de gegevensverwerking vaststelt. Nu FYN de gegevens gaat verwerken voor eigen doeleinden (profilering), is FYN voortaan aan te merken als verantwoordelijke voor dit doel.

5.1.4 FYN als verantwoordelijke: aanbevelingen

Nu FYN aan te merken is als verantwoordelijke zodra er wordt geprofileerd, moet FYN voldoen aan de eisen die de Wbp en de AVG stellen aan een rechtmatige gegevensverwerking. Hieronder wordt aanbevolen aan welke verplichtingen FYN in de rol als verantwoordelijke moet voldoen volgens de Wbp en de AVG.

DOELEINDEN FORMULEREN

Nu FYN voortaan aangemerkt wordt als verantwoordelijke, is het gehouden om doeleinden te formuleren.

FYN wordt geadviseerd om het doeleinde als volgt te formuleren:

- FYN verwerkt persoonsgegevens in zowel de hoedanigheid van bewerker als verantwoordelijke. In de hoedanigheid van verantwoordelijke verwerkt FYN de persoonsgegevens voor het profileren. Het doel van het profileren is om de persoonlijkheidsprofielen om te zetten in geanonimiseerde statistieken en deze te verstrekken aan derden ten behoeve van marketingdoeleinden.

RECHTVAARDIGINGSGROND VOOR HET PROFILEREN

FYN kan de gegevensverwerking ten behoeve van profilering alleen rechtvaardigen door toestemming te hebben van de betrokkenen. Voor het profileren is onder andere toestemming vereist als het de betrokkene in aanmerkelijke mate treft. Het omnichannelsysteem van FYN is vergelijkbaar met een DMP. Besproken is dat betrokkenen wiens persoonsgegevens zijn verzameld door middel van een DMP in aanmerkelijke mate worden getroffen. De toestemming moet bestaan uit een duidelijke, actieve handeling die vrij, specifiek en ondubbelzinnig is. Als voorbeeld is gegeven dat een elektronische verklaring (het klikken op een vakje op de website) aan te merken is als een duidelijke, actieve handeling die een vrije, specifieke en ondubbelzinnige toestemming tot stand brengt. FYN wordt geadviseerd om op de website van de retailers een balk in te voegen met de mededeling dat de gegenereerde persoonsgegevens gebruikt kunnen worden voor het profileren. Deze mededeling moet de button 'accepteren' hebben. Pas als de consument op de betreffende button klikt, wordt toestemming gegeven voor het profileren.

BEWAARTERMIJN

FYN zal voor het profileren de persoonsgegevens in zijn eigen database opslaan. Geconstateerd is dat FYN nog geen programma heeft ontwikkeld dat de database te zijner tijd kan opschonen door de persoonsgegevens te verwijderen. De persoonsgegevens worden daardoor oneindig in de database bewaard. De wet schrijft

voor dat persoonsgegevens niet langer bewaard mogen worden dan noodzakelijk is om de gestelde doeleinden te verwezenlijken. Nu profileren het doeleinde van FYN wordt, luidt het advies dat de persoonsgegevens die nodig zijn voor het opstellen van de persoonlijkheidsprofielen, bijvoorbeeld de klantdata over de maanden januari tot en met maart, worden verwijderd zodra er profielen zijn opgesteld met deze gegevens. Het doel is dan immers verwezenlijkt: er zijn profielen opgesteld en deze zijn omgezet in statistieken die verstrekt kunnen worden aan de leveranciers.

OVEREENKOMST GEGEVENSVERSTREKKING

Nu geconstateerd is dat de retailer degene is die de gegevens verzamelt en deze aan FYN zal verstrekken ten behoeve van profilering, wordt aanbevolen dat deze afspraken op schrift worden gesteld. De wet kijkt immers bij de gegevensverstrekking op welke wijze deze gegevens zijn verkregen. Als aan de verstrekking van persoonsgegevens een overeenkomst ten grondslag ligt, wordt de wijze van verkrijging van persoonsgegevens minder snel als onrechtmatig aangemerkt. Daarnaast wordt bij een verstrekking van persoonsgegevens gekeken naar de getroffen beveiligingsmaatregelen. Momenteel zijn de getroffen maatregelen conform de wet. Zodra de AVG van kracht is, is FYN gehouden om een beleid te ontwikkelen. Dit beleid moet toetsen of de maatregelen technisch en organisatorisch doeltreffend zijn. Aanbevolen wordt dan ook dat FYN een dergelijk beleid zo spoedig mogelijk opstelt. Met name nu de wet bij het verstrekken van persoonsgegevens rekening houdt met de getroffen beveiligingsmaatregelen. Daarnaast is geconstateerd dat de AP het klik- en surfgedrag als gegeven van gevoelige aard aanmerkt. Ook vanwege dit feit is het van belang dat de beveiligingsmaatregelen vaak getoetst worden op hun technische en organisatorische doeltreffendheid.

De bovenstaande verplichtingen gelden zowel op grond van de Wbp als van de AVG. Hieronder worden de verplichtingen behandeld die alleen op grond van de AVG zullen gelden.

PROFILEREN REGISTREREN

Onder de AVG zal het verplicht zijn om een register bij te houden van de verwerkingsactiviteiten. Dit register omvat informatie die betrekking heeft op de verwerking van persoonsgegevens. Het register moet de gegevens bevatten die in hoofdstuk twee paragraaf 2.2.2.1 zijn besproken. Deze plicht geldt echter alleen voor organisaties met ten minste 250 werknemers, tenzij de verwerking een risico vormt voor de rechten en vrijheden van de betrokkene of zodra er bijzondere gegevens verwerkt worden. Of de verwerking een risico vormt voor de rechten en vrijheden van de betrokkene, is een afweging die de verantwoordelijke moet maken. De AVG merkt op dat het gebruik van nieuwe technologieën een aanwijzing is dat de verwerking van persoonsgegevens een hoog risico met zich meebrengt. Het omnichannelsysteem dat FYN gebruikt, kan aangemerkt worden als een nieuwe technologie. Aanbevolen wordt dan ook dat FYN voor de zekerheid een register bijhoudt zodra er wordt geprofileerd. Dit komt ook ten goede aan het overzicht: FYN weet dan welke handelingen het verricht heeft als er iets fout mocht gaan en is hiermee in staat om sneller het probleem in het systeem te verhelpen.

BEVEILIGING: PRIVACY BY DESIGN

Privacy by design houdt in dat FYN voorafgaand aan het profileren moet onderzoeken welke waarborgen het nog meer kan treffen om de privacy van de betrokkenen te kunnen beschermen. Om daadwerkelijk privacyverhogende maatregelen te nemen, wordt geadviseerd om het volgende te doen:

- De persoonsgegevens wissen nadat de persoonlijkheidsprofielen zijn opgesteld.
- In het gegevensverwerkingsprogramma inbouwen dat een waarschuwing verschijnt zodra meer persoonsgegevens worden ingevoerd dan noodzakelijk is voor het profileren.

- Een checklist opstellen om te controleren of de persoonlijkheidsprofielen die omgezet zijn in statistieken daadwerkelijk goed geanonimiseerd zijn, zodat de leveranciers niet in staat zijn om de statistieken op een zodanige wijze om te zetten dat zij herleidbaar zijn naar een natuurlijk persoon.

De AVG gaat verantwoordelijken voortaan verplichten om een procedure (een beleid) te ontwikkelen. Deze procedure moet toetsen of de beveiligingsmaatregelen op technisch en organisatorisch gebied doeltreffend zijn. FYN heeft een dergelijk beleid niet. FYN wordt dan ook geadviseerd om zo spoedig mogelijk over te gaan tot het opstellen van dit beleid.

Daarnaast zijn de huidige beveiligingsmaatregelen niet op schrift gesteld. Nu aan FYN wordt aanbevolen om te voldoen aan de registratieplicht, is het noodzakelijk dat er een beschrijving gegeven kan worden van de technische en organisatorische beveiligingsmaatregelen. Geadviseerd wordt dan ook dat de huidige en de te treffen maatregelen op schrift worden gesteld.

PIA VOORAFGAAND AAN HET PROFILEREN

FYN is verplicht om voorafgaand aan het profileren een PIA uit te voeren. Bij het nemen van besluiten die tot stand komen door middel van onder andere profilering is een PIA verplicht. In dit geval worden de persoonlijkheidsprofielen gebruikt om een besluit te kunnen nemen, namelijk het versturen van aan personen gerichte aanbiedingen. De profielen worden door FYN omgezet in statistieken. Op basis van deze statistieken passen de leveranciers van de retailers hun marketingstrategie aan. De persoonlijkheidsprofielen hebben namelijk tot gevolg dat de leveranciers gericht kunnen adverteren. De personen van wie de persoonlijke voorkeuren en interesses in kaart zijn gebracht, worden daardoor benaderd met gerichte aanbiedingen. Bij het uitvoeren van een PIA is FYN verplicht om advies in te winnen bij de FG. In de documentatie van de PIA moeten de gegevens worden opgenomen die in hoofdstuk twee paragraaf 2.2.2.1 zijn genoemd.

EEN FUNCTIONARIS GEGEVENSBESCHERMING BENOEMEN

Zodra FYN overgaat tot het profileren, is FYN verplicht een FG aan te stellen. FYN heeft in de rol als bewerker geen wettelijke plicht tot het aanstellen van een FG. FYN kan dit echter wel op vrijwillige basis doen. Geadviseerd wordt om hier zo snel mogelijk toe over te gaan, ook indien er nog niet is begonnen met profileren. Als er eerder een FG wordt aangesteld, kan deze persoon meer kennis opdoen van het systeem waarmee FYN werkt en daardoor zijn taak beter verrichten wanneer begonnen wordt met profileren.

MOGELIJKHEID TOT DATAPORTABILITEIT

Onder de AVG zal de betrokkene het recht van dataportabiliteit hebben. Dit recht kan door de betrokkene onder andere worden uitgeoefend als de verwerking van de persoonsgegevens, die geautomatiseerd dient te zijn, gerechtvaardigd wordt door een beroep te doen op de toestemming van de betrokkene. Geconstateerd is dat FYN de gegevensverwerking ten behoeve van profilering alleen kan rechtvaardigen door hiervoor toestemming te hebben van de betrokkene. Ook is besproken dat de gegevensverwerking door FYN geautomatiseerd plaatsvindt. Nu een betrokkene voldoet aan de vereisten om een beroep te kunnen doen op dit recht, is FYN gehouden om aan dit recht tegemoet te komen zodra de betrokkene hierom verzoekt. Geadviseerd wordt dat FYN interoperabele formaten gaat ontwikkelen om de gegevensoverdraagbaarheid mogelijk te maken.

5.2 Conclusies en aanbevelingen Tw

Het klik- en surfgedrag zal geregistreerd worden door middel van tracking cookies. Daarom is het cookie-artikel uit de Tw geraadpleegd. Hieronder worden aanbevelingen gegeven waaraan voldaan moet zijn voor het plaatsen van tracking cookies.

5.2.1 Cookies: conclusie

Voor het plaatsen van tracking cookies is het vereist dat er toestemming is verkregen en dat de betrokkene hierover is geïnformeerd. De betrokkene (de consument) wordt bij het bezoeken van de website door middel van een balk geïnformeerd dat er tracking cookies geplaatst worden en dient voor het plaatsen van deze cookies toestemming te geven door het aanklikken van de button 'accepteren'. Als er geen toestemming wordt gegeven, kunnen de consumenten gewoon de overige onderdelen van de website raadplegen. De toestemming wordt op correcte wijze gegeven: pas na het aanklikken van de button 'accepteren' wordt het klik- en surfgedrag geregistreerd. Hierdoor wordt voldaan aan het toestemmingsvereiste. De toestemming moet immers bestaan uit een actieve handeling. De MvT van de Tw merkt het aanklikken van een button als een actieve handeling aan.

5.2.2 Cookies: aanbeveling

Nu er geprofileerd zal worden, wordt FYN geadviseerd om de volgende maatregelen te nemen om ook aan de informatieplicht te voldoen:

- In de mededeling die in de balk wordt weergegeven (en waar op de button 'accepteren' geklikt moet worden) zodra de website van de retailer wordt bezocht, opnemen dat FYN beschikking krijgt over het geregistreerde klik- en surfgedrag.
- In de mededeling die in de balk wordt weergegeven (en waar op de button 'accepteren' geklikt moet worden) zodra de website van de retailer wordt bezocht, opnemen dat de data die verzameld worden door middel van het klik- en surfgedrag, gebruikt zullen worden voor profilering.
- In de mededeling die in de balk wordt weergegeven (en waar op de button 'accepteren' geklikt moet worden) zodra de website van de retailer wordt bezocht, opnemen dat de data die verzameld worden door middel van het klik- en surfgedrag, gebruikt zullen worden voor profilering en dat op basis van de resultaten van de persoonlijkheidsprofielen gerichte aanbiedingen worden verstuurd.

Literatuurlijst

Berkvens & Jakimowicz 2016

J. Berkvens & C. Jakimowicz, *Tekstuitgave Privacyverordening met geïntegreerde overwegingen, Wbp- en Richtlijn 95/46/EG-teksten en verwijstabellen*, Den Haag: Boom Juridische uitgevers 2016.

Engelfriet, Meij & Kager 2017

A. Engelfriet, L. Meij & P. Kager, *De Algemene Verordening – Editie 2017 – artikelsgewijs commentaar*, Amsterdam: Ius Mentis 2017.

Hooghiemstra & Nouwt 2016

T.F.M. Hooghiemstra & S. Nouwt, *Sdu commentaar Wet bescherming persoonsgegevens*, Den Haag: Sdu Uitgevers 2016.

Kranenborg & Verhey 2011

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

Overige bronnen

Wet- en regelgeving:

- Wet bescherming persoonsgegevens
- Telecommunicatiewet
- Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG algemene verordening gegevensbescherming (*PbEU* 2016, L 119/1)
- 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 (*PbEG*, L 281/31-50)

Jurisprudentie:

- HvJ EU 13 mei 2014, C-131/12, ECLI:EU:C:2014:317 (*Google/Agencia Española*).
- Cbp 16 januari 1998, 97.V.906.

Elektronische bronnen:

- www.autoriteitpersoonsgegevens.nl, geraadpleegd februari 2017
- www.ictrecht.nl, geraadpleegd februari 2017
- www.europadecentraal.nl, geraadpleegd februari 2017
- www.considerati.com, geraadpleegd maart 2017
- www.privacycompany.eu, geraadpleegd maart 2017
- www.justitia.nl, geraadpleegd maart 2017
- www.home.kpmg.be, geraadpleegd maart 2017
- www.acm.nl, geraadpleegd maart 2017
- www.ensie.nl, geraadpleegd maart 2017
- www.flynth.nl, geraadpleegd april 2017
- www.retailwatching.nl, geraadpleegd april 2017
- www.nrc.nl, geraadpleegd mei 2017

Documenten:

- Opinie van de Groep Gegevensbescherming Artikel 29, nr. 2 van 2010.
- Richtlijnen voor functionarissen voor de gegevensbescherming (FG's) van de Artikel- 29 Werkgroep.
- L.B. Sauerwein en J.J. Linnemann, *Handleiding voor verwerker van persoonsgegevens Wet bescherming persoonsgegevens*, Den Haag: Ministerie van Justitie 2002.

Kamerstukken:

- *Kamerstukken II* 1997/98, 25892, 3 (MvT).
- *Kamerstukken II* 2013/14, 33902, 3 (MvT).

Afbeeldingen:

- FYN Software (z.j.). Omnichannel [Foto].

Geraadpleegd van

<https://fynsoftware.nl/omnichannel>

- FYN Software z.j. Cross Channel [Foto].

Geraadpleegd van

<https://fynsoftware.nl/omnichannel>

- MeganO'Neill, M. (2012, 18 september). TMI: Too Much Information Online?[Foto].
Geraadpleegd van
<http://www.adweek.com/digital/personal-information-online-infographic/>