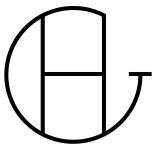


HoGent

Faculteit Bedrijf en Organisatie

Welke impact heeft de General Data Protection Regulation (GDPR) op de data van een kmo?

Tom Vandevelde

Scriptie voorgedragen tot het bekomen van de graad van
professionele bachelor in de toegepaste informatica

Promotor:
Chantal Teerlinck
Copromotor:
Robbie De Sutter

Instelling: double pass

Academiejaar: 2017-2018

Tweede examenperiode

Faculteit Bedrijf en Organisatie

Welke impact heeft de General Data Protection Regulation (GDPR) op de data van een kmo?

Tom Vandevelde

Scriptie voorgedragen tot het bekomen van de graad van
professionele bachelor in de toegepaste informatica

Promotor:
Chantal Teerlinck
Copromotor:
Robbie De Sutter

Instelling: double pass

Academiejaar: 2017-2018

Tweede examenperiode

Woord vooraf

De Bacheloropleiding Toegepaste Informatica aan de HoGent wordt afgesloten door het maken van een bachelorproef. Het geeft je de mogelijkheid al je verworven kennis doorheen de opleiding om te zetten in een duurzaam onderzoek en zo een bijdrage te leveren aan de maatschappij.

In dit onderzoek heb ik gekozen de General Data Protection Regulation (GDPR) – ook gekend als de Algemene Verordening Gegevensbescherming (AVG) – te bespreken. Privacy van persoonsgegevens is in de hedendaagse cultuur een heel belangrijk thema geworden. Op 25 mei 2018 zal de nieuwe verordening in werking treden om de opslag, verwerking en verdeling van persoonsgegevens van EU-burgers beter te beschermen.

Kmo's zijn zich niet altijd bewust van de impact die de verordening kan hebben op hun data en zijn ook niet altijd voorbereid op de veranderingen die de wetgeving kan teweegbrengen. De nood aan dergelijk onderzoek met duidelijke richtlijnen doorheen het implementatieproces is van niet te onderschatten belang voor een kmo.

Aangezien het voeren van een (eerste) onderzoek een behoorlijke inspanning vereist en het allesbehalve een sinecure is om de opdracht tot een goed einde te brengen, is het noodzakelijk gedurende het onderzoek te kunnen terugvallen op de steun, begeleiding en expertise van anderen. Hieronder wens ik voor deze personen mijn oprechte dank uit te spreken.

Een woord van dank aan mijn coördinator, mevrouw Chantal Teerlinck voor de opvolging, begeleiding en de constructieve feedback doorheen mijn onderzoek.

De heer Robbie De Sutter die als vakexpert in GDPR mij doorheen dit onderzoek nuttige tips en suggesties heeft aangereikt.

De heer Joost Roelens die als legal advisor de verordening door en door kent en mij doorheen dit onderzoek op juridisch vlak heeft ondersteund.

De heer Jo Van Hoecke en mevrouw Elke Vandersteen voor de structurele verbetering en het nalezen van mijn scriptie.

Een speciaal dankwoord voor mijn partner, Jenny Vander Eeckt en kinderen, Tibbe en Kobe die mij doorheen de opleiding steeds hebben gesteund. Een carrièreswitch maken, vergt niet alleen veel inspanning en toewijding van uzelf maar ook van uw partner en kinderen. Deze opleiding tot een goed einde brengen, zou niet haalbaar geweest zijn zonder hun oneindige steun en motivatie.

Verder wil ik iedereen bedanken die mij doorheen de opleiding heeft gesteund en geholpen en er zo mede voor heeft gezorgd deze opleiding tot een goed einde te brengen.

Samenvatting

Privacy van persoonsgegevens is in de hedendaagse cultuur een heel belangrijk topic geworden. Op 25 mei 2018 zal de General Data Protection Regulation (GDPR) – ook gekend als de Algemene Verordening Gegevensbescherming (AVG) – in werking treden om de opslag, verwerking en verdeling van persoonsgegevens van EU-burgers beter te beschermen.

Kmo's zijn zich niet altijd bewust van de impact die de regulatie kan hebben op hun data. Ook zijn ze niet altijd voorbereid op deze veranderingen waardoor ze nood hebben aan richtlijnen doorheen het implementatieproces.

Dit onderzoek biedt kmo's een naslagwerk van een diepgaande analyse van de verordening, en hoe deze een impact kan hebben op de organisatie. Verder bevat dit onderzoek een praktische toelichting van de noodzakelijke stappen naar GDPR-compliance. Alsook wordt dieper ingegaan op het recht op gegevenswissing ("recht op vergetelheid") (Europese Unie [EU], 2016, art. 17), en hoe dit recht een impact kan hebben op een kmo. Om dit te onderzoeken werd eerst de manuele workload nagegaan die gepaard gaat wanneer 1 % van het klantenbestand zijn recht tot gegevenswissing wenst uit te oefenen. In dit onderzoek werd dit gedaan voor het klantenbestand van double pass, het bedrijf waarvoor dit onderzoek mede tot stand kwam. Achteraf kon aan de hand van een businesscase de Return On Investment (ROI) worden nagegaan bij automatisatie van dit proces.

De opgeleverde conclusies tonen aan dat de verordening enorm is aangescherpt tegenover de vroegere richtlijn (EU, 1995), en dat deze een degelijke impact kan hebben op de organisatie. Ook mogen de administratieve boetes niet worden onderschat, hoewel twee recente artikelen van Data News (2017, 2018b) aantonen dat dit deels ongegrond is. Alsook wordt aangetoond dat de verordening een positieve impact kan hebben voor een

kmo. Dit zowel voor de administratieve lasten en kosten die vroeger gepaard gingen met verschillende wetgevingen doorheen de EU, als voor de optimalisatie van bestaande bedrijfsprocessen binnen de organisatie. De businesscase toonde aan dat de ROI redelijk snel kan worden bereikt, maar dat dit sterk afhankelijk zal zijn van het aantal aanvragen tot gegevenswissing die een kmo effectief zal binnenkrijgen eens de verordening actief is.

In dit onderzoek is het nog niet duidelijk hoe er zal worden gecontroleerd bij kmo's, hoe de toezichthoudende autoriteit zich kenbaar zal maken en op basis van welke criteria ze bepaalde bedrijven gaan controleren. Het spreekt voor zich dat een organisatie niet zomaar eender wie zal toegang verlenen tot hun data indien deze zich niet kenbaar kan maken. Volgens een artikel van Data News (2018b) is de Privacycommissie op de dag van schrijven evenwel zelf nog niet klaar waardoor kmo's omtrent controles nog geen duidelijkheid hebben.

Inhoudsopgave

Lijst van figuren

Lijst van tabellen

Termen en afkortingen

AVG Algemene Verordening Gegevensbescherming. 3, 5

CBPL Commissie voor de Bescherming van de Persoonlijke Levenssfeer. 27

DPA Data Protection Authority. 8, 11, 27, 28, 35, 39, 42, 47–49, 55, 56
DPIA Data Protection Impact Assessment. 11, 28, 34, 39, 42–44, 51
DPO Data Protection Officer. 8, 28, 34, 39, 41, 42, 53, 56

FG Functionaris Gegevensbescherming. 28

GBA Gegevensbeschermingsautoriteit. 27
GDPR General Data Protection Regulation. 3, 5, 17–19, 21, 23, 25–28, 32–34, 36, 40, 42–44, 46–48, 51, 54–56, 61, 65, 66
GEB Gegevensbeschermingseffectbeoordeling. 28

ROI Return On Investment. 5, 6, 18, 51, 57, 63, 64, 66

WP29 Article 29 Data Protection Working Party. 28, 43

1. Inleiding

1.1 Achtergrond

In de huidige hoogtechnologische maatschappij wordt het beschermen van persoonsgegevens heel belangrijk. Er bestaan diverse diensten en services waar mensen gebruik van kunnen maken. Nieuwe technologieën hebben het gebruik hiervan vergemakkelijkt. Hierdoor worden echter ook veel persoonsgegevens verzameld en verwerkt. Denk maar aan de registratie van een online formulier om deel te nemen aan een wedstrijd. Dit is slechts een van de vele diensten waar mensen gebruik van maken en verklaart meteen ook de kwetsbaarheid van persoonsgegevens en waarom mensen al snel het overzicht verliezen van waar hun gegevens bewaard zijn.

Sinds 24 oktober 1995 bestaat er al de Europese richtlijn 95/46/EG (EU, 1995) om persoonsgegevens betere bescherming te bieden. Een richtlijn legt echter enkel een bepaald doel vast waaraan alle EU-lidstaten moeten voldoen door deze richtlijn om te zetten in hun huidige wetgeving (EU, 2018). Dit verklaart ook meteen waarom er 28 (het Verenigd Koninkrijk is nog steeds volwaardig lid van de EU, red.) verschillende wetgevingen bestaan over de verwerking van persoonsgegevens.

Mede door de steile opmars van technologieën zoals sociale media en clouddiensten is de grootste privacywetgeving sinds twintig jaar ontstaan. De GDPR bouwt eigenlijk verder op de Europese richtlijn uit 1995 en behoudt de basisconcepten en principes. Er worden echter wel enkele nieuwe elementen toegevoegd zodat de verordening in lijn is met de huidige snelle technologische ontwikkelingen van de afgelopen twintig jaar (CBPL, 2018e).

De nieuwe verordening is heel omvangrijk (i.e. 88 A4-bladzijden) en bevat 99 artikelen die worden toegelicht door 173 overwegingen. Een verordening is bindend in al haar

onderdelen en rechtstreeks van toepassing op alle EU-lidstaten (EU, 2018). Hierdoor moeten lidstaten geen afzonderlijke implementatie meer doen in hun huidige nationale wetgeving zoals bij de Europese richtlijn van 1995 het geval was. De start van de GDPR leidt ook meteen tot de intrekking van deze Europese richtlijn (EU, 2016, art. 94).

De privacy van persoonsgegevens in lijn brengen met de huidige snelle technologische ontwikkelingen van vandaag is een eerste hoofdzaak van de GDPR, een tweede is een geharmoniseerde wetgeving doorheen alle EU-lidstaten.

Uiteindelijk werd de verordening na vier jaar voorbereiding goedgekeurd op 14 april 2016 en zal deze twee jaar later, op 25 mei 2018 in werking treden.

1.2 Probleemstelling

Kmo's zijn zich niet altijd bewust van de impact die de verordening kan hebben op hun data evenals van het risico een administratieve geldboete op te lopen. Deze kunnen oplopen tot twintig miljoen euro of 4 % van de totale wereldwijde jaaromzet in het voorgaande boekjaar, afhankelijk van welke het hoogste is (EU, 2016, art. 83).

Volgens een onderzoek van Data News en IRIS, vier maand voor de deadline, blijkt dat er nog veel werk voor de boeg is en dat 29 % van de Belgische bedrijven niet klaar dreigt te zijn voor de intrede van de GDPR. Verder legt het onderzoek een duidelijk verschil bloot tussen grote bedrijven en kmo's waaruit blijkt dat vooral deze laatste nog veel werk voor de boeg heeft. Slechts 15 % van de kmo's zegt al in een vergevorderde fase te zitten. (Data News, 2018a).

Uit bovenstaande blijkt dat de GDPR een enorme impact kan hebben op de financiële situatie, de doelstellingen en zelfs het voortbestaan van een organisatie. Dit geeft meteen ook het belang van een diepgaande analyse van de verordening voor een kmo aan. Mede daardoor kwam dit onderzoek tot stand op vraag van double pass, een bedrijf met als ambitie de jeugdopleiding van voetbalclubs te optimaliseren door middel van audits, adviesverstrekking en een erkend kwaliteitslabel (double pass, 2017).

1.3 Onderzoeksvraag

Dit onderzoek wil meer transparantie bieden naar GDPR-compliance. Dit wordt gedaan door eerst een overzicht te geven van de stand van zaken binnen het onderzoeksdomein met speciale aandacht voor de centrale vraag in dit onderzoek, namelijk de impact van GDPR op de data van een kmo. Als bijkomende onderzoeksvragen wordt artikel 17, het recht op gegevenswissing ("recht op vergetelheid") (EU, 2016) onderzocht en wordt de workload die gepaard gaat wanneer 1 % van het klantenbestand zijn gegevens wenst te verwijderen, nagegaan. Aan de hand van een businesscase wordt naderhand de ROI van een automatisatie van dit proces onderzocht.

1.4 Onderzoeksdoelstelling

De opgeleverde conclusies moeten kmo's helpen persoonsgebonden data te beheren en te verwerken conform de nieuwe verordening. Het moet bedrijven die nog niet of deels compliance zijn, helpen de overstap hiernaar te maken en de huidige bedrijfsprocessen aan te passen zodoende dat de verwerking van persoonsgegevens binnen de kmo juridisch en conform de GDPR is. Kmo's die reeds compliance zijn maar internationale projecten hebben, kunnen terugvallen op dit onderzoek om hun compliance-proces te versnellen bij privacywetgevingen buiten Europa. Uit het onderzoek zal ook blijken of het automatisatieproces al dan niet een kostenbesparing kan opleveren voor double pass.

1.5 Opzet van deze bachelorproef

De rest van deze bachelorproef is als volgt opgebouwd:

Op basis van een literatuurstudie wordt in Hoofdstuk 2 een overzicht gegeven van de stand van zaken binnen het onderzoeksdomein.

In Hoofdstuk 3 wordt de methodologie toegelicht en worden de gebruikte onderzoekstechnieken besproken om een antwoord te kunnen formuleren op de onderzoeksvragen.

Tenslotte wordt in Hoofdstuk 4 de conclusie van het onderzoek geformuleerd waarbij een aanzet wordt gegeven voor toekomstig onderzoek binnen dit domein.

2. Stand van zaken

De inhoud van dit hoofdstuk gaat verder op de inleiding en geeft op basis van een literatuurstudie de huidige stand van zaken weer binnen de GDPR. Na dit hoofdstuk worden in de methodologie de onderzoeksvragen verder uitgewerkt.

Voor dit hoofdstuk wordt doorgenomen, is het voor de lezer belangrijk te weten dat er in dit hoofdstuk wordt van uitgegaan dat de kmo in de rol van verwerkingsverantwoordelijke opereert. Bij bepaalde delen die specifiek van toepassing zijn voor de verwerker zal dit in het onderzoek duidelijk worden aangegeven. Beide rollen worden nader toegelicht in sectie 2.5.

2.1 Belangrijkste veranderingen & voordelen

Zoals in de inleiding vermeld, is de verordening aangepast aan de hedendaagse verwerking van persoonsgebonden gegevens. Hieronder worden de belangrijkste veranderingen besproken. Alsook hoe een kmo de GDPR kan aangrijpen als een kans om zo zijn bedrijfsprocessen verder te optimaliseren, eerder dan deze te beschouwen als een noodzakelijke implementatie om compliance de nieuwe verordening te handelen.

2.1.1 Belangrijkste veranderingen

Volgens Wegwijs in de AVG voor kmo's (EU, 2018) kunnen deze veranderingen worden samengevat in drie krachtlijnen: de risico-gebaseerde aanpak, verantwoordingsplicht en transparantie:

- De *risico-gebaseerde aanpak* zorgt ervoor dat de verplichtingen worden afgestemd op de risicofactor die de verwerking inhoudt. Dit wil zeggen dat sommige kmo's aan hogere verplichtingen zullen moeten voldoen aangezien de verwerkingsactiviteit een hoger risico inhoudt voor de persoonsgebonden gegevens.
- De *verantwoordingsplicht* houdt in dat een kmo moet kunnen verantwoorden dat hij compliance de verordening handelt, voor welk doel hij specifieke persoonsgegevens verwerkt en hoelang deze worden bewaard. Dit kan a.d.h.v. workflows, documenten, procedures en dergelijke.
- *Transparantie* heeft zowel intern als extern een impact. Intern moeten alle medewerkers op de hoogte zijn van alle verwerkingsactiviteiten die er binnen de kmo plaatsvinden. Alsook de sensibilisering van medewerkers is noodzakelijk zodat deze weten hoe om te gaan met persoonsgebonden data. Extern moeten kmo's transparant handelen naar de betrokkene toe zodat deze weet voor welke verwerkingsactiviteit zijn gegevens worden verwerkt, wat zijn rechten zijn en hoe hij deze rechten kan uitoefenen.

Verder wil de verordening EU-burgers een hogere bescherming van hun persoonsgegevens bieden. Alsook deze toegankelijker maken zodat ze hun gegevens vlotter kunnen consulteren, wijzigen en/of aanpassen.

Bij verwerking van persoonsgegevens dienen organisaties de nodige *toestemming* te hebben van de betrokkene. *Passende beveiligingsmaatregelen* dienen te worden genomen zodoende de nodige bescherming te kunnen bieden. In geval van een datalek zijn kmo's verplicht dit te *melden* aan de toezichthoudende autoriteit.

Zoals hierboven vermeld berust een verwerking op de toestemming van de betrokkene. Volgens artikel 6 (EU, 2016) kan deze ook gegrond zijn op basis van een noodzaak. Een verwerking kan noodzakelijk zijn in de volgende gevallen:

- voor de uitvoering van een overeenkomst waarbij de betrokkene partij is;
- om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;
- om de vitale belangen van de betrokkene of van een ander natuurlijk persoon te beschermen;
- voor het vervullen van een taak van algemeen belang;
- voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde.

2.1.2 Voordelen

Volgens een publicatie van de Europese Commissie (EC, 2015) zullen kmo's zoals double pass gebaat zijn bij een geharmoniseerde regelgeving doorheen alle Europese lidstaten. Dit resulteert in lagere administratieve lasten en kosten die vroeger werden uitgegeven om elke wetgeving individueel uit te pluizen.

Mede door deze geharmoniseerde wetgeving wordt het makkelijker gegevens te verwerken

over de landgrenzen heen en hebben organisaties nu te maken met één toezichthoudende autoriteit wat naar schatting een globale kostenbesparing van 2,3 miljard euro per jaar oplevert.

Oneerlijke concurrentie wordt tegengegaan doordat de verordening van toepassing is voor zowel Europese organisaties als voor organisaties buiten Europa wanneer er sprake is van de verwerking van Europese persoonsgegevens.

Kennisgevingen aan de toezichthoudende autoriteiten zijn niet meer nodig waardoor een kostenbesparing voor de organisaties wordt verwezenlijkt. Hiertegenover staat wel dat bedrijven bij de verwerking van persoonsgegevens compliance de verordening moeten handelen, en dat ze dit ook moeten aantonen in geval van controle door de toezichthoudende autoriteit.

2.2 Materieel toepassingsgebied

De GDPR is van toepassing op geheel of gedeeltelijk geautomatiseerde verwerkingen en op verwerkingen van persoonsgegevens die in een bestand zijn opgenomen of bestemd zijn daarin te worden opgenomen (EU, 2016, art. 2).

De verordening is niet van toepassing op ongeordende dossiers zonder enige geautomatiseerde index.

Volgens het onderzoek van Data News (2018a) gaf 7.5 % van de respondenten aan dat hun bedrijf geen concrete maatregelen heeft genomen voor de GDPR, oordelend dat de verordening niet van toepassing is voor hun bedrijf. Ondanks deze opvatting is de kans heel klein dat een organisatie geen enkele vorm van persoonsgegevens verwerkt en zodus niet onder de verordening valt.

2.3 Territoriaal toepassingsgebied

De GDPR is vooral van toepassing op de verwerking van persoonsgegevens door een verwerkingsverantwoordelijke of verwerker waarvan de organisatie in de Europese Unie is gevestigd. De verordening is echter ook van toepassing op de verwerking van persoonsgegevens van EU-burgers door een buiten de EU gevestigde organisatie. Dit kan bij het aanbieden van goederen of diensten aan EU-burgers (zelfs indien dit kosteloos gebeurt, red.), of indien men deze burgers hun gedrag gaat monitoren voor zover dit gedrag zich in de EU vertoont.

De verordening heeft dus een ruim territoriaal toepassingsgebied waarbij men organisaties buiten de EU ook wil laten genieten van de Europese markt dit op voorwaarde dat ze compliance de GDPR handelen. Zo wordt oneerlijke concurrentie met Europese kmo's die sowieso onder de verordening vallen, tegengegaan.

2.4 Basisbegrippen

Om de verordening goed te begrijpen en toe te passen is het noodzakelijk een goede kennis te hebben van enkele basisbegrippen zoals persoonsgegevens, verwerking en dergelijke.

Onderstaande informatie hieromtrent komt deels uit het artikel *Wegwijs in de AVG voor kmo's* (EU, 2018) en deels uit artikel 4 van de EU (2016) waar alle definities duidelijk staan beschreven. De belangrijkste begrippen worden hieronder verder toegelicht.

2.4.1 Persoonsgegevens

Als kmo is het zinvol een interne audit uit te voeren om alle persoonsgebonden gegevens in kaart te brengen. Om dit correct uit te voeren is het noodzakelijk te begrijpen wat er juist wordt verstaan onder het begrip *persoonsgegevens*.

Deze term is in de verordening heel ruim gedefinieerd en omvat alle gegevens die betrekking hebben op een natuurlijk persoon („de betrokkene") waardoor deze direct of indirect kan worden geïdentificeerd.

De identificering van de betrokkene kan gebeuren aan de hand van diverse aspecten zoals een naam, telefoonnummer, code, identificatienummer, online identificator, locatiegegevens of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van deze natuurlijke persoon. Denk hierbij aan contactgegevens van klanten, personeel of leveranciers maar evenzeer personeelsevaluaties, camerabeelden of gepseudonimiseerde persoonsgegevens waarvoor een sleutel bestaat om deze gegevens terug om te zetten naar de oorspronkelijke persoonsgegevens.

Er zijn wel wat uitzonderingen op bovenstaande omschrijving inzake persoonsgegevens. Zo zijn gegevens van overleden personen of rechtspersonen geen persoonsgegevens. Bij deze laatste kan men bijvoorbeeld denken aan het e-mailadres of telefoonnummer van een kmo.

Indirecte persoonsgegevens

Bij *indirecte persoonsgegevens* spreekt men van gegevens die niet direct aan een persoon kunnen worden gekoppeld maar waar dit in combinatie met andere gegevens wel mogelijk is. Een voorbeeld hiervan kan een IP-adres zijn.

Gevoelige persoonsgegevens

Dit zijn persoonsgegevens waarvan de verwerking een hoog risico met zich kan meebrengen en die in de eerste plaats niet mogen worden verwerkt tenzij aan bepaalde voorwaarden wordt voldaan. Er wordt dieper ingegaan op de verwerking van gevoelige persoonsgegevens in sectie 2.8.1.

2.4.2 Verwerking

Dit is een tweede begrip dat in de verordening heel ruim is gedefinieerd. Het omvat iedere bewerking die wordt uitgevoerd op persoonsgegevens al dan niet uitgevoerd via geautomatiseerde procedés. Voorbeelden hiervan kunnen zijn het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

Een belangrijke opmerking hieromtrent is te vermelden dat de wet niet kan worden omzeild door alle persoonsgegevens op papieren dragers te bewaren. Dit aangezien het bijhouden van systematisch geordende bestanden op papier ook een verwerking is voor de GDPR.

2.4.3 Toestemming

”Elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt” (EU, 2016, art. 4.11).

Vrije toestemming

Dit betekent dat de toestemming niet mag gebonden zijn aan de aanvaarding van de algemene voorwaarden, alsook dat deze niet mag gebonden zijn aan negatieve gevolgen indien er geen toestemming wordt verleend.

Een voorbeeld hiervan kan zijn dat een club deelneemt aan een audit om zo de gewenste kwalificatie te krijgen om interprovinciaal voetbal te kunnen spelen. Hiervoor worden de ouders door double pass gevraagd een online enquête in te vullen. Als voorwaarde om deel te nemen, wordt echter gevraagd de geolokalisatie te activeren om naderhand te gebruiken voor direct marketing (e.g. gerichte, regiogebonden reclame van sportbenodigdheden). Double pass gaat hier in de fout aangezien dit voor de uitvoering van de enquête niet noodzakelijk is.

Specifieke toestemming

Een toestemming moet *specifiek* en gericht zijn op één verwerking voor het realiseren van de in de verwerking gespecificeerde doeleinden.

In bovenstaand voorbeeld van de enquête kan het niet dat een ouder toestemming geeft om deel te nemen aan deze enquête *en* ook toestemming geeft om reclame over commerciële diensten van de kmo te ontvangen. Dit kan door de kmo echter wel worden gerealiseerd door voor elke verwerking apart een toestemming te vragen aan de hand van twee opt-ins.

In overweging 32 van de EU (2016) wordt beschreven dat het gebruik van *reeds aangekruiste vakjes (i.e. pre-ticked opt-in boxes) of inactiviteit* niet mag gelden als toestemming. Dit heeft als gevolg dat bestaande verwerkingen met een toestemming door middel van

vooraf aangekruiste vakjes niet meer rechtsgeldig zijn. Indien de kmo deze verwerking wenst verder te zetten, dient hij voor 25 mei 2018 een nieuwe toestemming te vragen aan de betrokkene.

Geïnformeerde toestemming

Een betrokkene moet in een begrijpbare taal worden uitgelegd welke persoonsgegevens worden verwerkt en voor welke doeleinden. Er moet ook in duidelijke taal worden geïnformeerd hoe de betrokkene zijn toestemming te allen tijde terug kan intrekken.

Ondubbelzinnige toestemming

De toestemming moet duidelijk zijn aan de hand van een verklaring of een duidelijke handeling (e.g. het aanvinken van een niet vooraf aangevinkt vakje).

2.5 Sleutelrollen

In vorige sectie werd al aangegeven dat er voor een correcte implementatie en toepassing van de verordening de nodige kennis inzake basisbegrippen is vereist. Dit geldt ook voor de verschillende rollen die gedefinieerd staan in de GDPR. Het is voor een kmo heel belangrijk te weten welke rol de organisatie speelt in een specifieke verwerking zodoende de verordening op een correcte manier te implementeren. Elk van deze rollen brengt namelijk verschillende verantwoordelijkheden en verplichtingen met zich mee welke later in dit hoofdstuk worden besproken.

Onderstaande informatie hieromtrent komt deels uit het artikel *Wegwijs in de AVG voor kmo's* (EU, 2018) en deels uit artikel 4 van de EU (2016) waar al deze rollen duidelijk staan beschreven. De belangrijkste rollen worden hieronder verder toegelicht.

2.5.1 Betrokkene

Een natuurlijk persoon die aan de hand van gegevens direct of indirect kan worden geïdentificeerd.

2.5.2 Verwerkingsverantwoordelijke

Een natuurlijk persoon of rechtspersoon, een dienst of ander orgaan die de doeleinden van de verwerking bepaalt, alsook de middelen waarmee de persoonsgegevens worden verwerkt.

Een kmo kan de verwerking van persoonsgegevens ook gezamenlijk met een andere organisatie uitvoeren. In dit geval fungeren zij als *gezamenlijke verwerkingsverantwoordelijken*

en moeten zij de betrokkene op een transparante manier meedelen wie welke verantwoordelijkheid heeft in de verwerking. Alsook welke verhouding zij hebben tegenover de betrokkene zodat deze laatste de mogelijkheid heeft zijn rechten uit te oefenen.

2.5.3 Verwerker

De verwerker, meestal een derde partij buiten de onderneming, verwerkt persoonsgegevens in functie van de verwerkingsverantwoordelijke. Tussen beiden wordt een overeenkomst gesloten waarin duidelijk beschreven staat voor welk doel de gegevens worden verwerkt, wat de verwerking juist inhoudt en hoelang de gegevens bewaard mogen blijven.

> Een KMO [*sic*] mag persoonsgegevens nooit langer bewaren dan noodzakelijk is om de vooropgestelde doeleinden te bereiken. Zodra deze doeleinden zijn volbracht of wegvallen, moet een KMO de persoonsgegevens wissen. Immers, bij gebrek aan een doeleinde valt de noodzaak tot het bewaren en verwerken weg. Daarom moet een KMO maximale bewaartermijnen vastleggen voor al haar persoonsgegevens. (CBPL, 2018e)

De verwerker mag een deel van de verwerking enkel uitbesteden aan een *gezamenlijke verwerker* wanneer ze hiervoor de schriftelijke toelating hebben van de verwerkingsverantwoordelijke.

Het is de verantwoordelijkheid van de verwerkingsverantwoordelijke om enkel samen te werken met organisaties die ook GDPR-compliance zijn.

2.5.4 Data Protection Authority (DPA)

Voor elke lidstaat wordt een DPA - ook gekend als de toezichthoudende autoriteit - aangesteld. Dit zijn onafhankelijke overheidsinstanties die toezien op de correcte toepassing van de GDPR in desbetreffende lidstaat.

Verder hebben ze een adviserende rol waarbij ze organisaties deskundig advies kunnen verstrekken. Alsook zijn ze bevoegd controles uit te voeren bij de organisaties en klachten af te handelen indien er inbreuken worden gemaakt tegenover de verordening.

Er mag meer dan één toezichthoudende autoriteit per lidstaat zijn. Een overzicht van alle toezichthoudende autoriteiten in de EU kan worden gevonden op de website van de European Commission (EC, 2018). In België is dit op het moment van schrijven de *Commissie voor de bescherming van de persoonlijke levenssfeer (CBPL)*, alsook de *Privacycommissie* genoemd. Vanaf 25 mei 2018 zal deze echter worden vervangen door de *Gegevensbeschermingsautoriteit (GBA)*. In dit onderzoek wordt de term DPA gebruikt indien er algemeen over de toezichthoudende autoriteiten wordt gesproken, en de Privacycommissie indien er specifiek wordt gedoeld op de toezichthoudende autoriteit van België.

2.5.5 Data Protection Officer (DPO)

Volgens de CBPL (2018a) wordt er in de GDPR een nieuwe rol geïntroduceerd, namelijk de DPO - ook gekend als de functionaris voor gegevensbescherming (FG). Zijn rol is toe te zien op de gegevensverwerkingen binnen de organisatie. Dit houdt in dat hij de kmo informeert en adviseert om de verordening correct na te leven. Alsook zal hij de kmo extra advies verlenen inzake een Data Protection Impact Assessment (DPIA) - ook gekend als een gegevensbeschermingseffectbeoordeling (GEB), en zal hij controleren of de verwerkingen GDPR-compliance zijn. Ten slotte treedt hij op als contactpunt tussen de kmo en de DPA.

Een DPO is wel niet voor elke kmo verplicht maar sommige zullen verplicht worden deze rol op te nemen in hun organigram. Welke kmo's juist onder deze verplichting vallen, wordt diepgaander besproken in sectie 2.8.3.

2.5.6 WP29

De Article 29 Data Protection Working Party (WP29) - in het Nederlands gekend als de Groep Gegevensbescherming artikel 29 - is een groep die alle nationale toezichthouders, waaronder ook de CBPL, omvat. Haar taak is advies te geven over de toepassing van de Europese privacywetgeving. Vanaf 25 mei 2018 vervangt het Europees Comité voor gegevensbescherming de WP29.

2.6 Rechten

Een grote verandering die de GDPR teweegbrengt, is de uitbreiding van de rechten voor de betrokkene. Persoonsgegevens overdragen of het recht hebben vergeten te worden, zijn twee nieuw geïntroduceerde termen in de verordening. Deze sectie geeft een uitgebreide toelichting welke rechten een betrokkene te gelde kan maken tegenover een kmo.

Voor deze rechten verder worden toegelicht, zijn er drie belangrijke aandachtspunten waar een kmo dient rekening mee te houden:

1. Het belang te weten dat de betrokkene deze rechten uitoefent tegenover de verwerkingsverantwoordelijke die hierin kan worden bijgestaan door de verwerker. Alhoewel de verwerkingsverantwoordelijke en de verwerker *ook* rechten hebben, zijn het toch vooral plichten die hun door de GDPR worden opgelegd. Deze worden verder toegelicht in 2.7.
2. Dat het voor een kmo interessant is duidelijke procedures te definiëren om deze verzoeken te behandelen. Alsook een centraal contactpersoon aan te stellen om deze verzoeken tijdig en op een vlotte manier te verwerken. Op deze manier stelt de kmo zich heel transparant op tegenover de betrokkenen wat voor deze laatste een enorme boost in het imago en vertrouwen van de kmo zal geven.
3. Dat de verordening in artikel 13 en 14 een onderscheid maakt tussen de te verstrekken

informatie wanneer de persoonsgegevens zijn verzameld bij de betrokkene zelf (i.e. rechtstreeks) of wanneer deze zijn verkregen vanuit een andere bron (i.e. onrechtstreeks). Tabel 2.1 bevat een overzichtelijke weergave van deze vergelijking.

Informatie	Rechtstreeks	Onrechtstreeks
Doeleinden en rechtsgrond van de verwerking	√	√
Identiteit en contactgegevens van de verwerkingsverantwoordelijke en de DPO (als er een DPO is)	√	√
De ontvangers of categorieën ontvangers van de gegevens	√	√
Bij doorgifte buiten de EU: het bestaan van een adequaatheids-besluit of passende waarborgen en hoe u hiervan een kopie kan krijgen	√	√
Uitleg over het gerechtvaardigde belang van de verwerkingsverantwoordelijke als de verwerking steunt op deze rechtsgrond	√	
De categorieën van verwerkte gegevens		√

Tabel 2.1: Vergelijkingstabel basisinformatie bij rechtstreekse en onrechtstreekse inzameling van gegevens (CBPL, 2018e, p. 22)

Uit Tabel 2.1 kan worden afgeleid dat bij rechtstreekse inzameling de betrokkene recht heeft op informatie over het gerechtvaardigd belang waar de verwerkingsverantwoordelijke zijn verwerking op berust. Dit in tegenstelling tot een verwerking die berust op een onrechtstreekse inzameling. Het gerechtvaardigd belang wordt later in dit hoofdstuk nader toegelicht (zie sectie 2.7.2).

Bij double pass worden de persoonsgegevens voor de audits verkregen via de database van de voetbalfederatie van het desbetreffende project. In dit specifiek geval spreekt men dus van een onrechtstreekse inzameling van persoonsgegevens waar de betrokkene het recht heeft over de categorieën van de verwerkte gegevens.

Onderstaande content komt grotendeels uit de EU (2016) en de CBPL (2018e).

2.6.1 Recht van inzage

Indien een verwerkingsverantwoordelijke de persoonsgegevens van een betrokkene verwerkt, heeft deze laatste volgens artikel 15 van de EU (2016) het recht deze gegevens in te zien en hieromtrent extra informatie op te vragen.

De verwerkingsverantwoordelijke dient hier kosteloos gevolg aan te geven, tenzij de verzoeken van de betrokkene ongegrond of buitensporig zijn. Bij repetitieve herhaling mag de verwerkingsverantwoordelijke hiervoor een administratieve vergoeding vragen of weigeren gevolg te geven aan het verzoek (EU, 2016, art. 12.5).

2.6.2 Recht op rectificatie

Volgens artikel 16 van de EU (2016) heeft de betrokkene het recht om onjuiste gegevens aan te passen en/of zijn gegevens verder de updaten. De betrokkene heeft ook het recht irrelevante of verboden gegevens van hem te wissen.

Belangrijke opmerking inzake de rectificatie van persoonsgegevens is te vermelden dat deze voor de verwerkingsverantwoordelijke onder de kennisgevingsplicht van de verordening vallen (EU, 2016, art. 19). Deze kennisgevingsplicht wordt verder toegelicht in sectie 2.7.1.

2.6.3 Recht op gegevenswissing („Recht op vergetelheid")

Afleidend uit artikel 17 van de EU (2016) kan er worden samengevat dat een betrokkene het recht heeft zijn persoonsgegevens te verwijderen, en dat de verwerkingsverantwoordelijke hier gevolg aan moet geven. Op deze eenvoudige interpretatie kunnen wel een paar bemerkingen worden gemaakt. Deze sectie probeert deze bemerkingen op een overzichtelijke manier uit de doeken te doen.

Beroep doen op het recht

De betrokkene kan het recht enkel inroepen in volgende gevallen:

- indien de gegevens niet langer noodzakelijk zijn voor een kmo om de doeleinden te vervullen;
- indien de betrokkene een eerder gegeven toestemming terug intrekt;
- indien de organisatie onrechtmatig gegevens verwerkt;
- indien de gegevens moeten worden gewist door het toedoen van een wettelijke verplichting;
- indien de kmo moet tegemoetkomen aan een succesvol ingediend bezwaar;
- indien minderjarigen [1] hun gegeven toestemming voor een dienst van de informatiemaatschappij [2] terug wensen in te trekken (i.e. online diensten zoals Facebook, Instagram...).

> Wanneer de verwerkingsverantwoordelijke de persoonsgegevens openbaar heeft gemaakt en overeenkomstig lid 1 verplicht is de persoonsgegevens te wissen, neemt hij, rekening houdend met de beschikbare technologie en de uitvoeringskosten, redelijke maatregelen, waaronder technische maatregelen, om verwerkingsverantwoordelijken die de persoonsgegevens verwerken, ervan op de hoogte te stellen dat de betrokkene de verwerkingsverantwoordelijken heeft verzocht om iedere koppeling naar, of kopie of reproductie van die persoonsgegevens te wissen. (EU, 2016, art. 17.2)

Uit bovenstaande kan een kmo de volgende belangrijke informatie afleiden: *rekening houdend met de beschikbare technologie, redelijke maatregelen nemen*. Misschien laat de

[1] Uit artikel 8 van de EU (2016) blijkt dat bij kinderen onder de 16 jaar een verwerking slechts geldig is indien er voorafgaand een toestemming of machtiging tot toestemming is gegeven door de persoon die de ouderlijke verantwoordelijkheid voor het kind draagt. De lidstaten hebben bij wet de toestemming om deze grens te verlagen zolang deze niet onder de 13 jaar ligt.

[2] "Elke dienst van de informatiemaatschappij, dat wil zeggen elke dienst die gewoonlijk tegen vergoeding, langs elektronische weg, op afstand en op individueel verzoek van een afnemer van diensten wordt verricht." Europese Unie (2015, art. 1.b).

verordening daar wel voer tot discussie toe. Maar voor een kmo kan dit wel aangegrepen worden om te zeggen dat alles wat in hun mogelijkheden lag gedaan is om iedereen die deze gegevens verwerkt, op de hoogte te stellen.

Weigering van het recht door de kmo

Bovengenoemd recht kan in sommige gevallen ook worden geweigerd door de kmo. Deze laatste moet dan wel terugvallen op één van de onderstaand gedefinieerde punten:

- wanneer de kmo zijn recht op vrijheid van meningsuiting en informatie wenst uit te voeren;
- wanneer dit noodzakelijk is om zijn wettelijke plichten of een taak van algemeen belang te vervullen;
- bij de instelling, uitoefening of onderbouwing van een rechtsvordering;
- bij archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statische doeleinden (onder specifieke voorwaarden, red.).

Ook voor dit recht heeft de verwerkingsverantwoordelijke kennisgevingsplicht.

2.6.4 Recht op beperking van gegevensverwerking

Volgens de CBPL (2018e) en artikel 18 van de EU (2016) heeft de betrokkene het recht een beperking van verwerking aan te vragen, een soort *bevriezing* van zijn gegevens. De kmo mag de gegevens dan nog wel bewaren maar moet de verwerkingsactiviteiten wel stopzetten.

Een eerste voorbeeld hiervan kan zijn wanneer de betrokkene de correctheid van deze gegevens betwist. De gegevens worden dan bevroren voor een periode zolang de kmo nodig heeft om deze correctheid te verifiëren.

Als tweede voorbeeld kan dit gebeuren in geval van een onrechtmatige verwerking. De betrokkene kan dan vragen om het gebruik van zijn persoonsgegevens te beperken in plaats van deze persoonsgegevens te wissen.

Als derde kan dit recht worden aangewend in geval van een lopende procedure van het recht van bezwaar. Zolang er wordt onderzocht of de gerechtvaardigde belangen van de kmo zwaarder doorwegen dan die van de betrokkene, worden de gegevens geblokkeerd.

Ten slotte kan dit recht door de betrokkene worden aangewend in geval van een rechtsvordering. Een voorbeeld hiervan zou kunnen zijn dat double pass een audit heeft uitgevoerd in een club en de dataretentie hiervan verloopt. Een trainer wordt echter ontslagen in deze club en wil aan de hand van deze gegevens bewijzen hoelang hij bij deze club actief is geweest. Deze persoon kan zich dan beroepen op bovenstaand recht en zich richten tot double pass met de vraag deze gegevens voorlopig te blokkeren.

Ook voor dit recht heeft de verwerkingsverantwoordelijke kennisgevingsplicht.

2.6.5 Recht op gegevensoverdraagbaarheid

Een recht dat ruimte voor interpretatie biedt. Enerzijds zegt de GDPR dat de verwerkingsverantwoordelijke de betrokkene de mogelijkheid moet bieden zijn data op te vragen in een overzichtelijk, elektronisch formaat zodat deze zijn gegevens in dit formaat kan overdragen aan een andere verwerkingsverantwoordelijke (i.e. de concurrentie). Anderzijds is het belangrijk te vermelden dat dit alleen noodzakelijk is indien dit technisch mogelijk is voor de verwerkingsverantwoordelijke. Er kan dus de vraag worden gesteld of de kmo dit zelf mag bepalen?

Volgens artikel 20 van de EU (2016) en uit de CBPL (2018e) kan dit recht door de betrokkene worden ingeroepen indien:

- de verwerking is gebaseerd op een toestemming of een overeenkomst; en
- het enkel over geautomatiseerde verwerkingen (i.e. geen papieren documenten) gaat.

Alsook komen niet alle persoonsgegevens in aanmerking voor overdraagbaarheid. Zelf ontwikkelde data door de kmo op basis van doorgegeven data, komen niet in aanmerking.

De betrokkene moet zijn data ontvangen in een gestructureerde en machinaal leesbare vorm zodat deze data kan worden hergebruikt bij een andere verwerkingsverantwoordelijke. Denk hierbij aan bestandsformaten zoals XML, JSON en CSV. Het rechtstreeks overplaatsen van data naar een ander technisch platform van een andere verwerkingsverantwoordelijke is zoals eerder aangegeven enkel noodzakelijk indien dit technisch mogelijk is.

2.6.6 Recht van bezwaar

Volgens artikel 21 van de EU (2016) heeft de betrokkene steeds het recht om bezwaar in te dienen tegen de verwerking van zijn persoonsgegevens. In dat geval moet de kmo de verwerking van de persoonsgegevens van deze betrokkene direct staken, tenzij er kan worden aangetoond dat de kmo zijn belangen zwaarder doorwegen dan de belangen, rechten en vrijheden van de betrokkene. Indien de kmo hiervan gebruik maakt, is het verplicht te documenteren waarom hun belangen zwaarder doorwegen, alsook dit aan de betrokkene mee te delen.

Er kan geen beroep worden gedaan op dit recht indien de verwerkingsverantwoordelijke belast is met een bij wet opgelegde verwerking, evenals bij een verwerking waarbij de betrokkene zelf toestemming heeft gegeven. Bij deze laatste moet de toestemming even eenvoudig kunnen worden ingetrokken dan ze is gegeven.

Een verwerking waar de betrokkene van dit recht kan gebruikmaken, is bijvoorbeeld wanneer een kmo zijn persoonsgegevens verwerkt voor direct marketing.

2.6.7 Recht om niet te worden onderworpen aan geautomatiseerde besluitvorming, waaronder profilering

> Profilering is elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen. (EU, 2016, art. 4.5)

Profilering is dus eigenlijk een vorm van automatische verwerking van persoonsgegevens waarbij men een persoonlijk profiel gaat opbouwen van deze persoon door zijn gedrag te analyseren en evalueren. Een bekend voorbeeld van een organisatie die aan profilering doet, is Facebook. Op basis van uw persoonlijk profiel kan Facebook bepaalde content tonen aan de gebruiker door middel van advertenties. Op zich is profilering dus eigenlijk niet slecht en mede daardoor wordt het ook gedoogd in de verordening. Maar de GDPR heeft wel een volledig andere kijk op dit topic wanneer profilering wordt gekoppeld aan geautomatiseerde besluitvormingen. Dan valt deze verwerking onder artikel 22 van de EU (2016).

Geautomatiseerde besluitvorming is van toepassing wanneer persoonsgegevens volledige automatisch worden verwerkt en daaruit bepaalde conclusies/beslissingen volgen die voor de betrokkene rechtsgevolgen kunnen hebben of hem dermate nadelig kan treffen. Het gaat hier dus om verwerkingen waar de beslissing niet kan worden bijgestuurd door een menselijke tussenkomst. In dergelijke situaties kan de betrokkene zich beroepen op het recht om niet te worden onderworpen aan geautomatiseerde besluitvorming.

In overweging 71 van de EU (2016) worden omtrent dergelijke besluitvormingen twee voorbeelden aangehaald. Enerzijds de automatische weigering van een online ingediende kredietaanvraag, anderzijds online ingediende sollicitaties zonder menselijke tussenkomst.

Toch zijn er een aantal gevallen waar geautomatiseerde besluitvorming is toegestaan, indien:

- de verwerkingsverantwoordelijke is belast met een bij wet toegelaten verwerking (e.g. voorkoming van belastingfraude en -ontduiking);
- de besluitvorming berust op de uitdrukkelijke toestemming van de betrokkene; of
- ze is noodzakelijk voor de uitvoering van een overeenkomst tussen de verwerkingsverantwoordelijke en betrokkene.

Wanneer de verwerking berust op een overeenkomst of op een toestemming is de verwerkingsverantwoordelijke verplicht passende maatregelen te nemen om de rechten en vrijheden en de gerechtvaardigde belangen van de betrokkene te beschermen. De betrokkene moet minstens het recht hebben op een menselijke tussenkomst, alsook om zijn standpunt kenbaar te maken en het besluit aan te vechten.

Ten slotte is geautomatiseerde besluitvorming bij bijzondere categorieën (i.e. gevoelige gegevens) enkel mogelijk indien hiervoor uitdrukkelijke toestemming door de betrokkene werd gegeven, of indien een zwaarwegend algemeen belang op de grond van het Unierecht of nationaal recht van toepassing is. Doch moeten er steeds maatregelen worden getroffen om de gerechtvaardigde belangen van de betrokkene te beschermen (EU, 2016, art. 22.4).

2.7 Plichten

Zoals in 2.6 al werd besproken, is het beter beschermen van de betrokkene een hoofddoel van de nieuwe verordening. Dit wil men mede bewerkstelligen door verwerkingsverantwoordelijken en verwerkers plichten op te stellen.

Eerst en vooral moeten kmo's voldoen aan een paar *basisprincipes*. Maar aangezien niet alle verwerkingen dezelfde zijn, is het mogelijk dat een kmo moet voldoen aan een paar *extra plichten* afhankelijk van de risicofactor verbonden aan de verwerking. Deze factor wordt medebepaald door de aard en gevoeligheid van de persoonsgegevens inzake de bescherming van de grondrechten en fundamentele vrijheden van een persoon.

Twee voorbeelden van extra verplichtingen zijn: het aanstellen van een DPO en het uitvoeren van een DPIA.

Gebaseerd op onderzoek uit de EU (2016) en de CBPL (2018e), wordt in deze sectie dieper ingegaan op de basisprincipes. Eerst worden de beginselen inzake verwerking van persoonsgegevens toegelicht, waarna dieper wordt ingezoomd op de rechtmatigheid van de verwerking ofwel de grondrechten waarop een verwerking berust. Een kmo moet aan beide voldoen om te kunnen spreken van een *rechtsgeldige verwerking* en GDPR-compliance te zijn. De bijkomende plichten voor verwerkingen met een hogere risicofactor worden besproken in sectie 2.8.

2.7.1 Beginselen inzake verwerking van persoonsgegevens

Hieronder worden een aantal beginselen inzake de verwerking van persoonsgegevens nader toegelicht. Een deel van deze beginselen kan worden gevonden in artikel 5 van de EU (2016).

Transparantie

Artikel 12 van de GDPR definieert dat de verwerkingsverantwoordelijke betrokkenen proactief moet informeren, duidelijk moet communiceren en ervoor moet zorgen dat de uitoefening van hun rechten wordt gefaciliteerd.

Proactief informeren:

De gegevens moeten transparant worden verwerkt ten aanzien van de betrokkene. De

verordening wil hiermee bewerkstelligen dat het voor de betrokkene duidelijk moet zijn te weten welke gegevens er worden verwerkt en voor welke doeleinden. Deze doeleinden moeten stroken met de vooraf bepaalde doeleinden gedefinieerd voor deze verwerking. Indien er toch andere doeleinden zouden gelden, is de kmo verplicht ofwel de betrokkene opnieuw toestemming te vragen, ofwel door te zorgen dat de verwerking berust op een rechtsgeldig grondrecht.

Duidelijke communicatie:

Een tweede belangrijk punt onder transparantie is dat de verwerkingsverantwoordelijke duidelijk moet communiceren naar de betrokkene toe. Hieronder wordt verstaan eenvoudig en in begrijpbare taal, dit zonder veel juridisch taalgebruik of complexe formuleringen.

Rechten faciliteren:

Ten slotte wordt de verwerkingsverantwoordelijke verplicht de betrokkene te informeren over zijn rechten, alsook de uitvoering hiervan te faciliteren (e.g. door middel van elektronische middelen).

Hoeveel tijd heeft de kmo om gevolg te geven aan een verzoek van de betrokkene?

> De verwerkingsverantwoordelijke dient te worden verplicht onverwijld en ten laatste binnen een maand op een verzoek van de betrokkene te reageren, en om de redenen op te geven voor een eventuele voorgenomen weigering om aan dergelijke verzoeken gehoor te geven. (EU, 2016, overw. 59)

Deze reactietijd heeft voornamelijk betrekking op de artikelen 15 tot en met 22 van de EU (2016). De verordening legt de verwerkingsverantwoordelijke op binnen één maand te reageren met een verlenging mogelijk van nog eens twee maand afhankelijk van het aantal verzoeken en de complexiteit van het verzoek.

Wat wordt er verstaan onder reageren?

Uit onderzoek van de verordening is gebleken dat de verwerkingsverantwoordelijke gevolg moet geven aan het verzoek. Wanneer de termijn wordt verlengd, is de verwerkingsverantwoordelijke nog steeds verplicht de betrokkene binnen de maand in kennis te stellen van dergelijke verlenging.

Kan de verwerkingsverantwoordelijke het verzoek negeren/weigeren?

De verordening laat de verwerkingsverantwoordelijke inderdaad toe een verzoek te negeren/weigeren. Hij blijft in dit geval wel nog steeds verplicht de betrokkene binnen de maand in te lichten met de reden van weigering en hoe deze hiertegen klacht kan indienen bij de DPA.

Een mogelijk voorbeeld hiervan kan zijn indien het verzoek ongegrond of buitensporig is. Al zou de kmo in het laatste geval toch gevolg kunnen geven aan het verzoek indien de betrokkene akkoord gaat hiervoor een correcte administratieve vergoeding te betalen.

Minimale gegevensverwerking

De GDPR doelt hiermee op het feit dat de verwerkingsverantwoordelijke enkel persoonsgegevens mag verwerken die strikt noodzakelijk zijn voor het bereiken van de vooraf bepaalde doeleinden van de verwerking.

Correctheid van gegevens

Persoonsgegevens moeten correct zijn en de betrokkene moet, door middel van een verzoek, de mogelijkheid hebben zijn gegevens in te kijken (i.e. recht op inzage) en indien nodig aan te passen (i.e. recht op rectificatie). De kmo is verplicht hieraan gevolg te geven (zie 2.7.1, Transparantie).

Bewaartermijn

Een kmo mag de persoonsgegevens nooit langer bewaren dan noodzakelijk om de vooropgestelde doeleinden te bereiken. Zodra de doeleinden zijn bereikt, dienen de gegevens te worden gewist omdat de noodzaak tot bewaring en verwerking wegvalt.

Volgens de EU (2016) overweging 39 is het belangrijk dat een kmo voor elke verwerking van persoonsgegevens maximale bewaartermijnen oplegt om ervoor te zorgen dat de gegevens niet langer dan noodzakelijk worden bewaard.

In de wetgeving zelf worden geen bewaartermijnen gedefinieerd. De duur wordt medebepaald door enerzijds het type verwerking en anderzijds het soort persoonsgegevens. De bewaartermijn van een verwerking kan dus bij wet zijn vastgelegd. In dit onderzoek worden drie voorbeelden toegelicht die voor een kmo belangrijk zijn, namelijk de verwerking van persoonsgegevens in een boekhouding, bij een sollicitatie en bij een ontslag.

- Boekhouding: persoonsgegevens opgenomen in de boekhouding moeten na zeven jaar worden gewist.
- Sollicitaties: bij niet aanwerving moet de kmo de persoonsgegevens betreffende de sollicitant wissen, tenzij deze laatste hierover wordt geïnformeerd en hem de mogelijkheid tot verzet wordt geboden.
- Ontslag: de kmo mag het personeelsdossier betreffende deze persoon archiveren zolang er een mogelijkheid tot rechtsvordering kan lopen tegen dit ontslag. Daarna moet dit dossier worden gewist.

Stappenplan inzake bewaartermijnen?

1. Inventariseer de bewaring van persoonsgegevens voor elke verwerking.
2. Argumenteer waarom deze bewaartermijn is gerechtvaardigd voor dit type verwerking.
3. Beperk de toegankelijkheid per verwerking.
4. Optioneel: archiveer de persoonsgegevens zodra dit mogelijk is.
5. Wis de gegevens indien de noodzaak tot bewaring wegvalt.
6. Bouw mechanismen in om te verifiëren dat de gegevens ook effectief worden gewist.

De wetgeving draagt op om te *archiveren* zodra dit mogelijk is voor een dossier. Archivering is echter enkel toegestaan om wettelijke voorschriften inzake verjaring of verplichte bewaartermijnen na te komen, anders moeten de gegevens direct worden gewist. Alsook moet de toegankelijkheid tot deze gearchiveerde dossiers worden beperkt en moet er worden gestreefd naar bewaringen met enkel strikt noodzakelijke persoonsgegevens.

Soms is er ook de misvatting van kmo's te veronderstellen dat dossiers met persoonsgebonden gegevens na het verstrijken van de looptijd *moeten* worden gewist. Dit is echter niet correct aangezien kmo's deze gegevens kunnen blijven bewaren indien ze eerst worden geanonimiseerd (pseudonimiseren is niet voldoende, red.).

Als laatste punt omtrent de bewaartermijnen wil dit onderzoek aantonen dat korte bewaartermijnen ook bepaalde voordelen kunnen hebben, zoals:

- een kmo kan niet meer aansprakelijk worden gesteld voor iets wat ze niet meer heeft;
- minder risico op datalekken en eventueel inbreuken te maken tegenover de rechten en belangen van een persoon waardoor alsook boetes worden vermeden; en
- minder administratie omdat de rechten van de betrokkenen inzake inzage, rectificatie en gegevenswissing niet meer van toepassing zijn.

Meldplicht datalekken

Elke kmo is verplicht passende veiligheidsmaatregelen te nemen en datalekken te melden aan de toezichthoudende autoriteit na het vaststellen van deze lek. Het thema beveiliging wordt in dit onderzoek nader toegelicht in sectie 2.11.

Verantwoordingsplicht

Zoals eerder vermeld in sectie 2.1.2 paragraaf 4 zijn kennisgevingen aan de toezichthoudende autoriteiten niet meer nodig. Hiertegenover staat wel dat een kmo zijn verwerkingen moet kunnen verantwoorden. Het is dus de plicht van de kmo bepaalde keuzes te documenteren om zo in geval van controle te kunnen aantonen dat de verordening wordt nageleefd.

Kennisgevingsplicht

Dit is van toepassing wanneer de betrokkene een rectificatie, gegevenswissing of verwerkingsbeperking van zijn persoonsgegevens doorvoert.

Wanneer persoonsgegevens door de verwerkingsverantwoordelijke eerder zijn doorgegeven aan derde partijen (i.e. iedere ontvanger van deze persoonsgegevens), is het van belang dat deze door de verwerkingsverantwoordelijke op de hoogte worden gesteld in geval dat de betrokkene een van bovenstaande acties heeft doorgevoerd. Dit tenzij het onmogelijk is of onevenredig veel inspanningen vergt. De verwerkingsverantwoordelijke dient de betrokkene op de hoogte te stellen van deze ontvangers indien deze hem hieromtrent verzoekt.

2.7.2 Rechtmatigheid van de verwerking

Een tweede topic gecatalogeerd onder de basisprincipes is het rechtsgeldig grondrecht waar een verwerking op kan berusten.

Zoals gedefinieerd in artikel 6 van de EU (2016) en beschreven in de vierde paragraaf van 2.1.1 zijn er zes mogelijke rechtsgronden. Bij kmo's zal de verwerking echter voornamelijk gebaseerd zijn op *de toestemming, overeenkomst, naleving van een wettelijke verplichting of het gerechtvaardigd belang*. Deze vier grondrechten worden hieronder nader toegelicht.

Voor deze vier grondrechten worden toegelicht, wil dit onderzoek meegeven dat het voor een kmo belangrijk is te documenteren op welke rechtsgrond de verwerking berust, en dit voor elke verwerking.

De toestemming:

Dit begrip werd al uitgebreid toegelicht in sectie 2.4.3.

De belangrijkste verplichting voor een kmo is hier dat deze toestemming *aantoonbaar* moet zijn en de kmo moet kunnen bewijzen dat de betrokkene toestemming heeft gegeven (e.g. registratie van datum opt-in).

Een tweede verplichting hieromtrent is dat de kmo verplicht is de intrekking van de toestemming *even toegankelijk* te maken als dat de toestemming is gegeven. Een voorbeeld hiervan kan zijn dat een betrokkene deelneemt aan een enquête en zijn toestemming voor de verwerking hiervan verleent aan de hand van een opt-in, maar moet bellen naar de kmo om zijn toestemming terug in te trekken. Deze toestemming is niet rechtsgeldig aangezien de drempel voor het bellen naar de kmo hoger ligt dan dat de betrokkene zich online zou kunnen uitschrijven aan de hand van een opt-out.

De overeenkomst:

Een tweede rechtsgeldig grondrecht voor de verwerking is een overeenkomst tussen de kmo (i.e. de verwerkingsverantwoordelijke) en de betrokkene (e.g. klant, leverancier, werknemer). De kmo heeft dan de toelating de persoonsgegevens gedefinieerd in deze overeenkomst te verwerken.

Het meest voor de hand liggend voorbeeld is hier een overeenkomst tussen werkgever en werknemer. De werkgever dient bepaalde persoonsgegevens te verwerken om het loon te kunnen uitbetalen. De arbeidsovereenkomst wordt hier als rechtsgeldig grondrecht aanzien voor de verwerking.

De naleving van een wettelijke verplichting:

Een kmo mag ook rechtmatig gegevens verwerken indien dit door wet is opgelegd (e.g. een organisatie is bij wet verplicht bepaalde persoonsgegevens van werknemers door te geven aan de fiscus of de instellingen van de sociale zekerheid).

Het gerechtvaardigd belang:

Een vierde rechtsgrond waar een kmo zijn verwerking op kan verhalen, is het gerechtvaardigd belang. Volgens de EC (z.d.-b) wordt van dit belang gesproken indien een kmo bepaalde persoonsgegevens moet verwerken om hun bedrijfsactiviteiten te kunnen uitvoeren. De verwerking berust dan niet op een toestemming, een overeenkomst of een wettelijke verplichting.

Belangrijk is te vermelden deze rechtsgrond niet rechtsgeldig is wanneer de belangen of de grondrechten en fundamentele vrijheden van de betrokkene zwaarder doorwegen dan het gerechtvaardigd belang van de verwerkingsverantwoordelijke.

Ook een expliciete toestemming is niet vereist voor het gerechtvaardigd belang, maar de betrokkene heeft wel het recht bezwaar aan te tekenen tegen de verwerking. Zoals vermeld in sectie 2.6.6 dient de kmo de verwerking van deze persoonsgegevens dan direct te staken, tenzij er kan worden aangetoond dat hun belangen zwaarder doorwegen. Een opt-out systeem is dus steeds noodzakelijk zodat de betrokkene de mogelijkheid heeft zijn rechten uit te oefenen.

Een voorbeeld van het gerechtvaardigd belang is direct marketing. In overweging 47 van de EU (2016, p. 9) wordt hieromtrent het volgende omschreven: ”De verwerking van persoonsgegevens ten behoeve van direct marketing kan worden beschouwd als uitgevoerd met het oog op een gerechtvaardigd belang.” Hieruit kan worden afgeleid dat een kmo de toelating heeft een eerder verworven e-mailadres van een klant te gebruiken om deze te informeren over nieuwe producten en diensten. Wel moet deze klant zich even makkelijk terug kunnen uitschrijven voor dergelijke e-mails (e.g. opt-out systeem).

2.8 Bijkomende plichten - Verwerkingen met hoge risicofactor

Zoals eerder aangegeven in de introductie van sectie 2.7 wordt de verwerkingsverantwoordelijke soms bijkomende plichten opgelegd door de verordening. Er wordt dan gesproken over gevoelige gegevens. Deze sectie belicht deze gegevens en gaat dieper in op de bijkomende plichten die dan van toepassing worden.

Zo is er voor dergelijke verwerkingen soms de nood aan een register, een DPO of moet er een DPIA worden uitgevoerd. Het is voor kmo’s niet altijd evident te weten of ze gevoelige gegevens verwerken en zodus onder deze categorie van verwerkingen vallen. Daarom wordt de kmo door de toezichthoudende autoriteiten ook steeds aangeraden te documenteren waarom zij van mening zijn dat deze stappen niet noodzakelijk waren. In geval van controle kan dit worden aangetoond aan de DPA waarna deze zal aangeven of eventuele bijsturing inzake verplichtingen noodzakelijk is of niet.

Onderstaande informatie in deze sectie is gebaseerd op informatie uit de EU (2016) en uit de CBPL (2018e).

2.8.1 Gevoelige gegevens

Eerst en vooral wordt de term gevoelige gegevens eens onder de loep genomen. Wat wordt hier eigenlijk juist onder verstaan en waarom genieten deze gegevens een hogere bescherming? Eigenlijk kan dit vrij logisch worden verklaard aangezien deze gegevens een hoger risico inhouden voor de vrijwaring van de belangen, rechten en vrijheden van de betrokkene. Deze persoonsgegevens mogen ten slotte enkel worden verwerkt indien er aan strikte voorwaarden wordt voldaan die beschreven staan in de artikelen 8, 9 en 10 van de verordening. Deze artikelen bevatten trouwens ook een paar extra uitzonderingsgronden waar bijkomend op de normale rechtsgronden aan moet worden voldaan.

Kinderen

Een eerste vorm van gevoelige gegevens vinden we onder artikel 8 van de EU (2016) en heeft betrekking tot de persoonsgegevens van kinderen. Volgens overweging 38 en artikel 8 van de EU (2016) moeten kinderen een hogere vorm van bescherming krijgen en moeten hun persoonsgegevens extra voorzichtig worden behandeld. De GDPR legt voor kinderen onder de 16 jaar strikte regels op waardoor de verwerking van deze persoonsgegevens enkel is toegelaten na de toestemming van een ouder of voogd. Het is de taak van de verwerkingsverantwoordelijke om na te gaan of deze toestemming ook effectief werd gegeven door de ouders of voogd en dit te bewijzen in geval van controle.

De GDPR laat wel toe bovenvermelde leeftijdsgrens van 16 jaar te verlagen tot een leeftijd van 13 jaar. Dit kan door elke EU-lidstaat afzonderlijk worden bepaald. Op het moment van schrijven was volgens de CBPL (2018c) nog niet duidelijk of België deze leeftijdsgrens al dan niet zou verlagen.

Ten slotte worden kmo's in het *13 stappenplan* van de Privacycommissie aangeraden de privacyverklaring te schrijven in een voor kinderen begrijpbare taal (CBPL, 2016).

Bijzondere categorieën van persoonsgegevens

Artikel 9 heeft betrekking op biometrische (e.g. een vingerscan), medische of genetische gegevens van een natuurlijk persoon. Dit is een tweede vorm van gevoelige gegevens waaronder alsook persoonsgegevens vallen zoals ras, seksuele geaardheid, politieke voorkeur, religieuze overtuigingen tot zelfs het lidmaatschap bij een vakbond.

Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten

Als laatste vorm van gevoelige gegevens handelt artikel 10 van de EU (2016) over gerechtelijke gegevens zoals strafrechtelijke veroordelingen en strafbare feiten.

2.8.2 Register verwerkingsactiviteiten

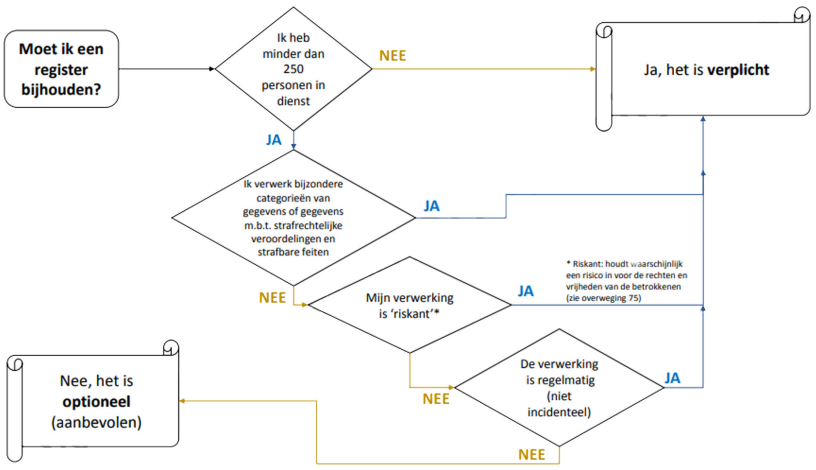
Artikel 30 van de EU (2016) handelt over het register van verwerkingsactiviteiten. Dit register biedt een overzicht en bevat cruciale informatie over alle verwerkingen van de kmo. Het register moet minimaal de volgende informatie bevatten:

- de naam en contactinformatie van de verwerkingsverantwoordelijke en DPO;
- de verwerkingsdoeleinden;
- het soort persoonsgegevens dat wordt opgevraagd;
- alle ontvangers van persoonsgegevens en eventuele doorgiftes aan landen buiten de EU;
- indien mogelijk, de termijnen gedefinieerd voor de bewaring van persoonsgegevens;
- indien mogelijk, welke beveiligingsmaatregelen er voor de verwerking werden getroffen.

Een register is wel niet voor elke kmo verplicht. Zo is het niet nodig voor kmo's met minder dan 250 werknemers in dienst. Indien de kmo aan deze voorwaarde voldoet, kan het nog steeds zijn dat ze wordt verplicht een register bij te houden. Dit kan in volgende gevallen:

- er worden gegevens verwerkt die risico's inhouden voor de rechten en vrijheden van betrokkenen;
- de verwerking komt voor op regelmatige basis en is niet incidenteel;
- er worden bijzondere categorieën van gegevens verwerkt of persoonsgegevens in verband met strafrechtelijke veroordelingen en strafbare feiten.

In Figuur 2.1 wordt schematisch een mooi overzicht gegeven wanneer het noodzakelijk is een register op te stellen.



Figuur 2.1: Schema om te bepalen of er voor de verwerking al dan niet een register noodzakelijk is (CBPL, z.d.-b)

Alhoewel het register voor een kmo niet steeds van toepassing is, wordt bijhouden van

zo'n register door de Privacycommissie toch sterk aangeraden. Een kmo kan het maken van een register trouwens ook beschouwen als een hulpmiddel. Dankzij het register krijgt de kmo een inzicht over de risico's van zijn verwerkingen, weet het wat zijn noodzakelijke verplichtingen zijn in de GDPR, hebben ze een overzicht van alle ontvangers per verwerking en kan er bijzonder snel worden gehandeld in geval van een datalek.

Ten slotte wenst dit onderzoek aan te geven dat de Privacycommissie online een modelregister aanbiedt dat door de kmo's kan worden gebruikt (CBPL, 2018d).

2.8.3 Aanstelling DPO

De rol van een DPO werd al deels toegelicht in sectie 2.5.5 waar ook werd aangegeven dat deze niet altijd verplicht is voor een kmo. In de EU (2016) kan alle informatie omtrent deze rol worden gevonden in de artikelen: 37, 38 en 39.

Een DPO is verplicht in onderstaande gevallen:

- de verwerking wordt verricht door een overheidsinstantie of overheidsorgaan (niet voor gerechten in de uitoefening van hun rechterlijke taken);
- de verwerkingsverantwoordelijke is hoofdzakelijk belast met verwerkingen die regelmatig en stelselmatige observatie op grote schaal van betrokkenen vereisen;
- de verwerkingsverantwoordelijke is hoofdzakelijk belast met grootschalige verwerking van bijzondere categorieën van gegevens, of de verwerking van persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten.

Ondanks deze rol niet altijd verplicht is, kan deze toch een meerwaarde betekenen voor de kmo. Hij kan een niet te miskennen rol spelen in het databeschermingsbeleid van het bedrijf. De DPO kan bovendien in functie van zijn werkgever (i.e. de verwerkingsverantwoordelijke of verwerker) opereren als bemiddelaar of tussenpersoon tussen kmo, DPA en/of betrokkene.

2.8.4 Uitvoering DPIA

In onderstaand artikel omtrent de DPIA werd voor dit onderzoek vertrokken vanuit de CBPL (2018e), de CBPL (2018b) en de EU (2016).

Een DPIA is een verplichting die wordt ingeroepen voor verwerkingen die *waarschijnlijk hoge risico's inhouden*. Gedurende de uitvoering van de DPIA wordt een evaluatie gemaakt van de risico's die de verwerking kan inhouden voor de rechten en vrijheden van de betrokkenen, alsook hoe deze risico's kunnen worden ingeperkt.

Eigenlijk is de DPIA er gekomen omdat men af wou van het systeem gedefinieerd in de oude richtlijn (EU, 1995). Daar moest een verwerking van persoonsgegevens steeds worden gemeld bij de toezichthoudende autoriteit. Dit bracht voor een kmo een enorme administratieve rompslomp en financiële lasten met zich mee. In de huidige verordening verplicht men de kmo een DPIA uit te voeren zodra er een waarschijnlijkheid is dat de

verwerking een hoog risico kan inhouden.

Een DPIA moet minstens de volgende elementen bevatten:

- een gedetailleerde beschrijving van de verwerkingen en doeleinden (het register kan hiervoor een vertrekpunt vormen);
- een beoordeling van de noodzaak van de verwerking in functie van doeleinden;
- een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen; en
- de beoogde maatregelen om deze risico's tegen te gaan.

Artikel 35.3 van de EU (2016) definieert drie verwerkingen waarvoor een DPIA verplicht is:

1. bij een systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen, waaronder profilering, waarop besluiten worden gebaseerd die de betrokkene aanzienlijk kan treffen;
2. bij grootschalige verwerking van bijzondere categorieën van persoonsgegevens of van gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten; of
3. bij stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten.

Indien de kmo oordeelt dat hun verwerking niet valt onder de drie bovenstaand vermelde verwerkingen kan het zich de vraag stellen of hun verwerking een hoog risico kan vormen voor de rechten en vrijheden van een natuurlijk persoon. Indien deze vraag positief wordt beantwoord, moet er alsnog een DPIA worden uitgevoerd. In alle andere gevallen is een DPIA niet nodig maar zal de kmo deze beslissing moeten rechtvaardigen en documenteren.

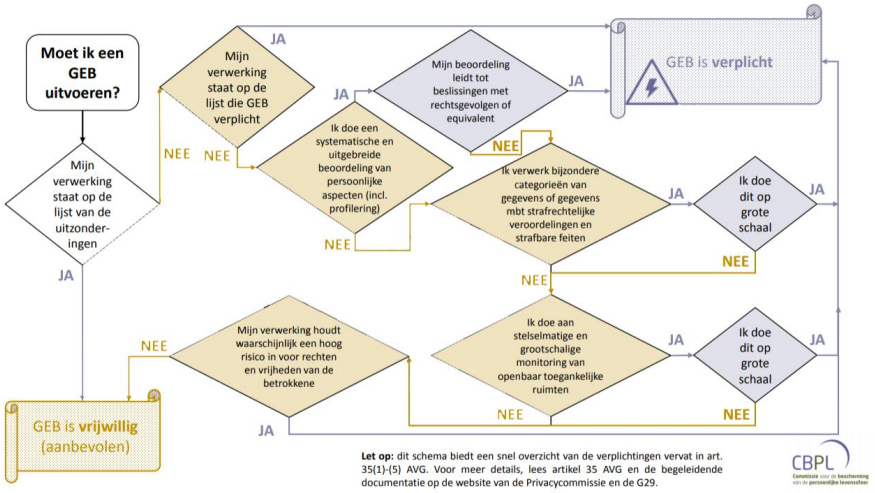
Om kmo's te helpen heeft de WP29 een schematische voorstelling gemaakt met een negental factoren die helpen te beoordelen of een hoog risico al dan niet van toepassing is voor de verwerking (zie Figuur 2.2).

Ten slotte is het belangrijk voor een kmo dat deze DPIA wordt uitgevoerd voor de verwerking van start gaat, en dat er tijdens de verwerking periodiek wordt geëvalueerd of de beoordeling en genomen maatregelen nog steeds up-to-date zijn.

2.9 Beroep doen op externe dienstverleners (outsourcing)

Onder outsourcing kan worden verstaan dat bepaalde delen van de verwerking worden uitbesteed aan externe dienstverleners, verwerkers genoemd. Artikel 28 en 29 van de EU (2016) handelen enerzijds over de verwerker zelf en anderzijds over de samenwerking tussen de verwerkingsverantwoordelijke en de verwerker.

Een veelvoorkomend vorm van outsourcing kan de uitbesteding zijn van loonadministratie. Een ander voorbeeld hiervan is een online platform geconnecteerd met de cloud. Bij double pass wordt deze structuur toegepast om de clubs online hun audit te laten beheren. Deze vorm van verwerkingen is toegelaten in de GDPR maar houdt een aantal speciale



Figuur 2.2: Schema om te bepalen of een verwerking mogelijks een hoog risico inhoudt waardoor een DPIA noodzakelijk is (CBPL, z.d.-a)

aandachtspunten in waar een verwerkingsverantwoordelijke rekening mee moet houden.

Zo mag er volgens de verordening enkel worden samengewerkt met partijen die zelf GDPR-compliance zijn. Dit om ervoor te zorgen dat de rechten en belangen van de betrokkenen gevrijwaard blijven.

Een tweede belangrijke factor is een *verwerkingsovereenkomst* die moet worden gesloten. In deze overeenkomst moet beschreven staan dat de verwerker enkel maar persoonsgegevens mag verwerken die door de kmo zijn gedefinieerd. Er mag dus enkel worden gehandeld in opdracht van de verwerkingsverantwoordelijke.

Tenslotte moet de verwerkingsverantwoordelijke erop toezien dat de externe dienstverlener de eerder vastgelegde contractuele verplichtingen nakomt. De externe dienstverlener is mede daardoor verplicht alle informatie door te geven aan de verwerkingsverantwoordelijke om zo aan te tonen dat de verplichtingen worden nagekomen.

2.10 Doorgifte buiten de EU

Dit thema wordt behandeld in hoofdstuk V van de EU (2016). Binnen de EU zijn doorgiftes van persoonsgegevens vrij, en zodus zonder bijkomende voorwaarden. Wanneer deze gegevens echter worden doorgegeven aan derde landen of internationale organisaties, is het voor een kmo wel belangrijk te weten dat hiervoor bijkomende voorwaarden van toepassing zijn. Hierdoor blijft de veiligheid van de persoonsgegevens gevrijwaard en blijven de rechten van de betrokkene behouden. Deze laatste heeft dan nog steeds de mogelijkheid zijn rechten uit te oefenen.

De persoonsgegevens mogen aan derde landen (i.e. buiten de EU) of internationale

organisaties worden doorgegeven indien aan één van de twee onderstaande voorwaarden wordt voldaan:

- de bestemming is erkend door de Europese Commissie als een bestemming met een gelijkaardig beschermingsniveau als in de EU; of
- de verwerker neemt extra privacybeschermingen op in de overeenkomst waardoor een gelijkaardig beschermingsniveau wordt aangeboden, maar dan op contractuele basis.

Een belangrijke bron van informatie omtrent dit thema, kan worden gevonden op de overzichtspagina van de EC (z.d.-a). Op het moment van schrijven, was dit online platform wel enkel te consulteren in het Engels, maar het kan kmo's goed op weg helpen inzake doorgiftes van persoonsgegevens buiten de EU. Het platform bevat namelijk een lijst van landen die een gelijkaardig beschermingsniveau bieden als in de EU en waar zodus geen bijkomende voorwaarden noodzakelijk zijn (i.e. Adequacy of the protection of personal data in non-EU countries). Alsook biedt het modelcontracten aan die kunnen worden gebruikt indien men een gelijkaardig beschermingsniveau wenst te bieden op basis van een contract (i.e. Model contracts for the transfer of personal data to third countries). Deze modelovereenkomsten zijn zowel beschikbaar tussen een Europese verwerkingsverantwoordelijke en een verwerkingsverantwoordelijke buiten de EU, als tussen een Europese verwerkingsverantwoordelijke en een verwerker buiten de EU.

2.11 Beveiliging

Persoonsgegevens moeten worden beschermd. De beveiliging van een verwerking is trouwens een basisbeginsel van de verordening (EU, 2016, art. 5). Volgens overweging 78 van dezelfde verordening moeten hiervoor technische en organisatorische maatregelen worden genomen.

2.11.1 Waarom is beveiliging noodzakelijk?

Er wordt dagelijks met veel persoonlijke data gewerkt. Verlies van data kan dus sneller gebeuren dan een kmo zou willen. Denk maar aan volgende voorbeelden:

- verlies van een usb-stick met persoonlijke data op;
- inbraak in een databestand door een hacker;
- verlies van papieren documenten met persoonsgegevens;
- gebruik van een openbaar wifi-netwerk waardoor onbevoegden toegang krijgen tot gevoelige data op jouw telefoon of laptop.

Verder is het aan te raden geen onbekende of onbevoegde personen binnen te laten op plaatsen waar persoonlijke data is bewaard (e.g. serverruimtes). Alsook van een paar basiszaken inzake privacy in het achterhoofd te houden zoals je pc te locken wanneer je uw werkplek verlaat en te kijken op de afzender van een e-mail bij het openen van ingesloten links in deze e-mail (e.g. phishing). Beveiliging is dus zeker noodzakelijk zodoende data

breaches te voorkomen.

2.11.2 Hoe kan de kmo hiertegen maatregelen treffen?

Er kan worden overwogen elke verwerking te gaan beoordelen tegenover de mogelijke verwerkingsrisico's om zo gepaste maatregelen te treffen en de risico's te beperken.

Deze verwerkingsrisico's worden in overweging 83 van de EU (2016) nader toegelicht en omvatten: vernietiging, verlies, wijziging en ongeoorloofde verstrekking van of ongeoorloofde toegang tot verwerkte gegevens.

Om de beveiliging van persoonsgegevens te verbeteren, worden er in de verordening ook een aantal beveiligingsmaatregelen aangereikt zoals:

- pseudonimisering;
- versleuteling;
- beperken van toegankelijkheid van de verwerkingssystemen;
- zorgen voor een tijdig herstel van de beschikbaarheid van en toegang tot persoonsgegevens bij een fysiek of technisch incident; en
- procedures die de doeltreffendheid van de technische en organisatorische maatregelen periodiek testen.

Data protection by design and by default

Privacy by design en *Privacy by default* - ook wel *gegevensbescherming door ontwerp en door standaardinstellingen* genoemd - zijn twee verschillende begrippen uit artikel 25 van de EU (2016) die kunnen helpen bij de beveiliging van persoonsgegevens. Alhoewel ze in hetzelfde artikel in de GDPR worden besproken, is er toch een duidelijk verschil tussen beide. Hieronder wordt dieper ingegaan op beide methodieken en worden de verschillen verder toegelicht.

Data protection by design:

Kmo's moeten ernaar streven om tijdens de ontwikkeling van nieuwe producten en diensten zoveel mogelijk rekening te houden met de privacy van persoonsgegevens.

Er moet tijdens de start van de ontwikkeling kritisch nagedacht worden over welke persoonsgegevens noodzakelijk zijn voor de verwerking. Het doel van privacy by design is om enkel de noodzakelijke gegevens op te vragen, alsook de bewaartermijn en de toegang tot een strikt minimum te beperken. Er wordt verder ook al rekening gehouden met noodzakelijke bedrijfsprocessen voortkomend uit de verzoeken van betrokkenen (e.g. gegevens opvragen, wijzigen en/of verwijderen). Door met deze stappen van in het begin rekening te houden, wordt de bescherming van persoonsgegevens verder geoptimaliseerd.

Een bijkomend voordeel voor een kmo bij dergelijke ontwikkelingen is dat men de kost van herontwikkelingen tot een strikt minimum gaat herleiden. Deze kostprijs is doorgaans

de hoogste kost bij ontwikkeling van nieuwe systemen.

Data protection by default:

Deze term van de GDPR heeft meer betrekking op de instellingen van bestaande systemen zoals programma's, applicaties, websites... Deze worden dan zodanig ingesteld dat de gebruiker een zo hoog mogelijke privacy van zijn gegevens geniet.

Een voorbeeld hiervan kan zijn om een gebruiker zijn persoonsgegevens standaard niet te delen met de overige gebruikers van het platform, of door standaard een melding te tonen wanneer er wordt ingeschreven op een nieuwsbrief of gegevens worden gedeeld.

Verschil tussen beide:

Waarbij privacy by design van in het begin de focus legt op het optimaliseren van de privacy tijdens de ontwikkeling van nieuwe systemen, legt privacy by default vooral de focus op hoe men deze systemen kan instellen zodoende de gebruiker van deze systemen een zo hoog mogelijke privacy te garanderen.

2.11.3 Datalek, wat nu?

Eerst en vooral is er, zoals eerder aangegeven in 2.7.1, een *meldplicht* voor datalekken.

> Daarom moet de verwerkingsverantwoordelijke, zodra hij weet dat een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, de toezichthoudende autoriteit onverwijld en waar mogelijk niet meer dan 72 uur nadat hij er kennis van heeft genomen, in kennis stellen van de inbreuk in verband met persoonsgegevens, tenzij de verwerkingsverantwoordelijke conform het verantwoordingsbeginsel kan aantonen dat het onwaarschijnlijk is dat deze inbreuk risico's voor de rechten en vrijheden van natuurlijke personen met zich brengt. (EU, 2016, overw. 85)

Uit bovenstaand citaat kan worden afgeleid dat een kmo een datalek binnen de tijdspanne moet melden aan de DPA zodra het op de hoogte hiervan is. Dit moet wel worden gedaan binnen de 72 uur, tenzij er kan worden bewezen dat de datalek geen directe gevaren inhoudt voor de persoonsgegevens. Soms moet de kmo ook rechtstreeks de betrokkene verwittigen (e.g. bij eventuele financiële verliezen of identiteitsdiefstal).

Om deze datalekken te melden, moeten de DPA's hieromtrent procedures publiceren. Dit is op de dag van schrijven nog niet overal het geval maar op de website van de Privacycommissie kunnen dergelijke formulieren reeds worden gedownload.

Ten slotte is het belangrijk te vermelden dat een kmo zal worden gesanctioneerd indien ze de datalek niet meldt, dit bijkomend op de eventuele boete voor de datalek zelf.

2.12 Controles

Er is nog maar heel weinig duidelijkheid naar kmo's toe hoe er door de toezichthoudende autoriteiten zal worden gecontroleerd en hoe een controleur zich kenbaar maakt tijdens een controle. Het spreekt namelijk voor zich dat kmo's niet zomaar iedereen zullen binnenlaten om deze personen toegang te verlenen tot hun bedrijfsdocumenten.

Volgens een artikel van Data News (2017) waar onder meer bevoegd staatssecretaris voor Privacy Philippe De Backer spreekt, krijgt de Privacycommissie de mogelijkheid audits uit te voeren bij bedrijven. Er wordt echter ook aangegeven dat de nadruk van de Privacycommissie ligt op preventie en sensibilisering, en niet op het controleren van bedrijven ter plaatse. Ook in het geval van overtredingen is het niet de bedoeling direct te sanctioneren maar eerder om te informeren, begeleiden en advies te verstrekken. Indien een bedrijf een overtreding maakt en op korte termijn de nodige correcties aanbrengt, is dit voor hun een afgehandelde zaak. Sanctionering is dus een allerlaatste middel om in te grijpen indien een kmo geen gevolg geeft aan de opmerkingen van de Privacycommissie.

In een tweede artikel van Data News (2018b) wordt dit verhaal bevestigd door Willem Debeuckelaere, hoofd van de Privacycommissie. Debeuckelaere zegt wel dat er gaat worden gecontroleerd op zaken die foutlopen, maar daarom niet ter plaatse. Alsook dat er zal worden opgetreden enkel indien bedrijven niet meegaan in de opmerkingen van de Privacycommissie.

2.13 Administratieve geldboeten

In 2.12 werd al aangegeven dat de Privacycommissie niet de prioriteit heeft kmo's te beboeten. Toch kan er in twee optieken een administratieve geldboete worden opgelegd. Enerzijds kan dit wanneer een betrokkene klacht indient bij de Privacycommissie wanneer hij van mening is dat de kmo fouten maakt tegenover de verordening, en dat hij daardoor schade heeft geleden. Anderzijds kan een boete volgen indien de kmo geen gevolg geeft aan eerder opgelegde opmerkingen door de Privacycommissie.

Volgens artikel 31 van de EU (2016) moet zowel de verwerkingsverantwoordelijke als de verwerker samenwerking verlenen aan de DPA.

Slagkracht DPA:

Volgens de CBPL (2018e) heeft de Privacycommissie de mogelijkheid een berisping of waarschuwing te geven, dwingen een verzoek van de betrokkene in te willigen, dwingen binnen een bepaalde termijn GDPR-compliance te zijn, dwingen de verwerking te bevriezen of te verbieden, en om boetes op te leggen.

Boetetarieven:

Er wordt in de verordening gehandeld met twee tarieven inzake boetes (zie artikel 83 punten 4, 5 en 6 van de EU (2016)).

Enerzijds kan een kmo worden onderworpen aan boetes tot tien miljoen euro of 2 % van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is. Dit kan men catalogeren als de 'kleine' boetes (e.g. inbreuk tegenover het vragen van de toestemming van een kind voor diensten van de informatiemaatschappij, inbreuk tegenover privacy by design and default...).

Anderzijds kan een kmo worden onderworpen aan boetes tot twintig miljoen euro of 4 % van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is. Dit kan men catalogeren als de 'hogere' boetes (e.g. inbreuken tegenover de basisbeginselen van gegevensverwerking waaronder de voorwaarden voor toestemming, rechten van de betrokkenen, doorgiftes van persoonsgegevens aan derde landen en internationale organisaties, niet-naleving van een bevel van de DPA...).

Schadevergoeding:

Elke betrokkene heeft het recht een schadevergoeding te eisen via de rechtbank voor de geleden schade. De betrokkene kan zich zowel tot de verwerkingsverantwoordelijke als tot de verwerker richten. Beiden kunnen aansprakelijk worden gesteld voor de schade, tenzij er kan worden aangetoond dat ze niet verantwoordelijk zijn voor de geleden schade.

Terugvordering:

In een samenwerking tussen enerzijds een verwerkingsverantwoordelijke en anderzijds de verwerker kan het mogelijk zijn dat de betrokkene zijn klacht richt tot de verwerkingsverantwoordelijke ondanks dat de verwerker verantwoordelijk is voor de geleden schade. In dit geval kan de verwerkingsverantwoordelijke zich naderhand richten tot de verwerker om een terugvordering van de betaalde schadevergoeding te eisen (e.g. alle data wordt opgeslagen in de cloud waar er een datalek voorkomt die de data van de verwerkingsverantwoordelijke treft).

3. Methodologie

In voorgaand hoofdstuk werd een uitvoerige stand van zaken weergegeven omtrent het onderzoeksdomein met de nadruk op de impact voor een kmo. Dit hoofdstuk zal een meer praktische toelichting geven van de stappen die een kmo dient te ondernemen tijdens het proces naar GDPR-compliance. Verder wordt de procedure gevolgd tijdens een aanvraag tot gegevenswissing nader toegelicht, wordt de manuele workload in kaart gebracht wanneer 1 % van het klantenbestand van double pass zou gebruikmaken van zijn recht tot gegevenswissing, en tenslotte wordt in een businesscase de ROI nagegaan bij automatisatie van dit proces. In een volgend hoofdstuk worden de conclusies van dit onderzoek neergeschreven.

3.1 Compliance-proces kmo

De onderstaande procedure is vertrokken vanuit het 13 stappenplan van de CBPL (2016), aangepast aan de noden en behoeften van de organisatie double pass.

Aangezien double pass vrij gevoelige data verwerkt die mogelijks een hoog risico kunnen inhouden voor de rechten en vrijheden van natuurlijke personen, werd beslist een DPIA uit te voeren.

3.1.1 Bewustmaking

In de eerste plaats dient een kmo, dus ook double pass, zich bewust te worden van de gevolgen die de verordening kan hebben op de organisatie. Een goede inwerking in de wetgeving en voorafgaand onderzoek omtrent de GDPR is een absolute must om het gehele

compliance-proces tot een goed einde te kunnen brengen.

3.1.2 Data flows

Bedrijfsprocessen

Na het inwerken in de wetgeving werden bij double pass data flows uitgetekend. Deze flows helpen een inzicht te krijgen in alle mogelijke datastromen van de organisatie. Data flows worden best per bedrijfsproces opgesplitst in documenten.

Bij double pass kunnen er drie soorten bedrijfsprocessen worden onderscheiden, namelijk:

- interne processen inzake persoonsgegevens van werknemers, sollicitanten en dergelijke;
- processen voor het leveren van diensten (e.g. audits); en
- processen tussen double pass en subcontractors of external suppliers.

Bij het maken van data flows is het alsook van belang te weten welke rol (i.e. verwerkingsverantwoordelijke of verwerker) double pass speelt in de huidige flow. Vorig hoofdstuk verduidelijkte namelijk dat er afhankelijk van de rol andere plichten en verantwoordelijkheden gelden.

Het grootste bedrijfsproces binnen double pass is het auditen van clubs. De corebusiness van double pass is namelijk de jeugdopleiding binnen voetbalclubs te optimaliseren. De audits worden in opdracht van een voetbalfederatie gedaan, dus double pass fungeert in dit proces in de rol van verwerker. Uiteraard kan dit onmogelijk worden bewerkstelligd zonder het verzamelen van data, waaronder persoonsgegevens. Om al deze data te uploaden, wordt door de club gebruik gemaakt van een online platform.

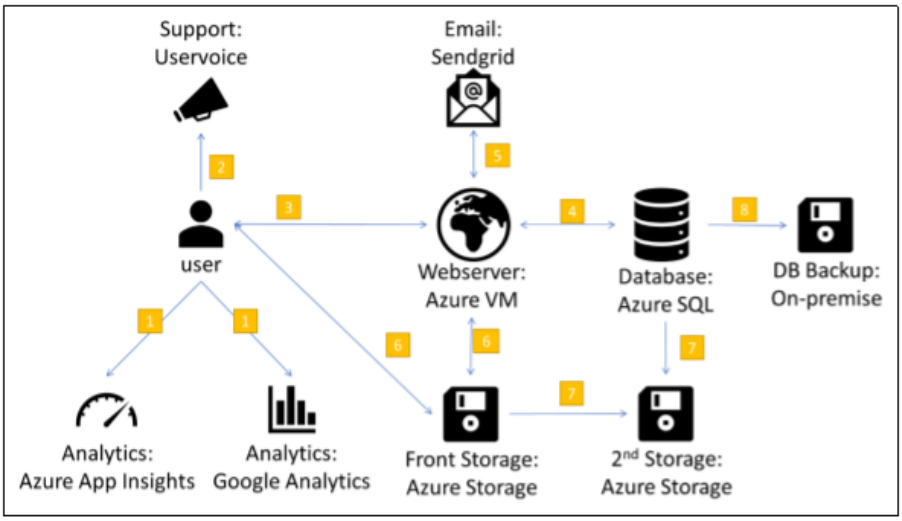
Hoe wordt er te werk gegaan?

Aan de hand van high level tekeningen worden de data flows voor elk proces in kaart gebracht. Figuur 3.1 toont een voorbeeld van dergelijke tekening. De data flows worden aangeduid op de tekening met pijlen, en de nummers zorgen doorheen het document voor meer verduidelijking van de flow.

Na het uitdenken van alle mogelijke data flows voor een specifiek bedrijfsproces kan de organisatie zich richten op het maken van een data mapping of register van de verwerkingsactiviteiten.

3.1.3 Data mapping (i.e. register verwerkingsactiviteiten)

Zoals reeds vermeld in 3.1.2 kan er gestart worden met het maken van het register eens alle data flows zijn uitgetekend. Dit wordt gedaan om een overzicht te krijgen van alle verwerkingen die gebeuren binnen de organisatie. Aan de hand van voorgaande data flows



Figuur 3.1: Global overview data flow external user PASS Online system (double pass, 2018a)[1]

is het nu ook veel visueler hoe deze flows lopen en wie welke rol juist heeft in een bepaalde verwerking. Een gedeeltelijk voorbeeld van dit document kan worden bekeken in Bijlage B.

Het document is opgebouwd uit volgende onderdelen:

- een algemene identificatie van de organisatie en eventueel aangestelde DPO;
- een algemeen overzicht van alle verwerkingen; en
- elke verwerking in detail uitgewerkt (automatisch toegevoegd aan overzicht, red.).

Wat bevat één specifieke verwerking in detail?

De volgende informatie wordt gecapteerd in het document:

- korte beschrijving van de verwerking;
- rol van double pass in deze verwerking;
- rechtsgrond voor de verwerking;
- persoonsgegevens die worden opgevraagd (verwijzing extern bestand);
- toegangsrechten tot deze persoonsgegevens (verwijzing extern bestand);
- verwerkingsdoeleinden;
- alle ontvangers en doorgiftes aan landen buiten de EU;
- dataretentie;
- genomen beveiligingsmaatregelen;
- naam en contactinformatie verwerkingsverantwoordelijke of verwerker (afhankelijk van de eerder gekozen rol, red.); en
- extra informatie over de verwerking (optioneel).

[1] Bron afkomstig van het intranet (niet publiekelijk toegankelijk) van double pass.

In bovenstaande opsomming valt op dat er twee verwijzingen naar aparte documenten zijn. De eerste verwijzing refereert naar een document dat alle verzamelde persoonsgegevens voor de desbetreffende verwerking in kaart brengt (zie Bijlage B, Screenshot 1). De tweede verwijzing refereert naar een document dat een matrix van alle toegangsrechten bevat, per verwerking en per werknemer van double pass (zie Bijlage B, Screenshot 2). Het voordeel van dergelijke werkwijze wordt gedaan om de documenten overzichtelijker te houden en meer flexibiliteit in te bouwen (e.g. niet elke verwerking moet afzonderlijk worden gewijzigd indien bepaalde toegangsrechten voor een werknemer wijzigen). Alsook biedt het document met de matrix van toegangsrechten een duidelijk overzicht van al deze rechten en kan het makkelijk worden gewijzigd.

De GDPR als een zegen voor een kmo

De GDPR kan door de kmo inderdaad worden aanzien als een zegen. Het biedt hen namelijk de mogelijkheid de gecapteerde data voor hun verwerkingen eens grondig te analyseren en voor de opgevraagde persoonsgebonden informatie de noodzaak te bepalen voor het bereiken van hun verwerkingsdoeleinden. Waarschijnlijk wordt al snel duidelijk dat er voor bepaalde verwerkingen onnodige persoonsgegevens worden opgevraagd. Dit laatste gold ook deels voor sommige verwerkingen van double pass.

3.1.4 Communicatie

Als een kmo persoonsgegevens verwerkt, is het zijn plicht als verwerkingsverantwoordelijke de betrokkene te informeren. Meestal wordt dit gedaan in de vorm van een *privacyverklaring*. Deze verklaring moet worden opgesteld in een duidelijke en begrijpbare taal voor de betrokkene.

Verder dient de privacyverklaring bepaalde informatie te bevatten zoals de identiteit van de verantwoordelijke, waarom en voor welke doeleinden de persoonsgegevens van de betrokkene worden verwerkt, hoelang zijn gegevens zullen bewaard blijven en of deze worden uitgewisseld buiten de Europese Unie.

Een tweede aspect van de privacyverklaring is dat deze moet bevatten hoe een betrokkene een klacht kan indienen bij de toezichthoudende autoriteit indien hij van mening is dat zijn persoonsgegevens niet correct worden verwerkt. Op het moment van schrijven is dit voor België de Privacycommissie.

Ten slotte kan de privacyverklaring worden aanzien als het uithangbord van de onderneming om aan te tonen hoe de kmo met persoonsgegevens omspringt. Indien de privacyverklaring niet duidelijk of onvolledig is, zal dit misschien een allereerste aanzet zijn voor de toezichthoudende autoriteit om de kmo aan verdere controle te onderwerpen. Bovendien straalt het vertrouwen uit naar klanten wanneer wordt gemerkt dat de kmo confidentieel met hun gegevens omspringt.

double pass

Bij double pass is er een privacyverklaring op de corporate website voor verwerkingen waar double pass de verwerkingsverantwoordelijke is. Alsook zijn er privacyverklaringen op de online platforms die de clubs gebruiken voor hun audit. In dit laatste geval is double pass de verwerker en is het eigenlijk de privacyverklaring van de desbetreffende voetbalfederatie die wordt gepubliceerd, dit in samenspraak met double pass om tegemoet te komen aan de noodzakelijk informatie voor de audit.

Deze privacyverklaringen worden door de legal advisor van double pass, de heer Joost Roelens, onder de loep genomen en zodoende aangepast om compliant de nieuwe verordening te zijn.

3.1.5 Procedures

Het moet duidelijk zijn voor elke werknemer van double pass hoe er moet gehandeld worden inzake de GDPR-wetgeving. Zo worden er procedures opgesteld voor bijvoorbeeld een datalek of wanneer de betrokkene zijn rechten wil uitoefenen. Deze procedures moeten de werkwijze voor dergelijke afhandelingen vergemakkelijken en er alsook voor zorgen dat iedereen in de organisatie dezelfde werkwijze hanteert.

Deze procedures zijn op het moment van schrijven nog volop in ontwikkeling, maar Figuur 3.2 laat reeds een deel zien van de procedure ontwikkelt voor het verwittigen van de DPA in geval van een datalek. De gegevens inzake verschillende DPA's kunnen worden geraadpleegd, alsook links naar documenten voor het melden van een datalek.
Opgelet: niet elke toezichthoudende autoriteit biedt op het moment van schrijven dergelijke documenten aan.

Notify DPA in case of data breach

1 DPA list per country

See an up-to-date list at http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612080

1.1 Belgium

Commission de la protection de la vie privée
Commissie voor de bescherming van de persoonlijke levenssfeer
Rue de la Presse 35 / Drukpersstraat 35
1000 Bruxelles / 1000 Brussel
Tel. +32 2 274 48 00
Fax +32 2 274 48 35
e-mail: commission@privacycommission.be
Website: http://www.privacycommission.be/

Art 29 WP Vice-President: Willem DEBEUCKELAERE, President of the Belgian Privacycommission

Fill in the form:
https://eforms.privacycommission.be/privacy-commission/forms/pdf/melding-gegevenslek.pdf

Figuur 3.2: Procedure - Notify DPA in case of data breach (double pass, 2018b)[2]

[2]Bron afkomstig van het intranet (niet publiekelijk toegankelijk) van double pass.

3.1.6 DPO

Volgens de verordening is double pass momenteel niet verplicht een DPO aan te stellen. Indien er in de toekomst medische data gaat worden verzameld om clubs beter te kunnen begeleiden, zal double pass onder artikel 37.1c van de EU (2016) vallen en een DPO moeten aanstellen.

3.1.7 Internationaal

Double pass werkt internationaal en daarmee moet er ook worden bepaald onder welke toezichthoudende autoriteit dat de kmo valt. Volgens de CBPL (2016) voorziet de verordening hiervoor enigszins een complexe regeling om te bepalen welke toezichthoudende autoriteit de leiding neemt in geval van een internationale klacht.

Double pass daarentegen valt echter gewoon onder de categorie met een traditionele hoofdzetel aangezien de leidende autoriteit wordt bepaald naargelang de hoofdvestiging van de organisatie, of de vestiging waar de beslissingen worden genomen omtrent gegevensverwerkingen. In het geval van double pass is deze vestiging in Brussel en zodus is de Privacycommissie momenteel de toezichthoudende autoriteit die hier de leiding zou nemen.

In het geval dat double pass verwerker is voor een voetbalfederatie in de EU, zal de klacht worden ingediend bij de DPA van het desbetreffende land. Deze zal dan worden beschouwd als leidende DPA om de klacht verder af te handelen. Uiteindelijk zal deze wel met de Belgische Privacycommissie samenwerken.

3.1.8 Bestaande contracten

In de bestaande contracten van double pass werknemers zal een addendum worden opgenomen waarin de handelswijze binnen de organisatie inzake GDPR zal worden toegelicht. Zo weten huidige en nieuwe werknemers hoe ze met persoonsgebonden data moeten omgaan en welke veiligheidsmaatregelen ze hiervoor in acht moeten nemen.

In de bestaande contracten tussen enerzijds double pass als verwerkingsverantwoordelijke en anderzijds een leverancier of onderaannemer moeten de nodige aanpassingen worden aangebracht inzake GDPR. Je mag als organisatie enkel met derde partijen samenwerken die zelf GDPR-compliance zijn. De verordening bepaalt wie welke verplichtingen heeft en welke beveiligingsmaatregelen er moeten worden genomen.

Beide types van bovenstaande contracten werden door double pass in kaart gebracht, onder meer door de eerder gemaakte data flows. Later werden ze gereviewd door de legal advisor van double pass.

3.2 Automatisatie gegevenswissing (”recht op vergetelheid”)

Bij double pass wensen we te onderzoeken of de gegevenswissing kan worden geautomatiseerd. We willen aan de hand van een businesscase de kosten afwegen tegenover de baten. Dit zal worden gedaan voor het proces waar we in opdracht van de voetbalfederatie clubs doorlichten aan de hand van een audit.

In deze sectie wordt dit proces nader toegelicht. In Sectie 3.3 zal de ROI worden toelicht aan de hand van een businesscase.

Korte beschrijving audit-proces

Clubs die deelnemen aan een audit krijgen toegang tot een online platform waar ze hun audit kunnen beheren. Op dit platform kan de club tot de vooropgestelde deadline de benodigde stavingsstukken uploaden, alsook om de nodige profielen (e.g. staf, trainers...) binnen de club in kaart te brengen door het creëren van online gebruikers. Na de registratie van een gebruiker krijgt deze toegang tot het platform en heeft deze de mogelijkheid zijn gegevens te bekijken, aan te passen of een online cv aan te maken.

Bij het verstrijken van de deadline worden al deze gegevens in een geëncrypteerde file geconverteerd. Deze wordt achteraf door een double pass medewerker (e.g. auditor, projectmanager) in een offline software tool geladen om het audit-proces verder te finaliseren. Deze tool is ontwikkeld door double pass en enkel toegankelijk op de bedrijfslaptops binnen de organisatie. Al deze laptops zijn versleuteld door encryptie. Alsook is er bij double pass, zoals eerder vermeld in dit onderzoek, een matrix met toegangsrechten (zie Bijlage B, Screenshot 2). Deze rechten bepalen of een medewerker al dan niet toegang krijgt tot de desbetreffende file.

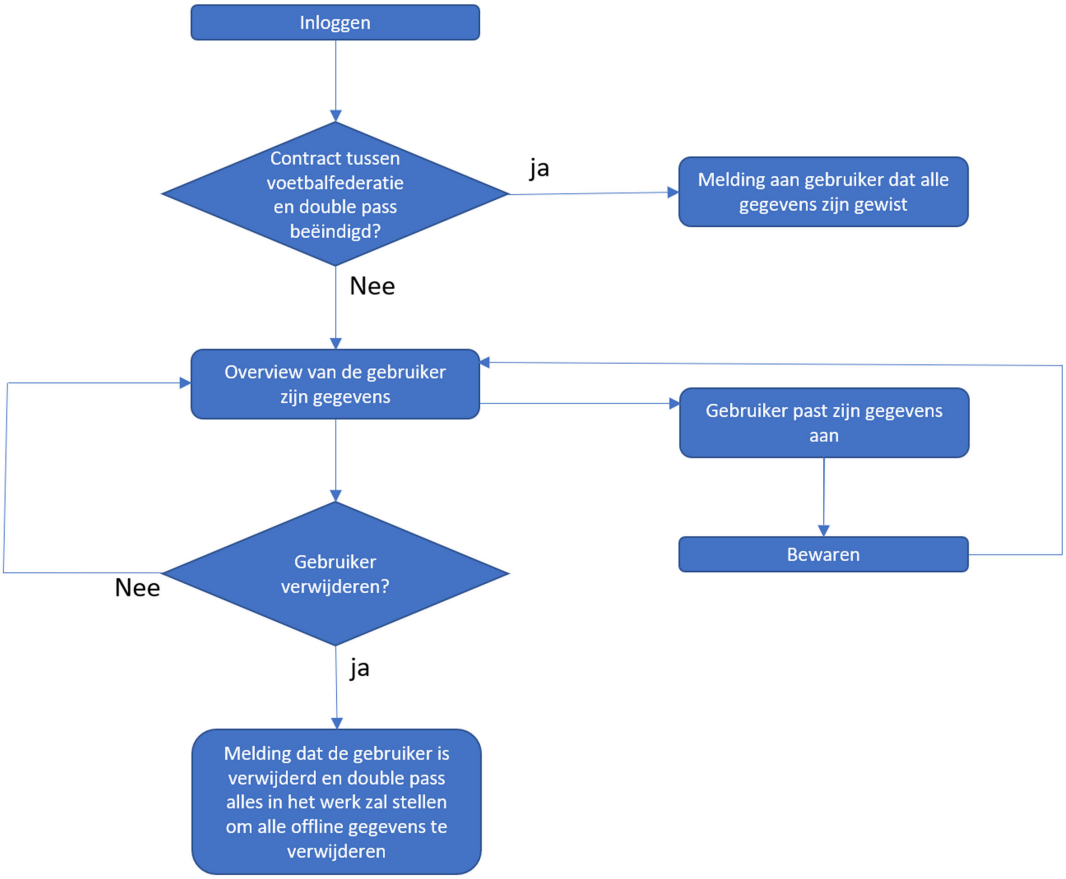
Automatisatie

In het audit-proces wensen we de gegevenswissing te automatiseren voor de gebruikers van het online platform. Er zou ook een aanvraag kunnen komen van een ouder en/of speler om zijn gegevens te wissen. Dit zou dan via de voetbalfederatie (i.e. de verwerkingsverantwoordelijke) moeten gebeuren, die dan op zijn beurt double pass als verwerker kan belasten gevolg te geven aan dit verzoek. Deze flow behoort echter niet tot deze procesoptimalisatie en wordt niet verder onderzocht.

De automatisatie zou worden bewerkstelligd door in de privacy policy een sectie te voorzien waarin de betrokkene wordt uitgelegd hoe hij zijn recht tot gegevenswissing kan uitoefenen. Hiervoor wordt hij doorgelinkt naar het online platform. Om het proces op dit platform te verduidelijken werden er eerst flow charts uitgetekend. De eerste flow chart (zie Figuur 3.3) verduidelijkt het frontend-gedeelte van de website. In de tweede flow wordt het backend-gedeelte toegelicht (zie Figuur 3.4).

Frontend-gedeelte:

In de flow van het frontend-gedeelte kan worden gezien dat de gebruiker eerst aanlogt. Hierna krijgt hij een melding te zien of er nog een actief contract is tussen de voetbalfederatie en double pass. Indien dit contract reeds is beëindigd, zijn er namelijk geen persoonsgegevens meer in de systemen van double pass en is alles reeds gedeletet. Indien dit niet het geval is, krijgt de gebruiker een overzicht van zijn gegevens. Hij kan kiezen om verder te gaan met de procedure en zijn gegevens te wissen, of hij kan kiezen zijn gegevens te wijzigen en te bewaren. Wanneer de gebruiker kiest zijn gegevens te wissen, toont het systeem een melding dat de online gegevens zijn verwijderd en double pass alles in het werk zal stellen om de overige offline gegevens uit zijn systemen te verwijderen.



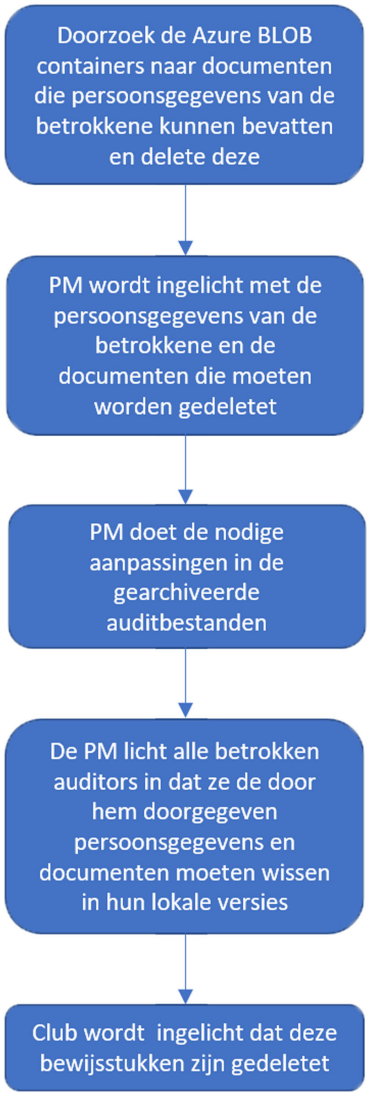
Figuur 3.3: Automatisatie gegevenswissing - Flow chart frontend (double pass, 2018c)[3]

Backend-gedeelte:

In de flow van het backend-gedeelte worden de Azure storage containers doorzocht, dit zijn containers waarin per audit alle bewijsstukken van de desbetreffende audit worden bewaard. Indien er met een crawler documenten worden gevonden die de desbetreffende persoonsgegevens bevatten, zullen deze worden vervangen door een template met gepaste tekst dat dit document werd verwijderd omwille van privacyredenen. De projectmanager zal worden ingelicht en krijgt de persoonsgegevens van de betrokkene door, alsook de

[3]Bron afkomstig van het intranet (niet publiekelijk toegankelijk) van double pass.

documenten die de desbetreffende persoonsgegevens bevatten uit de storage containers. Hij zal de gegevens verwijderen uit de gearchiveerde bestanden en op zijn beurt alle betrokken auditors inlichten om hetzelfde te doen in hun lokaal bewaarde versies van de audit. In principe is er één centraal kopie en kunnen de auditors deze versie aanpassen zodoende dat enkel deze versie moet worden bewerkt. Als laatste stap wordt de club ingelicht dat er bepaalde bewijsstukken niet kunnen worden gebruikt in de audit omwille van privacyredenen. Voor een actieve audit heeft de club dan de mogelijkheid deze bewijsstukken opnieuw te uploaden indien de betrokken persoonsgegevens hieruit werden verwijderd.



Figuur 3.4: Automatisatie gegevenswissing - Flow chart backend (double pass, 2018c)[4]

[4]Bron afkomstig van het intranet (niet publiekelijk toegankelijk) van double pass.

Simulatie manuele workload

In het onderzoeksvoorstel (zie Bijlage A) werd vooropgesteld om een prognose te doen wanneer 1 % van de gebruikers zijn gegevens wenst te verwijderen. Voor deze simulatie baseren we ons op de verwerking die double pass volbrengt voor de voetbalfederaties van hun Europese projecten (i.e. de Deense, Engelse, Duitse, Hongaarse, Belgische en Schotse voetbalfederaties). In de databank van deze projecten bevinden zich op de dag van schrijven 13.805 gebruikers. Afgerond komt dit overeen met 138 gebruikers die wensen gebruik te maken van hun recht tot gegevenswissing.

Workload van één aanvraag:

1. Gebruiker wissen uit databank.
2. Manueel zoeken in Azure storage containers via id van de club.
3. Manueel deze gevonden storage containers doorzoeken naar persoonsgegevens van de betrokkene die zijn recht tot gegevenswissing wenst uit te oefenen.
4. Gevonden files veranderen door default template files waarin staat dat de file persoonsgebonden informatie bevat en deze omwille van een verzoek tot gegevenswissing niet kan worden gebruikt voor de audit.
5. Aanmaken van een nieuw geëncrypteerd bestand.
6. Vervangen van het oude bestand door het nieuw geëncrypteerd bestand.
7. Aan projectmanager doorgeven om de persoonsgegevens uit de gearchiveerde auditfiles te halen en overige lokaal bewaarde versies aan te passen en/of verwijderen.
8. Projectmanager vraagt betrokken auditors om hetzelfde te doen.

Resultaat:

De schatting voor één aanvraag kan worden geschat op 1/2 mandag werk door iemand van de dienst IT & Technologie, dit afhankelijk van het aantal stavingsstukken dat de club heeft opgeladen. Indien dit wordt doorgetrokken naar de vooropgestelde 1 % en dus neerkomt op 138 aanvragen, zal dit ongeveer overeenkomen met 69 mandagen werk.

Na het globaal in kaart brengen waarop de automatisatie van het recht op gegevenswissing zou worden toegepast én wat de manuele workload hiervoor zou betekenen, wordt in Sectie 3.3 de businesscase hiervoor uitgeschreven.

3.3 Businesscase

Businesscase - Procesoptimalisatie double pass OPTIMISING PLAYER POTENTIAL

Onderwerp: Businesscase - Automatisatie gegevenswissing

Inhoudstafel:

Verantwoordelijken

	Naam	Functie	Handtekening	Datum
Opgesteld door	Tom Vandevelde	Software developer		09/05/2018
Goedgekeurd door	Hugo Schoukens	CEO		

Tabel 3.1: Businesscase - Verantwoordelijken

Historiek van aanpassingen

Datum	Reden voor aanpassing	Auteur	Versie
11/05/2018	Bijwerking risico's	Tom Vandevelde	v1

Tabel 3.2: Businesscase - Historiek van aanpassingen

3.3.1 Meerwaarde van dit project

Wat is het doel van dit project?

Dit project heeft als doel artikel 17, recht op gegevenswissing ("recht op vergetelheid") van de EU (2016) te automatiseren door op het online audit-platform voor clubs een procedure te voorzien waar betrokkenen hun gegevens desgewenst kunnen verwijderen. Op het platform is het reeds mogelijk dat een gebruiker zijn gegevens kan inkijken en/of wijzigen.

Wat is de aanzet/reden voor dit project?

Meer en meer gaat double pass bewust om met zijn bedrijfsprocessen. Objectiviteit, oprechtheid, confidentialiteit zijn core values van de organisatie. De GDPR wordt dus hoog in het vaandel gedragen aangezien vertrouwelijkheid van club- en persoonsgegevens voor de organisatie heel belangrijk zijn.

Een algemene doelstelling is om zo transparant mogelijk naar clubs en hun leden toe te handelen. Door op het online platform een procedure te voorzien waarmee gebruikers hun gegevens desgewenst kunnen wissen, toont double pass aan heel transparant te willen omspringen met persoonsgebonden informatie. Dit zal het vertrouwen in het bedrijf enkel maar ten goede komen.

Na onderzoek is gebleken dat het manueel opvolgen van dergelijk verzoek tot gegevenswissing door de betrokkene niet zo triviaal is (zie 3.2). Zelfs indien hiervoor uitgewerkte

procedures zijn opgemaakt, zal het nog niet eenvoudig zijn gevolg te geven aan dergelijke aanvragen.

Ten slotte komt double pass tegemoet aan zijn gebruikers door het platform naar hun toe te faciliteren wat meteen als positief gevolg heeft dat dit de werkdruk voor double pass medewerkers zal verlagen.

Wat is het eindresultaat voor de clubleden/doelgroepen?

Het project bestaat uit drie delen.

In het eerste deel kan er een onderzoek worden gedaan naar de vereisten van de gebruikers van het online platform en de betrokken medewerkers van double pass (i.e. IT-dienst, projectmanagers en auditors).

In het tweede deel wordt het bestaande e-platform uitgebreid met een procedure voor gegevenswissing. Het platform biedt gebruikers na het aanmelden reeds ondersteuning hun gegevens te bekijken en/of aan te passen. Door de uitbreiding van dit platform is er een vaste procedure omtrent gegevenswissing, en zal dergelijk verzoek vlotter, beter en eenvoudiger kunnen worden opgevolgd door double pass medewerkers.

Een derde deel bestaat uit de training en ondersteuning van het personeel + een eventuele demo naar de gebruikers toe.

3.3.2 Budgettaire impact op de organisatie

Looptijd: augustus 2018

Geschatte mandagen

- Voorbereiding: 3 mandagen
- Ontwikkeling: 15 tot 20 mandagen (gebaseerd op een medior/senior developer)
- Training: 5 mandagen

Geschat budget

23 tot 28 mandagen * uurloon werknemer, opgesplitst in:

- Business Analist: 3,5 mandagen (voorbereiding + demo online gebruikers)
- Development: 16 tot 21 mandagen (development + training geven)
- Hoofd audits + Projectmanagers: 3,5 mandagen (opleiding)

Benodigde competenties projectteam

- Business Analist (onderzoek vereisten gebruikers)
- Medior/senior developer

3.3.3 Kosten-batenoverzicht

Uit het resultaat van 3.2 kan worden afgeleid dat er ongeveer 69 mandagen nodig zijn om de verzoeken tot gegevenswissing af te handelen indien 1 % van het klantenbestand zijn recht hiertoe wenst uit te oefenen. Sectie 3.3.2 verduidelijkt dat voor de implementatie van het project naar schatting 23 tot 28 mandagen nodig zijn. De applicatie wordt geïmplementeerd door de IT-afdeling van double pass en geïnstalleerd op bestaande servers. Hierdoor is de onderhoudskost minimaal en wordt deze niet in rekening gebracht.

Indien de applicatie succesvol wordt geïmplementeerd zal dit tevens zorgen voor een verlaging van de werkdruk voor de IT-afdeling van double pass. Evenals wordt door de automatisatie de kans op fouten verkleind.

Om de ROI te berekenen, brengen we eerst de projectkosten (zie Tabel 3.3) in kaart waarna heel makkelijk de ROI kan worden afgelezen van Tabel 3.4.

Projectkosten

Kostensoort	2018
Business Analist (voorbereiding + demo online gebruikers)	3,5
Development (development + training geven)	16 - 21
Hoofd audits + Projectmanagers (opleiding)	3,5
Totaal projectkosten	23 - 28

Tabel 3.3: Projectkosten automatisatie gegevenswissing (uitgedrukt in mandagen)

ROI

# Aanvragen	Mandagen/aanvraag	Totaal mandagen
1	0,5	0,5
2	0,5	1
3	0,5	1,5
...	0,5	...
46	0,5	23
...	0,5	...
56	0,5	28
...	0,5	...
138	0,5	69

Tabel 3.4: ROI automatisatie gegevenswissing (uitgedrukt in mandagen)

Resultaat: Uit Tabel 3.4 kan worden afgeleid dat, afhankelijk van de benodigde tijd voor het development (i.e. 16 tot 21 mandagen), de ROI reeds tussen de 46^{e} en 56^{e} aanvraag kan worden bereikt.

3.3.4 Bijdrage aan de realisatie van de strategie

Tot welke strategische en of operationele doelstellingen draagt het project bij?

Bijdrage strategie

Kerntaak	Laag	Middel	Hoog
Jeugdopleiding optimaliseren			
Innovatie			√
Actief zijn wereldwijd			
Referentie in sportmanagement			
Vertrouwelijk			√
Oprechtheid		√	
Objectiviteit			
Aanpasbaarheid			
Flexibele aanpak naar klanten toe			√

Tabel 3.5: Bijdrage aan de realisatie van de strategie

Doelstelling interne werking

- Verbetering van de werkdruk door efficiëntere behandeling van verzoeken tot gegevenswissing met minder manuele handelingen.
- Vrijgekomen werktijd personeel nuttig aanwenden voor andere diensten/verbeteringen binnen de double pass organisatie.

3.3.5 Belangrijkste risico's

De aangevraagde verzoeken tot gegevenswissing via het online platform zouden lager kunnen uitvallen dan de verwachte resultaten vastgesteld door voorafgaand onderzoek. Hierdoor zal de ROI een langere duurtijd hebben of zelfs niet worden behaald (indien gebruikers hun gegevens gewoon wensen te laten staan tot de overeenkomst voor de verwerking afloopt, red.). De werkdruk voor het personeel zal dan echter ook niet verhogen.

4. Conclusie

In dit onderzoek werd een antwoord gezocht op de vraag: ”Welke impact heeft de General Data Protection Regulation (GDPR) op de data van een kmo?” Uit onderzoek is gebleken dat de nieuwe verordening (EU, 2016) enorm is aangescherpt tegenover de vroegere richtlijn (EU, 1995), waardoor het compliance-proces niet zo triviaal is en de verordening wel degelijk een enorme impact heeft op de data van een kmo. Anderzijds wordt door twee artikelen van Data News (2017, 2018b) aangetoond dat de toezichthoudende autoriteiten eerder een sensibiliserende rol hebben waardoor de schrik direct te worden onderworpen aan administratieve boetes deels ongegrond is. Volgens voorgaand artikel worden deze boetes namelijk pas opgelegd indien de kmo geen gevolg geeft aan eerder opgelegde richtlijnen door de toezichthoudende autoriteit na doorlichting van de organisatie.

Een opvallende vaststelling uit het onderzoek is dat de verordening, ondanks de impact die deze heeft op de data van een kmo, enkele niet te onderschatten voordelen voor deze laatste met zich meebrengt. Kmo’s kunnen dus ook positief tegen de nieuwe verordening aankijken. De geharmoniseerde wetgeving zorgt bijvoorbeeld voor minder administratieve lasten en kosten. Dit aangezien kmo’s de toezichthoudende autoriteit niet meer in kennis dienen te stellen, en omdat plaatselijke wetgevingen niet meer afzonderlijk moeten worden uitgepluisd. Dit laatste is vooral van toepassing wanneer de kmo een verwerking verricht in een andere EU-lidstaat dan waar zijn hoofdzetel is gevestigd, of bij doorgiftes van persoonsgegevens binnen de EU. Bij deze doorgiftes heeft de kmo trouwens maar één toezichthoudende autoriteit.

Een tweede belangrijk voordeel is dat kmo’s beter worden beschermd tegen oneerlijke concurrentie aangezien de verordening van toepassing is op de verwerking van Europese persoonsgegevens en zodoende ook van toepassing is voor organisaties buiten Europa die verwerkingen verrichten van dergelijke persoonsgegevens.

Ten slotte kan de kmo de verordening aanwenden om de huidige bedrijfsprocessen te optimaliseren door voor iedere verwerking in kaart te brengen welke data wordt gecapteerd, en zich de vraag te stellen of deze noodzakelijk is voor het bereiken van de vooropgestelde doeleinden van deze verwerking.

Bovenstaande resultaten concluderen deels dat de verordening door een niet zo triviale implementatie wel degelijk een grote impact heeft op de organisatie, maar dat dit anderzijds deels positief kan worden beschouwd.

Om de onderzoeksvraag bijkomend te staven, worden in Sectie 3.1 de noodzakelijke stappen naar GDPR-compliance pragmatisch benaderd. Dit helpt kmo's de reflectie te maken van de wetgeving naar de praktijk, en kan worden aangewend als basis binnen de eigen organisatie. Deze benadering kan zeker als een meerwaarde binnen dit onderzoeksdomein worden beschouwd.

Een bijkomende onderzoeksvraag was artikel 17 van de EU (2016) nader toelichten. Nadien werd de manuele workload in kaart gebracht wanneer 1 % van het klantenbestand van double pass zijn recht tot gegevenswissing zou wensen uit te oefenen. De businesscase verduidelijkte achteraf, op basis van de voordien berekende manuele workload, of een automatisatie van dit proces een snelle ROI kan opleveren. De resultaten hebben uitgewezen dat een snelle ROI (i.e. tussen de 46^{e} en 56^{e} aanvraag, afhankelijk van de benodigde tijd voor het development) kan worden bereikt. Echter zal dit sterk afhankelijk zijn van het aantal aanvragen tot gegevenswissing dat double pass effectief zal binnenkrijgen eens de verordening actief is.

De resultaten van de snelle ROI werden enigszins verwacht, doch is het ondanks de businesscase heel moeilijk in te schatten wanneer deze uiteindelijk bereikt zal worden waardoor bijkomend onderzoek misschien noodzakelijk is.

Afsluitend kan worden geconcludeerd dat dit onderzoek mede heeft geleid tot bijkomende vragen inzake controles bij kmo's. Het is namelijk niet duidelijk in welke vorm dit zal gebeuren, hoe de toezichthoudende autoriteit zich kenbaar zal maken, en op basis van welke criteria bepaalde bedrijven gaan worden gecontroleerd. Bijkomend onderzoek rond deze materie is aangewezen aangezien organisaties niet zomaar eender wie zullen toegang verlenen tot hun data indien er geen duidelijke afspraken hieromtrent zijn. Op het moment van schrijven was volgens een artikel van Data News (2018b) de Privacycommissie zelf nog niet klaar waardoor het voor kmo's nog onduidelijk is hoe deze materie zal worden aangepakt.

A. Onderzoeksvoorstel

Het onderwerp van deze bachelorproef is gebaseerd op een onderzoeksvoorstel dat vooraf werd beoordeeld door de promotor. Dat voorstel is opgenomen in deze bijlage.

Welke impact heeft de General Data Protection Regulation (GDPR) op de data van een kmo?

Onderzoeksvoorstel Bachelorproef

Tom Vandevelde[1]

Samenvatting
Privacy van persoonsgegevens is in de hedendaagse cultuur een heel belangrijk topic geworden. Op 25 mei 2018 zal de General Data Protection Regulation (GDPR) – ook gekend als de Algemene Verordening Gegevensbescherming (AVG) – in werking treden om de opslag, verwerking en verdeling van persoonsgegevens van EU-burgers beter te beschermen. Kmo's zijn zich niet altijd bewust van de impact die de regulatie kan hebben op hun data. Ook zijn ze niet altijd voorbereid op deze veranderingen waardoor ze nood hebben aan richtlijnen doorheen het implementatieproces. Het doel van dit onderzoek is kmo's een soort naslagwerk te bieden door eerst een diepgaande analyse uit te voeren van het onderzoeksdomein en te onderzoeken welke impact GDPR heeft op de data van een kmo. Verder willen we met dit onderzoek een antwoord bieden op een paar belangrijke vragen zoals het recht op gegevenswissing („recht op vergetelheid") – Artikel 17 (Europese Unie [EU], 2016), nagaan welke workload er gepaard gaat wanneer 1 % van het klantenbestand zijn gegevens wil verwijderen en onderzoeken we of automatisatie hier een kostenbesparing kan opleveren. De opgeleverde conclusies moeten kmo's helpen persoonsgebonden data te beheren en te verwerken conform de nieuwe regulatie. In de toekomst kan dit onderzoek bedrijven met internationale projecten helpen hun compliantproces te versnellen bij privacywetgevingen buiten Europa.

Sleutelwoorden
Onderzoeksdomein. Andere (Data Protection) — General Data Protection Regulation — Algemene Verordening Gegevensbescherming — Privacy

Contact: [1] tom.vandevelde.u1913@student.hogent.be;

Inhoudsopgave

1. Introductie

Na vier jaar voorbereiding werd de General Data Protection Regulation (GDPR) op 14 april 2016 door het Europees Parlement goedgekeurd. Na een transitieperiode van twee jaar zal de wetgeving op 25 mei 2018 in voege treden en leiden tot de intrekking van de bestaande Richtlijn 95/46/EG (EU, 1995).

Informatie- en communicatietechnologieën hebben ons leven vergemakkelijkt. Deze diensten verzamelen echter heel veel persoonsgegevens. Deze zijn niet altijd relevant en worden ook niet altijd op een even veilige manier bewaard. Europa wil met de nieuwe regulatie ervoor zorgen dat persoonsgebonden informatie van EU-burgers beter wordt beschermd. De regulatie moet mede zorgen dat EU-burgers weten welke gegevens worden verzameld en voor welk doel ze worden verwerkt. Ze zullen het recht hebben hun gegevens op te vragen, te wijzigen of te verwijderen.

Dit onderzoek komt mede tot stand op vraag van double pass, een bedrijf met als ambitie de jeugdopleiding van voetbalclubs te optimaliseren door middel van audits, adviesverstrekking en een erkend kwaliteitslabel (double pass, 2017).

Echter dienen alle bedrijven die persoonsgebonden data van EU-burgers verwerken GDPR-compliant te zijn, onafhankelijk hun grootte en locatie. Noodzakelijke aanpassingen aan de huidige bedrijfsprocessen inzake bewaring en verwerking van persoonsgegevens zullen sowieso een zware impact hebben op een bedrijf. Grote bedrijven hebben echter meer slagkracht tegenover kmo's, maar beiden zullen zelf verantwoordelijk zijn voor de aanpassingen van de bestaande infrastructuur en de kosten die daarmee gepaard gaan. Bedrijven die niet compliant zijn op 25 mei 2018, riskeren administratieve geldboeten tot 20 miljoen euro of 4 % van de totale wereldwijde jaaromzet in het voorgaande boekjaar, afhankelijk van welke het hoogste is (EU, 2016, art. 83).

Enerzijds is dit onderzoek voor een kmo dus noodzakelijk aangezien de huidige bedrijfsprocessen in kaart moeten worden gebracht, er onderzocht moet worden welke regelge-

vingen reeds voldaan zijn en waar er nog zou moeten worden bijgestuurd. Anderzijds kunnen bedrijven de regulatie ook als een kans beschouwen om deze processen eens kritisch onder de loep te nemen en te optimaliseren.

Het doel van dit onderzoek is GDPR in zijn algemene vorm toe te lichten en een soort naslagwerk te creëren waar kmo's op kunnen terugvallen doorheen het implementatieproces om de huidige data op een vlotte manier te kunnen omzetten conform de nieuwe regulatie.

De centrale vraag in dit onderzoek is na te gaan welke impact GDPR heeft op een kmo en welke aanpassingen aan de huidige processen inzake het verwerken van persoonsgegevens nodig zijn zodoende dat de verwerking van persoonsgegevens binnen een kmo juridisch en conform GDPR is.

Als bijkomende onderzoeksvragen onderzoeken we het recht op gegevenswissing („recht op vergetelheid") – Artikel 17 (EU, 2016), gaan we na welke workload er gepaard gaat wanneer 1 % van het klantenbestand zijn gegevens wil verwijderen en onderzoeken we of automatisatie hier een kostenbesparing kan opleveren.

2. State-of-the-art

GDPR bevat nog veel grijze zones (i.e. zaken die voor interpretatie vatbaar zijn) in de regelgeving. De Commissie voor de bescherming van de persoonlijke levenssfeer (CBPL) – ook gekend als De Privacycommissie – fungeert als onafhankelijk controleorgaan in België. Hun opdracht is erop toezien dat de privacy bij de verwerking van persoonsgegevens wordt geëerbiedigd (Commissie voor de Bescherming van de Persoonlijke Levenssfeer [CBPL], 2017). Deze website is een goede opstart om GDPR beter in kaart te brengen. De publicatie *Bereid je voor in 13 stappen* (CBPL, 2016) verleent toegang tot een goed stappenplan voor bedrijven in het proces naar GDPR-compliance.

De bachelorproef bevat een literatuurstudie die GDPR in zijn algemene vorm zal toelichten. De verordening (EU) 2016/679 (EU, 2016) is hier de beste bron van informatie. Al komen we tot de vaststelling dat Artikel 37, het al dan niet verplicht aanstellen van een Data Protection Officer (DPO) toch nog ruimte tot interpretatie biedt.

3. Methodologie

Het onderzoek zal bestaan uit een grondige literatuurstudie over GDPR met als nadruk de centrale onderzoeksvraag en Artikel 17, het recht op gegevenswissing. Tijdens deze studie zal er steeds afgetoetst worden welke impact het betreffende heeft op de data van een kmo.

In het tweede deel van de bachelorproef richten we ons op de bijkomende onderzoeksvragen. Eerst onderzoeken we a.d.h.v. een simulatie de workload in het bedrijf (procedures, loonkost…) die gepaard gaat wanneer 1 % van het klantenbestand zijn gegevens wil verwijderen. Daarna onderzoeken we de return on investment (ROI) van het al dan niet hebben van een automatisatieproces.

4. Verwachte resultaten

Het resultaat van het onderzoek moet een duidelijk naslagwerk bieden aan een kmo om het implementatieproces naar GDPR-compliance te versnellen. Het moet ook duiding geven over Artikel 17, het recht op gegevenswissing.

De verschillende simulaties i.v.m. de workload bij gegevenswissing zullen de rendabiliteit van een automatisatieproces moeten weerleggen of versterken.

5. Verwachte conclusies

De aangereikte conclusies moeten meer transparantie bieden i.v.m. GDPR-compliance. Alsook zal het de overstap hiernaar en de aanpassingen van de huidige bedrijfsprocessen vergemakkelijken. Aangezien sommige kmo's ook internationale projecten hebben, kan dit onderzoek het compliantproces versnellen bij privacywetgevingen buiten Europa.

Uit de doorgevoerde analyse a.d.h.v. uitgewerkte simulaties zou de rendabiliteit van een automatisatieproces voor gegevenswissing naar voor moeten komen.

Referenties

Commissie voor de Bescherming van de Persoonlijke Levenssfeer. (2016). Bereid je voor in 13 stappen. Verkregen van https://www.privacycommission.be/sites/privacycommission/files/documents/STAPPENPLAN%20NL%20-%20V2.pdf

Commissie voor de Bescherming van de Persoonlijke Levenssfeer. (2017). De Privacycommissie in een notendop. Verkregen van https://www.privacycommission.be/nl/de-privacycommissie-een-notendop

double pass. (2017). Vlaanderen. Verkregen van https://www.doublepass.com/vlaanderen/

Europese Unie. (1995). 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. Verkregen van http://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:31995L0046&from=NL

Europese Unie. (2016). Verordening (EU) 2016/679 van het Europees Parlement en de raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming). Verkregen van http://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32016R0679&from=NL

B. Register verwerkingsactiviteiten

Om alle verwerkingsactiviteiten van een kmo in kaart te brengen, maakt de kmo een register met een overzicht van al deze verwerkingen. In deze bijlage wordt een voorbeeld van zo'n register getoond, gebaseerd op de organisatie double pass.

Records of processing activities - Identification

Based on article 30 of the GDPR

1. Data double pass

Name	double pass		
Street	Baron R. de Vironlaan 130A/ 102	City	Dilbeek
Postal Code	1700	Country	Belgium
Enterprise number	0869.780.984		
Legal form	NV		

2. Data DPO (currently no DPO needed)

Name DPO	/	Intern or extern?	
Email address		Telephone number	

Records of processing activities - Overview

Based on article 30 of the GDPR

Nr	Name processing activity	Date last modifications	Sensitive data?
1	Assessment Belgium	01/05/2018	No
2	HR Salary Payments	03/05/2018	Yes
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			

Record of processing activity

Based on article 30 of the GDPR

Date last modification: 01/05/2018

1. Processing activity

Short description	Assessment Belgium
Role double pass (choose from dropdown)	Processor
Legal base for processing (choose from dropdown) (see article 6 of the GDPR for more information)	Contractual agreement
Which data is collected	GDPR - Overview data.xlsx
User rights	double pass user rights matrix.xlsx
Purpose of the processing	Assessment of clubs

2. Transfer of personal data to third countries or international organisations

Transfers to third countries (outside EU)? (choose from dropdown)	No
If yes, which one?	

3. Data retention

How long is the data stored?	5 years

4. Security

Which security measures are taken? (choose from dropdown)	Information Security Policy Operational Security Privacy by design

5. Data of the Controller

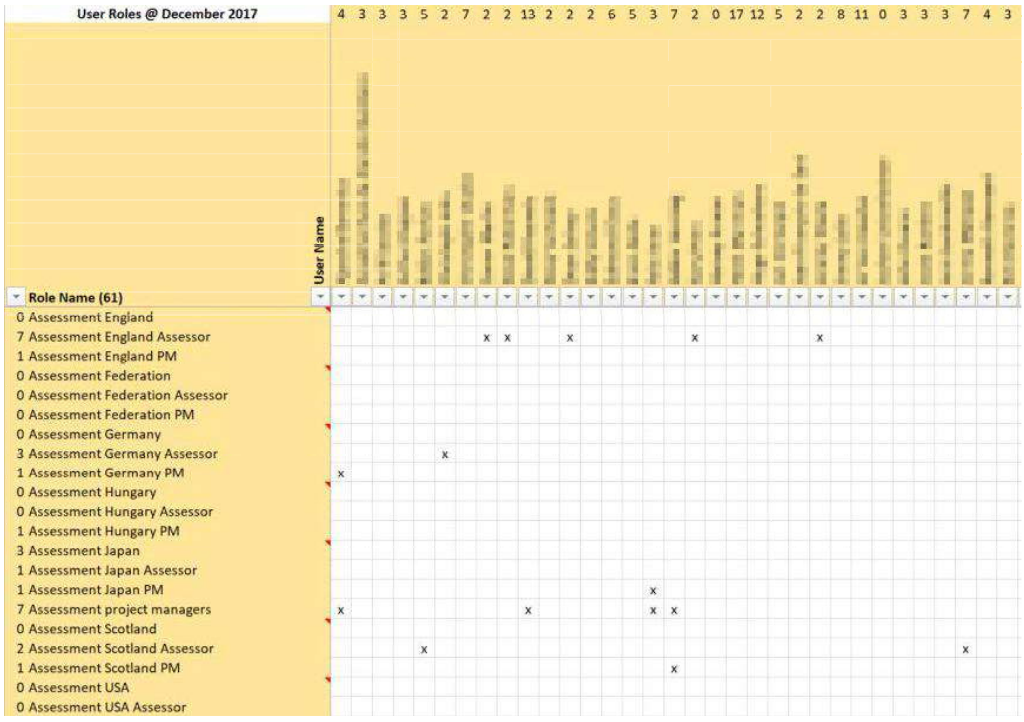
Name	Voetbal Vlaanderen
Street	
Postal Code	
City	
Country	
Enterprise number	
Legal form	

6. Extra information about the processing activity (optional)

Screenshot 1: GDPR - Overview data

Type of data subject	PI
0. Identification	
0.0 Audit Administration	
Assessor	Name
0.1 General Information	
Official Representative of the Club, Academy Manager, Head of Academy Coaching, Contact Person for the Audit	Surname, first name, club telephone number, mobile telephone number, email address
0.2 Academy Teams	
0.3 Senior Teams	
0.4 Leadership at Club Level	
Senior Management Team of the club , Technical Board of the club	function in club, name, years in club

Screenshot 2: double pass user rights matrix



Bibliografie

Commissie voor de Bescherming van de Persoonlijke Levenssfeer. (2016). Bereid je voor in 13 stappen. Verkregen van https://www.privacycommission.be/sites/privacycommission/files/documents/STAPPENPLAN%20NL%20-%20V2.pdf

Commissie voor de Bescherming van de Persoonlijke Levenssfeer. (2018a). De Functionaris voor Gegevensbescherming: een nieuwe figuur! Verkregen van https://www.privacycommission.be/nl/themadossier-functionaris-voor-gegevensbescherming

Commissie voor de Bescherming van de Persoonlijke Levenssfeer. (2018b). Gegevensbeschermingseffectbeoordeling. Verkregen van https://www.privacycommission.be/nl/gegevensbeschermingseffectbeoordeling-0

Commissie voor de Bescherming van de Persoonlijke Levenssfeer. (2018c). Heb ik onder de AVG toestemming nodig om persoonsgegevens van kinderen te verwerken? Verkregen van https://www.privacycommission.be/nl/heb-ik-onder-de-avg-toestemming-nodig-om-persoonsgegevens-van-kinderen-te-verwerken

Commissie voor de Bescherming van de Persoonlijke Levenssfeer. (2018d). Model voor een Register van de verwerkingsactiviteiten. Verkregen van https://www.privacycommission.be/nl/model-voor-een-register-van-de-verwerkingsactiviteiten

Commissie voor de Bescherming van de Persoonlijke Levenssfeer. (2018e). WEGWIJS in de AVG voor KMO's. Verkregen van https://www.privacycommission.be/sites/privacycommission/files/documents/KMO_NL.pdf

Commissie voor de Bescherming van de Persoonlijke Levenssfeer. (z.d.-a). Schema GEB. Verkregen van https://www.privacycommission.be/sites/privacycommission/files/documents/Schema_GEB.pdf

Commissie voor de Bescherming van de Persoonlijke Levenssfeer. (z.d.-b). Schema Register. Verkregen van https://www.privacycommission.be/sites/privacycommission/files/documents/Register%20NL.pdf

Data News. (2017). Hervormde Privacycommissie krijgt slagkracht. Verkregen van http://datanews.knack.be/ict/nieuws/hervormde-privacycommissie-krijgt-slagkracht/article-longread-926811.html

Data News. (2018a). De grote GDPR enquête: Belgische bedrijven dreigen deadline te missen. Verkregen van http://datanews.knack.be/ict/nieuws/de-grote-gdpr-enquete-belgische-bedrijven-dreigen-deadline-te-missen/article-longread-959299.html

Data News. (2018b). Willem Debeuckelaere, hoofd van de Privacycommissie: "We zijn helemaal niet klaar". Verkregen van http://datanews.knack.be/ict/nieuws/willem-debeuckelaere-hoofd-van-de-privacycommissie-we-zijn-helemaal-niet-klaar/article-normal-965253.html

double pass. (2017). Vlaanderen. Verkregen van https://www.doublepass.com/vlaanderen/

double pass. (2018a). External user PASS Online system. Verkregen van https://doublepass.sharepoint.com/:w:/t/IT/EWQrO1HdKHVFt3zOM2xgYb4B8KO5-M23zVFilR7efUsZ6A?e=UA4snr

double pass. (2018b). Notify DPA in case of data breach. Verkregen van https://doublepass.sharepoint.com/:w:/t/IT/EWqS0JP7vidIiVfsZ4IbmGYByVqiWMJelmIcOIJkPTUTkg

double pass. (2018c). Right to be forgotten - Flow charts. Verkregen van https://doublepass.sharepoint.com/:p:/t/IT/EYnqQQvsmNVAmv5Y0S2p63wByS0kXJhqhN57Ngux7YNmnw?e=Na3GWG

European Commission. (2018). An overview of the National Data Protection Authorities. Verkregen van http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612080

European Commission. (z.d.-a). Data transfers outside the EU. Verkregen van https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu_en

Europese Commissie. (2015). Overeenstemming over hervorming van de EU-gegevensbescherming van de Commissie geeft stimulans aan digitale eengemaakte markt. Verkregen van http://europa.eu/rapid/press-release_IP-15-6321_nl.htm

Europese Commissie. (z.d.-b). Wat betekent „grond van gerechtvaardigd belang"? Verkregen van https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-does-grounds-legitimate-interest-mean_nl

Europese Unie. (1995). 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. Verkregen van http://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:31995L0046&from=NL

Europese Unie. (2015). Richtlijn (EU) 2015/1535 van het Europees Parlement en de raad van 9 september 2015 betreffende betreffende een informatieprocedure op het gebied van technische voorschriften en regels betreffende de diensten van de informatiemaatschappij (codificatie). Verkregen van https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32015L1535&from=NL

Europese Unie. (2016). Verordening (EU) 2016/679 van het Europees Parlement en de raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening

gegevensbescherming). Verkregen van http://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32016R0679&from=NL

Europese Unie. (2018). Verordeningen, richtlijnen en andere rechtshandelingen. Verkregen van https://europa.eu/european-union/eu-law/legal-acts_nl