Really-IT AVG-bestendig?

Praktijkgericht juridisch onderzoek naar de gevolgen van de Algemene verordening gegevensbescherming voor IT-dienstverlener Really-IT

Auteur: J.B.J.R. (Julian) de Corte
Studentnummer: 2067416

Afstudeerorganisatie: Really-IT
Afstudeermentor: Mevrouw S. Harreman
Afstudeerperiode: 5 februari tot en met 28 mei 2018

Onderwijsinstelling: Juridische Hogeschool Avans-Fontys
Opleiding: HBO-Rechten
Locatie: Tilburg

Eerste afstudeerdocent: De heer Mr. F.A.C. Klaassen
Tweede afstudeerdocent: Mevrouw Mr. M. van Bree

Tilburg, mei 2018

Really-IT AVG-bestendig?

Praktijkgericht juridisch onderzoek naar de gevolgen van de Algemene verordening gegevensbescherming voor IT-dienstverlener Really-IT

(Logo)

Auteur: J.B.J.R. (Julian) de Corte
Studentnummer: 2067416

Afstudeerorganisatie: Really-IT
Afstudeermentor: Mevrouw S. Harreman
Afstudeerperiode: 5 februari tot en met 28 mei 2018

Onderwijsinstelling: Juridische Hogeschool Avans-Fontys
Opleiding: HBO-Rechten
Locatie: Tilburg

Eerste afstudeerdocent: De heer Mr. F.A.C. Klaassen
Tweede afstudeerdocent: Mevrouw Mr. M. van Bree

Tilburg, mei 2018

Voorwoord

Voor u ligt het onderzoeksrapport ‘‘Really-IT AVG-bestendig?’’ met aanbevelingen. Dit onderzoeksrapport heb ik ter afsluiting van mijn opleiding HBO-Rechten aan de Juridische Hogeschool Avans-Fontys opgesteld voor IT-dienstverlener Really-IT in Waspik. De aanleiding van dit onderzoek is het van toepassing zijn van de Algemene verordening gegevensbescherming per 25 mei 2018 en de gevolgen die deze privacywetgeving heeft voor Really-IT.

Graag wil ik in het bijzonder een aantal personen bedanken die mij gedurende de stageperiode geholpen hebben bij het tot stand brengen van dit onderzoeksrapport. Allereerst wil ik mijn stagementor, mevrouw S. Harreman, bedanken voor haar prettige begeleiding en positieve instelling gedurende de stage. Ook wil ik de heer R. van de Put en de heer D. van de Put bedanken dat zij mij geïntroduceerd hebben in de IT-branche en het beantwoorden van mijn vragen op dit gebied. Daarnaast wil ik de heer X en de heer X bedanken voor de medewerking aan de interviews en de kennis die zij mij hierdoor hebben verleend. Verder wil ik mevrouw X, juridisch adviseur bij ICTWaarborg, bedanken voor de antwoorden op mijn vragen. Tot slot wil ik mijn stagedocent, de heer mr. F.A.C. Klaassen, bedanken voor zijn feedback en ondersteuning gedurende de stageperiode.

Julian de Corte

Tilburg, mei 2018

Inhoudsopgave

Bijlagen

Bijlage 3 Interview Susanne Harreman

Bijlage 4 Interview Roland van de Put

Bijlage 5 Raamwerk interview cliënten Really-IT

Bijlage 6 Interview X

Bijlage 7 Interview X

Bijlage 8 Participerend observatieonderzoek

Bijlage 9 Huidig reparatieformulier Really-IT

Bijlage 10 Gedragscode ICTWaarborg

Bijlage 11 Contact mevrouw X, juridisch adviseur ICTWaarborg

Samenvatting

Really-IT is een kleine IT-dienstverlener gevestigd in Waspik. Zij houdt zich bezig met werkzaamheden zoals het leveren van software, het maken van een periodieke back-up en het uitvoeren van reparaties voor cliënten. Bij het uitvoeren van deze werkzaamheden verwerkt Really-IT persoonsgegevens. Op 25 mei 2018 is de AVG van toepassing voor organisaties die persoonsgegevens verwerken. Het van toepassing zijn van de AVG heeft de aanleiding gevormd om de huidige werkwijze rondom privacy van Really-IT te onderzoeken. Gedurende dit onderzoek heeft de volgende vraag centraal gestaan: 'Welke aanbevelingen voor een privacybeleid kunnen worden afgeleid uit een toetsing van de huidige werkwijze rondom privacy van Really-IT aan de Algemene verordening gegevensbescherming?'

Om deze vraag te beantwoorden is allereerst bekeken hoe de huidige werkwijze rondom privacy van Really-IT vormgegeven is. Hierbij is gebruik gemaakt van interviews, documentanalyse en observatie. Op dit moment hanteert Really-IT geen privacybeleid. Er is namelijk geen op schrift gesteld beleid waaruit blijkt hoe Really-IT met privacy omgaat. Doordat er niets op schrift is gesteld is nagegaan of Really-IT, ondanks het ontbreken van een privacybeleid, toch rekening houdt met privacy. Really-IT neemt maatregelen om persoonsgegevens te beveiligen. Zij maakt namelijk gebruik van een virusscanner, firewalls, encryptie, periodieke back-ups, wachtwoorden en de monitoring van inlogpogingen. Daarnaast is het pand door alarmsystemen en sloten beveiligd. Ook gaan de medewerkers op een betrouwbare manier om met persoonsgegevens en daarnaast hebben zij een geheimhoudingsbeding. De cliënten hebben hierdoor het gevoel dat er op een juiste wijze met hun persoonsgegevens omgegaan wordt. De AVG is vervolgens geanalyseerd om na te gaan welke bepalingen van toepassing zijn op Really-IT bij de uitvoering van haar werkzaamheden. Uit de analyse blijkt dat Really-IT gedurende haar werkzaamheden aan te merken is als verwerkingsverantwoordelijke en verwerker. De werkwijze van Really-IT is vervolgens getoetst aan de bepalingen van de AVG om na te gaan in hoeverre deze hieraan voldoet. Uit de toetsing is gebleken dat de werkwijze op dit moment niet aan alle beginselen en verplichtingen voldoet. Zo houdt Really-IT geen rekening met het beginsel van rechtmatigheid, behoorlijkheid en transparantie, het beginsel van doelbinding, het beginsel van juiste persoonsgegevens en het beginsel van opslagbeperking. Ook voldoet Really-IT niet aan het beginsel van integriteit en vertrouwelijkheid. De maatregelen die Really-IT neemt zijn weliswaar aan te merken als passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen, maar doordat zij geen rekening houdt met de meld- en registratieplicht van datalekken, wordt niet aan een juiste persoonsgegevensbeveiliging voldaan. Daarnaast heeft Really-IT geen verwerkersovereenkomsten gesloten met cliënten, die als verwerkingsverantwoordelijke aangemerkt kunnen worden, en sub-verwerkers. Ook heeft zij geen verwerkingsregister opgesteld vanuit haar rol van verwerkingsverantwoordelijke en verwerker. Doordat zij niet aan deze beginselen en verplichtingen voldoet, voldoet zij niet aan haar verantwoordingsplicht. Het is Really-IT aan te bevelen om invulling te geven aan de beginselen voor de verwerking van persoonsgegevens. Hierbij is het van belang om transparante informatie omtrent deze beginselen vast te leggen in een privacyverklaring zodat deze aan de cliënt gecommuniceerd kan worden. Het is daarnaast van belang om invulling te geven aan de meld- en registratieplicht van datalekken. Hierdoor kan Really-IT namelijk voldoen aan een juiste persoonsgegevensbeveiliging. Daarnaast dient zij de verplichtingen op het gebied van het opstellen en verzenden van verwerkersovereenkomsten en het opstellen van een verwerkingsregister te hanteren. Middels deze aanbevelingen zullen de beginselen en verplichtingen invulling krijgen doordat zij op schrift worden gesteld en hieruit voortvloeit hoe Really-IT met privacy omgaat. Hierdoor ontstaat een privacybeleid.

Lijst van afkortingen

AVG	Algemene verordening gegevensbescherming
EU	Europese Unie
FG	Functionaris voor gegevensbescherming
IT	Informatietechnologie
Jo.	Juncto
PIA	Privacy Impact Assessment
Richtlijn	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
Wbp	Wet bescherming persoonsgegevens

Hoofdstuk 1. Inleiding

In dit hoofdstuk is het probleem beschreven dat ten grondslag ligt aan dit onderzoek. Vervolgens is de doelstelling en de centrale vraag benoemd. Er zal daarnaast naar voren komen welke deelvragen opgesteld zijn om de centrale vraag te beantwoorden. Verder zullen de onderzoeksstrategieën, bronnen en methoden die voor het onderzoek zijn gebruikt vermeld worden. Tot slot is er een leeswijzer voor dit onderzoek opgenomen.

1.1 Probleembeschrijving

Op 25 mei 2018 is de Algemene verordening gegevensbescherming (hierna: AVG) van toepassing voor de gehele Europese Unie (hierna: EU). De AVG is sinds 25 mei 2016 in werking getreden[1] en totdat deze van toepassing is, zal de AVG naast de Wet bescherming persoonsgegevens (hierna: Wbp) bestaan. De Wbp is de Nederlandse implementatie van de Europese richtlijn bescherming persoonsgegevens[2] (hierna: Richtlijn). De Richtlijn heeft als doel om de bescherming van grondrechten en fundamentele vrijheden met betrekking tot de verwerking van persoonsgegevens en het vrije verkeer van deze persoonsgegevens in de EU te waarborgen[3]. Doordat er snelle technologische ontwikkelingen, globalisering en een significante stijging in het aantal verzamelde en gedeelde persoonsgegevens hebben plaatsgevonden, zijn er nieuwe uitdagingen voor de bescherming van persoonsgegevens ontstaan[4]. Deze ontwikkelingen vereisen een krachtig en coherenter kader voor gegevensbescherming[5]. De Richtlijn kan haar doelstellingen niet langer waarborgen doordat lidstaten verschillende beschermingsniveaus aangaande de bescherming van persoonsgegevens hanteren aangezien zij deze richtlijn verschillend interpreteren in hun nationale wetgeving[6]. Wanneer de AVG van toepassing is, vervalt de Richtlijn en de bijbehorende implementatie daarvan in de Wbp en zijn de lidstaten van de EU verplicht zich aan de AVG te houden. Zij kunnen zich dan niet langer beroepen op nationale wetgeving en zullen gebonden zijn aan dezelfde privacywetgeving.

De AVG is in het leven geroepen zodat de natuurlijke personen in de EU een consistent niveau van gegevensbescherming geboden kan worden en er voorkomen wordt dat verschillen in privacywetgeving het vrije verkeer van persoonsgegevens op de interne markt hinderen[7]. Hierbij is het van belang dat er rechtszekerheid en transparantie geboden worden aan natuurlijke personen en dat er door de AVG voorzien wordt in dezelfde verplichtingen en verantwoordelijkheden voor de verwerkingsverantwoordelijken en verwerkers[8]. Om dit te bereiken zullen huidige privacyrechten verbeterd en uitgebreid worden, dienen organisaties meer verantwoording af te leggen bij het verwerken van persoonsgegevens[9] en zal er vanaf 25 mei 2018 één verordening gevolgd worden die voor de gehele EU geldt zonder dat er nationale wetten geïmplementeerd en steeds herzien dienen te worden[10].

---

[1] www.autoriteitpersoonsgegevens.nl (zoek op: AVG)
[2] Richtlijn 95/46/EG (PbEG 1995 L 281/31)
[3] Overweging 3 Verordening (EU) 2016/679.
[4] Overweging 6 Verordening (EU) 2016/679.
[5] Overweging 7 Verordening (EU) 2016/679.
[6] Overweging 9 Verordening (EU) 2016/679.
[7] Overweging 13 Verordening (EU) 2016/679.
[8] Overweging 13 Verordening (EU) 2016/679.
[9] www.autoriteitpersoonsgegevens.nl (zoek op: AVG)
[10] N. Krijgsman, J. Terstegge & K. Versmissen, *Grip op de AVG*, Deventer: Wolters Kluwer 2017, p. 17.

De veranderingen op het gebied van privacywetgeving hebben gevolgen. Zo ook voor Really-IT. Really-IT is een IT-dienstverlener. Zij houdt zich bezig met het leveren en ondersteunen van het beheer, onderhoud en het beveiligen van computers en servers van haar cliënten. Daarnaast houdt zij zich bezig met het repareren van computers en andere gegevensdragers. Zij zorgt ervoor dat de beveiliging up-to-date is en dat cliënten te allen tijde bij hun gegevens kunnen. Om haar werkzaamheden uit te voeren, heeft Really-IT inzage in de gegevens en gegevensdragers die zij dient te beveiligen of repareren. Daarnaast dient zij gegevens op te slaan, al dan niet op een externe server, om een back-up te maken voor haar cliënten. Door het uitvoeren van deze werkzaamheden komt het voor dat er persoonsgegevens ingezien, opgeslagen en dus verwerkt worden. Dit zorgt ervoor dat de AVG van toepassing is op de werkzaamheden van Really-IT en dat naleving van de AVG van belang is.

Op dit moment loopt Really-IT tegen het probleem aan dat er nog geen sprake is van een implementatie van de AVG in de huidige werkwijze rondom privacy. Wanneer dit niet aangepakt wordt, kan dit tot grote problemen leiden. Iedere organisatie die zich met de verwerking van persoonsgegevens bezighoudt dient zich namelijk per 25 mei 2018 aan de AVG te houden. Wanneer dit niet het geval is, heeft dat consequenties. Zo kunnen er door de Autoriteit Persoonsgegevens hoge boetes toebedeeld worden. Het is voor Really-IT dan ook noodzakelijk om een juiste implementatie van de AVG in de werkwijze rondom privacy door te voeren. Om dit te realiseren is een onderzoek gedaan naar de huidige werkwijze rondom privacy en welke aanpassingen er gedaan dienen te worden zodat de werkwijze voldoet aan de eisen gesteld in de AVG. Er kunnen vervolgens aanbevelingen gedaan worden waardoor een privacybeleid gecreëerd kan worden dat in overeenstemming met de AVG zal zijn wanneer deze op 25 mei 2018 van toepassing is. Er is door Really-IT namelijk de wens uitgesproken dat zij door het onderzoeksrapport en de bijbehorende aanbevelingen een overzicht krijgt van de beginselen en verplichtingen die voortvloeien uit de AVG. Tot slot is er een beroepsproduct opgesteld waarin wordt opgenomen hoe Really-IT in de praktijk aan een aantal aanbevelingen, zoals deze uit het onderzoeksrapport voortvloeien, kan voldoen. Er wordt namelijk een beroepsproduct aangeleverd dat praktisch bruikbare modellen bevat die als leidraad bij de naleving van de AVG gehanteerd kunnen worden.

1.2 Doelstelling

De doelstelling is om op maandag 28 mei 2018 een onderzoeksrapport aan te leveren bij Really-IT waarin middels aanbevelingen beschreven staat wat er aan de huidige werkwijze rondom privacy veranderd dient te worden zodat beleidsbepalers deze veranderingen door kunnen voeren en op schrift kunnen stellen waardoor een privacybeleid ontstaat. Door deze veranderingen kan een privacybeleid gecreëerd worden dat in overeenstemming zal zijn met de AVG wanneer deze op 25 mei 2018 van toepassing is. Het onderzoek zal onder andere de aspecten waar rekening mee gehouden dient te worden op het gebied van de AVG en de huidige werkwijze rondom privacy van Really-IT toelichten. Naast het aanleveren van dit onderzoeksrapport, zal er een beroepsproduct voor Really-IT opgesteld worden. Middels dit beroepsproduct wordt inzichtelijk op welke manier de aanbevelingen die uit dit onderzoeksrapport voortvloeien, in de praktijk invulling kunnen krijgen doordat er praktisch bruikbare modellen voor de naleving van de AVG aangeleverd worden. Door het aanleveren van dit onderzoeksrapport en het beroepsproduct, zal het voor Really-IT duidelijk worden op welke manier zij haar werkwijze aan dient te passen zodat er een privacybeleid gecreëerd

kan worden dat in overeenstemming met de AVG zal zijn en op deze manier kan zij de privacy van haar cliënten kan waarborgen.

1.3 Centrale vraag

Welke aanbevelingen voor een privacybeleid kunnen worden afgeleid uit een toetsing van de huidige werkwijze rondom privacy van Really-IT aan de Algemene verordening gegevensbescherming?

1.4 Deelvragen, bronnen, methoden, verantwoording en onderzoeksstrategieën

Onderstaand zullen de deelvragen die in dit onderzoeksrapport behandeld worden, beschreven worden. Vervolgens zal per deelvraag beschreven worden welke onderzoeksstrategieën, bronnen en methoden zijn gebruikt om de deelvraag te beantwoorden.

1.4.1 Deelvraag 1

Hoe is de huidige werkwijze rondom privacy van Really-IT vormgegeven?

a. Wat voor organisatie is Really-IT?
b. Hoe is de huidige werkwijze rondom privacy van Really-IT tot stand gekomen?
c. Op welke manier is de huidige werkwijze rondom privacy van Really-IT bekend bij cliënten?

Bij de beantwoording van deze deelvraag is een onderzoek naar de praktijk gedaan. Hierbij is een casestudy uitgevoerd. De casestudy bestaat uit een combinatie van semigestructureerde interviews, participerende observatie en een documentanalyse om zo een volledig beeld te krijgen van de huidige werkwijze rondom privacy van Really-IT.

Er zijn allereerst interviews afgenomen bij de drie medewerkers van Really-IT. Het raamwerk voor de interviews met de medewerkers is terug te vinden in de bijlage[11]. Door deze interviews komt naar voren wat voor organisatie Really-IT is, hoe deze in elkaar steekt en wat het belang van beveiliging in de IT-branche is. Doordat de medewerkers dagelijks werkzaamheden namens Really-IT verrichten zijn zij een betrouwbare bron omdat dit een weergave geeft van de huidige situatie die niet door andere personen vergaard kan worden. Naast de medewerkers zijn er een tweetal cliënten op semigestructureerde wijze geïnterviewd om vanuit een ander perspectief dan dat van de medewerkers en de bevindingen van de onderzoeker, een beeld te krijgen van de huidige werkwijze rondom privacy. Het raamwerk voor de interviews met de cliënten is terug te vinden in de bijlage[12]. Deze cliënten zijn geïnterviewd omdat zij een inzicht geven in de wijze waarop Really-IT aan hen bekend maakt dat zij persoonsgegevens verwerken, hoe zij omgaat met persoonsgegevens en om een inzicht te creëren in de organisatie.

Het is daarnaast van belang geweest om verschillende werkprocessen te observeren. Hierbij is gebruik gemaakt van participerende observatie waarbij de vrije variant van observatie gehanteerd is om zo de focus over het gehele werkproces te houden. Door het analyseren van de werkprocessen omtrent reparaties en IT-dienstverlening is in kaart gebracht wat voor persoonsgegevens van cliënten gevraagd worden en of zij geïnformeerd worden over de

[11] Bijlage 1 Raamwerk interview medewerkers Really-IT
[12] Bijlage 5 Raamwerk interview cliënten Really-IT

verwerking. Daarnaast is de algehele omgang met persoonsgegevens geobserveerd op basis van waarnemingsvragen. Naast het observeren van de werkprocessen zijn er door middel van een documentanalyse verschillende documenten, die gebruikt worden in de werkprocessen van Really-IT, geanalyseerd om na te gaan of er rekening gehouden wordt met privacy. Hierbij is gekeken naar documenten zoals fysieke dossiers en de opslag hiervan binnen het kantoor, reparatieformulieren en e-mailcorrespondentie.

1.4.2 Deelvraag 2

Welke bepalingen op het gebied van privacywetgeving die voortvloeien uit de Algemene verordening gegevensbescherming zijn van belang voor Really-IT?

Ter beantwoording van deze deelvraag is er gebruik gemaakt van de onderzoeksstrategie rechtsbronnen- en literatuuronderzoek. Er heeft namelijk een onderzoek naar het recht plaatsgevonden. Deze deelvraag is uitgewerkt door middel van een inhoudsanalyse. Hierbij is de AVG geanalyseerd om helder te krijgen welke bepalingen van belang zijn voor Really-IT. Naast de wet zijn er ook andere bronnen geraadpleegd. Zo is er vakliteratuur zoals het boek Grip op de AVG[13] bestudeerd. Dit boek draagt bij aan de interpretatie van en geeft daarnaast een verdieping op hetgeen in de AVG is vastgelegd. Daarnaast zijn er documenten zoals kamerstukken en meer specifiek het amendement bestudeerd dat betrekking heeft op het feit dat de Autoriteit Persoonsgegevens bij de toepassing van de AVG rekening dient te houden met de specifieke behoefte van micro-ondernemingen[14]. Op basis hiervan is de Aanbeveling van de Commissie[15] omtrent de definitie van kleine-, middelgrote- en micro-ondernemingen bestudeerd om na te gaan of Really-IT aangemerkt kan worden als micro-onderneming. Ook heeft er telefonisch contact plaatsgevonden met een deskundig persoon om een verdieping te krijgen op het gebied van de AVG. Het gaat hier om een juridisch adviseur van ICTWaarborg, mevrouw X. De e-mailcorrespondentie en informatielijst naar aanleiding van het telefonisch contact zijn opgenomen in de bijlage[16]. Really-IT is als (aspirant)lid aangesloten bij ICTWaarborg. ICTWaarborg houdt zich als belangenbehartiger onder andere bezig met het informeren van haar leden met betrekking tot de AVG en wat dit voor gevolgen heeft. Daarnaast zijn er media zoals websites geraadpleegd. Zo is de Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming[17] op de website van de Rijksoverheid bestudeerd. Daarnaast is de website van de Autoriteit Persoonsgegevens geraadpleegd. Deze websites hebben bijgedragen aan een verdieping op de bepalingen zoals deze uit de AVG voortvloeien. Hierdoor is er een nieuw inzicht aan deze bepalingen gegeven en heeft het raadplegen van deze websites bijgedragen aan het vergaren van kennis betreffende de AVG. De Autoriteit Persoonsgegevens is de toezichthoudende autoriteit die zich in Nederland bezighoudt met de toepassing van de AVG. Hierdoor kan de informatie die door haar verleend wordt als betrouwbaar geacht worden.

1.4.3 Deelvraag 3

---

[13] N. Krijgsman, J. Terstegge & K. Versmissen, *Grip op de AVG*, Deventer: Wolters Kluwer 2017.

[14] *Kamerstukken II* 2017/18, 34851, 15, p. 1.

[15] Artikel 2 lid 3 Bijlage Aanbeveling 2003/361/EG van de Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen, PbEU 2003, L 124 van 20 mei 2003.

[16] Bijlage 10 Contact mevrouw X, juridisch adviseur ICTWaarborg

[17] B.W. Schermer & D. Hagenauw & N. Falot, 'Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming', Den Haag: Ministerie van Justitie en Veiligheid 2018.

In hoeverre voldoet de huidige werkwijze rondom privacy van Really-IT aan de bepalingen die voortvloeien uit de Algemene verordening gegevensbescherming?

Deze deelvraag is beantwoord door op basis van de huidige werkwijze rondom privacy van Really-IT, zoals naar voren komt in deelvraag een, en de wet- en regelgeving betreffende de AVG die van toepassing is op Really-IT, zoals naar voren komt in deelvraag twee, te redeneren op welke gronden de huidige werkwijze rondom privacy voldoet aan de bepalingen van de AVG. Om dit te bewerkstelligen is een schema opgesteld waarin de beginselen en verplichtingen zoals deze naar voren komen bij deelvraag twee, getoetst worden aan de huidige werkwijze volgens deelvraag een. Dit schema geeft duidelijk en overzichtelijk aan in hoeverre de huidige werkwijze rondom privacy van Really-IT voldoet aan de AVG. In dit schema komt namelijk het relevante beginsel of de verplichting, die uit de AVG voortvloeit, naar voren. Vervolgens wordt aangegeven of de huidige werkwijze hieraan voldoet. Daarna wordt een toelichting gegeven zodat inzichtelijk is waarom er wel of niet voldaan wordt aan deze bepaling. Er is gekozen om deze deelvraag te beantwoorden door middel van een schema omdat dit zorgt voor duidelijkheid en overzichtelijkheid. Er zijn een aantal beginselen en verplichtingen van toepassing op Really-IT en door in een schema aan te geven waar de huidige werkwijze wel en niet aan voldoet is meteen duidelijk waar ruimte voor verbetering ligt.

1.5 Leeswijzer

In het tweede hoofdstuk van dit onderzoeksrapport zal beschreven worden op welke manier de huidige werkwijze rondom privacy van Really-IT is vormgegeven. Hoofdstuk drie geeft vervolgens aan met welke bepalingen uit de AVG rekening gehouden dient te worden door Really-IT. Daarnaast geeft hoofdstuk vier, door een toetsing van de huidige werkwijze rondom privacy van Really-IT aan de AVG, aan in hoeverre de huidige werkwijze voldoet aan de beginselen en verplichtingen die uit de AVG voortvloeien. In hoofdstuk vijf zullen de conclusies en aanbevelingen van dit onderzoek gegeven worden. Hierdoor zal de centrale vraag van dit onderzoek beantwoord worden.

Hoofdstuk 2. De huidige werkwijze rondom privacy van Really-IT

Om na te gaan hoe de huidige werkwijze rondom privacy van Really-IT is vormgegeven, is het van belang om mee te lopen met de organisatie. Door het interviewen van de medewerkers en cliënten van Really-IT, het observeren en analyseren van de werkprocessen en een documentanalyse kan er een omschrijving gegeven worden van de huidige werkwijze rondom privacy. Op deze manier komt naar voren hoe Really-IT in de praktijk werkt met persoonsgegevens en hoe de algehele werkwijze is vormgegeven.

2.1 Really-IT als organisatie

Really-IT is een IT-dienstverlener die is opgericht op 1 november 2014 en gevestigd is in Waspik. Waspik is een klein dorp met ongeveer 5000 inwoners[18] gelegen in Noord-Brabant. Op dit moment zijn er drie personen werkzaam bij Really-IT. Het is een klein en gemoedelijk IT-bedrijf waar klantvriendelijkheid en sociaal contact hoog in het vaandel staan[19]. Er wordt dan ook getracht om vanuit deze beleving zaken te doen. De cliënten zijn veelal bekenden en woonachtig in dezelfde hechte gemeenschap. Hierdoor is er sprake van een ontspannen werksfeer, ver weg van de drukke stad waarbij alles geregeld en gedocumenteerd is. Door deze beleving is het voor hen in de eerste plaats dan ook belangrijker om de contacten en sociale werkwijze die zij hanteren te handhaven, dan te voldoen aan de formaliteiten die voortvloeien uit verschillende wetgeving. Dit zou een valkuil voor de toepassing van de AVG kunnen zijn.

De werkzaamheden die bij Really-IT uitgevoerd worden hebben betrekking op IT-dienstverlening. Wanneer men denkt aan IT-diensten kan dit gedefinieerd worden als diensten die door een derde partij, zoals Really-IT, geleverd worden voor het plannen, bouwen, beheren en ondersteunen van informatiesystemen[20]. Informatiesystemen zijn op haar beurt een geheel van onderling met elkaar verbonden componenten die samenwerken om informatie te verzamelen, op te slaan en te bewerken om binnen een bepaalde organisatie besluitvorming, coördinatie en het beheer te ondersteunen[21]. Bij een informatiesysteem kan gedacht worden aan een fysieke computer, ook wel hardware genoemd, en de daarbij behorende programma's, ook wel software genoemd, die afgestemd en gebruikt worden voor de doeleinden die de cliënt graag vervuld ziet worden. Om dit dan weer nader te specificeren voor de werkzaamheden van Really-IT, kan hierbij gedacht worden aan het samenstellen en gebruiksklaar maken van een computer met verschillende tekenprogramma's, zoals Adobe Illustrator[22], voor een grafisch ontwerper.

Really-IT houdt zich daarnaast bezig met het leveren van onderhoud en het beveiligen van computers en servers van haar cliënten. Zij zorgt ervoor dat de beveiliging up-to-date is en dat cliënten te allen tijde bij hun gegevens kunnen. Cliënten kunnen verschillende modules afnemen bij Really-IT[23]. Het afnemen van een bepaalde module houdt in dat er voor een vast bedrag per maand een bepaalde dienst wordt afgenomen. Daarnaast kunnen er bij Really-IT allerlei benodigdheden op het gebied van software en hardware aangeschaft worden. Hierbij

[18] www.oozo.nl (zoek op: cijfers Waalwijk Waspik)
[19] www.really-it.nl
[20] www.acm.nl (zoek op: Onderzoeksrapport Marktafbakening in de IT-dienstverlening, p. 5.)
[21] www.acm.nl (zoek op: Onderzoeksrapport Marktafbakening in de IT-dienstverlening, p. 5.)
[22] www.adobe.com (zoek op: Adobe Illustrator)
[23] www.really-it.nl (zoek op: basis modules)

kan gedacht worden aan volledige licenties voor software zoals Microsoft Office 365[24] en programma's voor grafisch ontwerpen. Daarnaast kan men denken aan hardware zoals laptops, computers, usb-sticks, harddisks, wifi-aansluitingen en opladers. Ook is er een reparatiedienst aanwezig waar cliënten terecht kunnen met computers of andere gegevensdragers. Dit probleem wordt dan aangepakt op de werkplaats.

2.2 Totstandkoming huidige werkwijze

Really-IT voert verschillende werkzaamheden uit waarbij persoonsgegevens verwerkt worden. Doordat Really-IT persoonsgegevens verwerkt, is het van belang om een privacybeleid te volgen. Het opstellen en naleven van een privacybeleid is onder de Wbp namelijk ook al van belang. Een privacybeleid is een op schrift gesteld beleid waarin naar voren komt hoe een organisatie met privacy omgaat. Het vastleggen van een privacybeleid dient te gebeuren omdat de medewerkers bekend dienen te zijn met het beleid dat gevolgd moet worden op het gebied van privacy. Ook is het van belang om dit beleid op te stellen zodat het medegedeeld kan worden aan cliënten. Zo weten zij op welke manier hun persoonsgegevens beveiligd worden, waar ze een klacht in kunnen dienen en hoe er in het algemeen met hun persoonsgegevens wordt omgegaan. Op dit moment is er geen privacybeleid opgesteld door Really-IT. Doordat er geen dergelijk beleid is opgesteld dient de huidige werkwijze rondom privacy van Really-IT bestudeerd te worden. Op deze manier kan achterhaald worden hoe zij, aangezien zij niets op schrift heeft gesteld, in de praktijk met privacy omgaat.

Het ligt in de aard van IT-dienstverleners om vanuit hun werkgebied gegevens goed te beveiligen. IT-dienstverleners zijn namelijk naast privacywetgeving gebonden aan strenge regels vanuit hun brancheorganisaties zoals ICTWaarborg. Deze regels worden opgesteld omdat IT-dienstverleners dagelijks te maken krijgen met de verwerking van persoonsgegevens en het hun corebusiness is om deze gegevens en producten te beveiligen door middel van wachtwoorden, encryptie, virusscanners en beveiligde opslaglocaties.

Om na te gaan hoe op dit moment met privacy wordt omgegaan, is het van belang om de werkzaamheden die door Really-IT uitgevoerd worden, te beschrijven. Zo kan er bekeken worden hoe de huidige werkwijze vormgegeven is, hoe er omgegaan wordt met persoonsgegevens en kunnen daarnaast de procedures van de werkzaamheden worden bekeken. Om zo duidelijk mogelijk de huidige situatie te beschrijven is het raadzaam om praktische situaties te omschrijven en hoe er op dat moment gehandeld wordt. De informatie betreffende de praktische situaties is vergaard door interviews met de cliënten en medewerkers van Really-IT[25], een documentanalyse en een participerend observatieonderzoek waarbij gebruik is gemaakt van vrije observatie[26].

2.2.1 Werkwijze op het gebied van reparaties

Op het moment dat een cliënt binnenkomt met een product zoals een computer of laptop die gerepareerd dient te worden, komt de cliënt terecht bij de helpdesk waar de problemen betreffende het product toegelicht kunnen worden[27]. De klachtomschrijving en de gegevens om de cliënt te bereiken worden vervolgens voor de administratie van Really-IT op een

[24] www.microsoft.com (zoek op: Office 365)

[25] Bijlage 1-7 Raamwerk medewerkers Really-IT, Interview Dennis van de Put, Susanne Harreman, Roland van de Put, Raamwerk cliënten Really-IT, Interview X en X

[26] Bijlage 8 Participerend observatieonderzoek

[27] Bijlage 8 Participerend observatieonderzoek

reparatieformulier genoteerd. Daarnaast wordt er een notitie aangemaakt in het systeem om de voortgang van de reparatie te volgen. Het reparatieformulier zal voor de beeldvorming worden toegevoegd in de bijlage[28]. Ter administratie worden de volgende persoonsgegevens van de cliënt genoteerd: naam, adres, woonplaats, postcode, e-mailadres, telefoonnummer(s) en de inlognaam en wachtwoord van het betreffende product. De genoemde informatie wordt aan de cliënt gevraagd zodat deze bereikbaar is en er op het afgeleverde product ingelogd kan worden zodat het probleem verholpen kan worden. Het reparatieformulier wordt enkel door Really-IT gehouden en de cliënt verkrijgt hiervan geen kopie. De cliënt ondertekent niets en er wordt geen toestemming gevraagd betreffende het verwerken van persoonsgegevens. Vervolgens wordt een indicatie gegeven betreffende de reparatieduur. Daarna vertrekt de cliënt, zonder een bon of andere vorm van administratie om aan te tonen dat het product van hem is. Het product wordt vervolgens bewaard op de werkbanken. Deze producten worden verder niet geadministreerd. Voor wat betreft de fysieke maatregelen is het pand beveiligd met verschillende alarmsystemen en daarnaast is het kantoor afgesloten met een deur die voorzien is van een slot. Ook is er een aparte ruimte waar de server en andere aansluitingen van Really-IT gevestigd zijn. Deze ruimte is beveiligd met een afgesloten deur waarvan de sleutel in een kluis bewaard wordt. Daarnaast heeft Really-IT een externe server in het Datacenter Brabant[29]. Verder hebben de medewerkers van Really-IT een geheimhoudingsbeding. De zaken met betrekking tot de beveiliging van het pand en dat de medewerkers een geheimhoudingsbeding hebben, zijn terug te vinden in de uitwerking van het interview met Dennis van de Put[30], Roland van de Put[31] en het participerende observatieonderzoek[32].

De volgende stap is de reparatie van het product. Er wordt allereerst onderzocht of het probleem, zoals aangekaart door de cliënt, het daadwerkelijke probleem is. Wanneer het probleem en de geschatte duur van de werkzaamheden vastgesteld kunnen worden, wordt er contact opgenomen met de cliënt. Deze dient vervolgens toestemming te geven om de werkzaamheden te laten uitvoeren. Tijdens het bekijken van het product komt het uiteraard voor dat er persoonlijke informatie verwerkt wordt. Wanneer er namelijk een laptop nagekeken dient te worden om deze op te schonen of een e-mailadres in te stellen, komt het voor dat er persoonsgegevens zichtbaar zijn en opgeslagen worden door de uitvoerder van de werkzaamheden. Doordat deze persoonsgegevens ingezien worden en er bijvoorbeeld een back-up van deze gegevens gemaakt wordt, worden persoonsgegevens verwerkt terwijl er geen uitdrukkelijke toestemming van de cliënt heeft plaatsgevonden om deze persoonsgegevens te verwerken. De cliënt gaat in eerste instantie namelijk akkoord met de reparatiewerkzaamheden en niet met de verwerking van persoonsgegevens. De werkzaamheden van Really-IT impliceren echter de toestemming aangezien het werk dat zij dient te verrichten niet uitgevoerd kan worden zonder persoonsgegevens in te zien, te bewerken of op te slaan. Wanneer het product gerepareerd is wordt de cliënt hierover ingelicht en kan hij het gerepareerde product ophalen.

2.2.2 Werkwijze op het gebied van IT-dienstverlening

Indien cliënten een dienst bij Really-IT willen afnemen, nemen zij doorgaans telefonisch contact op. Er wordt vervolgens afgesproken wat voor dienstverlening de cliënt wenst te ontvangen. Op basis hiervan wordt een offerte opgesteld en deze dient ondertekend te

[28] Bijlage 9 Huidig reparatieformulier Really-IT
[29] Bijlage 8 Participerend observatieonderzoek
[30] Bijlage 2 Interview Dennis van de Put
[31] Bijlage 4 Interview Roland van de Put
[32] Bijlage 8 Participerend observatieonderzoek

worden om de dienstverlening in te laten gaan. Indien de cliënt akkoord gaat zal er een afspraak gemaakt worden om de betreffende dienstverlening uit te voeren. Het kan hierbij gaan om het creëren van een online werkplek, het bieden van hulp op afstand waarbij er vanuit het kantoor van Really-IT toegang verschaft wordt tot de computer van de cliënt zodat problemen verholpen kunnen worden of het maken van een periodieke back-up.

Deze dienstverlening is beveiligd conform strenge maatregelen. Really-IT is namelijk aangesloten bij brancheorganisatie ICTWaarborg[33]. Deze brancheorganisatie zorgt ervoor dat de werkzaamheden die Really-IT uitvoert, voldoen aan strenge technische maatregelen op het gebied van reparaties en IT-dienstverlening. De beveiliging van online werkplekken wordt bijvoorbeeld geregeld door een aparte omgeving te creëren waar alleen de belanghebbenden bij kunnen. Ook is deze omgeving afgesloten en beveiligd met wachtwoorden en andere technische maatregelen zodat alleen Really-IT en haar cliënt bij deze omgeving kunnen.

Een van deze technische maatregelen is het gebruik van de erkende virusscanner Bitdefender[34] door Really-IT. Een virusscanner is software die ervoor zorgt dat er een constante scan plaatsvindt op het gebied van virussen. Zo wordt er naar verschillende bestanden gekeken om virussen te identificeren, te blokkeren en waar mogelijk te verwijderen. De virusscanner waar Really-IT gebruik van maakt heeft verschillende prijzen[35] gewonnen en kan dus aangemerkt worden als een betrouwbare virusscanner. Dit wordt ook ondersteund door de Consumentenbond. Zij geven aan dat zij 22 virusscanners getest hebben en dat de virusscanner van Bitdefender als beste uit de test komt[36]. Really-IT draagt de zorg voor het installeren van de virusscanner, eventuele toekomstige updates en bewaking van een juiste voortgang. Really-IT heeft daarnaast een flink vertrouwen in deze virusscanner. Mocht er namelijk toch een virus het systeem van een cliënt infecteren, dan zorgt Really-IT ervoor dat dit virus en eventuele verdere aantastingen die dit ten gevolge heeft, kosteloos worden verholpen[37].

Ook worden er periodieke back-ups gemaakt. Een back-up is een kopie van gegevens opgeslagen op een bepaalde gegevensdrager van Really-IT, zoals een computer of externe server. Er vindt één- tot tweemaal daags een back-up plaats. Door deze back-up is er in het geval van calamiteiten te allen tijde een recente back-up beschikbaar zodat de werkprocessen en informatie van cliënten gewaarborgd blijven.

Daarnaast wordt er gebruik gemaakt van firewalls. Een firewall zorgt ervoor dat een computer of systeem beveiligd wordt tegen inkomende dreigingen zoals virussen of pogingen om gehackt te worden. Deze firewall controleert het binnenkomende netwerkverkeer om de hiervoor genoemde dreigingen buiten de deur te houden. Bij Really-IT is sprake van een firewall voor het verkeer dat binnen het netwerk van Really-IT wil komen. Het netwerkverkeer naar buiten staat open. Door het gebruik van deze firewalls is de omgeving waarin Really-IT werkt volgens de experts van Really-IT zeer veilig maar niet onaantastbaar. Dit is een juiste constatering aangezien geen enkele beveiliging in de IT-wereld als onaantastbaar beschouwd kan worden.

[33] www.ictwaarborg.nl
[34] www.bitdefender.nl
[35] www.bitdefender.com
[36] www.bitdefender.nl (zoek op: thuis speciale aanbieding)
[37] www.really-it.nl (zoek op: basis modules computers antivirus)

Vervolgens wordt er bijgehouden of er pogingen plaatsvinden om in te loggen op de accounts en omgevingen van Really-IT en haar cliënten. Deze pogingen worden door Microsoft bijgehouden en zij kunnen bij verdachte omstandigheden Really-IT hierover informeren. Op basis van deze informatie kan Really-IT actie ondernemen door bijvoorbeeld contact op te nemen met de cliënt van wie het systeem aangeeft dat er verdachte pogingen tot inloggen op gebruikersaccounts plaatsvinden. De cliënt kan vervolgens kijken of het gaat om het meermaals foutief invoeren van een wachtwoord door een medewerker of dat er sprake is van een onrechtmatige poging van buitenaf. Dit is dus een extra waarborg op het al bestaande beveiligingssysteem op basis van wachtwoorden, back-ups, firewalls en een virusscanner.

2.2.3 Datalekken

Op grond van de Wbp dient er onder de huidige wetgeving al rekening gehouden te worden met datalekken. Artikel 34a lid 1 Wbp geeft aan dat een datalek een inbreuk op de beveiliging is die leidt tot (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. Het gaat hier om een inbreuk van de beveiliging zoals deze in artikel 13 Wbp genoemd wordt. Dit is een inbreuk waardoor verlies of enige vorm van onrechtmatige verwerking voorkomt. Het gaat hier in de praktijk bijvoorbeeld om het door verlies of diefstal verloren gaan van bestanden waarin persoonsgegevens zijn opgenomen. Er kan hierbij gedacht worden aan het verlies van een usb-stick, diefstal van laptops en het foutief zenden van een e-mail waardoor persoonsgegevens bij personen terecht komen die onbevoegd zijn om van deze gegevens kennis te nemen. Er is tot op heden geen protocol vastgesteld indien een dergelijk datalek zich voordoet. Artikel 13 Wbp geeft aan dat er passende maatregelen genomen dienen te worden om persoonsgegevens te beveiligen tegen verlies of onrechtmatige verwerking. De medewerkers van Really-IT gaan ervan uit dat de persoonsgegevens die men verwerkt voldoende beveiligd zijn door de beveiligingsmaatregelen die zij nemen. Dit blijkt uit het interview met Roland van de Put[38]. Daarnaast is er tot op heden geen sprake geweest van een datalek zoals het verlies van bepaalde bestanden of diefstal van een computer waar persoonsgegevens in voorkomen. Hierdoor heeft er ook geen melding en documentatie plaatsgevonden zoals artikel 34a lid 1 jo. 34a lid 8 Wbp vereist. Wel is er sprake geweest van een inbreuk zoals het verzenden van een e-mail naar een onbevoegde[39]. In dit specifieke geval was er echter geen sprake van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. Hierdoor werd deze inbreuk onder de Wbp niet gezien als een datalek. Deze inbreuk dient hierdoor niet gemeld of gedocumenteerd te worden.

2.2.4 Opslag

Documenten worden niet fysiek opgeslagen. Grotendeels worden deze opgeslagen in de onlinedatabase van Really-IT en deze documenten staan op een beveiligde server. Verder wordt er qua fysieke opslag zo min mogelijk bewaard. Zo zullen reparatieformulieren en informatie die hierop betrekking heeft enkel worden bewaard voor zover het gaat om een lopende reparatie. Vervolgens worden de betreffende documenten ingescand en opgeslagen en zal het fysieke document vernietigd worden zoals blijkt uit het interview met Susanne Harreman[40]. Deze documenten zijn niet meer fysiek beschikbaar maar blijven wel in de database en het e-mailverkeer opgeslagen. Hierdoor komt het voor dat er persoonsgegevens van cliënten in de database van Really-IT opgeslagen blijven, terwijl deze niet meer nodig zijn

[38] Bijlage 4 Interview Roland van de Put
[39] Bijlage 2 Interview Dennis van de Put
[40] Bijlage 3 Interview Susanne Harreman

voor het verlenen van een dienst. Het verwijderen van fysieke documenten gebeurt met de gedachte dat de beveiliging van de database en server voldoende zijn en dat het daarnaast bewaren van fysieke documenten alleen maar risico's met zich mee kan brengen gelet op het door diefstal of verlies in verkeerde handen komen van persoonsgegevens.

2.3 Bekendheid huidige werkwijze bij cliënten

Indien cliënten een bepaalde reparatie uit laten voeren of IT-dienstverlening afnemen, gaan zij ervan uit dat hun gegevens goed beveiligd worden. Zij zijn van mening dat zij bij een bekwaam bedrijf hun gegevens stallen en dat deze zorg draagt voor een goede beveiliging en service. Indien zij deze mening niet hadden, zouden zij geen cliënt zijn van Really-IT. Dit komt naar voren in het interview met de heer X[41]. Het is vanzelfsprekend dat er persoonsgegevens ingezien, opgeslagen en dus verwerkt gaan worden wanneer men een IT-dienstverlener in een computer laat kijken of gegevens in een back-up laat opslaan. De verwerking van persoonsgegevens is namelijk inherent verbonden aan de werkzaamheden die de IT-dienstverlener uit dient te voeren in het kader van de overeenkomst. In de praktijk is het niet zo dat cliënten vragen hebben betreffende privacy. Zij zijn namelijk van mening dat hun persoonsgegevens op een juiste manier bewaard en beveiligd worden. Wel hebben zij het gevoel dat het bij kan dragen om een en ander op papier te krijgen. Dit vloeit ook voort uit het interview met de heer X[42] en de heer X[43]. Zo kunnen de cliënten meer inzage krijgen in wat er daadwerkelijk verwerkt wordt qua persoonsgegevens. Daarnaast wordt er op de website van Really-IT geen gebruik gemaakt van cookies[44]. Hieruit blijkt dat Really-IT zo min mogelijk persoonsgegevens wil verwerken. Zij wil deze persoonsgegevens daarnaast alleen verwerken indien dit noodzakelijk is voor de uitvoering van de betreffende overeenkomst. Daarnaast worden deze gegevens niet verder verwerkt dan waar zij in eerste instantie voor worden gevraagd. Dit is dan ook bekend bij de cliënten. Er is echter niets op papier vastgesteld waardoor aangetoond kan worden dat de cliënten op de hoogte zijn van de werkwijze rondom privacy van Really-IT. De cliënten gaan er echter vanuit dat de persoonsgegevens op een juiste manier beveiligd worden en deze alleen gebruikt worden voor de uitvoering van de overeenkomst.

2.4 Tussenconclusie

Er is bij Really-IT geen sprake van een privacybeleid. Er is namelijk geen schriftelijk beleid opgesteld waaruit af te leiden is hoe Really-IT met privacy omgaat. Bij gebrek aan een dergelijk privacybeleid is de praktijk bekeken. Op deze manier is de huidige werkwijze geanalyseerd en bekeken of er in de praktijk rekening gehouden wordt met privacy. In de praktijk blijkt dat Really-IT in haar huidige werkwijze rekening houdt met privacy. Really-IT beveiligd persoonsgegevens namelijk door verschillende beveiligingsmaatregelen. Het gaat hier om technische maatregelen zoals een virusscanner, firewalls, encryptie, periodieke back-ups, wachtwoorden en de monitoring van inlogpogingen. Daarnaast gaat het om fysieke maatregelen waarbij het pand beveiligd wordt met alarmsystemen en afgesloten deuren naar het kantoor. Ook hebben de medewerkers een geheimhoudingsbeding en daarnaast weten de medewerkers dat zij op een betrouwbare manier met persoonsgegevens om dienen te gaan omdat een goede beveiliging van persoonsgegevens in de aard van IT-dienstverleners ligt. Verder worden de gegevens enkel gebruikt voor zover dit nodig is voor de uitvoering van

[41] Bijlage 7 Interview X
[42] Bijlage 6 Interview X
[43] Bijlage 7 Interview X
[44] Bijlage 4 Interview Roland van de Put

overeenkomsten. Het komt echter voor dat deze gegevens langer worden bewaard dan nodig aangezien deze opgeslagen blijven in de onlinedatabase. De werkwijze is daarnaast in zoverre vormgegeven dat de cliënten ervan uitgaan dat er goed met hun persoonsgegevens wordt omgegaan. Er wordt cliënten echter niet medegedeeld wat er precies van hen verwerkt wordt op het gebied van persoonsgegevens.

Doordat Really-IT geen privacybeleid heeft opgesteld, is het belangrijk om te kijken naar de bepalingen die voortvloeien uit de AVG. Er is op dit moment namelijk wel aandacht voor privacy door de huidige werkwijze, maar het schriftelijk vaststellen van belangrijke bepalingen ontbreekt. Door het analyseren van de bepalingen die voortvloeien uit de AVG, kan bekeken worden in hoeverre deze bepalingen van toepassing zijn op Really-IT.

Hoofdstuk 3. Bepalingen Algemene verordening gegevensbescherming

Op 25 mei 2016 is de AVG in werking getreden[45]. Om het beoogde doel van de AVG te bereiken zullen huidige privacyrechten verbeterd en uitgebreid worden, dienen organisaties meer verantwoording af te leggen bij het verwerken van persoonsgegevens en dient er één verordening gevolgd te worden door de lidstaten van de EU. Organisaties krijgen tot en met 25 mei 2018 de tijd om de AVG te implementeren in hun privacybeleid.

Om na te gaan of de AVG van toepassing is op de werkzaamheden van Really-IT, dient de AVG nader bestudeerd te worden. Zo kunnen de bepalingen die van belang zijn voor Really-IT worden toegelicht.

3.1 Algemene bepalingen

Op grond van artikel 1 AVG worden er door de AVG regels vastgesteld betreffende de bescherming van natuurlijke personen in verband met de verwerking en het vrije verkeer van persoonsgegevens. De verordening beschermt de grondrechten en de fundamentele vrijheden van personen en vooral hun recht op de bescherming van persoonsgegevens.

Artikel 2 AVG geeft het materiële toepassingsgebied van de verordening aan. Op grond van artikel 2 lid 1 AVG is de verordening van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen. Artikel 3 AVG geeft op haar beurt, in het territoriale toepassingsgebied, aan dat de verordening van toepassing is op de verwerking van persoonsgegevens indien een organisatie of bedrijf activiteiten uitvoert binnen de EU.

Artikel 4 AVG geeft vervolgens de definities van begrippen aan die voortvloeien uit de verordening. In artikel 2 AVG wordt het van toepassing zijn van de verordening op de geheel of gedeeltelijk geautomatiseerde verwerking, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen genoemd. Hierdoor is het van belang om na te gaan wat de begrippen persoonsgegevens, verwerking en geautomatiseerde verwerking inhouden om na te gaan of de werkzaamheden van Really-IT binnen het materiële toepassingsgebied van de AVG vallen. Conform artikel 4 lid 1 AVG worden persoonsgegevens gekenmerkt als alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Deze natuurlijke persoon wordt onder de AVG aangemerkt als betrokkene. Het gaat bij persoonsgegevens om identificeerbaarheid die kan worden afgeleid uit een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of een of meer elementen die kenmerkend zijn voor onder andere de fysieke en sociale identiteit van een natuurlijke persoon.. Artikel 4 lid 2 AVG geeft aan dat er sprake is van verwerking indien er een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen en gebruiken van gegevens plaatsvindt. Zoals in hoofdstuk twee naar voren is gekomen, houdt Really-IT zich bezig met het leveren en ondersteunen van het beheer, onderhoud en het beveiligen van computers en servers van hun cliënten. Aangezien Really-IT voor de uitvoering van haar werkzaamheden persoonsgegevens, zoals namen en andere gegevens waardoor natuurlijke personen te identificeren zijn, opslaat, bijwerkt of wijzigt is er sprake van de verwerking van

[45] www.autoriteitpersoonsgegevens.nl (zoek op: AVG)

persoonsgegevens. Het is namelijk niet mogelijk om de werkzaamheden, zoals het uitvoeren van periodieke back-ups van de bedrijfsgegevens van een cliënt, uit te voeren zonder het opslaan van persoonsgegevens. Er dient vervolgens nagegaan te worden of er sprake is van een geautomatiseerde verwerking van persoonsgegevens bij de uitvoering van de werkzaamheden van Really-IT. Er is sprake van een geautomatiseerde verwerking van persoonsgegevens wanneer persoonsgegevens verwerkt worden middels computers, tablets, servers, smartphones en andere vergelijkbare apparaten[46]. Really-IT dient voor het uitvoeren van haar werkzaamheden persoonsgegevens op te slaan in computers, servers en databases aangezien zij een IT-dienstverlener is.

Bij de uitvoering van de werkzaamheden van Really-IT is dus sprake van de geautomatiseerde verwerking van persoonsgegevens conform artikel 2 lid 1 AVG. Hierdoor is de AVG materieel van toepassing op de werkzaamheden van Really-IT. De AVG is daarnaast, conform artikel 3 AVG, territoriaal van toepassing op de werkzaamheden van Really-IT doordat haar werkzaamheden binnen de EU plaatsvinden.

Er worden daarnaast in artikel 4 lid 7 jo 8 AVG twee andere belangrijke begrippen genoemd. We hebben het hier dan over de begrippen verwerkingsverantwoordelijke en verwerker. Het is interessant om naar deze begrippen te kijken omdat Really-IT in verschillende verhoudingen met haar cliënten staat. Er dient dan ook per cliënt gekeken te worden welk begrip van toepassing is en in welke verhouding men volgens de AVG met Really-IT staat.

Allereerst geeft artikel 4 AVG een omschrijving van deze begrippen. In artikel 4 lid 7 AVG spreekt men over verwerkingsverantwoordelijke. Dit is een natuurlijk persoon of rechtspersoon die, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Dit begrip is relevant voor Really-IT. Wanneer het gaat om cliënten die bijvoorbeeld enkel een virusscanner afnemen of een reparatie laten uitvoeren, bepaalt Really-IT zelf het doel van en de middelen voor de verwerking van persoonsgegevens. Zij bepaalt namelijk zelf welke gegevens zij dient te verwerken om op deze manier het doel, bijvoorbeeld het verlenen en uitvoeren van de virusscanner of reparatie, te realiseren. In dit geval kan Really-IT aangemerkt worden als verwerkingsverantwoordelijke.

Daarnaast geeft artikel 4 lid 8 AVG een omschrijving van het begrip verwerker. Het gaat volgens dit artikel om een natuurlijke persoon of rechtspersoon die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. In de meeste gevallen wordt Really-IT door bedrijven benaderd om een bepaalde IT-dienstverlening te leveren. Het gaat hier dan bijvoorbeeld om het faciliteren van een online werkplek voor alle medewerkers van een bedrijf, het op afstand ondersteunen van een medewerker wanneer deze moeilijkheden ondervindt, het maken van periodieke back-ups en de beveiliging up-to-date te houden. In deze gevallen heeft Really-IT inzicht in bepaalde persoonsgegevens, slaat zij deze op en dus verwerkt zij deze. Really-IT stelt in deze betrekking niet het doel van en de middelen voor de verwerking van persoonsgegevens vast. De cliënt stelt in dit geval namelijk zelf, doordat zij bepaalde informatie van haar medewerkers in een periodieke back-up wil laten opslaan, het doel van en de middelen voor de verwerking van persoonsgegevens vast. Doordat deze informatie vervolgens verwerkt wordt door Really-IT, is zij verwerker. In de meeste gevallen is er sprake van een verhouding tussen dit soort cliënten en Really-IT. Hierbij zijn de cliënten de verwerkingsverantwoordelijke en Really-IT de verwerker. Dit biedt een ander perspectief voor

[46] B.W. Schermer & D. Hagenauw & N. Falot, 'Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming', Den Haag: Ministerie van Justitie en Veiligheid 2018, p. 28.

de invulling van andere begrippen en regelingen die conform de AVG geregeld dienen te worden.

3.2 Beginselen

Bij de uitvoering van de werkzaamheden van Really-IT is er sprake van de verwerking van persoonsgegevens. Het is van belang dat er op een correcte wijze met deze gegevens wordt omgegaan. Artikel 5 AVG geeft aan welke beginselen in acht gehouden dienen te worden wanneer persoonsgegevens verwerkt worden.

Op grond van artikel 5 lid 1 sub a AVG moeten persoonsgegevens ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant worden verwerkt. Dit wordt ook wel het beginsel van rechtmatigheid, behoorlijkheid en transparantie genoemd. Een rechtmatige gegevensverwerking houdt in dat de verwerking niet in strijd mag zijn met het Unierecht of het lidstatelijk recht[47]. Daarnaast wordt de rechtmatigheid van de verwerking gebaseerd op een van de grondslagen zoals genoemd in artikel 6 AVG. De eis dat een gegevensverwerking behoorlijk dient te zijn wordt vormgegeven door de verwerking verantwoord plaats te laten vinden[48]. Een transparantie verwerking houdt vervolgens in dat er op een duidelijke en heldere manier aan de betrokkene gecommuniceerd wordt dat er persoonsgegevens van hem verwerkt worden, waarom deze persoonsgegevens verwerkt worden, in hoeverre dit gebeurd, door wie en welke rechten hij gedurende deze verwerking heeft[49].

Artikel 5 lid 1 sub b AVG geeft vervolgens het beginsel van doelbinding aan. Persoonsgegevens moeten voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en deze mogen niet met onverenigbare wijze met die doeleinden worden verwerkt. Dit houdt in dat, voordat persoonsgegevens verwerkt worden, er nagegaan en vastgelegd wordt waarom deze persoonsgegevens verzameld gaan worden[50]. De persoonsgegevens dienen daarnaast op een gerechtvaardigde wijze verzameld te worden. Hiervan is sprake als de verwerking gebaseerd is op een van de grondslagen conform artikel 6 AVG[51]. Daarnaast is het belangrijk om persoonsgegevens verenigbaar met de vooraf bepaalde doeleinden te verwerken[52]. Dit houdt in dat de persoonsgegevens alleen gebruikt mogen worden voor het doel waarvoor ze in eerste instantie zijn verstrekt. Indien deze gegevens vervolgens voor een ander doel gebruikt gaan worden is hier een nieuwe grondslag voor nodig en is er dus geen sprake van verenigbaar gebruik[53].

Op grond van artikel 5 lid 1 sub c AVG dienen de persoonsgegevens toereikend te zijn, ter zake dienend en beperkt te zijn tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt. Het gaat hier om het beginsel van minimale gegevensverwerking.

---

[47] N. Krijgsman, J. Terstegge & K. Versmissen, *Grip op de AVG*, Deventer: Wolters Kluwer 2017, p. 55.

[48] B.W. Schermer & D. Hagenauw & N. Falot, 'Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming', Den Haag: Ministerie van Justitie en Veiligheid 2018, p. 22.

[49] Overweging 39 Verordening (EU) 679/2016. jo. www.nederlandict.nl (zoek op: transparantie en het recht op informatie)

[50] N. Krijgsman, J. Terstegge & K. Versmissen, *Grip op de AVG*, Deventer: Wolters Kluwer 2017, p. 56.

[51] B.W. Schermer & D. Hagenauw & N. Falot, 'Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming', Den Haag: Ministerie van Justitie en Veiligheid 2018, p. 35-36.

[52] N. Krijgsman, J. Terstegge & K. Versmissen, *Grip op de AVG*, Deventer: Wolters Kluwer 2017, p. 56.

[53] N. Krijgsman, J. Terstegge & K. Versmissen, *Grip op de AVG*, Deventer: Wolters Kluwer 2017, p. 56.

Gegevens mogen niet verwerkt worden indien zij niet nodig of niet relevant zijn voor het uitvoeren van de doeleinden die vastgesteld zijn[54].

De verwerkte persoonsgegevens dienen volgens het beginsel van juistheid van persoonsgegevens, dat voortvloeit uit artikel 5 lid 1 sub d AVG, correct en actueel te zijn. Indien dit niet het geval is, dienen deze persoonsgegevens gerectificeerd of gewist te worden. De verwerkingsverantwoordelijke dient alle redelijke maatregelen te nemen om ervoor te zorgen dat hij juiste persoonsgegevens verwerkt.

Daarnaast dienen persoonsgegevens conform artikel 5 lid 1 sub e AVG te worden bewaard op een manier die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de hiervoor genoemde doeleinden noodzakelijk is of dat deze verwijderd worden[55] indien zij niet langer nodig zijn. Het gaat hierbij om het beginsel van opslagbeperking. Het is bij dit beginsel van belang om de opslagperiode te beperken tot een minimum[56]. Om dit te realiseren dient er gebruik gemaakt te worden van bewaartermijnen om te bepalen wanneer persoonsgegevens gewist dienen te worden of dient er een periodieke toetsing van deze persoonsgegevens plaats te vinden om na te gaan of deze verwijderd dienen te worden[57].

Tot slot is er het beginsel van integriteit en vertrouwelijkheid. Bij dit beginsel is het van belang dat persoonsgegevens op een passende manier beveiligd dienen te worden door het nemen van technische of organisatorische maatregelen volgens artikel 5 lid 1 sub f AVG. Door het nemen van deze maatregelen dienen persoonsgegevens onder meer beveiligd te zijn tegen ongeoorloofde of onrechtmatige verwerking, onopzettelijk verlies, vernietiging of beschadiging. Om een dergelijke beveiliging te realiseren dient er gekeken te worden naar de bepalingen met betrekking tot persoonsgegevensbeveiliging, vastgelegd in hoofdstuk 4 afdeling 2 van de AVG. Meer specifiek gaat het hier om de bepalingen met betrekking tot beveiliging van persoonsgegevens, vormgegeven door passende technische en organisatorische maatregelen en de melding van een inbreuk met betrekking tot persoonsgegevens conform artikel 32 jo. 33 jo. 34 AVG.

Artikel 5 lid 2 AVG geeft aan dat de verwerkingsverantwoordelijke verantwoordelijk is voor het naleven van de beginselen genoemd in artikel 5 lid 1 AVG. Hij dient deze naleving aan te kunnen tonen. Dit wordt ook wel de verantwoordingsplicht genoemd. Naast het aantonen van het naleven van de beginselen genoemd in artikel 5 lid 1 AVG, dient de verwerkingsverantwoordelijke ook aan te kunnen tonen dat hij aan zijn verplichtingen volgens de AVG voldoet door deze te documenteren[58]. Deze verplichtingen zullen in het verdere verloop van dit hoofdstuk aan bod komen.

3.3 Grondslag

Artikel 6 AVG geeft uitleg betreffende de rechtmatigheid van de verwerking. Conform artikel 6 lid 1 AVG is de verwerking alleen rechtmatig indien en voor zover aan minimaal een van de voorwaarden zoals genoemd in sub a tot en met f is voldaan:

---

[54] N. Krijgsman, J. Terstegge & K. Versmissen, *Grip op de AVG*, Deventer: Wolters Kluwer 2017, p. 58.
[55] N. Krijgsman, J. Terstegge & K. Versmissen, *Grip op de AVG*, Deventer: Wolters Kluwer 2017, p. 59.
[56] Overweging 39 Verordening (EU) 679/2016.
[57] Overweging 39 Verordening (EU) 679/2016.
[58] B.W. Schermer & D. Hagenauw & N. Falot, 'Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming', Den Haag: Ministerie van Justitie en Veiligheid 2018, p. 51.

a) er dient toestemming te zijn gegeven door de betrokkene voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;

b) er sprake is van een noodzakelijke verwerking voor de uitvoering of de voorbereiding van een overeenkomst waarbij de betrokkene partij is;

c) de verwerking noodzakelijk is om te voldoen aan een wettelijke verplichting van de verwerkingsverantwoordelijke;

d) de verwerking noodzakelijk is om de vitale belangen van de betrokkene te beschermen;

e) de verwerking noodzakelijk is voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag waaraan de verwerkingsverantwoordelijke dient te voldoen;

f) de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke.

In artikel 6 lid 1 sub a tot en met f AVG wordt toestemming als eerste voorwaarde genoemd. Het kan in de toekomst voorkomen dat Really-IT op grond van artikel 6 lid 1 sub a AVG persoonsgegevens wil verwerken. Een voorbeeld hiervan is dat zij persoonsgegevens wil gaan verwerken voor een nieuwsbrief. De regels op het gebied van toestemming worden allereerst gegeven in artikel 4 lid 11 AVG. Volgens artikel 4 lid 11 AVG is dit de toestemming van de betrokkene. Het gaat om een vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling de betreffende verwerking van persoonsgegevens aanvaardt. Deze actieve handeling kan gevormd worden door de betrokkene op een vakje te laten klikken op de website waardoor hij toestemming geeft[59]. Indien er sprake is van een verwerking van persoonsgegevens gebaseerd op toestemming van de betrokkene, dan dient deze toestemming volgens artikel 7 AVG aan een aantal voorwaarden te voldoen. Zo dient de verwerkingsverantwoordelijke gelet op artikel 7 lid 1 AVG aan te tonen dat de verwerking van persoonsgegevens op basis van voorafgaande toestemming heeft plaatsgevonden. Het verzoek om toestemming voor de verwerking van persoonsgegevens dient in een toegankelijke vorm en in duidelijke en eenvoudige taal gepresenteerd te worden. Daarnaast dient het verzoek los te staan van andere zaken waarvoor toestemming gegeven kan worden volgens artikel 7 lid 2 AVG. De betrokkene heeft, gelet op artikel 7 lid 3 AVG, het recht om zijn toestemming te allen tijde in te trekken en deze intrekking dient even eenvoudig te geschieden als het geven van de toestemming. Indien Really-IT op basis van toestemming persoonsgegevens van cliënten wil verwerken, dient zij rekening te houden met de regels op het gebied van toestemming.

Het ligt voor de hand dat Really-IT op basis van artikel 6 lid 1 sub b AVG persoonsgegevens verwerkt. Het is namelijk noodzakelijk om gegevens van de cliënt te verwerken om de overeenkomst uit te voeren of voor te bereiden. Er kan bijvoorbeeld geen virusscanner worden afgenomen indien Really-IT de naam van de cliënt niet kan noteren ter administratie. Daarnaast kan er om dezelfde reden geen back-up worden gemaakt indien men geen persoonsgegevens aan Really-IT verstrekt om te verwerken. Het verwerken van persoonsgegevens hoort impliciet bij de werkzaamheden die Really-IT uit dient te voeren en de IT-dienstverlening die zij leveren op basis van een overeenkomst.

[59] N. Krijgsman, J. Terstegge & K. Versmissen, *Grip op de AVG*, Deventer: Wolters Kluwer 2017, p. 63.

Het is niet van belang om de andere voorwaarden zoals genoemd in artikel 6 lid 1 sub c tot en met f AVG te behandelen. Deze zijn namelijk niet van toepassing op de werkzaamheden van Really-IT.

3.4 Bijzondere persoonsgegevens

Naast de gebruikelijke persoonsgegevens bestaan er conform artikel 9 AVG ook bijzondere persoonsgegevens. Dit zijn persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken. Daarnaast zijn genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon of gegevens over gezondheid of met betrekking tot iemands seksuele geaardheid bijzondere persoonsgegevens. Het is in beginsel verboden om deze bijzondere persoonsgegevens te verwerken. Indien er echter sprake is van een voorwaarde zoals genoemd in artikel 9 lid 2 AVG dan is het geoorloofd om deze gegevens te verwerken. Artikel 9 lid 2 sub a AVG geeft bijvoorbeeld aan dat er uitdrukkelijke toestemming dient te zijn van de betrokkene voor de verwerking van dergelijke gegevens.

Er worden over het algemeen geen bijzondere persoonsgegevens door Really-IT verwerkt. Het is niet de corebusiness om bijzondere persoonsgegevens te verwerken. Toch kan het voorkomen dat er door de diensten die Really-IT aanbiedt, zoals het maken van periodieke back-ups, bijzondere persoonsgegevens worden verwerkt. Dit kan voorkomen doordat de verwerkingsverantwoordelijke bijzondere persoonsgegevens, zoals pasfoto's, in zijn bestanden heeft opgeslagen en Really-IT daar vervolgens een back-up van maakt en deze dus verwerkt. Het is voor Really-IT echter niet na te gaan wat de cliënten in hun back-ups opslaan. Op dit moment wordt de informatie van cliënten opgeslagen in back-ups en deze worden verder niet ingezien. De back-ups worden door encryptie beveiligd waardoor Really-IT niet naar de inhoud van de back-up kan kijken. Indien Really-IT iedere back-up van een cliënt dient te controleren op de gegevens die zij hierin opslaan om een onderscheid te maken tussen bijzondere en normale persoonsgegevens, dan zorgt dit juist voor een inbreuk op hun privacy. Daarnaast zou hier veel tijd in gaan zitten waardoor het niet werkbaar is om dergelijke werkzaamheden uit te voeren. De back-up moet dus gezien worden als een dienst die verder losstaat van de verwerking van bijzondere persoonsgegevens. Het is het opslaan van data die voor onbevoegden onbekend en beveiligd is en daarnaast wordt deze niet ingezien door Really-IT. Zij fungeert enkel als aanbieder van een opslagpunt. Zij zorgt ervoor dat deze gegevens beveiligd worden. Zo kan zij de informatie opnieuw aanbieden aan de cliënt indien deze informatie onverhoopt verloren is gegaan.

3.5 De rechten van de betrokkenen

Bij de toepassing van de AVG dient gekeken te worden naar de rechten van de betrokkene. Het is relevant om naar deze bepalingen te kijken omdat Really-IT verschillende cliënten heeft. Zoals gezegd treedt zij op in de rol van verwerkingsverantwoordelijke en daarnaast als die van verwerker. Door naar de bepalingen te kijken die van toepassing zijn op deze cliënten, kan naar voren komen hoe er met hen gecommuniceerd dient te worden, welke informatie Really-IT aan hen kan verstrekken en welke rechten zij hebben.

3.5.1 Transparante informatie en communicatie

Om de rechten van de betrokkenen te waarborgen is onder andere artikel 12 AVG van toepassing. Artikel 12 lid 1 AVG geeft aan dat de informatie en communicatie tussen de verwerkingsverantwoordelijke en de betrokkene in begrijpelijke, transparante, beknopte, makkelijk toegankelijke vorm en in duidelijke en eenvoudige taal moet plaatsvinden. De

verwerkingsverantwoordelijke dient hiervoor passende maatregelen te nemen. Dat de informatie tussen de verwerkingsverantwoordelijke en de betrokkene onder andere op een transparante wijze plaats dient te vinden, geeft aan dat de informatieplicht uit artikel 12 AVG nauw samenhangt met het beginsel van rechtmatigheid, behoorlijkheid en transparantie zoals genoemd in artikel 5 lid 1 sub a AVG[60]. De hiervoor bedoelde informatie heeft betrekking op de informatie die op grond van artikel 13 jo. 14 AVG verstrekt dient te woorden door Really-IT aan de betrokkene, de rechten die betrokkene gedurende de gegevensverwerking heeft conform artikel 15 tot en met 22 AVG en de melding van een inbreuk met betrekking tot persoonsgegevens van de betrokkene volgens artikel 34 AVG. Deze informatie kan vastgelegd worden in een privacyverklaring die aan de cliënt bekend gemaakt dient te worden[61].

Op grond van artikel 12 lid 3 AVG dient de verwerkingsverantwoordelijke binnen een maand na ontvangst van een verzoek als genoemd in artikelen 15 tot en met 22 AVG, informatie te verschaffen omtrent het gevolg van dat verzoek. Het gaat hierbij om een verzoek van de betrokkene ten op zichten van de rechten die hij gedurende de verwerking van persoonsgegevens heeft. Het is daarnaast van belang dat de verwerkingsverantwoordelijke de betrokkene kan identificeren om een gevolg te geven aan een dergelijk verzoek conform artikel 12 lid 2 AVG. Indien het gaat om een complex verzoek, dan kan deze termijn met nog eens twee maanden worden verlengd. De verwerkingsverantwoordelijke dient de betrokkene binnen de eerstgenoemde termijn, die van een maand, te informeren over een mogelijke verlenging.

Indien de verwerkingsverantwoordelijke conform artikel 12 lid 4 AVG geen gevolg geeft aan het verzoek van betrokkene, dan dient hij binnen een maand na ontvangst van het verzoek kenbaar te maken waarom hij hiervoor gekozen heeft. Daarnaast dient hij hem te informeren over de mogelijkheid om een klacht in te dienen bij de toezichthoudende autoriteit en over het feit dat hij beroep bij de rechter in kan stellen. De informatieverstrekking die de verwerkingsverantwoordelijke jegens de betrokkene dient te verschaffen op basis van de artikelen 13, 14, 15 tot en met 22 en 34 AVG dient kosteloos te zijn. Hiervan is geen sprake indien de verzoeken van de betrokkene ongegrond of buitensporig zijn. In dat geval kan hij een redelijke vergoeding in rekening brengen gebaseerd op de administratieve kosten om een dergelijk verzoek te honoreren of weigeren een gevolg te geven aan het verzoek conform artikel 12 lid 5 sub a jo b AVG.

Artikel 13 AVG geeft aan dat er bepaalde gegevens verstrekt dienen te worden door de verwerkingsverantwoordelijke indien de persoonsgegevens bij de betrokkene zelf worden verzameld. Wanneer Really-IT in de rol van verwerkingsverantwoordelijke handelt, vraagt zij de persoonsgegevens bij de cliënt op. In dat geval zal aan hem informatie betreffende de naam, adres, woonplaats en het e-mailadres opgevraagd worden. Op grond van artikel 13 lid 1 sub a tot en met f AVG dient de verwerkingsverantwoordelijke bij de verkrijging van persoonsgegevens de volgende informatie te verstrekken aan de betrokkene:

a) de identiteit en de contactgegevens van de verwerkingsverantwoordelijke;

---

[60] Overweging 39 Verordening (EU) 679/2016. jo. www.nederlandict.nl (zoek op: transparantie en het recht op informatie)

[61] B.W. Schermer & D. Hagenauw & N. Falot, 'Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming', Den Haag: Ministerie van Justitie en Veiligheid 2018, p. 51.

b) indien van toepassing, de contactgegevens van de functionaris gegevensbescherming;

c) de verwerkingsdoeleinden waar de persoonsgegevens voor worden verwerkt en daarnaast de rechtsgrond hiervan;

d) de gerechtvaardigde belangen van de verwerkingsverantwoordelijke indien de verwerking gebaseerd is op artikel 6 lid 1 sub f AVG;

e) indien van toepassing, de ontvangers of categorieën van ontvangers van de persoonsgegevens;

f) indien van toepassing, dat de verwerkingsverantwoordelijke het voornemen heeft de persoonsgegevens door te geven aan een organisatie in een derde land.

Artikel 13 lid 2 sub a tot en met f AVG geeft vervolgens een aantal aanvullende eisen waaraan voldaan dient te worden door de verwerkingsverantwoordelijke. Deze informatie dient naast de in artikel 13 lid 1 AVG genoemde informatie genoemd te worden om ervoor te zorgen dat de verwerking transparant en behoorlijk is. Het gaat hier om het verstrekken van de volgende informatie:

a) gedurende welke periode persoonsgegevens zullen worden opgeslagen of wanneer hiervoor geen vaste periode is de criteria die deze opslag motiveren;

b) het recht van de betrokkene om zijn recht van inzage, rectificatie, wissing, bezwaar en gegevensoverdraagbaarheid te verzoeken. Hij kan daarnaast vragen om een beperking van de verwerking van persoonsgegevens;

c) het recht van de betrokkene om toestemming zoals genoemd in artikel 6 lid 1 sub a AVG te allen tijde in te trekken;

d) het recht om een klacht in te dienen door de betrokkene bij de toezichthoudende autoriteit;

e) dat het verstrekken van persoonsgegevens een noodzakelijke voorwaarde is om de overeenkomst te sluiten en dat de betrokkene ingelicht wordt over de gevolgen indien deze gegevens niet worden verstrekt;

f) of er sprake is van geautomatiseerde besluitvorming en in dat geval dient relevante informatie en de gevolgen van deze verwerking verschaft te worden.

Artikel 14 AVG geeft aan dat er bepaalde gegevens verstrekt dienen te worden door de verwerkingsverantwoordelijke indien de persoonsgegevens niet van de betrokkene zijn verkregen. Aangezien Really-IT in haar rol van verwerkingsverantwoordelijke altijd informatie van de cliënt zelf verkrijgt is dit artikel niet van toepassing op Really-IT.

3.5.2 Recht van inzage

Op grond van artikel 15 AVG heeft de betrokkene recht van inzage. Dit houdt op grond van artikel 15 lid 1 AVG in dat de betrokkene inzicht kan krijgen over het feit of de verwerkingsverantwoordelijke gegevens van hem verwerkt. Daarnaast kan hij inzage in deze gegevens vragen. De zaken waarover de betrokkene inzage kan vragen staan genoemd in artikel 15 lid 1 sub a tot en met h AVG. Het gaat hier om informatie betreffende de verwerkingsdoeleinden, de betrokken categorieën van persoonsgegevens, de ontvangers of categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt en de bewaartermijnen of criteria die de termijn van het bewaren bepalen. Daarnaast dient

bekend gemaakt te worden dat de betrokkene het recht heeft om de verwerkingsverantwoordelijke te verzoeken om persoonsgegevens te rectificeren, te wissen, te laten beperken en dat hij bezwaar tegen deze verwerking kan maken. Ook heeft de betrokkene het recht om een klacht in te dienen bij een toezichthoudende autoriteit. Vervolgens dient aan de betrokkene de bron van de informatie bekendgemaakt te worden indien persoonsgegevens niet bij hem zijn verzameld. Tot slot dient aan de betrokkene bekend gemaakt te worden of er sprake is van geautomatiseerde besluitvorming. Op grond van artikel 15 lid 3 AVG verkrijgt de betrokkene een kopie van de persoonsgegevens die worden verwerkt van de verwerkingsverantwoordelijke.

3.5.3 Recht op rectificatie

In artikel 16 AVG is het recht op rectificatie opgenomen. Wanneer er onjuiste persoonsgegevens van de betrokkene zijn verwerkt, heeft de betrokkene het recht om dit te laten rectificeren. De betrokkene heeft het recht om de persoonsgegevens volledig aangevuld te zien worden door de verwerkingsverantwoordelijke. Hierbij dienen de doeleinden van de verwerking in acht te worden genomen.

3.5.4 Recht op vergetelheid

In artikel 17 AVG wordt een recht genoemd dat een nieuwe bepaling is door het in werking treden van de AVG. Het gaat hier om het recht op vergetelheid. Op grond van artikel 17 lid 1 AVG heeft de betrokkene het recht om persoonsgegevens die op hem van toepassing zijn te laten verwijderen zonder onredelijke vertraging door de verwerkingsverantwoordelijke. De verwerkingsverantwoordelijke is verplicht om de persoonsgegevens van een betrokkene te verwijderen indien er sprake is van een van de gevallen zoals genoemd in artikel 17 lid 1 sub a tot en met f AVG:

a) de persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor zij zijn verwerkt;

b) de betrokkene trekt de toestemming waarop de verwerking overeenkomstig is in en er is geen andere rechtsgrond voor de gegevensverwerking;

c) de betrokkene maakt bezwaar tegen de verwerking;

d) de persoonsgegevens onrechtmatig zijn verwerkt;

e) de persoonsgegevens moeten worden gewist om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;

f) de persoonsgegevens zijn verzameld door een informatiemaatschappij bij een aanbod van diensten aan een kind.

3.5.5 Recht op beperking van de verwerking

Op grond van artikel 18 AVG heeft de betrokkene het recht op beperking van de verwerking. Hij heeft hier recht op indien er sprake is van een of meerdere voorwaarden zoals genoemd in artikel 18 lid 1 sub a tot en met d AVG. Het gaat in dit geval allereerst om situaties waarbij de juistheid van persoonsgegevens door de betrokkene wordt betwist. Daarnaast gaat het om de vraag of de verwerking onrechtmatig is en de betrokkene zich verzet tegen het wissen van deze gegevens. Hij verzoekt in plaats daarvan om beperking van de verwerking. Daarnaast kan het voorkomen dat de verwerkingsverantwoordelijke de persoonsgegevens niet meer nodig heeft voor de verwerkingsdoeleinden maar de betrokkene deze nog nodig heeft voor

de instelling, uitoefening of de onderbouwing van een rechtsvordering. Ten slotte is er sprake van het recht op beperking van verwerking indien de betrokkene in bezwaar gaat tegen de verwerking en op antwoord wacht.

3.5.6 Recht op dataportabiliteit

In artikel 20 AVG wordt het recht op overdraagbaarheid, ook wel het recht op dataportabiliteit, genoemd[62]. Dit is een van de nieuwe rechten die door de AVG in het leven is geroepen. Het recht op dataportabiliteit houdt volgens artikel 20 lid 1 AVG in dat de betrokkene het recht heeft om de persoonsgegevens die van hem verwerkt worden door de verwerkingsverantwoordelijke, in een gestructureerde, gangbare en machinaal leesbare vorm te verkrijgen. Hij kan deze gegevens daarnaast vrij overdragen aan een andere verwerkingsverantwoordelijke zonder dat hij gehinderd wordt door de huidige verwerkingsverantwoordelijke. De betrokkene kan dit recht inroepen wanneer er sprake is van de voorwaarden zoals genoemd in artikel 20 lid 1 sub a AVG. Het gaat hier dan om een verwerking die berust op toestemming of op een overeenkomst en waarbij sprake is van geautomatiseerde verwerking zoals respectievelijk genoemd in artikel 6 lid 1 sub a jo b AVG. De betrokkene heeft op grond van artikel 20 lid 2 AVG gedurende de uitoefening van het recht op dataportabiliteit het recht om zijn persoonsgegevens van de ene verwerkingsverantwoordelijke naar een andere verwerkingsverantwoordelijke te laten verzenden indien dit technisch mogelijk is.

3.5.7 Recht van bezwaar

Op grond van artikel 21 AVG heeft de betrokkene recht van bezwaar indien de verwerking van persoonsgegevens noodzakelijk is voor de vervulling van een taak van algemeen belang of de uitoefening van een taak in het kader van het openbaar gezag zoals genoemd in artikel 6 lid 1 sub e AVG. Daarnaast kan er bezwaar gemaakt worden indien de verwerking van persoonsgegevens gebaseerd is op noodzakelijkheid voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke conform artikel 6 lid 1 sub f AVG. De verwerkingsverantwoordelijke dient op het moment dat de betrokkene in bezwaar gaat, de verwerking van zijn persoonsgegevens te staken. Deze staking hoeft niet plaats te vinden indien de gerechtvaardigde belangen van de verwerkingsverantwoordelijke omtrent de verwerking zwaarder wegen dan de belangen, grondrechten en fundamentele vrijheden van de betrokkene[63].

3.5.8 Geautomatiseerde individuele besluitvorming

Volgens artikel 22 lid 1 AVG mag de betrokkene niet onderworpen worden aan een besluit waaraan rechtsgevolgen zijn verbonden of waardoor hij op andere wijze in aanmerkelijke mate getroffen wordt indien dit besluit gebaseerd is op enkel geautomatiseerde verwerking. In artikel 22 lid 2 sub a tot en met c AVG worden hierop uitzonderingen gegeven. Zo mag de betrokkene wel onderworpen worden aan een op enkel geautomatiseerde verwerking gebaseerd besluit indien het besluit gebaseerd is op noodzakelijkheid voor de totstandkoming van een overeenkomst tussen de betrokkene en verwerkingsverantwoordelijke, het op basis van een Unierechtelijke of lidstaatrechtelijke regel die van toepassing is op de verwerkingsverantwoordelijke is toegestaan en hij beschermingsmaatregelen neemt voor de

[62] N. Krijgsman, J. Terstegge & K. Versmissen, *Grip op de AVG*, Deventer: Wolters Kluwer 2017, p. 74.
[63] Overweging 69 Verordening (EU) 679/2016.

rechten, vrijheden en gerechtvaardigde belangen van de betrokkene of indien het besluit gebaseerd is op de uitdrukkelijke toestemming van de betrokkene.

3.6 De verwerkingsverantwoordelijke en de verwerker

Voor dit onderzoek is het van belang om na te gaan welke bepalingen voor Really-IT van toepassing zijn. Zoals eerder in dit hoofdstuk naar voren is gekomen, is Really-IT in de verhouding tot haar cliënten vooral verwerker. Zij bepaalt namelijk meestal niet zelf het doel van en de middelen voor een bepaalde gegevensverwerking. Het komt echter in bepaalde situaties voor dat Really-IT dit wel doet. Het gaat hier dan om het uitgeven van een bepaalde dienst zoals de virusscanner of het uitvoeren van een reparatie. Om deze virusscanner te installeren dient Really-IT persoonsgegevens betreffende de naam, adres, woonplaats, e-mailadres en eventueel het bankrekeningnummer te verwerken om het maandbedrag te incasseren. Really-IT stelt in dit geval dus zelf het doel en de middelen van deze gegevensverwerking vast en daardoor is zij in dit geval verwerkingsverantwoordelijke. Om nadere uitleg aan de begrippen verwerkingsverantwoordelijke en verwerker te geven, en om daarnaast te weten te komen aan welke verplichtingen zij dient te voldoen, zullen de artikelen aan bod komen die dit regelen. Zo kan er vastgesteld worden welke bepalingen op Really-IT van toepassing zijn gelet op de begrippen verwerkingsverantwoordelijke en verwerker.

3.6.1 De verwerkingsverantwoordelijke

Op grond van artikel 24 lid 1 AVG dient de verwerkingsverantwoordelijke rekening houdend met de aard, omvang, de context en het doel van de verwerking, passende technische en organisatorische maatregelen te nemen. Hij dient deze maatregelen te evalueren en indien nodig te actualiseren. Hierbij dient ook rekening gehouden te worden met de waarschijnlijkheid en de uiteenlopende risico's met betrekking tot de rechten en vrijheden van de natuurlijke personen indien deze persoonsgegevens in verkeerde handen komen. Op deze manier kan de verwerkingsverantwoordelijke aantonen dat de verwerking in overeenstemming is met de bepalingen zoals in de AVG gegeven worden.

Wanneer Really-IT als verwerkingsverantwoordelijke handelt, verwerkt zij een aantal persoonsgegevens. Het gaat hier om persoonsgegevens betreffende de naam, adres, woonplaats en het e-mailadres. Indien de cliënt gebruik wil maken van een automatische incasso dan wordt ook zijn bankrekeningnummer verwerkt. Er wordt qua beveiliging geen onderscheid gemaakt tussen de beveiliging van deze gegevens en die van een periodieke back-up. Alle diensten die door Really-IT worden geleverd en uitgevoerd, worden op hetzelfde niveau beveiligd. Dit houdt in dat persoonsgegevens opgeslagen worden in een afgesloten systeem dat voorzien is van wachtwoorden, encryptie, monitoring van inlogpogingen en firewalls. Deze beveiligingsmaatregelen kunnen aangemerkt worden als technische maatregelen. Daarnaast worden deze gegevens bewaard op servers die in afgesloten ruimtes staan, wordt het pand van Really-IT beveiligd met alarmsystemen en sloten, hebben de medewerkers die in aanraking komen met deze gegevens een geheimhoudingsbeding en weten zij dat ze op een vertrouwelijke manier met persoonsgegevens om dienen te gaan omdat een goede beveiliging van persoonsgegevens in de aard van IT-dienstverleners ligt. Deze maatregelen kunnen aangemerkt worden als organisatorische maatregelen.

Artikel 24 lid 2 AVG geeft vervolgens aan dat de technische en organisatorische maatregelen, zoals genoemd in artikel 24 lid 1 AVG, vastgelegd moeten zijn in een passend gegevensbeschermingsbeleid wanneer dit in verhouding staat tot de verwerkingsactiviteiten. Artikel 24 lid 3 AVG geeft aan dat het aangesloten zijn bij goedgekeurde gedragscodes of

certificeringsmechanismen als bedoeld in artikel 40 jo 42 AVG bij kan dragen om aan te tonen dat aan de verplichtingen van de verwerkingsverantwoordelijke voldaan wordt. Artikel 40 AVG geeft aan dat het opstellen van gedragscodes voor specifieke verwerkingssectoren bevorderd dient te worden. Er wordt veel belang gehecht aan organisaties die door een gedragscode of certificeringsmechanisme aan willen tonen dat zij voldoen aan de bepalingen die uit de AVG voortvloeien[64]. Gedragscodes worden opgesteld door brancheorganisaties en zijn bedoeld om als organisatie zelf regels uit te werken en nader te specificeren op een bepaalde branche[65]. In dit geval gaat het dus om het specificeren van regels die uit de AVG voortvloeien op de IT-branche. Daarnaast wordt het conform artikel 42 AVG bevorderd om certificeringsmechanismen voor gegevensbescherming in te voeren. Ook kan het van belang zijn om keurmerken en zegels te hebben om gegevensbescherming te waarborgen. Op dit moment is Really-IT als (aspirant)lid aangesloten bij brancheorganisatie ICTWaarborg. Zij is daarnaast bezig met de certificeringsprocedure om officieel het keurmerk van ICTWaarborg uit te mogen dragen en om aan te tonen dat zij voldoet aan de gedragscode van ICTWaarborg[66]. Wanneer zij in de toekomst deze procedure met een goed resultaat heeft afgerond, kan het aangesloten zijn bij een dergelijke gedragscode volgens artikel 40 AVG bijdragen om aan te tonen dat de verwerkingsverantwoordelijke aan zijn verplichtingen heeft voldaan indien deze gedragscode wordt voorgelegd en goedgekeurd wordt door de Autoriteit Persoonsgegevens[67].

Er dient vervolgens naar artikel 25 AVG gekeken te worden. In artikel 25 AVG is een nieuw uitgangspunt vastgelegd door het van toepassing zijn van de AVG[68]. Het gaat hier om het beginsel gegevensbescherming door ontwerp en door standaardinstellingen. Dit wordt ook wel privacy by design en privacy by default genoemd[69].

Het is volgens dit beginsel van belang dat er al in een vroeg stadium, dus bij het ontwerpen van systemen en diensten, rekening gehouden moet worden met gegevensbescherming[70]. In artikel 25 lid 1 AVG wordt namelijk aangegeven dat de verwerkingsverantwoordelijke zowel bij de bepaling van de verwerkingsmiddelen als bij de verwerking zelf, passende technische en organisatorische maatregelen dient te nemen. Hierbij dient hij rekening te houden met de stand van de techniek, de uitvoeringskosten, de aard, de omgang, de context, het doel van de verwerking en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen die betrokken zijn bij de verwerking. Op deze manier kunnen gegevensbeschermingsbeginselen zoals minimale gegevensverwerking, op een doeltreffende manier worden uitgevoerd en worden de nodige waarborgen in de verwerking ingebouwd ter naleving van de verordening en de bescherming van de rechten van de betrokkenen. Volgens artikel 25 lid 2 AVG dient de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen te treffen om ervoor te zorgen dat er standaard alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor het specifieke doel van de verwerking. Deze maatregelen dienen getroffen te worden aangaande de hoeveelheid

[64] N. Krijgsman, J. Terstegge & K. Versmissen, *Grip op de AVG*, Deventer: Wolters Kluwer 2017, p. 99.
[65] N. Krijgsman, J. Terstegge & K. Versmissen, *Grip op de AVG*, Deventer: Wolters Kluwer 2017, p. 99.
[66] Bijlage 10 Gedragscode ICTWaarborg
[67] N. Krijgsman, J. Terstegge & K. Versmissen, *Grip op de AVG*, Deventer: Wolters Kluwer 2017, p. 99.
[68] B.W. Schermer & D. Hagenauw & N. Falot, 'Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming', Den Haag: Ministerie van Justitie en Veiligheid 2018, p. 61.
[69] www.autoriteitpersoonsgegevens.nl (zoek op: privacy by design)
[70] Cuijpers, C. M. K. C., van Eecke, P., Kindt, E., & de Vries, H., 'Een eerste verkenning van het voorstel verordening bescherming persoonsgegevens', p. 13.

verzamelde persoonsgegevens, de mate waarin zij worden verwerkt, de termijn waarvoor zij worden opgeslagen en de toegankelijkheid daarvan.

3.6.2 De verwerker

Really-IT kan in de meeste gevallen, in de verhouding tussen haar en de cliënten, worden aangemerkt als verwerker. Zoals gezegd wordt Really-IT benaderd door bedrijven om IT-dienstverlening af te nemen. Het gaat hier dan bijvoorbeeld om het faciliteren van een online werkplek voor alle medewerkers van een bedrijf, het op afstand ondersteunen van een medewerker wanneer deze moeilijkheden ondervindt, het maken van een periodieke back-up en de beveiliging up-to-date houden. In deze gevallen heeft Really-IT inzicht in bepaalde persoonsgegevens, slaat zij deze op en dus verwerkt zij deze.

Artikel 28 AVG regelt de bepalingen met betrekking tot de verwerker. Op grond van artikel 28 lid 1 AVG dient de verwerkingsverantwoordelijke enkel een beroep te doen op een verwerker die voldoende garanties geeft met betrekking tot de technische en organisatorische maatregelen, zoals deze eerder naar voren zijn gekomen in artikel 24 AVG. Op deze manier voldoet de verwerking aan de vereisten van de AVG en is de bescherming van de rechten van de betrokkene gewaarborgd. Deze garanties zien voor de verwerker toe op haar deskundigheid, betrouwbaarheid en de middelen die zij gebruikt om ervoor te zorgen dat zij aan technische en organisatorische maatregelen voldoet waardoor zij in overeenstemming handelt met de bepalingen uit de AVG[71]. Indien de verwerker zich aansluit bij een goedgekeurde gedragscode of certificering, kan hij deze als element gebruiken om aan te tonen dat hij voldoende garanties biedt conform artikel 28 lid 5 AVG.

Conform artikel 28 lid 2 AVG mag de verwerker geen andere verwerker in dienst nemen voordat hij hiervoor specifieke of algemene toestemming heeft verkregen van de verwerkingsverantwoordelijke. Deze toestemming dient schriftelijk te worden vastgesteld. Really-IT maakt gebruik van sub-verwerkers. Dit zijn verwerkers die door Really-IT ingeschakeld worden om bepaalde diensten te verlenen. Deze sub-verwerkers dragen zorg voor het leveren van de licenties op het gebied van Microsoft office 365 en andere software. De verwerkingsverantwoordelijken zijn op de hoogte van het feit dat Really-IT in haar rol van verwerker gebruikt maakt van deze leveranciers om diensten te leveren. De verwerker mag op grond van artikel 29 AVG voor zover hij gegevens verwerkt voor de verwerkingsverantwoordelijke, deze enkel verwerken in opdracht van de verwerkingsverantwoordelijke.

3.6.3 De verwerkersovereenkomst

In artikel 28 lid 3 AVG wordt de verwerkersovereenkomst genoemd. Dit houdt in dat de verwerking wordt geregeld in een overeenkomst waardoor de verwerkingsverantwoordelijke en de verwerker zijn gebonden aan het Unierecht of lidstatelijke recht. Het is relevant om naar dit artikel te kijken omdat een dergelijke verwerkersovereenkomst gesloten dient te worden tussen een verwerkingsverantwoordelijke en Really-IT in haar rol van verwerker. Het uitgangspunt hierbij is dat de verwerkingsverantwoordelijke de overeenkomst naar Really-IT dient te verzenden. Dit vloeit ook voort uit het contact met een jurist van ICTWaarborg[72]. In deze overeenkomst dienen een aantal zaken opgenomen te worden. Er moet allereerst in de verwerkersovereenkomst aangegeven worden wat het onderwerp van de verwerking is, voor hoe lang deze aangegaan wordt, de aard en het doel van de verwerking, het soort

[71] Overweging 81 Verordening (EU) 679/2016.

[72] Bijlage 11 Contact mevrouw X, juridisch adviseur ICTWaarborg

persoonsgegevens dat verwerkt wordt en welke categorieën van betrokkenen er zijn. Daarnaast dienen de rechten en verplichtingen van de verwerkingsverantwoordelijke hierin omschreven te worden. In deze overeenkomst moeten daarnaast een aantal zaken zoals genoemd in artikel 28 lid 3 sub a tot en met h worden opgenomen. Het gaat hier om:

a) persoonsgegevens mogen uitsluitend worden verwerkt op basis van schriftelijke instructies van de verwerkingsverantwoordelijke;

b) de verwerker draagt de zorg voor een vertrouwelijke behandeling van de persoonsgegevens door hem en zijn medewerkers gebaseerd op een ondertekende of wettelijke geheimhoudingsplicht;

c) de verwerker dient alle beveiligingsmaatregelen zoals genoemd in artikel 32 AVG te nemen;

d) de verwerker dient te voldoen aan de voorwaarden genoemd in artikel 28 lid 2 jo 4 AVG betreffende het inschakelen van een andere verwerker;

e) de verwerker dient de verwerkingsverantwoordelijke bijstand te verlenen op het gebied van de technische en organisatorische maatregelen en de rechten van de betrokkenen;

f) de verwerker dient de verwerkingsverantwoordelijke bijstand te verlenen op het gebied van persoonsgegevensbeveiliging zoals voortvloeit uit de artikelen 32 tot en met 36 AVG;

g) de verwerker dient na afloop van de afgesproken verwerkersdiensten op verzoek en naar keuze van de verwerkingsverantwoordelijke alle persoonsgegevens te wissen of aan hem terug te bezorgen;

h) de verwerkingsverantwoordelijke dient alle informatie ter beschikking te stellen die nodig is voor de verwerker om aan de hiervoor genoemde verplichtingen te voldoen.

Naast de verwerkersovereenkomst tussen de verwerkingsverantwoordelijke en de verwerker, zoals genoemd in artikel 28 lid 3 AVG, dient er rekening gehouden te worden met een sub-verwerkersovereenkomst. Op grond van artikel 28 lid 4 AVG dient de verwerker bij het in dienst nemen van een andere verwerker, ook wel sub-verwerker genoemd, een overeenkomst op te stellen. Het gaat hier dan om eenzelfde soort verwerkersovereenkomst zoals genoemd in artikel 28 lid 3 AVG. Deze overeenkomst wordt echter opgesteld tussen de verwerker en de sub-verwerker. Aangezien Really-IT diensten afneemt van sub-verwerkers is het raadzaam om naar deze sub-verwerkersovereenkomst te kijken. Het is hierbij volgens artikel 28 lid 4 AVG belangrijk om dezelfde verplichtingen aan de sub-verwerker op te leggen zoals deze ook tussen de verwerkingsverantwoordelijke en verwerker conform artikel 28 lid 3 AVG opgenomen te dienen worden. Er dient vooral aangegeven te worden dat de sub-verwerker zal voldoen aan dezelfde strikte regels betreffende de technische en organisatorische maatregelen met betrekking tot de verwerking van persoonsgegevens. Indien de sub-verwerker zijn verplichtingen niet nakomt, blijft de verwerker aansprakelijk jegens de verwerkingsverantwoordelijke voor het niet nakomen van de verplichtingen van deze sub-verwerker.

3.6.4 Het verwerkingsregister

Conform artikel 30 AVG dient de verwerkingsverantwoordelijke een register bij te houden waarin aangegeven wordt wat voor verwerkingsactiviteiten er door haar uitgevoerd worden.

In dit verwerkingsregister dienen op grond van artikel 30 lid 1 sub a tot en met g AVG de volgende zaken opgenomen te worden:

a) de naam en contactgegevens van de verwerkingsverantwoordelijke;

b) de doeleinden voor de verwerking;

c) een beschrijving van de categorieën persoonsgegevens en betrokkenen;

d) de categorieën ontvangers van persoonsgegevens;

e) indien van toepassing, of persoonsgegevens worden doorgegeven aan een organisatie in een derde land;

f) indien mogelijk, de termijnen waarin de verschillende soorten categorieën gegevens dienen te worden gewist;

g) indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

In artikel 30 lid 2 AVG wordt vervolgens aangegeven dat er voor de verwerker ook de verplichting geldt om een verwerkingsregister bij te houden. Artikel 30 lid 2 sub a tot en met d AVG geeft aan wat er in het verwerkingsregister opgenomen dient te worden door de verwerker. Het gaat hierbij om de volgende zaken:

a) de naam en contactgegevens van de verwerkers en van iedere verwerkingsverantwoordelijke;

b) de categorieën van verwerkingen die voor iedere verwerkingsverantwoordelijke zijn uitgevoerd;

c) indien van toepassing, of persoonsgegevens worden doorgegeven aan een organisatie in een derde land;

d) indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

Het register dient conform artikel 30 lid 3 AVG schriftelijk te worden opgesteld. Een elektronisch register wordt hieronder ook inbegrepen. Indien de toezichthoudende autoriteit hierom vraagt, dient het verwerkingsregister ter beschikking gesteld te worden zodat deze ingezien kan worden volgens artikel 30 lid 4 AVG. De verwerkingsverantwoordelijke en de verwerker dienen op grond van artikel 31 AVG daarnaast samen te werken met de toezichthoudende autoriteit bij het vervullen van haar taken. Artikel 30 lid 5 AVG geeft aan dat het verwerkingsregister niet opgesteld dient te worden indien het gaat om ondernemingen of organisaties die minder dan 250 personen in dienst hebben tenzij:

- de verwerkingsactiviteiten een risico voor de rechten en vrijheden van de betrokkenen inhouden of;
- de verwerking niet-incidenteel is of;
- er bijzondere categorieën persoonsgegevens zoals genoemd in artikel 9 lid 1 AVG verwerkt worden of;
- er persoonsgegevens verwerkt worden die in verband staan met strafrechtelijke veroordelingen en strafbare zoals genoemd in artikel 10 AVG.

3.7 Persoonsgegevensbeveiliging

Het is van belang om persoonsgegevens goed te beveiligen en om maatregelen te nemen waardoor bepaalde risico's voorkomen worden. Door het nemen van de juiste maatregelen kan de bescherming van persoonsgegevens gewaarborgd worden.

3.7.1 Beveiligingsmaatregelen verwerking

Artikel 32 AVG geeft richtlijnen waaraan voldaan dient te worden wanneer er persoonsgegevens verwerkt worden. Op grond van artikel 32 lid 1 AVG dienen er passende technische en organisatorische maatregelen genomen te worden door de verwerkingsverantwoordelijke en de verwerker. Zij dienen deze maatregelen af te stemmen op het beoogde risico om zo een passend beveiligingsniveau te creëren voor de specifieke gegevensverwerking. Er dient hierbij rekening gehouden te worden met zowel de verwerkingsdoeleinden als de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen. Artikel 32 lid 1 sub a tot en met d AVG geeft vervolgens een aantal maatregelen aan waardoor een dergelijk beveiligingsniveau gecreëerd kan worden. Het gaat hier om:

a) de pseudonimisering en versleuteling van persoonsgegevens;

b) het garanderen van bekwame verwerkingssystemen en diensten gebaseerd op vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht;

c) wanneer er sprake is van een fysiek of technisch incident, de beschikbaarheid en de toegang tot persoonsgegevens hersteld kunnen worden;

d) het opstellen van een bepaalde procedure waardoor er op voorafgaande, specifieke tijdstippen beoordeeld en geëvalueerd kan worden of de genomen maatregelen zorgen voor een juiste beveiliging van de verwerking.

In artikel 32 lid 2 AVG wordt er gesproken over de beoordeling van een passend beveiligingsniveau. Er wordt hierbij rekening gehouden met de risico's die uit verwerking kunnen voortvloeien. Het gaat hier dan om de gevolgen van verlies, vernietiging, wijziging, ongeoorloofde verstrekking of toegang tot doorgezonden gegevens die verwerkt worden. Het maakt hierbij niet uit of dit per ongeluk of onrechtmatig heeft plaatsgevonden. Op grond van artikel 32 lid 3 AVG wordt aangegeven dat het aangesloten zijn bij een goedgekeurde gedragscode of een goedgekeurd certificeringsmechanisme gebruikt kan worden om aan te tonen dat er voldoende technische en organisatorische maatregelen worden genomen. Artikel 32 lid 4 AVG geeft vervolgens aan dat de verwerkingsverantwoordelijke en de verwerker maatregelen dienen te treffen zodat iedere natuurlijke persoon die onder hun gezag werkt en toegang heeft tot persoonsgegevens, deze enkel verwerkt voor de verwerkingsverantwoordelijke.

3.7.2 Melding en registratie inbreuk persoonsgegevens

Naast de technische en organisatorische maatregelen dient er ook rekening gehouden te worden met de melding van inbreuken met betrekking tot persoonsgegevens. Het gaat hier om de melding van een datalek en dit wordt ook wel de meldplicht genoemd[73]. Artikel 33 lid 1 AVG geeft aan dat de verwerkingsverantwoordelijke zo snel mogelijk, uiterlijk binnen 72 uur, nadat hij op de hoogte is van een dergelijke inbreuk, deze dient te melden aan de

[73] N. Krijgsman, J. Terstegge & K. Versmissen, *Grip op de AVG*, Deventer: Wolters Kluwer 2017, p. 50.

toezichthoudende autoriteit. Hij hoeft dit niet te doen indien de inbreuk geen risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Op grond van artikel 33 lid 2 AVG dient de verwerker de verwerkingsverantwoordelijke te informeren over een inbreuk met betrekking tot persoonsgegevens indien deze bij hem plaatsvindt. De melding zoals genoemd in artikel 33 lid 1 AVG dient op grond van artikel 33 lid 3 sub a tot en met d AVG het volgende te omschrijven:

a) de aard en de inbreuk met betrekking tot persoonsgegevens en indien mogelijk dient hierbij vermeld te worden om welke categorieën betrokkenen het gaat, de hoeveelheid betrokkenen en om welke persoonsgegevens het gaat;

b) de naam en contactgegevens van de persoon waar meer informatie van kan worden verkregen;

c) een inschatting van de gevolgen van de inbreuk;

d) de maatregelen die de verwerkingsverantwoordelijke heeft beoogd te nemen of heeft genomen om de inbreuk te verhelpen of de maatregelen tegen nadelige gevolgen van de inbreuk.

Indien er zich een inbreuk voordoet dienen op grond van artikel 33 lid 5 AVG door de verwerkingsverantwoordelijke een aantal zaken gedocumenteerd te worden. Hij dient hierbij alle inbreuken, alle feiten omtrent deze inbreuken, de gevolgen van de inbreuken en de genomen herstelmaatregen te documenteren. Dit wordt ook wel de registratieplicht genoemd[74]. Op deze manier kan de toezichthouder controleren of er op een juiste manier gehandeld wordt. De inbreuk dient daarnaast gemeld te worden aan de betrokkene conform artikel 34 AVG. Dit dient te gebeuren indien het gaat om een hoog risico met betrekking tot de rechten en vrijheden van natuurlijke personen. In dat geval moet de verwerkingsverantwoordelijke dit onmiddellijk mededelen aan de betrokkene volgens artikel 34 lid 1 AVG. De mededeling dient een in duidelijke en eenvoudige taal aan te gegeven wat voor inbreuk met betrekking tot persoonsgegevens er heeft plaatsgevonden. Artikel 34 lid 2 AVG geeft daarnaast nog aan dat er in deze mededeling eveneens de gegevens zoals genoemd in artikel 33 lid 3 sub b tot en met d AVG dienen te worden genoemd. Artikel 34 lid 3 AVG geeft vervolgens een uitzondering op de mededeling zoals die aan betrokkene gedaan dient te worden. De mededeling hoeft niet gedaan te worden indien de verwerkingsverantwoordelijke voldaan heeft aan een voorwaarde zoals genoemd in artikel 34 lid 3 sub a tot en met c AVG en hij:

a) technische en organisatorische maatregelen heeft genomen die passend zijn voor de situatie en die zijn toegepast op de verwerking van persoonsgegevens waarop een inbreuk heeft plaatsgevonden zoals versleuteling;

b) na de inbreuk maatregelen heeft genomen om ervoor te zorgen dat er geen hoog risico meer is voor de rechten en vrijheden van natuurlijke personen;

c) indien er sprake is van inspanning die niet in verhouding staat tot de inbreuk, dan is een openbare mededeling of een andere mededeling waarbij de betrokkene wordt geïnformeerd voldoende.

[74] N. Krijgsman, J. Terstegge & K. Versmissen, *Grip op de AVG*, Deventer: Wolters Kluwer 2017, p. 50.

3.8 Privacy Impact Assessment

In artikel 35 AVG wordt de gegevensbeschermingseffectbeoordeling genoemd. Dit wordt ook wel Privacy impact assessment (hierna: PIA) genoemd[75]. Het uitvoeren van een PIA is een nieuwe bepaling die voortvloeit uit de AVG. Een PIA is een middel dat door de verwerkingsverantwoordelijke gebruikt kan worden om, voordat er een gegevensverwerking plaatsvindt, het privacyrisico van een verwerking in te schatten. Op basis hiervan kunnen er vervolgens maatregelen en aanpassingen worden ondernomen om deze risico's te verkleinen. Bepaalde organisaties kunnen verplicht zijn om een PIA uit te voeren. Op grond van artikel 35 lid 3 sub a tot en met c AVG worden een aantal situaties genoemd waarbij een PIA verplicht is. Het gaat hier om:

a) de systematische beoordeling van persoonlijke aspecten van natuurlijke personen, gebaseerd op geautomatiseerde verwerking zoals profiling en waarop besluiten gebaseerd zijn die (rechts)gevolgen hebben voor een natuurlijke persoon;

b) de grootschalige verwerking van bijzondere persoonsgegevens zoals genoemd in artikel 9 lid 1 AVG of strafrechtelijke veroordelingen en strafbare feiten als genoemd in artikel 10 AVG;

c) het op stelselmatige en grootschalige wijze monitoren van openbare ruimten.

Naast de criteria zoals die genoemd worden in artikel 35 lid 3 AVG, zijn er een aantal nadere criteria opgesteld door de werkgroep van Europese privacytoezichthouders[76]. Met deze criteria wordt nader uitgelegd wanneer er sprake is van een hoog privacyrisico aangezien dit niet duidelijk genoeg naar voren komt in de AVG. Er zijn negen criteria[77] opgesteld die een nadere indicatie geven van een verwerking die een hoog privacyrisico met zich meebrengt.

Indien er aan 2 of meer van deze criteria voldaan wordt kan er aangenomen worden dat er een PIA uitgevoerd dient te worden[78]:

1. Beoordelen van mensen op basis van persoonskenmerken
2. Geautomatiseerde beslissingen
3. Stelselmatige en grootschalige monitoring
4. Het verwerken van gevoelige gegevens (artikel 9 AVG)
5. Grootschalige gegevensverwerkingen
6. Gekoppelde databases
7. Gegevens over kwetsbare personen
8. Gebruik van nieuwe technologieën
9. Blokkering van een recht, dienst of contract.

[75] www.autoriteitpersoonsgegevens.nl (zoek op: in welke gevallen moet ik een PIA uitvoeren)
[76] www.autoriteitpersoonsgegevens.nl (zoek op: in welke gevallen moet ik een PIA uitvoeren)
[77] www.autoriteitpersoonsgegevens.nl (zoek op: in welke gevallen moet ik een PIA uitvoeren)
[78] Groep Gegevensbescherming Artikel 29, Richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking ''waarschijnlijk een hoog risico inhoudt'' in de zin van Verordening 2016/679, 4 april 2017, WP 248, p. 10-13.

3.9 Functionaris voor gegevensbescherming

Conform artikel 37 AVG dienen de verwerkingsverantwoordelijke en de verwerker in bepaalde omstandigheden een functionaris voor gegevensbescherming (hierna: FG) in te schakelen. Het is relevant om de FG te benoemen omdat het aanstellen van deze functionaris een nieuwe bepaling is die voortvloeit uit de AVG. De FG is een deskundig persoon die zich binnen de organisatie bezighoudt met het toezicht en de naleving van de bepalingen zoals die uit de AVG voortvloeien[79]. De FG houdt zich op grond van artikel 39 AVG bezig met het informeren en adviseren van een verwerkingsverantwoordelijke of verwerker en zijn medewerkers met betrekking tot de bescherming van persoonsgegevens, ziet toe op de naleving van de AVG en heeft contact en werkt samen met de toezichthoudende autoriteit.

De gevallen waarin een functionaris ingeschakeld dient te worden, worden genoemd in artikel 37 lid 1 sub a tot en met c AVG. Het moet hier gaan om situaties waarbij:

a) de verwerking door een overheidsinstantie wordt verricht;

b) verwerkingen als doel hebben om op grote schaal betrokkene op regelmatige en stelselmatige wijze te observeren of;

c) de verwerkingen hoofdzakelijk gericht zijn op de op grootschalige verwerking van bijzondere persoonsgegevens als genoemd in artikel 9 AVG en strafrechtelijke veroordelingen en strafbare feiten als genoemd in artikel 10 AVG.

3.10 Autoriteit Persoonsgegevens

Op grond van artikel 51 AVG dient iedere lidstaat een toezichthoudende autoriteit vast te stellen. Dit wordt genoemd in artikel 51 lid 1 AVG. In Nederland is de toezichthoudende autoriteit op het gebied van de AVG de Autoriteit Persoonsgegevens[80]. De taken van de Autoriteit Persoonsgegevens zijn vastgelegd in artikel 57 AVG. Op grond van dit artikel heeft de Autoriteit Persoonsgegevens een ruim aantal taken die vooral gericht zijn op het handhaven van de toepasselijkheid van de AVG en het publiek bekend maken met de regels en inhoud van de AVG. Daarnaast is het een belangrijke taak van de Autoriteit Persoonsgegevens om de verwerkingsverantwoordelijken en de verwerkers te informeren met betrekking tot hun verplichtingen die uit de AVG voortvloeien.

Naast de taken die de Autoriteit Persoonsgegevens uitvoert, heeft zij ook bevoegdheden verkregen om te zorgen dat de AVG nageleefd wordt. Deze bevoegdheden zijn opgenomen in artikel 58 AVG. Zo worden volgens dit artikel de bevoegdheden onderverdeeld in onderzoeksbevoegdheden en corrigerende maatregelen.

Artikel 58 lid 1 sub a tot en met f AVG geeft de onderzoeksbevoegdheden aan. Deze bevoegdheden zijn:

a) de verwerkingsverantwoordelijke en de verwerker gelasten om voor de uitvoering van haar taken alle relevantie informatie te verschaffen;

b) gegevensbeschermingscontroles te verrichten;

[79] www.autoriteitpersoonsgegevens.nl (zoek op: FG)

[80] Memorie van toelichting Uitvoeringswet Algemene verordening gegevensbescherming, p. 15.

c) de afgegeven certificeringen te toetsen;

d) de verwerkingsverantwoordelijke en verwerker in kennis te stellen van een beweerde inbreuk op de AVG;

e) toegang te krijgen tot alle persoonsgegevens en informatie van de verwerkingsverantwoordelijke en verwerker die noodzakelijk is voor de uitvoering van haar taken;

f) toegang tot alle middelen die voor de verwerking van persoonsgegevens gebruikt worden en daarnaast toegang tot bedrijfsruimte(n) te verschaffen.

Artikel 58 Lid 2 sub a tot en met j AVG geeft de corrigerende maatregelen aan. Deze maatregelen zijn:

a) de verwerkingsverantwoordelijke of verwerker waarschuwen dat zij met de beoogde verwerkingsmethode de bepalingen zoals opgesteld in de AVG schenden;

b) indien het hiervoor genoemde echter toch heeft plaatsgevonden kan zij deze berispen;

c) de verwerkingsverantwoordelijke of verwerker verzoeken gehoor te geven aan de rechten van de betrokkene;

d) de verwerkingsverantwoordelijke of verwerker gelasten hun verwerkingen in overeenstemming te brengen met de AVG;

e) de verwerkingsverantwoordelijke gelasten over een inbreuk met betrekking tot persoonsgegevens te informeren;

f) een tijdelijke of definitieve verwerkingsbeperking op te leggen;

g) het beperken van verwerkingen, het rectificeren of wissen van persoonsgegevens en daarnaast de ontvangers van deze persoonsgegevens hierover informeren;

h) een certificering intrekken of het betreffende orgaan een certificering in laten trekken;

i) naast of in plaats van de maatregelen zoals deze in dit lid naar voren komen, gelet op de omstandigheden van een bepaalde zaak, een administratieve geldboete op te leggen zoals vastgelegd in artikel 83 AVG;

j) het verzenden van gegevens naar een ontvanger in een derde land opschorten.

Op dit moment zijn er in totaal drie personen werkzaam bij Really-IT. Mede door het geringe aantal medewerkers kan Really-IT aangemerkt worden als micro-onderneming[81]. Really-IT voldoet aan de voorwaarden om aangemerkt te worden als micro-onderneming aangezien de omzet minder dan 2 miljoen euro is en zij daarnaast minder dan 10 werknemers in dienst heeft. Het is relevant om vast te stellen wat voor type onderneming Really-IT is aangezien er op 8 maart 2018 een amendement[82] is ingediend door Tweede Kamerlid Van der Staaij. Dit amendement is vervolgens ook aangenomen op 13 maart 2018[83]. Het genoemde amendement heeft betrekking op de toepassing van de AVG door de Autoriteit

[81] Artikel 2 lid 3 Bijlage Aanbeveling 2003/361/EG van de Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen, PbEU 2003, L 124 van 20 mei 2003

[82] *Kamerstukken II* 2017/18, 34851, 15, p. 1.

[83] Stemmingsoverzicht Tweede Kamer 13 maart 2018, kamerstuk 34851

Persoonsgegevens. Bij de toepassing dient de behoefte van een micro-, kleine- of middelgrote onderneming[84] in acht genomen te worden. Dit is, zoals ook in de toelichting van het amendement naar voren komt, van belang omdat het algemeen uitgangspunt[85] moet zijn dat Nederland niet onnodig extra lasten oplegt aan bedrijven en organisaties. Wanneer dit wel gebeurd, is er een groot risico dat er steeds meer verdergaande verplichtingen ontstaan voor deze organisaties. Het is van belang om administratieve lasten zo veel mogelijk te voorkomen voor deze ondernemingen aangezien zij door hun geringe omvang extra lasten hiervan zullen ondervinden. Gezien het feit dat de eisen die uit de AVG voortvloeien voor de genoemde ondernemingen extra belastend zijn, is het van belang dat de Autoriteit Persoonsgegevens hier rekening mee houdt. De definitieve invulling van dit amendement is op dit moment nog onbekend. Het is nu dus nog niet duidelijk hoe er in de praktijk rekening gehouden gaat worden met de behoefte van kleine ondernemingen zoals dat hiervoor beschreven is. Het is dan ook van belang voor de beleidsbepalers van Really-IT om deze ontwikkelingen in de gaten te houden. Zo zal voor hen ook duidelijk worden welke invulling aan dit amendement gegeven gaat worden en wat dit voor gevolgen heeft voor hen als micro-onderneming.

3.11 Sancties

Op grond van artikel 83 AVG worden sancties toebedeeld indien de bepalingen uit de AVG geschonden of niet nagekomen worden. In artikel 83 lid 1 AVG wordt aangegeven dat er administratieve boetes worden toebedeeld en dat deze doeltreffend, evenredig en afschrikkend dienen te zijn. In artikel 83 lid 2 AVG wordt aangegeven dat naast of in plaats van de maatregelen zoals genoemd in artikel 58 AVG, administratieve geldboeten worden opgelegd. Om de hoogte van de administratieve geldboete te bepalen dient er rekening gehouden te worden met de zaken genoemd in artikel 83 lid 2 sub a tot en met k AVG:

a) de aard, ernst en duur van de inbreuk gelet op de omvang, het doel van de verwerking en daarnaast het aantal betrokkene dat hierdoor geraakt is en de schade die dat berokkent heeft;

b) of er opzet of nalatigheid gepaard is met de inbreuk;

c) welke maatregelen heeft de verwerkingsverantwoordelijke of verwerker genomen om de schade te beperken;

d) in hoeverre de verwerkingsverantwoordelijke of de verwerker verantwoordelijk is voor de schade gelet op de technische en organisatorische maatregelen die hij genomen heeft;

e) eerdere inbreuken;

f) er sprake is van een samenwerking met de Autoriteit Persoonsgegevens om de schade van de inbreuk te beperken en verdere gevolgen te voorkomen;

g) op welke categorieën persoonsgegevens heeft de inbreuk betrekking;

h) of de inbreuk gemeld is en hoe de Autoriteit Persoonsgegevens op de hoogte is gesteld;

i) of artikel 58 lid 2 AVG in is acht genomen;

[84] *Kamerstukken II* 2017/18, 34851, 15, p. 1.
[85] *Kamerstukken II* 2017/18, 34851, 15, p. 1.

j) het aangesloten zijn bij gedragscodes en certificeringsmechanisme zoals genoemd in artikel 40 jo 42 AVG;

k) omstandigheden die naast het genoemde een verzachtende of verzwarende factor hebben.

Op grond van artikel 83 lid 3 AVG kan een verwerkingsverantwoordelijke of verwerker indien hij meerdere inbreuken pleegt door opzettelijkheid of nalatigheid hiervoor enkel beboet worden voor een geldboete die niet hoger is dan die op de meest indringende inbreuk is vastgesteld. Op grond van artikel 83 lid 4 sub a AVG kan er een geldboete opgelegd worden van 10 miljoen euro. Deze geldboete kan 2% van de jaaromzet in het vorige boekjaar betekenen indien dit hoger uitvalt. Het gaat hierbij om een overtreding van de verplichtingen van de verwerkingsverantwoordelijke en de verwerker zoals vastgelegd in de artikelen 8, 11, 25 tot en met 39, 42 en 43 AVG.

Artikel 83 lid 5 AVG geeft vervolgens aan dat er een geldboete van 20 miljoen euro of 4% van de jaaromzet kan worden opgelegd indien het gaat om een overtreding van de basisbeginselen van verwerking zoals deze naar voren komen in de artikelen 5, 6, 7 en 9 AVG. Daarnaast kan deze geldboete worden opgelegd indien de rechten van de betrokkene zoals genoemd in de artikelen 12 tot en met 22 AVG worden overtreden. Ten slotte kan deze geldboete worden opgelegd indien een bevel van de Autoriteit Persoonsgegevens genegeerd wordt.

3.12 Tussenconclusie

Really-IT houdt zich bezig met verschillende werkzaamheden om IT-dienstverlening te leveren. Door het uitvoeren van deze werkzaamheden, zoals het installeren van een virusscanner of het verzorgen van een periodieke back-up, verwerkt Really-IT persoonsgegevens van haar cliënten. Hierdoor is de AVG van toepassing op de werkzaamheden van Really-IT. Really-IT kan daarnaast aangemerkt worden als verwerkingsverantwoordelijke en als verwerker. Dit zorgt ervoor dat er meerdere bepalingen uit de AVG van belang zijn voor Really-IT. Zo dient Really-IT de beginselen voor de verwerking van persoonsgegevens in acht te nemen om aan te tonen dat zij voldoet aan haar verantwoordingsplicht. Zij dient daarnaast het verwerkingsregister in te vullen vanuit haar rol van verwerkingsverantwoordelijke en verwerker, verwerkersovereenkomsten te sluiten met verwerkingsverantwoordelijken en sub-verwerkers en de regels met betrekking tot persoonsgegevensbeveiliging in acht te nemen. Indien Really-IT zich niet houdt aan de regels die op haar van toepassing zijn, kan dit gevolgen hebben. De toezichthoudende autoriteit, de Autoriteit Persoonsgegevens, heeft namelijk onderzoeksbevoegdheden en corrigerende maatregelen tot haar beschikking bij de toepassing van de AVG. Hierbij dient de Autoriteit Persoonsgegevens rekening te houden met het feit dat Really-IT als micro-onderneming aangemerkt kan worden. Tot slot kan de Autoriteit Persoonsgegevens een administratieve geldboete opleggen indien de bepalingen uit de AVG geschonden of niet nagekomen worden.

Wanneer de huidige werkwijze rondom privacy van Really-IT getoetst wordt aan de bepalingen die voortvloeien uit de AVG, kan er nagegaan worden in hoeverre de werkwijze van Really-IT voldoet aan de bepalingen die uit de AVG voortvloeien.

Hoofdstuk 4. Toetsing huidige werkwijze aan AVG

Zoals uit hoofdstuk twee is gebleken, is er bij Really-IT geen sprake van een privacybeleid. Really-IT houdt echter wel rekening met privacy door de huidige werkwijze die op dit moment gehanteerd wordt. Het is belangrijk om de huidige werkwijze, zoals behandeld in hoofdstuk twee, te toetsen aan de relevante bepalingen uit de AVG, zoals behandeld in hoofdstuk drie. Op deze manier kan er geconcludeerd worden aan welke bepalingen, die uit de AVG voortvloeien, de huidige werkwijze van Really-IT voldoet. Daarnaast vloeit hieruit voort aan welke bepalingen de werkwijze van Really-IT nog niet voldoet. Wanneer in kaart is gebracht in hoeverre Really-IT aan de bepalingen uit de AVG voldoet, kan er gekeken worden waar ruimte voor verbetering ligt.

4.1 Beginselen en verplichtingen AVG

In onderstaand schema zal aangegeven worden in hoeverre de huidige werkwijze van Really-IT overeenkomt met de beginselen en verplichtingen die voor de verwerkingsverantwoordelijke en de verwerker gelden. Really-IT kan namelijk, zoals naar voren komt in hoofdstuk drie, aangemerkt worden als verwerkingsverantwoordelijke en verwerker. Er zal in het schema allereerst aangegeven worden om welke bepaling het gaat. Vervolgens zal aangegeven worden of de huidige werkwijze van Really-IT wel of niet voldoet aan de bepaling uit de AVG. De toelichting zal tot slot aangeven waarom de huidige werkwijze van Really-IT wel of niet voldoet aan de bepaling die uit de AVG voortvloeit.

Schema 1 Beginselen en verplichtingen AVG		
Rood = niet voldaan	Groen = voldaan	Grijs = Niet van toepassing
Bepalingen uit de AVG	Voldaan?	Toelichting
Beginselen hoofdstuk 3.2		
Beginsel van rechtmatigheid, behoorlijkheid en transparantie Hoofdstuk 3.2 Het beginsel van rechtmatigheid, behoorlijkheid en transparantie dient in samenhang met het kopje: Transparante informatie en communicatie hoofdstuk 3.5.1 bezien te worden.	Nee	Really-IT verwerkt persoonsgegevens op een rechtmatige wijze aangezien de verwerking niet in strijd is met het Unierecht of lidstatelijk recht en de verwerking gebaseerd is op een grondslag conform artikel 6 lid 1 sub b AVG. De verwerking is daarnaast behoorlijk omdat Really-IT op een verantwoorde manier persoonsgegevens ten opzichte van de cliënt verwerkt aangezien zij bijvoorbeeld niet meer informatie verwerkt dan nodig is voor de dienst die zij levert[86]. De verwerking is echter niet transparant aangezien er niet aan de cliënt gecommuniceerd wordt dat er persoonsgegevens verwerkt worden, door wie deze verwerkt worden, waarom deze verwerkt worden, in hoeverre deze verwerkt worden en welke rechten de cliënt hierbij heeft.
Beginsel van doelbinding Hoofdstuk 3.2	Nee	Really-IT dient persoonsgegevens te verwerken om overeenkomsten uit te voeren of voor te bereiden. Deze persoonsgegevens zijn namelijk

[86] N. Krijgsman, J. Terstegge & K. Versmissen, *Grip op de AVG*, Deventer: Wolters Kluwer 2017, p. 56.

		noodzakelijk om te verwerken aangezien Really-IT geen dienst zoals een virusscanner kan leveren indien zij de persoonsgegevens van haar cliënt niet heeft. De verwerking van persoonsgegevens is daarnaast gerechtvaardigd omdat deze gebaseerd is op een grondslag conform artikel 6 lid 1 sub b AVG. Really-IT heeft echter niet uitdrukkelijk omschreven en vastgesteld waarom zij persoonsgegevens dient te verwerken. Hierdoor zijn er geen specifieke doeleinden vastgesteld. Doordat er geen specifieke doeleinden omschreven en vastgesteld zijn wordt er niet voldaan aan dit beginsel.
Beginsel van minimale gegevensverwerking Hoofdstuk 3.2	Ja	Really-IT verwerkt enkel gegevens indien zij deze nodig heeft voor specifieke doeleinden zoals het uitvoeren en verlenen van een virusscanner ten behoeve van de uitvoering of voorbereiding van een overeenkomst. Really-IT maakt geen gebruik van cookies op haar website. Hierdoor is te zien dat Really-IT enkel persoonsgegevens verwerkt of wil verwerken die noodzakelijk zijn voor de uitvoering of voorbereiding van overeenkomsten en dat zij niet meer persoonsgegevens wil verwerken dan nodig.
Beginsel van juiste persoonsgegevens Hoofdstuk 3.2	Nee	Really-IT neemt geen maatregelen om onjuiste persoonsgegevens te wissen of te rectificeren.
Beginsel van opslagbeperking Hoofdstuk 3.2	Nee	De persoonsgegevens die Really-IT verwerkt worden in beginsel enkel bewaard gedurende de uitvoering of voorbereiding van de overeenkomst. Fysieke documenten worden na het uitvoeren van een reparatie vernietigd, ingescand en vervolgens opgeslagen in een onlinedatabase zoals blijkt uit hoofdstuk twee. Persoonsgegevens van cliënten blijven echter wel in de database en het e-mailverkeer opgeslagen terwijl deze niet meer nodig zijn voor het verlenen van een dienst. Hierdoor blijven deze persoonsgegevens langer opgeslagen dan nodig is. Doordat het voorkomt dat persoonsgegevens langer worden bewaard dan nodig is, wordt er niet voldaan aan het beginsel van opslagbeperking.
Beginsel van integriteit en vertrouwelijkheid.	Nee	Om een op het risico afgestemd beveiligingsniveau te waarborgen, dient er rekening gehouden te worden met de

Hoofdstuk 3.2		verwerkingsdoeleinden en de risico's voor de rechten en vrijheden van personen. Dit kan bereikt worden door juiste maatregelen te treffen op het gebied van persoonsgegevensbeveiliging. Een juiste vorm van persoonsgegevensbeveiliging kan geboden worden door het treffen van passende technische en organisatorische maatregelen en rekening te houden met de meld- en registratieplicht van datalekken. Really-IT neemt verschillende technische en organisatorische maatregelen om de beveiliging van persoonsgegevens te waarborgen. Zo maakt Really-IT gebruik van technische maatregelen zoals een virusscanner, firewalls, encryptie, periodieke back-ups, wachtwoorden en de monitoring van inlogpogingen om persoonsgegevens te beschermen. De organisatorische maatregelen zijn vormgegeven door de fysieke beveiliging van het pand en de omgang van de medewerkers van Really-IT met persoonsgegevens. Het pand is beveiligd met alarmsystemen en daarnaast zijn de deuren naar het kantoor en de kast waar de server zich bevindt, afgesloten met een slot. De medewerkers zijn daarnaast, door de aard van IT-dienstverlening, bekend met het feit dat er veilig met informatie zoals persoonsgegevens omgegaan dient te worden en hebben daarnaast een geheimhoudingsbeding. Deze maatregelen zijn passend voor de beveiliging van persoonsgegevens die door Really-IT verwerkt worden. Deze persoonsgegevens zijn zo namelijk beveiligd tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging. Really-IT houdt echter geen rekening met de meld- en registratieplicht van datalekken. Daarnaast is de certificeringsprocedure bij brancheorganisatie ICTWaarborg nog niet afgerond en is de gedragscode van ICTWaarborg nog niet goedgekeurd door de Autoriteit Persoonsgegevens. Hierdoor treft Really-IT wel passende technische en organisatorische maatregelen maar door het ontbreken van een deugdelijke documentatie op het gebied van datalekken, voldoet zij niet aan dit beginsel omdat er niet aan een juiste persoonsgegevensbeveiliging wordt voldaan zoals de AVG voorschrijft.

Verantwoordingsplicht Hoofdstuk 3.2	Nee	Really-IT dient op grond van artikel 5 lid 2 AVG aan te tonen dat zij de beginselen van artikel 5 lid 1 sub a t/m f AVG naleeft om te voldoen aan haar verantwoordingsplicht. Naast het naleven van de beginselen dient Really-IT de verplichtingen uit de AVG, die op haar van toepassing zijn, na te leven. Really-IT kan niet aantonen dat zij aan deze beginselen en verplichtingen voldoet. Er is namelijk niets op schrift gesteld en aan het merendeel van de beginselen en verplichtingen wordt niet voldaan.
Grondslag Hoofdstuk 3.3	Ja	Really-IT verwerkt als verwerkingsverantwoordelijke persoonsgegevens zoals: de naam, adres, woonplaats, e-mailadres, telefoonnummer en indien van toepassing het rekeningnummer van de cliënt in verband met een automatische incasso. Daarnaast verwerkt Really-IT als verwerker persoonsgegevens voor een verwerkingsverantwoordelijke. Het is voor Really-IT noodzakelijk om deze gegevens te verwerken voor de uitvoering of voorbereiding van een overeenkomst. Deze overeenkomst kan zonder deze verwerking niet uitgevoerd worden. Er is dus sprake van een noodzakelijke verwerking voor de uitvoering van een overeenkomst zoals genoemd in artikel 6 lid 1 sub b AVG. Er is dus een rechtmatige verwerking omdat er een grondslag is.
De rechten van betrokkenen hoofdstuk 3.5		
Transparante informatie en communicatie. Hoofdstuk 3.5.1 Hoort samen gezien te worden met het beginsel van rechtmatigheid, behoorlijkheid en transparantie.	Nee	De cliënten van Really-IT zijn van mening dat Really-IT op een juiste manier met haar persoonsgegevens omgaat. Really-IT verstrekt haar cliënten echter geen informatie betreffende de rechten die zij hebben, of zij deze in kunnen roepen en wat voor gevolgen een mogelijke inroeping heeft. Daarnaast is er niet op schrift gesteld waarom Really-IT persoonsgegevens verwerkt en op welke manier Really-IT met de persoonsgegevens van haar cliënten omgaat. Dergelijke informatie dient doorgaans aan de cliënt bekendgemaakt te worden door een privacyverklaring. Door het ontbreken van een privacyverklaring is er geen sprake van transparante informatie en communicatie jegens de cliënt.
De verwerkingsverantwoordelijke en de verwerker hoofdstuk 3.6		
De verwerkingsverantwoordelijke	Nee	Zie toelichting bij het kopje: Beginsel van integriteit en vertrouwelijkheid hoofdstuk 3.2

dient passende technische en organisatorische maatregelen te nemen om een verwerking in overeenstemming met de AVG aan te tonen Hoofdstuk 3.6.1		
Really-IT dient als verwerker voldoende garanties met betrekking tot technische en organisatorische maatregelen te nemen om een juiste beveiliging van persoonsgegevens te waarborgen Hoofdstuk 3.6.2	Nee	Zie toelichting bij het kopje: Beginsel van integriteit en vertrouwelijkheid hoofdstuk 3.2
Really-IT heeft als verwerker toestemming nodig voor het inschakelen van een sub-verwerker Hoofdstuk 3.6.2	Nee	Really-IT mag op grond van artikel 28 lid 2 AVG alleen een sub-verwerker inschakelen indien zij hiervoor specifieke of algemene toestemming heeft van de verwerkingsverantwoordelijke. Deze toestemming is op dit moment niet schriftelijk vastgelegd.
Really-IT mag als verwerker enkel persoonsgegevens verwerken voor de verwerkingsverantwoordelijke Hoofdstuk 3.6.2	Ja	Really-IT verwerkt, indien zij persoonsgegevens voor een verwerkingsverantwoordelijke verwerkt, enkel persoonsgegevens in opdracht van deze verwerkingsverantwoordelijke.
De verwerkersovereenkomst Hoofdstuk 3.6.3	Nee	Really-IT is zowel verwerkingsverantwoordelijke als verwerker. Hierdoor dient Really-IT verwerkersovereenkomsten op te stellen met verwerkingsverantwoordelijken en sub-verwerkers. Really-IT heeft echter geen verwerkersovereenkomsten met haar cliënten en sub-verwerkers opgesteld.
Het verwerkingsregister Hoofdstuk 3.6.4	Nee	Really-IT heeft minder dan 250 personen in dienst. Really-IT verwerkt echter op niet-incidentiele basis persoonsgegevens. Hierdoor dient zij een register van haar verwerkingsactiviteiten bij te houden. Doordat Really-IT zowel verwerkingsverantwoordelijke als verwerker is dient zij op grond van artikel 30 lid 1 jo 2 AVG het register vanuit het perspectief

		van zowel de verwerkingsverantwoordelijke als de verwerker op te stellen en bij te houden.
Persoonsgegevensbeveiliging hoofdstuk 3.7		
Beveiligingsmaatregelen verwerking Hoofdstuk 3.7.1	Nee	Zie toelichting bij het kopje: Beginsel van integriteit en vertrouwelijkheid hoofdstuk 3.2
Melding en registratie inbreuk persoonsgegevens Hoofdstuk 3.7.2	Nee	Really-IT maakt geen melding van een inbreuk met betrekking tot persoonsgegevens aan de Autoriteit Persoonsgegevens en de betrokkene conform artikel 33 jo 34 AVG. Op grond van artikel 33 lid 1 AVG hoeft de melding aan de Autoriteit Persoonsgegevens niet plaats te vinden indien de inbreuk geen risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Deze melding hoeft daarnaast niet aan de betrokkene gemeld te worden indien er geen sprake is van een hoog privacyrisico voor de betrokkene conform artikel 34 lid 1 AVG. Zoals in hoofdstuk twee naar voren is gekomen, is er sprake geweest van een inbreuk met betrekking tot persoonsgegevens. Deze inbreuk had echter geen gevolgen voor de rechten en vrijheden van natuurlijke personen. Er hoeft in dat geval dus geen melding plaats te vinden. Op grond van artikel 33 lid 5 AVG dient Really-IT echter alle inbreuken die betrekking hebben op persoonsgegevens, te registreren. Hierbij dienen de feiten van de inbreuk, de gevolgen en de genomen corrigerende maatregelen vermeld te worden. Hiervan is tot op heden geen sprake.
Privacy impact assessment hoofdstuk 3.8		
Privacy impact assessment (PIA) Hoofdstuk 3.8	Niet van toepassing	Wanneer Really-IT in haar rol van verwerkingsverantwoordelijke handelt, is er geen sprake van een situatie als genoemd in artikel 35 lid 3 sub a tot en met c AVG. Really-IT houdt zich namelijk niet bezig met de systematische beoordeling van persoonlijke aspecten van natuurlijke personen, verwerkt geen bijzondere persoonsgegevens op grootschalige wijze en houdt zich niet bezig met het op stelselmatige en grootschalige wijze monitoren van openbare ruimte. Daarnaast is er geen sprake van een criterium zoals genoemd door de Europese privacytoezichthouders.
Functionaris voor gegevensbescherming hoofdstuk 3.9		
Functionaris voor gegevensbescherming (FG)	Niet van toepassing	Voor Really-IT is het niet nodig om een FG in te schakelen. Er is geen sprake van een situatie

Hoofdstuk 3.9		zoals genoemd in artikel 37 lid 1 sub a tot en met c AVG. Really-IT is namelijk geen overheidsinstantie of overheidsorgaan maar een kleine IT-dienstverlener. Daarnaast houdt zij zich niet bezig met regelmatige en stelselmatige observatie van betrokkenen op grote schaal. Ook zijn de werkzaamheden van Really-IT niet gericht op de verwerking van bijzondere persoonsgegevens en strafrechtelijke gegevens op een grote schaal.

4.2 Tussenconclusie

Uit de toetsing van de huidige werkwijze rondom privacy van Really-IT, aan de AVG, blijkt dat aan een aantal bepalingen niet wordt voldaan. Het is van belang om deze bepalingen in overeenstemming met de AVG te brengen. Uit deze toetsing blijkt dat er niet voldaan wordt aan het beginsel van rechtmatigheid, behoorlijkheid en transparantie, het beginsel van doelbinding, het beginsel van juiste persoonsgegevens en het beginsel van opslagbeperking. Daarnaast voldoet zij niet aan het beginsel van integriteit en vertrouwelijkheid. Dit komt naar voren doordat er weliswaar passende technische en organisatorische maatregelen worden genomen, maar er door het ontbreken van de meld- en registratieplicht van datalekken niet voldaan wordt aan een juiste persoonsgegevensbeveiliging. Really-IT maakt daarnaast geen gebruik van een transparante informatie en communicatie jegens haar cliënten. Ook voldoet zij niet aan de verantwoordingsplicht, stelt zij vanuit haar rol van verwerkingsverantwoordelijke en verwerker geen (sub-)verwerkersovereenkomsten op, houdt zij geen verwerkingsregister bij en heeft zij geen schriftelijke toestemming om sub-verwerkers in te schakelen. Really-IT voldoet daarentegen wel aan het beginsel van minimale gegevensverwerking, heeft een grondslag om persoonsgegevens te mogen verwerken en verwerkt in haar rol van verwerker enkel persoonsgegevens voor de verwerkingsverantwoordelijke.

Hoofdstuk 5. Conclusies en aanbevelingen

In dit hoofdstuk is een antwoord gegeven op de centrale vraag van dit onderzoek: 'Welke aanbevelingen voor een privacybeleid kunnen worden afgeleid uit een toetsing van de huidige werkwijze rondom privacy van Really-IT aan de Algemene verordening gegevensbescherming?'. Er zal in dit hoofdstuk beschreven worden aan welke beginselen en verplichtingen, die voortvloeien uit de AVG, de werkwijze van Really-IT op dit moment niet voldoet en hoe zij in de toekomst haar werkwijze wel kan laten voldoen aan deze beginselen en verplichtingen middels aanbevelingen. Het naleven van deze aanbevelingen zal ervoor zorgen dat de beginselen en verplichtingen, die voortvloeien uit de AVG, invulling krijgen voor Really-IT doordat zij op schrift worden gesteld en hieruit voortvloeit hoe Really-IT met privacy omgaat. Hierdoor ontstaat er een privacybeleid dat Really-IT kan naleven tijdens de uitvoering van haar werkzaamheden waarbij persoonsgegevens verwerkt worden. Zodoende kan zij de bescherming van persoonsgegevens waarborgen en leeft zij de AVG na.

5.1 Beginsel van doelbinding

Really-IT dient aan te geven dat zij voor welbepaalde, uitdrukkelijke en gerechtvaardigde doeleinden persoonsgegevens dient te verwerken om aan het beginsel van doelbinding te voldoen volgens hoofdstuk drie. Really-IT verwerkt volgens hoofdstuk twee enkel persoonsgegevens om haar overeenkomsten, zoals het uitvoeren van IT-dienstverlening waarbij een virusscanner, back-up of een reparatie wordt uitgevoerd, na te komen of voor te bereiden. Hierdoor verwerkt Really-IT persoonsgegevens voor gerechtvaardigde doeleinden omdat er sprake is van een grondslag. Op dit moment heeft Really-IT echter niet uitdrukkelijk omschreven en vastgesteld waarom zij persoonsgegevens verwerkt en hierdoor voldoet zij niet aan het beginsel van doelbinding volgens hoofdstuk vier.

Aanbeveling
Really-IT dient, voordat persoonsgegevens verwerkt worden, specifieke doeleinden te omschrijven en vast te stellen om aan het beginsel van doelbinding te voldoen. De omschrijving en vaststelling van deze doeleinden kan vastgelegd worden in een privacyverklaring. Het is dan ook aan te bevelen om een privacyverklaring op te stellen en hierin specifieke doeleinden op te nemen.

5.2 Beginsel van juiste persoonsgegevens

Really-IT dient alle maatregelen te nemen om onjuiste persoonsgegevens te wissen of te rectificeren zoals uit hoofdstuk drie blijkt. Zodoende wordt de juistheid van gegevens gewaarborgd. Blijkens hoofdstuk twee neemt Really-IT geen maatregelen om onjuiste persoonsgegevens te wissen of te rectificeren. Hierdoor voldoet zij niet aan het beginsel van juiste persoonsgegevens volgens hoofdstuk vier.

Aanbeveling
Om erachter te komen of er sprake is van onjuiste persoonsgegevens in de administratie en bestanden van Really-IT, kan Really-IT een bericht jegens haar cliënten uitsturen. In dit bericht kan zij vragen of de persoonsgegevens die op dit moment bekend zijn bij Really-IT correct zijn, of dat deze gerectificeerd of gewist dienen te worden omdat er een verandering heeft plaatsgevonden. Een dergelijk bericht kan eens per 6 of 12 maanden verzonden worden. Daarnaast kan aan de cliënt medegedeeld worden dat hij zelf contact met Really-IT kan opnemen indien de persoonsgegevens die aan Really-IT gegeven zijn om te verwerken, veranderd zijn. Really-IT dient deze gegevens vervolgens aan te passen. Indien de

overeenkomsten met cliënten eindigen, kan Really-IT hen informeren over het feit dat zij de persoonsgegevens van hen gaat wissen omdat zij deze niet langer nodig heeft. Het is dan ook aan te bevelen om van deze maatregelen gebruik te maken om te voldoen aan het beginsel van juiste persoonsgegevens en deze maatregelen vast te leggen in een privacyverklaring.

5.3 Beginsel van opslagbeperking

Really-IT dient de persoonsgegevens die zij verwerkt enkel te bewaren voor de uitvoering of voorbereiding van een overeenkomst zoals in hoofdstuk drie naar voren komt. Op dit moment verwerkt Really-IT persoonsgegevens om overeenkomsten uit te voeren of voor te bereiden. Het komt echter voor dat de persoonsgegevens in een onlinedatabase worden bewaard terwijl dit voor de uitvoering van de overeenkomst niet langer nodig is volgens hoofdstuk twee. Hierdoor wordt er niet voldaan aan het beginsel van opslagbeperking blijkens hoofdstuk vier.

Aanbeveling
Het is voor Really-IT raadzaam om persoonsgegevens te verwijderen wanneer het niet langer nodig is om deze te verwerken. De verwerking dient tot een minimum beperkt te worden. Dit kan Really-IT bewerkstelligen door bewaartermijnen op te stellen of een periodieke toetsing voor het bewaren van deze persoonsgegeven te hanteren. Hierdoor kunnen persoonsgegevens gewist worden wanneer deze niet meer nodig zijn voor de uitvoering van de overeenkomst. Op deze wijze wordt de opslagbeperking van persoonsgegevens gerealiseerd en wordt er voldaan aan het beginsel.

5.4 Verwerkersovereenkomsten

Really-IT dient (sub-)verwerkersovereenkomsten op te stellen met haar cliënten en sub-verwerkers. Zij dient deze verwerkersovereenkomsten op te stellen volgens de regels die uit hoofdstuk drie voortvloeien. Zo dienen er allereerst verwerkersovereenkomsten opgesteld te worden met cliënten die aangemerkt kunnen worden als verwerkingsverantwoordelijke. De verantwoordelijkheid om deze verwerkersovereenkomst te zenden, ligt bij de cliënt. Daarnaast dienen er verwerkersovereenkomsten opgesteld te worden met partijen die door Really-IT ingeschakeld worden als sub-verwerker. In hoofdstuk vier is naar voren gekomen dat er op dit moment nog geen (sub-)verwerkersovereenkomsten worden opgesteld door Really-IT.

Aanbeveling
Het is aan te bevelen om verwerkersovereenkomsten op te stellen en te verzenden naar cliënten die aangemerkt kunnen worden als verwerkingsverantwoordelijke. Zo toont Really-IT aan dat zij het initiatief neemt om aan deze verplichting te voldoen en ligt het niet aan haar als deze verwerkersovereenkomst niet ingevuld wordt door de verwerkersverantwoordelijke. Daarnaast dient Really-IT sub-verwerkersovereenkomsten op te stellen en te verzenden naar sub-verwerkers.

5.5 Verwerkingsregister

Really-IT dient een register van haar verwerkingsactiviteiten bij te gaan houden blijkens hoofdstuk vier. Dit register dient zowel vormgegeven te worden vanuit haar rol van verwerkingsverantwoordelijke als die van verwerker. Er dient hierbij rekening gehouden te worden met de aspecten die gelden voor het opstellen van een verwerkingsregister zoals voortvloeit uit hoofdstuk drie.

Aanbeveling
Het is voor Really-IT aan te bevelen om een register van haar verwerkingsactiviteiten op te stellen en bij te gaan houden.

5.6 Transparante informatie en communicatie in samenhang met het beginsel van rechtmatigheid, behoorlijkheid en transparantie

Really-IT dient haar cliënten in de toekomst informatie te verstrekken betreffende de rechten die zij hebben, hoe zij deze in kunnen roepen en wat voor gevolgen een mogelijke inroeping heeft volgens hoofdstuk vier. Ook dient zij de manier waarop zij met persoonsgegevens omgaat op schrift vast te stellen. Op dit moment is er namelijk geen sprake van transparantie omdat de cliënt niet wordt geïnformeerd dat er persoonsgegevens van hem verwerkt worden, waarom deze gegevens verwerkt worden en in hoeverre deze verwerkt worden volgens hoofdstuk twee. Uit hoofdstuk drie blijkt wat er op schrift gesteld kan worden om de cliënten te informeren.

Aanbeveling
Het is voor Really-IT aan te bevelen om transparante informatie en communicatie tot uiting te brengen aan haar cliënten. Dit kan geschieden door de hiervoor genoemde informatie vast te leggen in een privacyverklaring. Op deze wijze wordt de cliënt op een transparante wijze geïnformeerd.

5.7 Persoonsgegevensbeveiliging in samenhang met het beginsel van integriteit en vertrouwelijkheid

Om persoonsgegevens te beveiligen tegen ongeoorloofde of onrechtmatige verwerking, onopzettelijk verlies, vernietiging of beschadiging dient Really-IT allereerst passende technische en organisatorische maatregelen te nemen zoals naar voren komt in hoofdstuk drie. Really-IT neemt technische en organisatorische maatregelen blijkens hoofdstuk twee om persoonsgegevens te beveiligen. De technische maatregelen worden vormgegeven door het gebruik van een virusscanner, firewalls, encryptie, periodieke back-ups, wachtwoorden en de monitoring van inlogpogingen. De organisatorische maatregelen bestaan uit de beveiliging van het pand door alarmsystemen, afgesloten deuren, de bekwame omgang met persoonsgegevens van de werknemers van Really-IT en hun geheimhoudingsbeding. Deze maatregelen zijn volgens hoofdstuk vier passend. Really-IT houdt op dit moment echter geen rekening met de meld- en registratieplicht van datalekken om de beveiliging van persoonsgegevens te waarborgen, zoals naar voren komt in hoofdstuk vier. Ook is de certificeringsprocedure bij ICTWaarborg op dit moment nog niet afgerond. Wanneer deze procedure is afgerond en de gedragscode van ICTWaarborg goedgekeurd wordt door de Autoriteit Persoonsgegevens, kan deze gedragscode als element gebruikt worden om aan te tonen dat Really-IT gebruik maakt van een juiste persoonsgegevensbeveiliging. Doordat er op dit moment geen rekening wordt gehouden met de meld- en registratieplicht van datalekken, voldoet Really-IT niet aan een juiste persoonsgegevensbeveiliging en het beginsel van integriteit en vertrouwelijkheid.

Aanbeveling
Het is voor Really-IT aan te bevelen om naast het uitvoeren van de technische en organisatorische maatregelen, invulling te geven aan de meld- en registratieplicht van datalekken om de beveiliging van persoonsgegevens te waarborgen. Indien een datalek zich in de toekomst voordoet, dient Really-IT deze te documenteren en waar nodig te melden aan de Autoriteit Persoonsgegevens en de cliënt. Wanneer Really-IT in de toekomst invulling geeft aan de meld- en registratieplicht van datalekken en gebruik blijft maken van passende

technische en organisatorische maatregelen, voldoet zij aan een juiste persoonsgegevensbeveiliging en het beginsel van integriteit en vertrouwelijkheid.

5.8 Verantwoordingsplicht

Really-IT is blijkens hoofdstuk drie verantwoordelijk voor de naleving van de beginselen en verplichtingen voor de verwerking van persoonsgegevens. Zij dient aan te tonen dat zij zich aan haar verantwoordingsplicht houdt. Op dit moment houdt Really-IT zich niet aan haar verantwoordingsplicht. Zij kan namelijk niet aantonen dat zij handelt conform de beginselen en verplichtingen voor de verwerking van persoonsgegevens omdat zij niet aan alle beginselen en verplichtingen voldoet en daarnaast niets op schrift heeft gesteld conform hoofdstuk vier.

Aanbeveling
Wanneer Really-IT de aanbevelingen in dit hoofdstuk hanteert, kan zij in de toekomst aantonen dat zij voldaan heeft aan haar verantwoordingsplicht. Het is dan ook aan te bevelen om invulling te geven aan de beginselen voor de verwerking van persoonsgegevens door deze te documenteren. Op deze manier kan er aangetoond worden dat er aan deze beginselen voldaan wordt. Naast het documenteren van de beginselen is het van belang dat de naleving van iedere verplichting, die van belang is voor Really-IT, wordt gedocumenteerd. Bij het documenteren van de beginselen en verplichtingen kan gedacht worden aan het opstellen van een verwerkingsregister, het opstellen van (sub-)verwerkersovereenkomsten, het opstellen van een privacyverklaring en de meld- en registratieplicht van datalekken na te leven.

5.9 Aanbevelingen in relatie tot het beroepsproduct

Wanneer Really-IT aan de aanbevelingen, zoals genoemd in dit hoofdstuk, gehoor geeft is er sprake van een juiste implementatie van de AVG in de werkwijze rondom privacy. Op deze wijze zijn namelijk de beginselen en verplichtingen die voortvloeien uit de AVG, die van toepassing zijn op Really-IT, op schrift gesteld waardoor een privacybeleid ontstaat. In het beroepsproduct zal aandacht worden besteed aan de uitwerking van een aantal beginselen en verplichtingen in praktisch bruikbare modellen. De verdere aanpak met betrekking tot de beginselen en verplichtingen dient genomen te worden door de beleidsbepalers van Really-IT. Het beroepsproduct zal praktisch bruikbare modellen bevatten waardoor Really-IT verwerkersovereenkomsten op kan stellen en verzenden jegens haar cliënten, die als verwerkingsverantwoordelijke aangemerkt kunnen worden, en sub-verwerkers. Daarnaast zal er een concept verwerkingsregister opgesteld worden vanuit de rol van Really-IT als verwerkingsverantwoordelijke en verwerker. Dit concept verwerkingsregister kan als leidraad dienen om aan deze verplichting te voldoen. Ook zal er een privacyverklaring in het beroepsproduct opgenomen worden. Deze privacyverklaring zal ervoor zorgen dat de informatie en communicatie omtrent de verwerking van persoonsgegevens op een transparante wijze plaats zal vinden. Indien Really-IT de in dit hoofdstuk genoemde aanbevelingen in combinatie met het beroepsproduct hanteert, wordt op schrift gesteld hoe Really-IT met privacy omgaat en hierdoor wordt een privacybeleid gecreëerd dat in overeenstemming met de AVG is.

Bronnenlijst

Literatuur
Krijgsman, Terstegge & Versmissen 2017.
N. Krijgsman, J. Terstegge & K. Versmissen, *Grip op de AVG*, Deventer: Wolters Kluwer 2017.

Personen
Interview Dennis van de Put
Interview Susanne Harreman
Interview Roland van de Put
Interview X
Interview X
Mailcontact X, juridisch adviseur ICTWaarborg

Publicatie
Cuijpers, C. M. K. C., van Eecke, P., Kindt, E., & de Vries, H., 'Een eerste verkenning van het voorstel verordening bescherming persoonsgegevens', p. 13.

Wet- en regelgeving
Algemene verordening gegevensbescherming
Richtlijn bescherming persoonsgegevens
Wet bescherming persoonsgegevens

Handleiding
B.W. Schermer & D. Hagenauw & N. Falot, 'Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming', Den Haag: Ministerie van Justitie en Veiligheid 2018.

Parlementaire stukken
Bijlage Aanbeveling 2003/361/EG van de Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen, PbEU 2003, L 124 van 20 mei 2003.

Kamerstukken II 2017/18, 34851, 15.

Memorie van toelichting Uitvoeringswet Algemene verordening gegevensbescherming.

Stemmingsoverzicht Tweede Kamer 13 maart 2018, kamerstuk 34851.

Richtsnoeren
Groep Gegevensbescherming Artikel 29, Richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking ''waarschijnlijk een hoog risico inhoudt'' in de zin van Verordening 2016/679, 4 april 2017, WP 248, p. 10-13.

Elektronische bronnen
www.acm.nl
www.adobe.com
www.autoriteitpersoonsgegevens.nl
www.bitdefender.nl
www.bitdefender.com

www.ictwaarborg.nl
www.microsoft.com
www.oozo.nl
www.really-it.nl
www.rijksoverheid.nl