Op weg naar een AVG compliant alumni(bureau)

‘Een praktijkgericht juridisch onderzoek naar de verwerking van persoonsgegevens binnen afdeling Development and Alumni Relations van Tilburg University, in het licht van de Algemene Verordening Gegevensbescherming’

Naam: Abdoullah Hachimi
Studentnummer: 2073108
Opleiding: HBO Rechten
Onderwijsinstelling: Juridische Hogeschool Avans-Fontys

Eerste afstudeerdocent: dhr. mr. B.C.M. Hooijdonk
Tweede afstudeerdocent: mw. M.M.N. Aerts

Afstudeerperiode: September 2017 – Januari 2018
Afstudeerorganisatie: Tilburg University, afdeling DARO
Afstudeermentor: Mw. F.F. Knoet

Tilburg, 9 januari 2018

Understanding Society

Op weg naar een AVG compliant alumni(bureau)

‘Een praktijkgericht juridisch onderzoek naar de verwerking van persoonsgegevens binnen afdeling Development and Alumni Relations van Tilburg University, in het licht van de Algemene Verordening Gegevensbescherming’

Naam: Abdoullah Hachimi
Studentnummer: 2073108
Opleiding: HBO Rechten
Onderwijsinstelling: Juridische Hogeschool Avans-Fontys

Eerste afstudeerdocent: Dhr. mr. B.C.M. Hooijdonk
Tweede afstudeerdocent: Mw. M.M.N. Aerts

Afstudeerperiode: September 2017 – Januari 2018
Afstudeerorganisatie: Tilburg University, afdeling DARO
Afstudeermentor: Mw. F.F. Knoet

Tilburg, 9 januari 2018

Voorwoord

Voor u ligt het door mij geschreven onderzoeksrapport: ‘Op weg naar een AVG compliant alumni(bureau)’. Dit onderzoeksrapport is geschreven ter afronding van mijn opleiding en in opdracht van Tilburg University, afdeling Development and Alumni Relations. In dit onderzoek staan de eisen die de Algemene Verordening Gegevensbescherming stelt aan het verwerken van persoonsgegevens centraal. Deze eisen zijn in dit onderzoek nader beschreven, om vervolgens de werkwijze van afdeling Development and Alumni Relations aan deze eisen te toetsen. Aan de hand van de uitkomst van deze toetsing zijn er conclusies getrokken en aanbevelingen gedaan om een AVG compliant alumnibureau te worden.

Hierbij grijp ik meteen de mogelijkheid om een aantal personen te bedanken voor hun bijdrage aan de uiteindelijke totstandkoming van dit onderzoeksrapport. Allereerst wil ik mijn stagementor mevrouw F.F. Knoet bedanken. Zij heeft mij geholpen door het verstrekken van de nodige informatie, het uitzetten van de lijnen met de juiste personen binnen de organisatie en door altijd beschikbaar te zijn voor het beantwoorden van mijn vragen, ondanks de drukte op kantoor. Daarnaast dank ik mijn stagebegeleiders de heer B. Hooijdonk en mevrouw M. Aerts voor het begeleiden, ondersteunen en geven van feedback bij de uitwerking van dit onderzoeksrapport. Ook wil ik graag alle andere collega’s, die in een andere vorm bijdrage hebben geleverd aan de totstandkoming van dit onderzoeksrapport, bedanken. Tot slot bedank ik de hele afdeling voor het feit dat ik betrokken werd bij de gezellige (alumni)-evenementen die georganiseerd werden door de afdeling.

Ik wens u veel leesplezier toe!

Abdoullah Hachimi

Tilburg, 9 januari 2018

Inhoudsopgave

Samenvatting

Development and Alumni Relations van Tilburg University is de afdeling die zorgt voor het creëren, onderhouden en versterken van de band met de alumni van Tilburg University. Zodra een student afstudeert aan Tilburg University, komt deze persoon in de database van Development and Alumni Relations terecht. Dit betekent dat persoonsgegevens worden verwerkt en de privacyregels hieromtrent in acht moeten worden genomen. Per 25 mei 2018 gaat de Algemene Verordening Gegevensbescherming van kracht. Dit moet volgens de Europese Commissie zorgen voor één uniforme privacywet binnen de gehele Europese Unie. Dit acht de Europese Commissie nodig, omdat geconstateerd is dat persoonsgegevens binnen de Europese Unie op gefragmenteerde wijze worden beschermd. De huidige Privacyrichtlijn heeft, mede dankzij moeilijk interpreteerbare bepalingen, ervoor gezorgd dat de lidstaten verschillende niveaus van bescherming van de rechten en vrijheden bij de verwerking van persoonsgegevens bieden. Daarom gaat per 25 mei 2018 de Algemene Verordening Gegevensbescherming van kracht en is het een goed moment om de verwerking van persoonsgegevens binnen Development and Alumni Relations te onderzoeken. Dit rapport is hiervan het resultaat en beantwoord de volgende centrale vraag: ''Welke aanbevelingen kunnen DARO worden gedaan, na de beoordeling van de werkwijze betreffende het verwerken van persoonsgegevens van oud-studenten aan de hand van de bepalingen uit de AVG, zodat DARO aan de eisen van de AVG kan voldoen door, indien nodig, de werkwijze aan te passen?''

De bepalingen uit de Algemene Verordening Gegevensbescherming, die voor Development and Alumni Relations relevant zijn, worden in het eerste inhoudelijke hoofdstuk beschreven. Het toepassingsbereik en de materiële normen waaraan de verwerking van persoonsgegeven moet voldoen worden als eerst behandelt. De verplichtingen van de verwerkingsverantwoordelijke en de rechten van betrokkene bij de verwerking van persoonsgegevens komen daarna aanbod. Het hoofdstuk eindigt met een korte beschrijving van de taken en bevoegdheden van de autoriteit die toezicht houdt op de verwerkingen van persoonsgegevens binnen Nederland.

Het volgende hoofdstuk brengt de werkwijze van Development and Alumni Relations met betrekking tot het verwerken van persoonsgegevens in kaart en wordt getoetst aan de bepalingen van de verordening. De werkwijze is bestudeerd door de verwerkte persoonsgegevens in de database te onderzoeken op basis van eigen observatie. Daarnaast zijn er enkele interne documenten geraadpleegd en hebben er interviews plaatsgevonden met bepaalde medewerkers, om een completer beeld van de werkwijze te vormen.

Het doel van dit onderzoek voltrekt zich in het laatste hoofdstuk, aangezien hierin de conclusies en aanbevelingen worden gepresenteerd, naar aanleiding van de toetsing van de werkwijze aan de bepalingen van de verordening. De algemene conclusie is dat de medewerkers van Development and Alumni Relations in hoge mate bewust zijn van de privacy van de betrokkenen en goed op weg zijn om te voldoen aan de verordening. Zo zijn de verwerkingen van de persoonsgegevens voor overgrote deel (op drie verwerkingen na) rechtmatig en worden hiervoor de nodige beveiligingsmaatregelen getroffen. Maar ondanks de goede weg moet de werkwijze op bepaalde aspecten worden aangepast. Zo dienen de gegevens over het oud-adres, favoriete professor en medische gegevens van de alumni uit de database gewist te worden, aangezien de verwerking hiervan niet relevant of onrechtmatig is. Daarnaast ontbreekt er een privacy beleid, terwijl dit wel nodig is. Ook worden de betrokkenen niet geïnformeerd over de verwerking van hun persoonsgegevens, maar dit moet wel gebeuren. Tot slot wordt Development and Alumni Relations aanbevolen om bij het informeren van de betrokkenen, hen ook de mogelijkheid te bieden om hun rechten uit te oefenen.

Lijst van afkortingen

AVG	Algemene Verordening Gegevensbescherming
AP	Autoriteit Persoonsgegevens
CvB	College van Bestuur van Tilburg University
DARO	Development and Alumni Relations
EC	Europese Commissie
EU	Europese Unie
LIS	Library and IT Services van Tilburg University
FG	Functionaris Gegevensbescherming
MT	Management Team van Tilburg University
PIA	Privacy Impact Assessment
RE	Raisers Edge (database)
Richtlijn	Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens
TiU	Tilburg University
Wbp	Wet bescherming persoonsgegevens
Werkgroep	De werkgroep binnen Tilburg University die bezig is met het implementeren van de AVG

Hoofdstuk 1 Inleiding

Dit hoofdstuk leidt het onderzoek in. Allereerst wordt er kennis gemaakt met de organisatie. Nadat de organisatie omschreven is, wordt de aanleiding en de daarop gebaseerde centrale vraag met deelvragen gepresenteerd. Vervolgens volgt per deelvraag een verantwoording van de gebruikte onderzoeksmethode en dit hoofdstuk sluit zich af met de leeswijzer.

1.1 De organisatie

Alumnus (meervoud: alumni) is Latijns voor 'leerling' of 'pleegkind'. In het Nederlands is alumnus standaardtaal voor 'oud-student, die aan een bepaalde universiteit is afgestudeerd.[1] Development & Alumni Relations (hierna: DARO) is de afdeling van Tilburg University (hierna: TiU) die in het leven is geroepen om een band te creëren, onderhouden en versterken met oud-studenten (alumni), bedrijven en fondsen. De alumni kunnen een bijdrage leveren bij onderzoeken en onderwijs en kunnen financiële en/of immateriële bijdragen leveren aan projecten van TiU. Zo krijgen alumni de mogelijkheid om in contact te komen en blijven met TiU en oud-studiegenoten.[2] DARO biedt de alumni toegang tot een groot netwerk van kennis en expertise. Zo organiseert DARO evenementen, kunnen de alumni bijvoorbeeld loopbaantrainingen volgen en hebben ze een mogelijkheid tot nascholing. DARO heeft een netwerk met meer dan 65.000 alumni (waarvan 5000 internationale alumni) verspreid over 120 landen. Alumni zijn erg belangrijk voor TiU. Zij zijn de beste ambassadeurs die een kennisinstelling kan wensen en betekenen de link met de maatschappij. Daarnaast zijn alumni de rolmodellen voor huidige studenten. Zo kunnen alumni onder andere komen spreken op de TiU en zo hun persoonlijke verhaal delen met de studenten. Daarnaast kunnen de alumni TiU financieel steunen door donateur te worden.

DARO bestaat uit tien medewerkers en wordt geleid door drs. F.F. Knoet, die managing director is. Hieronder werken de uitvoerende medewerkers die de hoofdwerkzaamheden uitvoeren en contact hebben met de alumni en andere relaties. Deze medewerkers houden zich onder andere bezig met het plannen van activiteiten/evenementen en fondswerving. Naast de uitvoerende medewerkers is er de database manager en het database team. Deze manager heeft de taak om de database te onderhouden, waarin de persoonsgegevens staan die DARO verwerkt. Verder bestaat het database team uit vier ondersteunende studenten, die werkzaamheden uitvoeren met betrekking tot de database.

1.2 Aanleiding

Iedere persoon in Nederland heeft het recht op eerbiediging van de persoonlijke levenssfeer.[3] Dit is een klassiek grondrecht, wat betekent dat de overheid zich niet zomaar mag bemoeien met het privé leven van de burgers. Dit recht is echter geen absoluut recht. Dit betekent dat deze grondrecht volgens het evenredigheidsbeginsel dient te worden afgewogen tegen andere grondrechten.[4] Het recht op de bescherming van de persoonsgegevens, wat onderdeel is van het recht op privacy, heeft de formele wetgever in een wet vastgelegd, namelijk in de Wet bescherming persoonsgegevens (hierna: Wbp). Het rechtmatig verwerken van persoonsgegevens zorgt ervoor dat de privacy van de persoon in kwestie wordt gewaarborgd. Op het moment van schrijven is de Wbp nog van toepassing op het verwerken van persoonsgegevens. Dit is de nationale wetgeving van Nederland op het gebied van privacyrecht, die na implementatie van de Europese Richtlijn 95/46/EG (hierna: de Richtlijn) tot stand is gekomen.[5] Dit gaat echter veranderen.

Per 25 mei 2018 gaat de Algemene Verordening Gegevensbescherming (hierna: AVG) van kracht. De AVG geldt voor de gehele Europese Unie (hierna: EU), dit wil zeggen dat binnen

[1] 'Alumnus, alumni' *www.taaladvies.net* 5 september 2017
[2] Alumni 'Net afgestudeerd?' *www.tilburguniversity.edu.nl*
[3] Artikel 10 lid 1 Grondwet jo. artikel 8 lid 1 Handvest EU jo. artikel 16 lid 1 VWEU.
[4] De Vries & Goudsmit, NJB 2016, p. 3.
[5] 'AVG – nieuwe Europese privacywetgeving' *www.autoriteitpersoonsgegevens.nl* 6 september 2017

de EU één uniforme privacywet geldt voor alle lidstaten. De Richtlijn, de Wbp en andere nationale wetgevingen op het gebied van privacywet komen na toepassing van de AVG te vervallen.[6] Aan de Wbp komt echter geen abrupt eind, want tussen de inwerkingtreding en toepassingsverklaring zit een termijn van twee jaar. Op 24 mei 2016 trad de AVG in werking, maar gaat pas vanaf 25 mei 2018 van kracht.[7] Gedurende de overgangstermijn van twee jaar zijn de Richtlijn en de Wbp nog steeds van toepassing en hebben organisaties de tijd om zich voor te bereiden en te voldoen aan de verscherpte regels uit de AVG.[8]

DARO verwerkt persoonsgegevens en slaat deze gegevens op in een database voor het uitvoeren van hun werkzaamheden. Studenten melden zich via Studielink aan bij TiU. Met de inschrijving via Studielink, kan de student zijn toestemming geven om zijn persoonsgegevens te verstrekken aan DARO. Dit is aan het begin van hun studieloopbaan aan de TiU. Pas aan het einde van hun studieloopbaan komt DARO daadwerkelijk in beeld. DARO krijgt wekelijks op maandag een link van de studentenadministratie waarin de persoonsgegevens staan van de kersverse afgestudeerden van de afgelopen week. Deze persoonsgegevens komen rechtstreeks uit Osiris, de database van de studentenadministratie. De inhoud van de link wordt gefilterd en omgezet tot één bestand waarin persoonsgegevens staan die relevant zijn voor DARO. Zo worden onder andere het administratienummer (hierna: ANR), het mailadres, de faculteit en studierichting opgeslagen in de database van DARO. De afgestudeerde wordt dus direct lid van het alumni netwerk. Het ontvangen van deze persoonsgegevens is een vorm van verwerking aangezien de gegevens in de database van DARO terechtkomen en vervolgens verwerkt en opgeslagen worden.

Naast de wettelijke regels uit de Wbp en de toekomstige AVG, heeft TiU een privacyreglement met betrekking tot de verwerking van persoonsgegevens van relaties. Dit reglement bevat, conform de Wbp, regels voor een zorgvuldige omgang met het verzamelen en verwerken van persoonsgegevens van relaties van TiU. Naast dit reglement, dat ook van toepassing is op DARO, hebben de medewerkers van DARO de beschikking over een korte instructie waarin staat hoe de afdeling dient om te gaan met de persoonsgegevens die DARO verwerkt. Een concreet beleidsstuk ontbreekt binnen DARO, terwijl dit gezien de activiteiten op het gebied van het verwerken van persoonsgegevens noodzakelijk is. In de database worden alle persoonsgegevens opgeslagen en bewaard en deze persoonsgegevens zijn toegankelijk voor alle medewerkers van DARO. Het verwerken van de persoonsgegevens in de database moet onderworpen worden aan de regels uit de AVG, om aan te kunnen tonen of deze verwerkingen rechtmatig zijn.

Daarnaast maakt DARO gebruik van een standaardmodel verwerkersovereenkomst. Dit is een overeenkomst tussen DARO en de partij die de persoonsgegevens voor DARO verwerkt. Met de invoering van de AVG zijn er specifieke punten genoemd die in een verwerkersovereenkomst in ieder geval terug moeten komen. Al met al heeft de invoering van de AVG gevolgen voor de werkwijze van afdeling DARO met betrekking tot het verwerken van persoonsgegevens.

1.3 Centrale vraag en deelvragen

De centrale vraag wordt aan de hand van de aanleiding geformuleerd. De centrale vraag luidt: ‘’Welke aanbevelingen kunnen DARO worden gedaan, na de beoordeling van de werkwijze betreffende het verwerken van persoonsgegevens van oud-studenten aan de hand van de bepalingen uit de AVG, zodat DARO aan de eisen van de AVG kan voldoen door, indien nodig, de werkwijze aan te passen?’’

[6] Artikel 46 Uitvoeringswet AVG
[7] De Vries & Goudsmit, NJB 2016, p. 1.
[8] ‘AVG – nieuwe Europese privacywetgeving: Algemene informatie AVG’ *www.autoriteitpersoonsgegevens.nl* 6 september 2017

Deelvragen

1. Welke juridische kader stelt de AVG aan de verwerking van persoonsgegevens en aan welke relevante bepalingen moet DARO voldoen bij de verwerking van persoonsgegevens?

2. Welke werkwijze past DARO momenteel toe bij het verwerken van persoonsgegevens?

3. In welke mate voldoet de werkwijze van DARO met betrekking tot het verwerken van persoonsgegevens aan de regels van de AVG en op welke punten dient DARO de werkwijze aan te passen?

1.4 Doelstelling

De doelstelling van dit onderzoek is om uiterlijk 9 januari 2018 een onderzoeksrapport op te leveren aan mevrouw F. F. Knoet, Managing Director bij DARO, waarin conclusies worden getrokken en aanbevelingen worden gedaan over het verwerken van persoonsgegevens binnen DARO, naar aanleiding van het analyseren en toetsen van de relevante bepalingen uit de AVG. Met behulp van dit onderzoek weet DARO hoe het ervoor staat en indien nodig, kan het haar werkwijze en privacy beleid aanpassen om per 25 mei 2018 AVG compliant te zijn.

1.5 Verantwoording

De Richtlijn en de Wbp worden in dit onderzoek niet behandelt. Het is immers de AVG die van toepassing is en vanaf mei 2018 van kracht gaat, waardoor de Richtlijn en de Wbp komen te vervallen.[9] Verder worden de interne gegevensverwerkingen achterwege gelaten. De focus ligt op de gegevensverwerkingen van alumni.

Dit onderzoek bestaat uit twee delen, namelijk een juridische deel en een praktijk deel. In het juridische deel wordt het geldend recht geanalyseerd. Deelvraag één betreft een analyse van het recht, aangezien de AVG wordt geanalyseerd. Het praktijk deel betreft de werkwijze van DARO met betrekking tot gegevensverwerking. De antwoorden op deelvraag twee brengen de gegevensverwerking van DARO in de praktijk in beeld. Uiteindelijk wordt de werkwijze in de praktijk getoetst aan het recht, in deelvraag drie.

Onderzoeksmethode

Voor het onderzoek van het recht is de meest voor de hand liggende onderzoeksmethode het rechtsbronnen- en literatuuronderzoek. Rechtsbronnen en relevante literatuur worden geraadpleegd zoals: de AVG, de Uitvoeringswet AVG en Kamerstukken. Voor het praktijk deel kan er gekozen worden uit twee onderzoeksmethoden. Namelijk de kwalitatieve of de kwantitatieve onderzoeksmethode. Voor het praktijk deel is gekozen voor de kwalitatieve onderzoeksmethode. De werkwijze van DARO wordt namelijk geanalyseerd en in kaart gebracht. Dit heeft niet zozeer te maken met cijfermatige gegevens, zoals wel het geval is bij een kwantitatieve onderzoeksmethode. De kwaliteit van de gegevensverwerkingen binnen DARO wordt uiteindelijk getoetst aan de eisen uit de AVG. Uit deze toetsing blijkt uiteindelijk in hoeverre de gegevensverwerkingen voldoen aan de regels uit de AVG.

Deelvraag 1

Deze deelvraag wordt beantwoord door het verrichten van rechtsbronnen- en literatuuronderzoek. Om de AVG goed in kaart te brengen wordt de inhoud hiervan geanalyseerd. De AVG zelf, maar ook andere bronnen worden geraadpleegd, zoals de Uitvoeringswet AVG, literatuur en Kamerstukken. Met deze inhoudsanalyse, worden de relevante bepalingen uit de AVG in kaart gebracht. Deze relevante bepalingen vormen uiteindelijk het toetsingskader van de AVG. Dit is van essentieel belang aangezien hieraan

[9] Richtlijn 95/46/EG

de werkwijze van DARO zal worden getoetst. Deze vraag wordt beantwoord door eerst in te gaan op de achtergrond van de AVG. Vervolgens worden de bepalingen die relevant en belangrijk zijn voor DARO behandelt. De rechtmatige verwerking van persoonsgegevens wordt als eerst geanalyseerd, als ook de beginselen uit de AVG. Vervolgens volgen de essentiële bepalingen over de verplichtingen van de verwerkingsverantwoordelijke en de rechten van betrokkenen. Niet minder belangrijk zijn de bepalingen omtrent de overeenkomst tussen verwerkingsverantwoordelijke en verwerker. Tot slot kunnen organisaties een sanctie opgelegd krijgen, door de Autoriteit Persoonsgegevens (hierna: AP), indien zij niet voldoen aan de bepalingen van de AVG.

Deelvraag 2
Het beantwoorden van deze deelvraag is nodig om de werkwijze van DARO in kaart te brengen en uiteindelijk aan de AVG te kunnen toetsen. Het antwoord hierop wordt met behulp van casestudy gevonden. De werkwijze met betrekking tot het verwerken van persoonsgegevens binnen DARO wordt namelijk bestudeerd. Wat belangrijk is om in ieder geval in kaart te brengen is: welke persoonsgegevens DARO verwerkt, het doel van deze verwerkingen, op grond van welke grondslag uit de AVG, wie de verantwoordelijke over de verwerkingen is, hoe deze gegevens verzameld worden, waar, hoe en voor hoelang worden deze gegevens bewaard, in hoeverre zorgt DARO voor het waarborgen van de rechten van de betrokkene en worden de betrokkene hierop gewezen? Dit zijn allemaal punten die geanalyseerd worden om de werkwijze van DARO in kaart te brengen. Deze punten worden beantwoord door zelf te observeren en door medewerkers van DARO te interviewen. De Managing Director van afdeling DARO wordt geïnterviewd, zij is immers verantwoordelijk voor het werk dat de medewerkers leveren. Daarnaast wordt de Database Manager geïnterviewd. Hij bezit de kennis en expertise over de inhoud van de database en hoe deze werkt. Ook wordt de Functionaris Gegevensbescherming geïnterviewd, aangezien dit de aangewezen persoon is, binnen TiU, op het moment dat het om de AVG gaat. Naast de interviews, worden ook het beleid, de nieuwe verwerkersovereenkomst en de database bekeken. Uiteindelijk is de werkwijze met betrekking tot het verwerken van persoonsgegevens in kaart gebracht en wordt de werkwijze getoetst aan de bepalingen uit de AVG.

Deelvraag 3
De relevante bepalingen die uit de AVG voortvloeien, vormen het toetsingskader voor het beantwoorden van deze vraag. De bevindingen die voortvloeien uit de vorige deelvraag over de werkwijze van DARO worden getoetst aan de relevante bepalingen uit de AVG. Dit maakt het een essentieel hoofdstuk aangezien de werkwijze wordt getoetst aan het geldend recht. Aan de hand van deze toetsing kunnen conclusies worden gevormd en vervolgens kunnen aanbevelingen worden gedaan met betrekking tot de werkwijze van DARO. De verkregen informatie uit deelvragen één en twee worden als bronnen geraadpleegd en aan elkaar getoetst.

1.6 Leeswijzer
Het onderzoeksrapport is als volgt opgebouwd. In het eerst volgende hoofdstuk worden de relevante bepalingen uit de AVG bestudeerd en beschreven. In het tweede hoofdstuk wordt de werkwijze van DARO in kaart gebracht en deze werkwijze wordt in het derde hoofdstuk getoetst aan de relevante bepalingen uit de AVG. Tot slot wordt het onderzoek afgesloten met een hoofdstuk conclusies en aanbevelingen, waarmee het doel van dit onderzoek zich voltrekt.

Hoofdstuk 2 Analyse van de Algemene Verordening Gegevensbescherming

Dit hoofdstuk staat in het teken van de AVG. Allereerst wordt de voorgeschiedenis van het gegevensbeschermingsrecht en de aanleiding voor de totstandkoming van de AVG besproken. Vervolgens worden de bepalingen die relevant zijn voor DARO geïnventariseerd en in kaart gebracht. Het hoofdstuk wordt afgesloten met een beschrijving van de toezichthoudende autoriteit en de sancties voor het niet naleven van de AVG.

2.1 Voorgeschiedenis en aanleiding AVG

Sinds 1983 is de bescherming van persoonsgegevens van individuen in de Grondwet opgenomen.[10] De Grondwet bevat de opdracht aan de formele wetgever om ter bescherming van de persoonlijke levenssfeer regels te stellen voor het vastleggen en verstrekken van persoonsgegevens. Ook over de rechten die betrokkenen met betrekking tot hun persoonsgegevens hebben bestaat een opdracht vanuit de Grondwet.[11] In 1988 resulteerde dit in een wet, namelijk de Wet persoonsregistratie. De bescherming van persoonsgegevens, is in de loop der jaren steeds meer een Europeesrechtelijke aangelegenheid geworden. In 1981 werd op niveau van de Raad van Europa het Dataprotectieverdrag aangenomen. In dit verdrag werden beginselen opgenomen voor de verwerking van persoonsgegevens, maar gedetailleerde regelgeving ontbrak in dit verdrag.[12]

De volgende stap van de Europese Unie (hierna: EU) was het stellen van regels met betrekking tot de bescherming van persoonsgegevens, onder andere met het oog op het bevorderen van de interne markt.[13] Dit leidde in 1995 tot de eerste Europese richtlijn op het gebied van gegevensbescherming, namelijk de Richtlijn, die gebaseerd is op het Dataprotectieverdrag. Tot op heden is dit de geldende basisrichtlijn voor de bescherming van persoonsgegevens. De Richtlijn werd in 2001 geïmplementeerd in Nederland en resulteerde in de Wbp. In 2008 heeft er een evaluatieonderzoek plaatsgevonden naar de werking van de Wbp. Uit dit onderzoek bleek dat de wet slechts beperkt leeft bij burgers en bedrijven.[14] Door de abstracte formulering bleek het een moeilijk toepasbare wet, waardoor de wet in de praktijk onvoldoende is ingevuld.[15] De conclusie luidde dat de doelstellingen van de Wbp slechts gedeeltelijk gerealiseerd zijn en dat de Wbp beperkt werd nageleefd.[16]

De Europese Commissie (hierna; EC) blijft op het standpunt dat de doelstellingen van de Richtlijn, de werking van de Europese markt en bescherming van de fundamentele rechten en vrijheden van natuurlijke personen waarborgen, nog steeds gelden. Het huidige rechtskader heeft volgens de EC niet kunnen voorkomen dat persoonsgegevens in de EU-lidstaten op gefragmenteerde wijze worden beschermd.[17] Het feit dat de Richtlijn in nationaal recht moest worden omgezet, bracht met zich mee dat de lidstaten verschillende niveaus van bescherming van de rechten en vrijheden bij gegevensverwerking bieden. Het gevolg hiervan is dat de Unieburgers en organisaties. Tot slot constateerde de EC dat de Richtlijn uit een tijd stamt waarin het internet nog nieuw en vol in ontwikkeling was.[18][19]

De wereld is op technologisch gebied constant in ontwikkeling. Dit heeft onder meer als gevolg dat de uitwisseling en verwerking van persoonsgegevens significant is gestegen.

[10] Artikel 10 Grondwet
[11] Artikel 10, tweede en derde lid, Grondwet
[12] *Kamerstukken II* 2011/12, 32 761, nr. 32.
[13] *Kamerstukken II* 2011/12, 32 761, nr. 32.
[14] Kranenborg & Verhey 2011, p. 171
[15] Kranenborg & Verhey 2011, p. 171
[16] *Kamerstukken II* 2011/12, 32 761, nr. 32.
[17] Kranenborg & Verhey 2011, p. 171
[18] *Kamerstukken II* 2011/12, 32 761, nr. 32.
[19] De Jong 2016

Deze stijging brengt nieuwe uitdagingen met zich mee wat betreft het beschermen van deze persoonsgegevens. Deze ontwikkelingen dienen er ook voor te zorgen dat het vrij uitwisselen van persoonsgegevens binnen de EU gemakkelijker wordt en dat deze persoonsgegevens beschermd worden.[2021] De bescherming van persoonsgegevens kan worden gerealiseerd door een krachtig en coherent juridisch kader te stellen dat streng gehandhaafd wordt. Dit kader moet er voor zorgen dat zowel de EU-burger als organisaties en overheidsinstanties meer controle krijgen over persoonsgegevens, wat voor alle partijen leidt tot meer rechtszekerheid en praktische zekerheid.[22]

Om bovenstaande doelen te realiseren heeft de EC gekozen voor het invoeren van een verordening als juridisch instrument. De verordening is in alle lidstaten direct toepasbaar waardoor omzetting hiervan verboden is voor lidstaten.[23] Dit betekent dat de verordening in alle lidstaten van de EU toepasbaar is zonder dat hiervoor nationaal recht ten grondslag dient te liggen. In tegenstelling tot dit omzettingsverbod, dienen lidstaten richtlijnen juist expliciet te implementeren in nationaal recht, waarbij lidstaten vrij zijn om te bepalen in welke vorm en met welke middelen zij de in die richtlijn voorgeschreven doelstellingen gaan bereiken.[24] Met de invoering van een rechtstreeks toepasbare verordening in alle lidstaten tracht de EC de juridische fragmentatie te verminderen en te zorgen voor meer rechtszekerheid, verdere harmonisatie en het creëren van een gelijke speelveld binnen de EU.[25]

2.2 Het toepassingsbereik van de AVG

De AVG strekt tot het beschermen van de grondrechten en de fundamentele vrijheden van natuurlijke personen. In het bijzonder betreft dit de bescherming van de persoonsgegevens van natuurlijke personen, bij verwerking hiervan. Ook strekt de AVG tot het bevorderen van het vrije verkeer van persoonsgegevens binnen de EU.[2627] Tot slot beperkt noch verbied de AVG het vrije verkeer van persoonsgegevens.[28]

Voor het toepassingsbereik van de AVG wordt er onderscheid gemaakt tussen materieel en territoriaal toepassingsgebied. Met materiele toepassingsgebied wordt hetgeen bedoeld waarop de AVG van toepassing is. De AVG is materieelrechtelijk van toepassing op de geheel of gedeeltelijke geautomatiseerde verwerking van persoonsgegevens, die in een bestand zijn opgenomen. Alsmede de verwerking van persoonsgegevens die bestemd zijn om in een bestand te worden opgenomen.[29] Als er over territoriale toepassingsgebied wordt gesproken, gaat het over de vraag wanneer de regels uit de AVG van toepassing zijn.[30] De AVG is territoriaal van toepassing op de gegevensverwerking van alle betrokkene uit de EU, ook al bevindt de verwerkingsverantwoordelijke zich buiten de EU.[3132] Dit betekent dat het territoriaal toepassingsgebied ten opzichte van de Richtlijn is vergroot. Aangezien voorheen de nationale privacywetgeving van een lidstaat, waarin de gegevensverwerkingen plaatsvonden van toepassing was. Dit zorgde voor knelpunten indien de verwerkingen niet binnen de EU, maar elders werden verricht.[33]

---

[20] De Vries & Goudsmit, NJB 2016, p. 8.
[21] Overweging 6 AVG
[22] Overweging 7 AVG
[23] *Kamerstukken II* 2011/12, 32 761, nr. 32.
[24] *Kamerstukken II* 2011/12, 32 761, nr. 32.
[25] *Kamerstukken II* 2011/12, 32 761, nr. 32.
[26] Artikel 1 lid 1 AVG
[27] Artikel 1 lid 2 AVG
[28] Artikel 1 lid 3 AVG
[29] Artikel 2 lid 1 AVG
[30] Zwenne & Mommers, *Tijdschrift voor Compliance* 2016, p. 7.
[31] Engelfriet 2017, p. 14.
[32] Artikel 3 AVG
[33] Zwenne & Mommers, *Tijdschrift voor Compliance* 2016, p. 7.

De begrippen persoonsgegevens, verwerkingen en verwerkingsverantwoordelijke worden hiervoor genoemd en worden nu uitgelegd. Persoonsgegevens zijn alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon; als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van identificator zoals een naam, identificatienummer, locatiegegevens of elementen die kenbaar zijn voor de identiteit van die natuurlijke persoon.[34] De betrokkene is dus de natuurlijke persoon waarvan de persoonsgegevens worden verwerkt. Een verwerking is een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens. Nagenoeg alle handelingen waarbij persoonsgegevens betrokken zijn, vallen dus onder de definitie van verwerken.[35] Tot slot is de verwerkingsverantwoordelijke een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat alleen of samen met anderen, het doel en de middelen voor de verwerking vaststelt.[36] Daarnaast wordt in de AVG gesproken van een verwerkingsverantwoordelijke en verwerker. Deze termen vervangen de termen zoals bekend in de Wbp, dit waren de termen bewerker en verantwoordelijke.[37]

2.3 De rechtmatige verwerking van persoonsgegevens

De verwerking van persoonsgegevens is volgens de AVG rechtmatig indien aan bepaalde voorwaarden en beginselen wordt voldaan. Allereerst wordt er ingegaan op de voorwaarden voor rechtmatige verwerking. Daarna worden de beginselen besproken die de verwerkingsverantwoordelijke in acht moet nemen tijdens het verwerken van persoonsgegevens.

2.3.1 De voorwaarden voor rechtmatige verwerking

In de AVG zijn zes rechtmatigheidsgrondslagen opgesomd waarmee aangetoond kan worden dat de gegevensverwerking rechtmatig is.[38] De verwerking van persoonsgegevens mag uitsluitend op één van deze zes grondslagen worden gebaseerd, om als rechtmatig te kunnen worden gekwalificeerd.[39] Dit zijn de volgende grondslagen:

- Toestemming van betrokkene voor de verwerking van persoonsgegevens;
- Verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij betrokkene partij is;
- Verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting van verwerkingsverantwoordelijke;
- Verwerking is noodzakelijk om de vitale belangen van betrokkene te beschermen;
- Verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang/ uitoefening van openbaar gezag;
- Verwerking is noodzakelijk voor de behartiging van gerechtvaardigde belangen van verwerkingsverantwoordelijke.

Toestemming van betrokkene voor de verwerking van persoonsgegevens[40]

Met toestemming van de betrokkene wordt in de zin van de AVG bedoeld: ''elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende

[34] Artikel 4 sub 1 AVG
[35] Artikel 4 sub 2 AVG
[36] Artikel 4 sub 7 AVG
[37] Zwenne & Mommers, *Tijdschrift voor Compliance* 2016, p. 4.
[38] Artikel 6 lid 1 AVG
[39] Engelfriet 2017, p. 43
[40] Artikel 6 lid 1 sub a AVG

verwerking van persoonsgegevens aanvaardt''.[41] De wilsuiting moet zich uiten in een actieve handeling. Stilzwijgen, het gebruik van reeds aangekruiste vakjes (zogenaamde 'opt-out') of inactiviteit mag dus niet als toestemming van de betrokkene worden aangemerkt.[42] Indien er meerdere verwerkingsactiviteiten met verschillende doeleinden zijn, dan moet de toestemming voor elk afzonderlijke verwerkingsactiviteit worden gegeven. De verwerkingsverantwoordelijke dient aan te kunnen tonen dat de betrokkene zijn toestemming voor de gegevensverwerking heeft gegeven.[43] Ook moet het verzoek om toestemming in een gemakkelijk toegankelijke vorm en in eenvoudige taal gepresenteerd worden.[44] De betrokkene dient altijd zijn toestemming in te kunnen trekken. [45] Het intrekken van de toestemming moet voor de betrokkene net zo eenvoudig zijn als het geven van toestemming. Aan het intrekken van de toestemming mogen geen nadelige gevolgen voor betrokkene kleven.[46]

Verwerking is noodzakelijk voor de uitvoering van een overeenkomst
Deze rechtmatigheidsgrondslag stelt dat de verwerking rechtmatig is indien dit noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is.[47] Het belangrijkste is om de noodzaak van de verwerking van de persoonsgegevens voor de uitvoering van een overeenkomst aan te kunnen tonen. Er is sprake van noodzaak indien de overeenkomst zonder de verwerking van persoonsgegevens, niet of niet goed kan worden nagekomen. Het voornaamste voorbeeld is de noodzaak van een webshop die de persoonsgegevens nodig heeft van een klant om zijn bestelling naar het juiste adres te kunnen versturen. Zonder het adres van de klant, kan de overeenkomst niet volledig of juist worden nagekomen omdat het product niet geleverd kan worden.

Verwerking is noodzakelijk om te voldoen aan wettelijke verplichting[48]
Indien een verwerkingsverantwoordelijke gegevens verwerkt om te voldoen aan een wettelijke plicht dan is dit toegestaan, mits deze verplichting een grondslag heeft in EU of lidstatelijk recht.[49]

Verwerking is noodzakelijk om de vitale belangen van betrokkene te beschermen[50]
Deze verwerkingsgrondslag is alleen toegestaan als de verwerking kennelijk niet op een andere rechtsgrond kan worden gebaseerd.[51] Met verwerking ter bescherming van het vitale belang van betrokkene wordt bedoeld dat de verwerking noodzakelijk is voor het leven van de betrokkene.[52] Voorbeelden zijn gegevensverwerking tijdens humanitaire noodsituaties of verwerkingen bij natuurrampen of door de mens veroorzaakte rampen. Ook het verwerken van persoonsgegevens tijdens en na een ongeval is noodzakelijk voor de vitale belangen van betrokkene.[53]

[41] Artikel 4 onder 11 AVG
[42] Overweging 32 AVG
[43] Engelfriet 2017, p.50.
[44] Artikel 7 lid 2 AVG
[45] Artikel 7 lid 3 AVG
[46] Overweging 42
[47] Artikel 6 lid 1 sub b AVG
[48] Artikel 6 lid 1 sub c AVG
[49] Overweging 45 AVG
[50] Artikel 6 lid 1 sub d AVG
[51] Engelfriet 2017, p. 45.
[52] Engelfriet 2017, p. 44.
[53] Overweging 46 AVG

Verwerking is noodzakelijk ter vervulling van een taak van algemeen belang/openbaar gezag
Voor deze verwerkingsgrondslag geldt ook dat de verwerking grondslag dient te hebben in EU of lidstatelijk recht.[54] Ook de taak van algemeen belang moet gebaseerd zijn op een wettelijke bepaling. Daarnaast moet betreffende wet vaststellen of de verwerkingsverantwoordelijke die is belast met een taak van algemeen belang dan wel met een taak in het kader van de uitoefening van het openbaar gezag, een overheidsinstantie, een andere publiekrechtelijke persoon of een privaatrechtelijke persoon is die uit algemeen belang gegevens verwerkt.[55] Het algemeen belang geldt dus niet alleen voor overheidsinstanties.[56]

Verwerking is noodzakelijk voor de behartiging van gerechtvaardigde belangen van verwerkingsverantwoordelijke
De noodzakelijke verwerking voor de behartiging van de gerechtvaardigde belangen van verwerkingsverantwoordelijke is rechtmatig. [57] De belangen of de grondrechten en fundamentele vrijheden van de betrokkene, die tot bescherming van persoonsgegevens dienen mogen niet zwaarder wegen dan de gerechtvaardigde belangen van de verwerkingsverantwoordelijke. Daarbij moet rekening worden gehouden met de redelijke verwachtingen van de betrokkene op basis van de verhouding met verwerkingsverantwoordelijke. ''Een dergelijk gerechtvaardigd belang kan bijvoorbeeld aanwezig zijn wanneer sprake is van een relevante en passende verhouding tussen de betrokkene en verwerkingsverantwoordelijke, in situaties waarin de betrokkene een klant is of in dienst is van verwerkingsverantwoordelijke''.[58] Noemenswaardig is het feit dat uitgesloten is dat overheidsinstanties in het kader van de uitoefening van hun taken een verwerking van persoonsgegevens baseren op gerechtvaardigd belang.[59] Verwerking van persoonsgegevens door de overheid moeten dus in beginsel gebaseerd kunnen worden op minstens een van de hierboven genoemde voorwaarden.

2.3.2. Beginselen van gegevensbescherming
De beschermingsbeginselen dienen door de verwerkingsverantwoordelijke, bij de verwerking van persoonsgegevens, nageleefd te worden en deze naleving dient verwerkingsverantwoordelijke aan te kunnen tonen.[60] De bewijslast voor het aantonen van deze naleving is uitdrukkelijk bij de verwerkingsverantwoordelijke gelegd.[61] De AVG kent zes beschermingsbeginselen die al deels bekend waren onder de Wbp.[62]
De beginselen zijn:

- Beginsel van rechtmatigheid, behoorlijkheid en transparantie;
- Beginsel van doelbinding;
- Beginsel van minimale gegevensverwerking;
- Beginsel van juistheid;
- Beginsel van opslagbeperking;
- Beginsel van integriteit en vertrouwelijkheid.

Beginsel van rechtmatigheid, behoorlijkheid en transparantie
Iedere verwerking van persoonsgegevens dient rechtmatig, behoorlijk en transparant te geschieden.[63] Voor betrokkene moet het duidelijk zijn dat zijn persoonsgegevens worden

[54] Artikel 6 lid 1 sub e AVG
[55] Overweging 45 AVG
[56] Engelfriet 2017, p. 45
[57] Artikel 6 lid 1 sub f AVG
[58] Overweging 47 AVG
[59] Overweging 47 AVG
[60] Artikel 5 lid 2 AVG
[61] De Jong 2016.
[62] Artikel 9 Wbp
[63] Artikel 5 lid 1 sub a AVG

verzameld en verwerkt en de manier waarop dit gebeurt.[64] In het kader van het transparantiebeginsel dient de informatie en communicatie over de gegevensverwerking voor de betrokkenen eenvoudig toegankelijk en begrijpelijk zijn. Tevens moet deze informatie in duidelijke en eenvoudige taal worden gepresenteerd aan betrokkene. Het komt er op neer dat de betrokkene in kennis moeten worden gesteld over de verwerking van persoonsgegevens, de reden voor de verwerking, wat de risico's zijn van deze verwerking en welke rechten de betrokkenen hebben en hoe zij deze rechten kunnen uitoefenen ten aanzien van de gegevensverwerking. [65]

Beginsel van doelbinding
De persoonsgegevens moeten voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen niet verder verwerkt worden voor andere doeleinden dan waarvoor de gegevens in eerste instantie verzameld werden.[66] De verwerkingsverantwoordelijke dient aantoonbaar te maken en vast te leggen voor welk specifiek doel de gegevensverwerking plaatsvindt, voordat de verwerking daadwerkelijk plaatsvindt.[67] Dit kan bijvoorbeeld in de vorm van een schriftelijke of elektronische omschrijving. Daarnaast dient de verwerkingsverantwoordelijke de specifieke en gerechtvaardigde doeleinden op te nemen in het verwerkingsregister.

Beginsel van minimale gegevensverwerking
De verwerking van persoonsgegevens moet toereikend, relevant zijn en beperkt worden tot wat noodzakelijk is voor de doeleinden.[68] Dit houdt in dat er niet meer persoonsgegevens dan nodig worden verwerkt om het doel van de gegevensverwerking te bereiken.[69] De verwerkingsverantwoordelijke moet nagaan of het doel van de verwerking niet op een alternatieve of minder privacy-belastende wijze kan plaatsvinden en of de verwerking daadwerkelijk noodzakelijk is. Het gevaar voor betrokkene ontstaat zodra dataminimalisatie leidt tot een onjuist of onvolledig beeld van de betrokkene. Dit moet door de verwerkingsverantwoordelijke voorkomen worden.[70]

Beginsel van juistheid
De persoonsgegevens dienen juist en actueel te zijn, om een onjuist beeld van betrokkene te voorkomen. [71] Indien er gegevens onjuist zijn dient de verwerkingsverantwoordelijke onmiddellijk de gegevens te actualiseren of te verwijderen. Het is de plicht van de verwerkingsverantwoordelijke om actief zorg te dragen voor de juistheid van de persoonsgegevens en niet af te wachten tot betrokkene klaagt over onjuiste of achterhaalde gegevens. Onjuiste gegevens kunnen namelijk leiden tot nadelige gevolgen voor betrokkene.[72]

Beginsel van opslagbeperking
De persoonsgegevens moeten in een zodanige vorm worden bewaard dat de betrokkene niet langer identificeerbaar is dan noodzakelijk voor de doeleinden van de gegevensverwerking.[73] De opslagperiode moet dus tot een strikt minimum worden beperkt om onnodige verdere verwerking te voorkomen. Dit kan de verwerkingsverantwoordelijke

[64] Engelfriet 2017, p. 39.
[65] Overweging 39 AVG
[66] Artikel 5 lid 1 sub b AVG
[67] Engelfriet 2017, p. 40.
[68] Artikel 5 lid 1 sub c AVG
[69] Engelfriet 2017, p. 41.
[70] Engelfriet 2017, p.41.
[71] Artikel 5 lid 1 sub d AVG
[72] Engelfriet 2017, p. 41.
[73] Artikel 5 lid 1 sub e AVG

doen door termijnen vast te stellen voor het vernietigen van persoonsgegevens of voor een periodieke toetsing hiervan.[74]

Beginsel van integriteit en vertrouwelijkheid
Dit beginsel ziet er op toe dat de verwerkingsverantwoordelijke technische en organisatorische beveiligingsmaatregelen treft zodat de beveiliging van persoonsgegevens gewaarborgd blijft. De verwerking zelf en het systeem waarin de verwerking plaatsvindt, moet integer en vertrouwelijk zijn. Dit betekent dat de verwerkingsverantwoordelijke de betrokkene moet kunnen garanderen dat de persoonsgegevens beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen (on)opzettelijk verlies, vernietiging of beschadiging door passende technische en organisatorische maatregelen te treffen. [75]

2.4 Categorie persoonsgegevens
De AVG maakt onderscheid tussen twee categorieën persoonsgegevens. De AVG kent namelijk een onderscheid tussen gewone persoonsgegevens, zoals naam en geboortedatum, en bijzondere persoonsgegevens. De bijzondere persoonsgegevens worden expliciet benoemd in de AVG.[76] Bijzondere persoonsgegevens zijn gegevens over:

- ras of etnische afkomst;
- politieke opvattingen;
- religieuze of levensbeschouwelijke overtuigingen;
- het lidmaatschap van een vakbond;
- verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon;
- gegevens over gezondheid;
- gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid

Op de verwerking van deze bijzondere persoonsgegevens rust een algeheel verbod. [77] Verwerking van deze categorie persoonsgegevens is enkel toegestaan in enkele uitzonderlijke gevallen. In de AVG worden tien grondslagen genoemd ter rechtvaardiging van de verwerking van bijzondere persoonsgegevens. [78] Deze grondslagen zijn geen op zichzelf staande rechtmatige grondslagen voor de verwerking van persoonsgegevens. Hiervoor dient de verwerkingsverantwoordelijke terug te grijpen op de rechtmatigheidsgrondslagen die de AVG kent.[79] De volgende grondslagen rechtvaardigen het verwerken van bijzondere persoonsgegevens:

- de betrokkene heeft uitdrukkelijke toestemming gegeven voor de verwerking;
- de verwerking is noodzakelijk voor de uitvoering van verplichtingen van verwerkingsverantwoordelijke op het gebied van het arbeids- en socialezekerheidsrecht;
- de verwerking is noodzakelijk ter bescherming van de vitale belangen van betrokkene indien de betrokkene fysiek of juridisch niet in staat is zijn toestemming te geven;
- de verwerking wordt verricht door een instantie zonder winstoogmerk die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is;
- de verwerking heeft betrekking op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt;
- de verwerking is noodzakelijk voor de instelling, uitoefening of onderbouwing van een rechtsvordering of wanneer gerechten handelen in het kader van hun bevoegdheid;

[74] Overweging 39 AVG
[75] Artikel 5 lid 1 sub f AVG
[76] Artikel 9 AVG
[77] Artikel 9 lid 1 AVG
[78] Artikel 9 lid 2 AVG
[79] Artikel 6 AVG

- de verwerking is noodzakelijk om redenen van zwaarwegend algemeen belang, op grond van Unierecht of lidstatelijk recht;
- de verwerking is noodzakelijk voor arbeidskundige en medische aangelegenheden;
- de verwerking is noodzakelijk om redenen van algemeen belang op het gebied van de volksgezondheid;
- de verwerking is noodzakelijk met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden overeenkomstig artikel 89 lid 1.

2.5 De verplichtingen van de verwerkingsverantwoordelijke

De AVG legt de verwerkingsverantwoordelijke enkele verplichtingen op. De verwerkingsverantwoordelijke dient deze verplichtingen na te leven en dit aan te tonen.

2.5.1. De verantwoordingsplicht

De verantwoordingsplicht is nieuw onder de AVG. De AVG staat in het teken van verantwoording van de compliance aan de AVG.[80] Deze plicht houdt in dat de verwerkingsverantwoordelijke moet kunnen verantwoorden op welke manier hij gegevens verwerkt en of dit in lijn is met de AVG.[81] Dit kan de verwerkingsverantwoordelijke doen door passende en effectieve maatregelen te treffen.[82] Deze passende en effectieve maatregelen dienen in een privacy beleid opgenomen te worden, dat door de verwerkingsverantwoordelijke opgesteld moet worden.[83] Dit privacy beleid dient de verwerkingsverantwoordelijke in de praktijk na te leven en de werking hiervan kan worden geëvalueerd en indien nodig geactualiseerd.[84] Indien verwerkingsverantwoordelijke niet kan aantonen dat de verwerkingen voldoen aan de AVG, dan wordt automatisch de AVG overtreden en kan er sanctie volgen.[85]

2.5.2 Registerplicht

De registerplicht houdt verband met de verantwoordingsplicht. De verwerkingsverantwoordelijke dient een register bij te houden met daarin alle verwerkingen van persoonsgegevens. Ook de verwerkingsactiviteiten van de verwerker, die onder de hoede valt van de verwerkingsverantwoordelijke dienen geregistreerd te worden in het register.[86] Het register dient in schriftelijke (elektronische) vorm worden opgesteld.[87] Het register bestaat uit de volgende gegevens [88]:

- de naam en contactgegevens van (gezamenlijke) verwerkingsverantwoordelijke(n), indien van toepassing de vertegenwoordiger van verwerkingsverantwoordelijke en van de functionaris gegevensbescherming (hierna: FG);
- de verwerkingsdoeleinden;
- een beschrijving van de categorieën van betrokkenen en van de categorieën persoonsgegevens;
- de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt;
- de doorgiften van persoonsgegevens aan derde landen of internationale organisatie, indien van toepassing;
- de beoogde opslagtermijnen waarbinnen de gegevens moeten worden gewist;
- een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen

[80] Zwenne & Mommers, *Tijdschrift voor Compliance* 2016, p. 11.
[81] Artikel 5 lid 2 AVG
[82] Artikel 24 lid 1 AVG
[83] Artikel 24 lid 2 AVG
[84] Artikel 24 lid 1 AVG
[85] Engelfriet 2017, p. 43.
[86] Artikel 30 lid 1 AVG
[87] Artikel 30 lid 3 AVG
[88] Artikel 30 lid 1 AVG

Niet iedere verwerkingsverantwoordelijke is verplicht een register bij te houden. Indien een organisatie of onderneming minder dan 250 medewerkers in dienst heeft, hoeft de verwerkingsverantwoordelijke geen register bij te houden. Zoals vele uitzonderingen kent ook deze uitzondering een tenzij-bepaling. Organisaties of ondernemingen met minder dan 250 medewerkers dienen namelijk wel een register bij te houden indien de verwerking een risico is voor de rechten en vrijheden van de betrokkene, de verwerking niet incidenteel plaatsvindt, het een verwerking van bijzondere persoonsgegevens betreft of de verwerking verband houdt met strafrechtelijke veroordelingen en feiten.[89] Met dit register kan de verwerkingsverantwoordelijke naleving van de AVG aantonen. Indien dit register ontbreekt, impliceert dit dat de AVG niet wordt nageleefd en niet wordt voldaan aan de AVG.[90]

2.5.3 Beveiliging van persoonsgegevens

''Rekening houdend met de aard, de omvang, de context en het doel van de verwerking, alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van betrokkenen, treft de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd''.[91] Passend wil zeggen dat er evenredigheid moet zijn tussen de privacy risico's die de verwerking met zich meebrengt en de getroffen beveiligingsmaatregelen. Hoe gevoeliger en bedreigender de gegevensverwerking is voor de privacy van de betrokkene, des te zwaarder zijn de eisen aan de beveiliging van deze persoonsgegevens.[92] De organisatorische maatregelen zien toe op de inrichting van de organisatie en van het verwerken van persoonsgegevens, zodat de medewerkers bewust worden van de beveiliging van persoonsgegevens. Voorbeelden zijn het opstellen van beleid, toekenning en deling van verantwoordelijkheden en bevoegdheden, trainingen en protocollen. De passende technische maatregelen zien toe op het optimaliseren van het technische systeem waarin de gegevens zijn opgeslagen. Voorbeelden zijn toegangscontroles en het maken van een back-up. Daarnaast dient de verwerkingsverantwoordelijke rekening te houden met de stand van de techniek en de uitvoeringskosten van desbetreffende maatregelen.[93]

De passende maatregelen kunnen onder meer bereikt worden door het volgende toe te passen en na te leven:

- pseudonimiseren en versleutelen van persoonsgegevens;
- op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en dienste te garanderen;
- bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig herstellen;
- op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.[94]

Privacy by design en privacy by default

De AVG verplicht de verwerkingsverantwoordelijke om passende en organisatorische maatregelen te treffen bij zowel de bepaling van de verwerkingsmiddelen (''privacy by design'') als bij de verwerking zelf (''privacy by default'') ter bescherming van de persoonsgegevens.[95]

Privacy by design verplicht de verantwoordelijke om bij het opzetten en ontwikkelen van een informatiesysteem, de bescherming van persoonsgegevens hoog in het vaandel te plaatsen

[89] Artikel 30 lid 5 AVG
[90] Overweging 82 AVG
[91] Artikel 32 lid 1 AVG
[92] Kranenborg & Verhey 2011, p. 99.
[93] Artikel 32 lid 1 AVG
[94] Artikel 32 lid 2 AVG
[95] Artikel 25 lid 1 AVG

en direct mee te nemen.[96] Dit houdt in dat vooraf duidelijk moet zijn dat de persoonsgegevens die verwerkt worden echt noodzakelijk zijn voor het beoogde doel. Indien blijkt dat dit noodzakelijk is, moet worden nagegaan of de gegevens niet geanonimiseerd, gepseudonimiseerd of op een andere manier versleuteld kunnen worden. Dit zorgt er voor dat niet voor iedereen die met de gegevens werkt, direct duidelijk is om welke persoon het gaat en dat bij een mogelijke datalek de gevolgen beperkt blijven. Vervolgens moet de toegang tot de gegevens beperkt worden tot de personen die daadwerkelijk de persoonsgegevens nodig hebben. Dit betreft zowel de fysieke als technische toegang tot de gegevens. Daarnaast mogen de gegevens niet langer bewaard worden dan nodig is voor het doel en moeten de gegevens vernietigd worden zodra ze niet meer relevant zijn. Tot slot moeten de betrokkene hun rechten eenvoudig uit kunnen oefenen.[97]

Bij ‘’privacy by default’’ gaat het er om dat de standaardinstellingen van het informatiesysteem zo privacy vriendelijk mogelijk moeten zijn. Het informatiesysteem moet standaard de minst mogelijke inbreuk op de privacy van betrokkene betekenen. In plaats van standaard openbaar, moet de betrokkene de keuze krijgen om de gegevens breder te delen. Dit ziet vooral toe op sociale media platformen. [98]

2.5.4 Data Protection Impact Assessment (PIA)

De verwerkingsverantwoordelijke dient bij een verwerking die een hoog risico meebrengt voor de rechten en vrijheden van betrokkene, een gegevensbeschermingseffectbeoordeling uit te voeren om het effect van de beoogde verwerkingsactiviteiten op de bescherming van de persoonsgegevens in kaart te brengen.[99] De verwerkingsverantwoordelijke kan hiermee de oorsprong, aard, het specifieke karakter en de ernst van het risico evalueren. Het resultaat dat hieruit volgt dient meegenomen te worden bij de bepaling van de passende maatregelen die genomen moeten worden om aan de verordening te voldoen.[100] Indien de organisatie een FG heeft aangewezen, wordt zijn advies ingewonnen bij het uitvoeren van de beoordeling.[101]

In volgende gevallen is een beoordeling verplicht:

- systematische en uitvoerige evaluatie van persoonlijke aspecten; daarbij inbegrepen profilering;
- het verwerken van bijzondere of strafrechtelijke persoonsgegevens op grote schaal;
- systematisch en op grote schaal volgen van openbare ruimten (zoals camerabewaking)[102]

Naast bovenstaande criteria, zal de toezichthoudende autoriteit een lijst publiceren van het verwerkingen van persoonsgegevens waarvoor een PIA wel of niet vereist is.[103]

Indien een verwerkingsverantwoordelijke een PIA uitvoert, dan dient de verantwoordelijke het volgende in ieder geval in de beoordeling op te nemen:

- een systematische beschrijving van de beoogde verwerkingen en verwerkingsdoeleinden, waaronder de gerechtvaardigde belangen die worden behartigd;
- een beoordeling van de noodzaak en evenredigheid van de verwerkingen met betrekking tot de doeleinden;

[96] Overweging 78
[97] A. Roosendaal ‘Privacy by Design als spil voor AVG-compliance’, *www.privacycompany.eu* 28 april 2017
[98] D. The ‘Privacy by Default: wat houdt het in en welke impact kan het hebben op een organisatie?’, *www.privacycompany.eu* 6 december 2016
[99] Artikel 35 lid 1 AVG
[100] Overweging 84 AVG
[101] Artikel 35 lid 2 AVG
[102] Artikel 35 lid 3 AVG
[103] De Vries & Goudsmit, NJB 2016, p. 9.

- een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen;
- de beoogde maatregelen om de risico's aan te pakken, waaronder waarborgen, veiligheidsmaatregelen en mechanisme om de bescherming van persoonsgegevens te garanderen en om aan te tonen dat aan deze verordening is voldaan.[104]

Mocht uit de beoordeling blijken dat de verwerking een hoog risico oplevert voor de rechten en vrijheden van betrokkenen, dan raadpleegt de verwerkingsverantwoordelijke voorafgaand aan de verwerking de toezichthoudende autoriteit, in Nederland is dit de Autoriteit Persoonsgegevens (hierna: AP).[105] De AP onderzoekt de verwerking en tot het moment dat het advies is gegeven, naar aanleiding van desbetreffende onderzoek, mag de verwerkingsverantwoordelijke deze verwerking niet plaats laten vinden.[106][107]

2.5.5 Meldplicht datalekken

Indien een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, informeert de verwerkingsverantwoordelijke de toezichthoudende autoriteit hierover, uiterlijk binnen 72 uur nadat het lek is ontdekt.[108] Sinds 1 januari 2016 gold deze meldplicht datalekken al onder de Wbp, maar nu dus ook onder de AVG. De AP meldt dat sinds de invoering van de meldplicht, het aantal meldingen zijn gestegen. In de eerste negen maanden van 2017 was er een verdubbeling van het aantal meldingen en dat waren er 7436. Dit komt neer op 30 meldingen gemiddeld per dag.[109]

Een datalek betekent dat er persoonsgegevens zijn vernietigd of verloren, gewijzigd, verstrekt of toegankelijk gemaakt op een manier die onrechtmatig is.[110] De persoonsgegevens komen, eenvoudig gezegd, terecht waar ze niet horen te komen.[111] Als het onwaarschijnlijk is dat een inbreuk een risico voor de betrokkene mee brengt hoeft er geen melding te worden gedaan, maar deze inbreuken moeten wel gedocumenteerd worden. Net als de meldplicht met betrekking tot datalekken, is het intern documenteren van alle datalekken een nieuwe verplichting in de AVG.

De melding aan de AP is vormvrij maar dient in ieder geval de volgende onderdelen te bevatten: de aard van de inbreuk, de contactgegevens van de FG, de waarschijnlijke gevolgen van de inbreuk en de maatregelen die verwerkingsverantwoordelijke neemt.[112] Mocht het datalek bij de verwerker plaatsvinden, dan informeert de verwerker de verwerkingsverantwoordelijke hierover zonder onredelijke vertraging.[113] In het geval het datalek een groot risico voor de betrokkene betekent, dan dient de betrokkene hierover door de verwerkingsverantwoordelijke te worden geïnformeerd.[114] Maar heeft de verwerkingsverantwoordelijke passende maatregelen getroffen en toegepast op de persoonsgegevens waarop de inbreuk betrekking heeft of maatregelen hebben genomen waardoor het hoge risico waarschijnlijk niet zal intreden, dan hoeft de mededeling aan de betrokkene niet te worden gedaan. Ook als de mededeling een onevenredige inspanning zou betekenen voor verwerkingsverantwoordelijke, behoeft de inbreuk geen melding aan de

[104] Artikel 35 lid 7 AVG
[105] Artikel 36 lid 1 AVG
[106] Artikel 36 lid 2 AVG
[107] Engelfriet 2017, p. 154.
[108] Artikel 33 AVG
[109] *'Meldingen van datalekken in jaar tijd verdubbeld'*, NU.nl, *www.nu.nl* 28 december 2017
[110] Artikel 4 onder 12 AVG
[111] Engelfriet 2017, p. 142.
[112] Artikel 33 lid 5 AVG
[113] Artikel 33 lid 2 AVG
[114] Artikel 34 lid 1 AVG

betrokkene.[115] Tot slot kan de AP, de verwerkingsverantwoordelijke verplichten om een melding te doen aan de betrokkene indien blijkt dat dit wel nodig is, maar nog niet is gedaan.[116]

2.5.6 De verwerkersovereenkomst

De verwerkingsverantwoordelijke die met een andere partij overeenkomt dat deze partij namens hem persoonsgegevens verwerkt, moet hiervoor een verwerkersovereenkomst sluiten.[117] Het inschakelen van een verwerker mag door verwerkingsverantwoordelijke alleen geschieden indien de verwerker afdoende garanties biedt met betrekking tot het toepassen van technische en organisatorische beveiligingsmaatregelen.[118] De AVG benoemt enkele specifieke bepalingen die zeker terug moeten komen in de verwerkersovereenkomst.[119] Dit zijn onder andere:

- de doeleinden van de verwerkingen;
- de categorie persoonsgegevens waarop de verwerkingen betrekking hebben;
- de betrokkene waarop de verwerkingen betrekking hebben;
- de passende organisatorische en technische beveiligingsmaatregelen;
- dat de persoonsgegevens uitsluitend worden verwerkt op basis van schriftelijke instructies van de verwerkingsverantwoordelijke;
- dat de verwerker waarborgt dat de tot het verwerken van de persoonsgegevens gemachtigde personen zich ertoe hebben verbonden vertrouwelijkheid in acht te nemen of via een wettelijke verplichting van vertrouwelijkheid zijn gebonden;
- dat de verwerker alle overeenkomstig artikel 32 vereiste maatregelen neemt;
- dat aan de voorwaarden voor het in dienst nemen van een andere verwerker wordt voldaan, op grond van de leden 2 en 4 van artikel 28 AVG;
- dat de verwerker de verwerkingsverantwoordelijke bijstand verleent bij het vervullen van diens plicht om verzoeken om uitoefening van de rechten van betrokkene te beantwoorden;
- dat de verwerker de verwerkingsverantwoordelijke bijstand verleent bij het vervullen van diens verplichtingen;
- dat de verwerkingsverantwoordelijke audits mag uitvoeren bij verwerker;
- dat na afloop de gegevens vernietigd of terug geleverd worden aan de verwerkingsverantwoordelijke.[120]

Tot slot mag de verwerker niet zonder voorafgaande schriftelijke toestemming van verwerkingsverantwoordelijke een andere verwerker in dienst nemen.[121]

2.6 De rechten van betrokkene bij verwerking persoonsgegevens

Volgens de EC is onder andere de versterking en nadere omschrijving van de rechten van betrokkenen een vereiste voor een doeltreffende bescherming van persoonsgegevens.[122] De betrokkene had onder de Richtlijn en de Wbp al enkele rechten die hij ten opzichte van de verwerkingsverantwoordelijke kon uitoefenen met betrekking tot de verwerking van zijn persoonsgegevens.[123] De AVG kent de betrokkenen (nieuwe) verregaande rechten toe.

2.6.1 Algemeen

De informatie omtrent de rechten van betrokkene, met betrekking tot de gegevensverwerking moet in een beknopte, transparante, begrijpelijke en gemakkelijk

[115] Artikel 34 lid 3 AVG
[116] Artikel 34 lid 4 AVG
[117] Overweging 81 AVG
[118] Artikel 28 lid 1 AVG
[119] Artikel 28 lid 3 AVG
[120] Artikel 28 lid 3 AVG
[121] Artikel 28 lid 2 AVG
[122] Overweging 11 AVG
[123] De Vries & Goudsmit, NJB 2016, p. 6.

toegankelijke vorm en in duidelijke en eenvoudige taal te worden gepresenteerd door de verwerkingsverantwoordelijke. Kort gezegd houdt dit in dat de informatie niet in lange verhalen verstopt mag zijn, eenvoudig te raadplegen moet zijn en niet in juridisch of technisch jargon mag worden gepresenteerd.[124] Deze informatie dient de betrokkene schriftelijk of via elektronische wegen te ontvangen. Ook kan deze informatie mondeling verstrekt worden indien de betrokkene hierom verzoekt en mits de identiteit van betrokkene is bewezen.[125]

Een verzoek van betrokkene om informatie of een beroep op zijn rechten, mag de verwerkingsverantwoordelijke weigeren, indien de verzoeken kennelijk ongegrond of buitensporig zijn, bijvoorbeeld vanwege hun repetitieve karakter. Deze buitensporigheid moet door de verwerkingsverantwoordelijke worden aangetoond. De verwerkingsverantwoordelijke mag in principe geen kosten in rekening brengen voor het verzoek, maar kan dit wel doen in het licht van de administratieve kosten voor het inwilligen van dit verzoek. De verwerkingsverantwoordelijke heeft vanaf het moment dat het verzoek binnen is gekomen, een maand de tijd om hier een reactie op te geven. Daarbij dient de verantwoordelijke, de betrokkene te informeren over de mogelijkheid om een klacht in te dienen bij de AP en beroep in te stellen bij de rechter.[126]

Indien de verwerkingsverantwoordelijke de persoonsgegevens van de betrokkene, niet via de betrokkene heeft verkregen, dient de verwerkingsverantwoordelijke de betrokkene over de gegevensverwerkingen en zijn rechten te informeren.[127] De verwerkingsverantwoordelijke dient de betrokkene de volgende informatie te verschaffen:

- de identiteit en contactgegevens van de verwerkingsverantwoordelijke;
- de contactgegevens van de functionaris voor gegevensbescherming;
- de rechtsgrond en verwerkingsdoeleinden waarvoor de persoonsgegevens zijn bestemd;
- de betrokken categorie van persoonsgegevens;
- de ontvangers of categorie ontvangers van de persoonsgegevens;
- de periode gedurende welke de persoonsgegevens zullen worden opgeslagen, of indien dat niet mogelijk is, de criteria om die termijn te bepalen;
- de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, indien de verwerking op artikel 6 lid 1 sub f gebaseerd is;
- dat de betrokkene het recht heeft de verwerkingsverantwoordelijke te verzoeken om inzage van en rectificatie of wissing van persoonsgegevens of om beperking van de hem betreffende verwerking, alsmede het recht tegen verwerking van bezwaar te maken en het recht op gegevensoverdraagbaarheid;
- wanneer de verwerking op artikel 6 lid 1 sub a of artikel 9 lid 2 sub a is gebaseerd, dat de betrokkene het recht heeft de toestemming te allen tijde in te trekken, zonder dat dit afbreuk doet aan de rechtmatigheid van de verwerking op basis van de toestemming vóór de intrekking daarvan;
- dat de betrokkene het recht heeft een klacht in te dienen bij een toezichthoudende autoriteit;
- de bron waar de persoonsgegevens vandaan komen;[128]

[124] Engelfriet, 2017 p. 70.
[125] Artikel 12 lid 1 AVG
[126] Artikel 12 lid 4 AVG
[127] Artikel 14 lid 1 AVG
[128] Artikel 14 lid 1 jo. lid 2 AVG

De informatie, zoals hiervoor beschreven, dient de verwerkingsverantwoordelijke te verstrekken:

- binnen een redelijke termijn, maar uiterlijk binnen één maand na de verkrijging van de persoonsgegevens, afhankelijk van de concrete omstandigheden waarin de persoonsgegevens worden verwerkt;
- indien de persoonsgegevens zullen worden gebruikt voor communicatie met de betrokkene, uiterlijk op het moment van het eerste contact met de betrokkene; of
- indien verstrekking van de gegevens aan een andere ontvanger wordt overwogen, uiterlijk op het tijdstip waarop de persoonsgegevens voor het eerst worden verstrekt.[129]

2.6.2 Recht op inzage

De betrokkene komt het recht toe informatie te verkrijgen van de verwerkingsverantwoordelijke over of en welke persoonsgegevens van hem worden verwerkt. Mochten zijn persoonsgegevens verwerkt worden, dan mag de betrokkene deze dus inzien.[130] De betrokkene kan hierom verzoeken en kan de persoonsgegevens inzien middels bijvoorbeeld een kopie van zijn persoonsgegevens. Het doel van dit recht is om invulling te kunnen geven aan de andere rechten van de betrokkene, namelijk het recht op rectificatie, vergetelheid en op beperking van de verwerking.[131] Zonder dat de betrokkene weet welke persoonsgegevens van hem worden verwerkt, kan hij niet om rectificatie van gegevens verzoeken. De verwerkingsverantwoordelijke dient een kopie van de verwerkte persoonsgegevens aan de betrokkene te verstrekken.[132]

Indien de betrokkene verzoekt om inzage, dan heeft hij recht op de volgende informatie:

- de verwerkingsdoeleinden;
- de categorieën van persoonsgegevens;
- de ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt;
- de opslagperiode van de persoonsgegevens;
- de rechten van de betrokkene met betrekking tot de verwerking van persoonsgegevens;
- het klachtenrecht van de betrokkene bij de AP;
- alle beschikbare informatie van de bron waar de persoonsgegevens zijn verzameld, indien de gegevens niet bij de betrokkene zelf zijn verzameld;
- de genomen passende waarborgen, indien de gegevens worden verstrekt aan derde landen.[133]

2.6.3 Recht op rectificatie

De betrokkene heeft het recht op rectificatie van onjuiste of onvolledige persoonsgegevens van hem.[134] Dit betekent dat de betrokkene kan verzoeken om onjuiste of onvolledige persoonsgegevens aan te vullen en te corrigeren. De verwerkingsverantwoordelijke heeft de plicht alle mogelijke maatregelen te treffen om onjuiste persoonsgegevens te corrigeren of aan te vullen.[135]

2.6.4 Recht op gegevenswissing

De betrokkene heeft het recht op vergetelheid.[136] Dit betekent dat de betrokkene kan verzoeken om volledige verwijdering/vernietiging van zijn persoonsgegevens bij de organisatie die zijn persoonsgegevens verwerkt. Dit is een uitwerking van de beginselen van

[129] Artikel 14 lid 3 AVG
[130] Artikel 15 lid 1 AVG
[131] Engelfriet 2017, p. 85.
[132] Artikel 15 lid 3 AVG
[133] Artikel 15 lid 1 jo lid 2 AVG
[134] Artikel 16 AVG
[135] Overweging 39 AVG
[136] Artikel 17 lid 1 AVG

juistheid en opslagbeperking, door de betrokkene het recht te geven om overbodige persoonsgegevens gewist te krijgen.[137] Indien de verwerkingsverantwoordelijke het verzoek op gegevenswissing van betrokkene honoreert en de gegevens wist, dient hij hierover ook andere verwerkingsverantwoordelijke op de hoogte te stellen.[138]

De verwerkingsverantwoordelijke dient zonder onredelijke vertraging gehoor te geven aan het verzoek en uiterlijk binnen één maand indien:

- de persoonsgegevens niet langer nodig zijn voor de doeleinden;
- de betrokkene zijn toestemming intrekt en er geen andere grondslag is waarop de verwerking berust;
- de betrokkene bezwaar maakt tegen de verwerking en er geen prevalerende dwingende gerechtvaardigde gronden zijn voor de verwerking;
- de persoonsgegevens onrechtmatig zijn verwerkt;
- de persoonsgegevens op grond van EU recht of lidstatelijk recht gewist dienen te worden;
- de persoonsgegevens in verband met een aanbod van diensten van de informatiemaatschappij zijn verzameld.[139]

2.6.5 Recht op beperking van de verwerking

Het recht op beperking van de verwerking is een nieuw recht dat de betrokkene toekomt.[140] Dit houdt in dat betrokkene een (tijdelijk) slot op de persoonsgegevens aanlegt, tot er een bepaald probleem of bezwaar is behandeld.[141] De betrokkene kan een beroep doen op dit recht in vier specifieke situaties, namelijk wanneer:

- de juistheid van de gegevens door betrokkene wordt betwist;
- de verwerking van gegevens onrechtmatig is maar de betrokkene geen wissing van gegevens wenst;
- de verwerkingsverantwoordelijke de gegevens niet meer nodig heeft maar de betrokkene wel, voor de instelling, uitoefening of onderbouwing van een rechtsgrond;
- de betrokkene bezwaar heeft gemaakt tegen de verwerking en in afwachting op de vraag of de gerechtvaardigde gronden van de verwerkingsverantwoordelijke zwaarder wegen dan die van betrokkene.[142]

Indien de verwerking wordt beperkt, betekent dit dat de verwerkingsverantwoordelijke de verwerking moet staken. De opslag van de gegevens is wel toegestaan, aangezien het mogelijk is dat een beperking wordt opgeheven.[143] Daarnaast kan de beperking gepasseerd worden door toestemming van betrokkene of indien de verwerkingsverantwoordelijke de gegevens nodig heeft om een rechtsvordering in te stellen tegen betrokkene, ter bescherming van de rechten van een ander of om gewichtige redenen van algemeen belang.[144] Tot slot dient de verwerkingsverantwoordelijke de betrokkene te informeren over het voornemen om de beperking op te heffen.[145] Dit voornemen kan bijvoorbeeld bestaan in het geval uit onderzoek blijkt dat het bezwaar ongegrond is. De betrokkene kan dan alsnog een klacht indienen bij de AP of de gang naar de rechter bewandelen.[146]

[137] Engelfriet 2017, p. 91.
[138] Artikel 17 lid 2 AVG
[139] Artikel 17 lid 1 AVG
[140] Artikel 18 AVG
[141] Engelfriet 2017, p. 95.
[142] Artikel 18 lid 1 AVG
[143] Engelfriet 2017, p. 97.
[144] Artikel 18 lid 2 AVG
[145] Artikel 18 lid 3 AVG
[146] Engelfriet 2017, p. 98.

2.6.6 Recht op overdraagbaarheid van gegevens
Het recht op overdraagbaarheid van gegevens is ook een nieuw recht onder de AVG.[147] Dit recht houdt in dat de betrokkene, een kopie van zijn persoonsgegevens kan eisen, die de betrokkene bij een andere dienstverlener kan gebruiken. De verwerkingsverantwoordelijke mag de betrokkene niet verhinderen bij de uitoefening van dit recht.[148] Daarnaast kan de betrokkene vragen om de persoonsgegevens door te laten zenden door de ene verwerkingsverantwoordelijke naar de andere, indien dit technisch mogelijk is.[149]

Het recht op overdraagbaarheid van gegevens komt de betrokkene echter alleen toe indien de verwerking berust op toestemming of een overeenkomst of de verwerking via geautomatiseerde procedés wordt verricht.[150] Mocht de betrokkene gebruik maken van dit recht, dan kan hij daarna nog steeds gebruik maken van het recht op gegevenswissing.[151] Tot slot mag een uitoefening van dit recht geen afbreuk doen aan de rechten en vrijheden van anderen.[152]

2.6.7 Recht van bezwaar
De betrokkene heeft het recht om bezwaar te maken tegen verwerking van zijn persoonsgegevens op basis van algemeen belang of een eigen gerechtvaardigd belang van verwerkingsverantwoordelijke.[153] Indien de betrokkene dit recht uitoefent, dient de verwerkingsverantwoordelijke de verwerkingen te staken, tenzij hij dwingende gerechtvaardigde gronden voor de verwerking aanvoert.

Indien een verwerkingsverantwoordelijke zich beroept op de grondslag ‘’taak van algemeen belang’’ of ‘’gerechtvaardigd eigen belang’’, dient er een belangenafweging te worden gemaakt ten opzichte van de privacy van de betrokkene. Vaak is deze belangenafweging abstract, maar kan de betrokkene verlangen om zijn specifieke geval mee te nemen in de belangenafweging. Dit is de reden dat het recht van bezwaar is ingevoerd aangezien dit recht bedoeld is om in verband met persoonlijke gronden een heroverweging af te kunnen dwingen. Het bezwaar moet dus gebaseerd zijn op de specifieke situatie die betrekking heeft op betrokkene en kan niet volstaan met algemene of principiële bezwaren.[154]

2.7 De Autoriteit Persoonsgegevens
Iedere lidstaat is verplicht om één leidende toezichthoudende autoriteit in te stellen.[155][156] Deze autoriteit moet bij wet worden aangesteld en dient volledig onafhankelijk te (kunnen) opereren.[157][158] De toezichthouder moet toezien op de naleving van de bepalingen uit de AVG, wat er op neer komt dat de toezichthouder de bescherming van de grondrechten van burgers ten aanzien van de verwerking van hun persoonsgegevens moet controleren.[159] De toezichthouder in Nederland is de Autoriteit Persoonsgegevens (hierna: AP).[160]

[147] Artikel 20 AVG
[148] Engelfriet 2017, p. 99.
[149] Artikel 20 lid 2 AVG
[150] Artikel 20 lid 1 sub a en b AVG
[151] Artikel 20 lid 3 AVG
[152] Artikel 20 lid 4 AVG
[153] Artikel 21 lid 1 AVG
[154] Engelfriet 2017, p. 103.
[155] Artikel 51 AVG
[156] De Vries & Goudsmit, NJB 2016, p. 5.
[157] Artikel 54 AVG
[158] Artikel 52 AVG
[159] Engelfriet 2017, p. 209.
[160] Artikel 6 Uitvoeringswet AVG

2.7.1 Taken en bevoegdheden AP

De toezichthouders krijgen vanuit de AVG bepaalde taken en bevoegdheden. Het doel van het instellen van een toezichthouder is het toezien op de naleving en handhaving van de AVG. Dit is de hoofdtaak van de AP. De afzonderlijke taken die de AP heeft, zijn uitgebreid beschreven in de AVG.[161] De taken die het meest naar voren komen zijn het creëren van bewustwording bij verwerkingsverantwoordelijke, verwerker en betrokkene door te adviseren en informeren. Daarnaast stelt de AP standaard bepalingen met betrekking tot verwerkersovereenkomsten en gegevensbeschermings-effectbeoordelingen vast. Tot slot dient er melding gemaakt worden van (sommige) datalekken bij de AP die zij zullen behandelen en registreren.

De AP heeft de volgende drie bevoegdheden:

- de onderzoeksbevoegdheden;
- de maatregelenbevoegdheden en;
- adviesbevoegdheden.

In het kader van de onderzoeksbevoegdheden heeft de AP de bevoegdheid om informatie in te winnen, controles en toetsingen te verrichten en toegang te verkrijgen tot alle bedrijfsruimten en informatie van de verwerkingsverantwoordelijke en verwerkers.[162] De maatregelenbevoegdheden betreffen onder andere het waarschuwen en berispen van verwerkingsverantwoordelijke, de verwerkingsverantwoordelijke gelasten de verzoeken van betrokkene in te willigen, de verwerkingen in overeenstemming met de AVG te brengen en een datalek aan betrokkene mede te delen. Ook kan het een verwerkingsbeperking of rectificering en/of wissing van gegevens opleggen aan verwerkingsverantwoordelijke. Daarnaast kan het een administratieve geldboete opleggen.[163] Tot slot heeft de AP adviesbevoegdheden.[164]

2.7.2 Aansprakelijkheid en sancties bij niet naleving AVG

Indien een verwerkingsverantwoordelijke of verwerker de verplichtingen uit de AVG niet nakomt, pleegt hij een onrechtmatige daad jegens de betrokkene.[165] Indien de betrokkene, als gevolg van niet nakoming van de verplichtingen, schade lijdt, ontvangt hij hiervoor een billijke schadevergoeding.[166] De feitelijke schade is in de praktijk lastig te kwantificeren, daarom ontvangt de betrokkene een billijke schadevergoeding.[167] De verwerkingsverantwoordelijke en verwerker zijn allebei hoofdelijk aansprakelijk. De betrokkene kan dus bij zowel verwerkingsverantwoordelijke als verwerker de geleden schade verhalen. Alleen als er sprake is van overmacht, kan de verwerkingsverantwoordelijke of verwerker aansprakelijkheid ontlopen.[168] De verwerker is aansprakelijk voor alle schade indien een specifieke verplichting dat tot hem strekt (zoals het inschakelen van een sub-verwerker zonder toestemming) of het niet op orde hebben van de beveiliging, maar ook het negeren van instructies schade veroorzaakt.[169]

De AP kan de verwerkingsverantwoordelijke sancties opleggen, zoals een administratieve geldboete.[170] De voorwaarden voor het opleggen van een geldboete zijn dat de sancties doeltreffend, evenredig en afschrikkend moet zijn. De sanctie moet zorgen voor het naleven van de AVG en moet er voor zorgen dat andere afschrikken en het gewenste gedrag gaan

[161] Artikel 57 AVG
[162] Artikel 58 lid 1 AVG
[163] Artikel 58 lid 2 AVG
[164] Artikel 58 lid 3 AVG
[165] Artikel 79 lid 2 AVG
[166] Artikel 36 lid 2 Uitvoeringswet AVG
[167] Engelfriet 2017, p. 278.
[168] Artikel 82 lid 3 jo. 6:75 BW
[169] Engelfriet 2017, p. 279.
[170] Artikel 83 AVG

vertonen. Daarnaast mag de sanctie niet disproportioneel zijn gezien de overtreding.[171] De AP kan aan zowel ondernemingen, overheden als particulieren geldboetes opleggen. Deze geldboete wordt aangemerkt als bestuurlijke boete in de zin van de Algemene wet bestuursrecht.[172]

De AVG kent twee categorieën overtredingen.

- Categorie één betreft de administratief georiënteerde verplichtingen en categorie twee betreft de principiële verplichtingen, zoals het verkrijgen van toestemming.[173][174] In geval van een overtreding van categorie één kan de AP een administratieve geldboete van maximaal 10.000.000,- of 2% van de wereldwijde omzet opleggen.
- In geval van een overtreding van categorie twee kan de AP een administratieve geldboete van maximaal 20.000.000,- of 4% van de wereldwijde omzet opleggen. De bepaling van de 4% van de wereldwijze omzet wordt toegepast indien het bedrag van dit percentage hoger is dan het maximale boetebedrag. Naast deze administratieve geldboete mag de AP ook een last onder bestuursdwang opleggen.[175]

De hoogte van de sanctie wordt uiteindelijk bepaald aan de hand van de omstandigheden van het concrete geval. De AP dient gemotiveerd, aan de hand van een door hun opgesteld boetebeleid, aan te kunnen geven hoe zij aan het bedrag is gekomen.[176] Doorslaggevende factoren bij het bepalen van de hoogte van het boetebedrag zijn de aard, ernst en duur van de inbreuk. Aan de hand van het aantal getroffen betrokkenen en door hen geleden schade wordt dit bepaald.[177] Andere factoren die onder andere meegewogen worden, zijn de opzettelijke of nalatige aard van de inbreuk, de genomen maatregelen ter beperking van de geleden schade en eerdere relevante inbreuken.[178]

[171] Engelfriet 2017, p. 281.
[172] Engelfriet 2017, p. 282.
[173] Engelfriet 2017, p. 285.
[174] Artikel 83 lid 4 jo lid 5 AVG
[175] Artikel 17 Uitvoeringswet
[176] Engelfriet 2017, p. 282.
[177] Engelfriet 2017, p. 283.
[178] Artikel 83 lid 2 AVG

Hoofdstuk 3 Werkwijze DARO

De werkwijze van DARO met betrekking tot het verwerken van persoonsgegevens wordt hier besproken. Allereerst wordt ingegaan op het type persoonsgegevens dat DARO verwerkt, als ook de reden en het doel van deze gegevensverwerkingen. Verschillende medewerkers van DARO zijn geïnterviewd. Hiermee is duidelijk geworden waarom en hoe de persoonsgegevens worden verwerkt. Daarnaast is de database waarin de persoonsgegevens verwerkt worden, geraadpleegd om precies te achterhalen welke gegevens hierin zijn opgenomen. Ook heeft er een documentanalyse plaatsgevonden. Het summiere interne privacybeleid van DARO zelf is bekeken, het inventarisatieschema waarin de verwerkingen van DARO staan en de verwerkersovereenkomst waarvan DARO gebruik maakt. Tot slot is het algemene privacybeleid van de TiU geraadpleegd omdat dit ook van toepassing is op de medewerkers van DARO.

3.1 Toepasselijkheid AVG

Voordat er in wordt gegaan op de voorwaarden waaraan DARO moet voldoen bij de gegevensverwerkingen, moet de AVG wel van toepassing zijn op DARO. Voor het toepassingsgebied wordt er onderscheid gemaakt tussen het materieelrechtelijke en territoriale toepassingsgebied, zoals in vorige hoofdstuk is beschreven. Het materieelrechtelijke criterium is dat er persoonsgegevens (geautomatiseerd) worden verwerkt. DARO verwerkt persoonsgegevens door deze in haar database te verwerken. Het territoriale criterium is dat de verwerkingsverantwoordelijke binnen de EU gevestigd is en/of dat de gegevensverwerkingen een EU-burger (be)treffen. DARO is gevestigd in Nederland en er worden persoonsgegevens van onder andere EU-burgers verwerkt. Dus de gegevensverwerkingen binnen DARO voldoen aan zowel de materieelrechtelijke en territoriale criteria en daarom is de AVG van toepassing op de gegevensverwerkingen.

3.2 De gegevensverwerkingen binnen DARO

3.2.1. De grondslag en doeleinden van gegevensverwerkingen

Zoals uit vorig hoofdstuk blijkt mogen persoonsgegevens alleen met een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel worden verwerkt. Binnen DARO worden er verschillende persoonsgegevens van betrokkene verwerkt. Voordat er wordt ingegaan op de type persoonsgegevens die DARO verwerkt, worden eerst de grondslagen en doeleinden waarop de gegevensverwerking berust besproken.

De gegevensverwerkingen door DARO moeten een welbepaald en uitdrukkelijk omschreven doel hebben. Het doel dat DARO, met behulp van de gestructureerde gegevensverwerking nastreeft, is: ‘’een zodanige band realiseren, onderhouden en versterken met alumni, bedrijven en fondsen overeenkomstig de missie en ambities van onze universiteit, zodat die partijen de universiteit financieel dan wel in natura willen ondersteunen om de universiteit te laten excelleren en promoten’’.[179] Dit doel heeft twee aspecten, enerzijds bestaat het namelijk uit alumni-relatiebeheer en anderzijds uit fondsenwerving. De gegevensverwerkingen zijn een onmiskenbare schakel voor DARO bij het realiseren van dit doel.

DARO baseert de gegevensverwerkingen op drie verschillende grondslagen, namelijk op: toestemming van betrokkene, gerechtvaardigd belang van verwerkingsverantwoordelijke en vitaal belang van betrokkene.[180] De verwerkingen die DARO baseert op de toestemming van betrokkene, betreft de verwerking van de bankgegevens en donatiegegevens van betrokkene. Maar ook bij het updaten van persoonsgegevens, met behulp van het ‘’update your details’’ formulier op de website, wordt de verwerking gebaseerd op toestemming van betrokkene.

[179] Bijlage A
[180] Bijlage A

De bankgegevens verkrijgt DARO op twee verschillende manieren. Uit het interview met de Managing Director blijkt dat alumni hun bankgegevens namelijk per telefoon of machtigingskaart kunnen doorgeven.[181] DARO kan hiermee donaties incasseren voor het universiteitsfonds. Met het invullen van de machtigingskaart geven alumni hun toestemming voor het incasseren van het bedrag maar ook voor het verwerken van de bankgegevens. Zonder de bankgegevens kan DARO de donaties namelijk niet incasseren. Daarnaast kunnen alumni hun bankgegevens per telefoon doorgeven. Het doorgeven van de bankgegevens per telefoon kan als actieve handeling worden gezien en verder kan er worden aangesloten bij bovenstaande redenering. Na het telefoongesprek wordt er verslag gemaakt van het gesprek en dit wordt in de database opgeslagen. Vervolgens wordt er een bevestigingsmail gestuurd waarin wordt aangegeven welke bankgegevens betrokkene heeft doorgegeven en de mededeling dat hiervan een bedrag wordt geïncasseerd. DARO verwerkt ook het land waar de alumni woont in de database. Deze verwerking wordt gebaseerd op de grondslag vitaal belang. De reden voor de keuze om dit te baseren op vitaal belang is niet duidelijk. De grondslag 'vitaal belang van betrokkene' ziet namelijk toe op het leven van een betrokkene en betreft bijvoorbeeld verwerkingen tijdens humanitaire noodsituaties etc. Alle andere gegevensverwerkingen worden gebaseerd op een gerechtvaardigd belang van DARO.

Wat tot verwarring leidt is het feit dat onderaan het formulier 'update your details', dat door betrokkene kan worden ingevuld, een toestemmingsvakje is opgenomen.[182] De betrokkene dient dus toestemming te geven voor het verwerken van zijn persoonsgegevens, naar aanleiding van een wijziging van zijn persoonsgegevens. Dit impliceert dat de eerdere verwerking van zijn persoonsgegevens ook op toestemming van betrokkene is gebaseerd, terwijl hierboven al is beschreven dat dit gebaseerd is op gerechtvaardigd belang. Dit leidt tot verwarring.

3.2.2 Plaats van de gegevensverwerkingen

DARO verwerkt de persoonsgegevens van betrokkene in hun database genaamd Raisers Edge (hierna: RE). Alle persoonsgegevens waarover DARO beschikt staan opgeslagen in RE. Indien er een verzoek om wijziging van persoonsgegevens door betrokkene wordt ingediend, wordt deze wijziging uiteraard in RE doorgevoerd. Aan de hand van de data in de database kan DARO gerichte mails sturen naar alumni en andere relaties. Voor het versturen van uitnodigingen voor evenementen, nieuwsbrieven en andere informatieve mails maakt DARO gebruik van het programma Mailplus. Met dit programma kan DARO, aan de hand van de geleverde data uit RE, zogenaamde mailinglijsten opstellen en versturen. Deze lijsten bevatten alle mailadressen en andere persoonsgegevens van alumni of relaties die DARO per mail wenst te bereiken. Bijvoorbeeld om deze groep uit te nodigen voor een specifieke evenement. In het geval DARO alle alumni van de Rechtenfaculteit wilt bereiken, worden de alumni die hieraan zijn afgestudeerd gefilterd. Vervolgens wordt deze groep in de mailinglijst ge-upload aan de hand van hun mailadressen. DARO stelt dan een mailing op die toegespitst is op deze specifieke groep en deze mail wordt dan automatisch verstuurd vanuit de mailinglijst. Deze mailinglijsten worden in het programma zelf ook opgeslagen, inclusief de persoonsgegevens. De mailinglijsten kunnen zo geprogrammeerd worden dat er na verloop van tijd of na afloop van een evenement, automatisch follow-ups worden verstuurd. Dit is de reden voor het opslaan van de mailinglijsten door Mailplus. De persoonsgegevens binnen DARO worden dus op twee plaatsen verwerkt, maar uitgangspunt voor de gegevensverwerkingen is RE. Alleen in RE worden de persoonsgegevens wekelijks verwerkt en worden wijzigingen van persoonsgegevens doorgevoerd. De verwerkingen in Mailplus vinden alleen plaats ten behoeve van het versturen van mails naar alumni.

[181] Bijlage F

[182] Alumni 'Update your details' *www.tilburguniversity.edu.nl*

3.3. De categorie persoonsgegevens binnen DARO

De AVG maakt onderscheid tussen twee categorieën persoonsgegevens. Het onderscheid bestaat uit enerzijds algemene persoonsgegevens en anderzijds bijzondere persoonsgegevens. De betrokkene van wie DARO persoonsgegevens verwerkt zijn die van alumni, corporate relaties en non-corporate relaties. De groep van alumni is het grootst, wat automatisch betekent dat RE voor het overgrote deel bestaat uit persoonsgegevens van alumni. RE bevat ongeveer 60-duizend alumni. Daarnaast verwerkt DARO gegevens van corporate relaties. Dit zijn personen die niet afgestudeerd zijn aan TiU, maar wel via een andere insteek een relatie hebben met de Universiteit, bijvoorbeeld de commissaris van de Koning. Tot slot worden ook gegevens van non-corporate relaties verwerkt in de database. Dit zijn personen die geen directe relatie hebben met DARO. Voorbeelden hiervan zijn studenten die doneren aan het universiteitsfonds of crowdfunding donateurs. De persoonsgegevens van al deze personen heeft DARO nodig om het doel van DARO te kunnen realiseren. In onderstaande tabel zijn de persoonsgegevens die DARO verwerkt verkort opgenomen en gecategoriseerd:

Gegevensverwerkingen DARO	
Naam	Voorletter, roepnaam, doopnaam, tussenvoegsels en achternaam
Geboorte	Geboortedatum, geboorteplaats en geboorteland
Adres	Straatnaam, postcode, woonplaats, land en oud-adres
Geslacht	Man of vrouw
Contactgegevens	Huis telefoonnummer, mobiele telefoonnummer, bedrijfstelefoonnummer en emailadres
Studie	Afgeronde studie(s)
Donaties	Bankrekeningen, donatiegegevens zowel oude als huidige en donatiegegevens in natura
Contactinformatie	Persoonlijke contactinformatie, contactvoorkeuren, aanmeldingen en aanwezigheid TiU events
Werkgever	Werkgeversinformatie
Relaties	Bijv. vader-zoon

Uit het inventarisatieschema blijkt dat DARO alleen algemene persoonsgegevens verwerkt. Het verwerken van bijzondere persoonsgegevens blijkt niet uit het inventarisatieschema.[183] Maar het is niet uitgesloten dat dit (on)bewust toch gebeurt. Zo komt het voor dat er door betrokkenen tijdens de belcampagne wordt aangegeven dat ze (ernstig) ziek zijn. Soms geven betrokkenen specifiek aan, aan welke ziekte ze lijden. De belstudenten hebben de opdracht om een korte notitie te maken van het telefoongesprek, tijdens de belcampagne. Hierin worden dergelijke persoonlijke omstandigheden van betrokkenen ook opgenomen. De notitie wordt opgeslagen in de database bij de gegevens van desbetreffende persoon. Het doel hiervan is om later te kunnen achterhalen waarom desbetreffende persoon niet wilt doneren of gecontacteerd wilt worden. Zo wordt voorkomen dat de persoon in toekomstige belcampagnes of andere correspondentie wordt gecontacteerd, terwijl hij heeft aangegeven dit niet meer te willen. Hierdoor worden er dus gegevens over de gezondheidsstatus van desbetreffende persoon verwerkt.[184] Dit betekent dat er ook bijzondere persoonsgegevens worden verwerkt.[185] Voor de verwerking van bijzondere persoonsgegevens geldt een algeheel verbod, tenzij voldaan wordt aan een van de tien voorwaarden.[186] Daarnaast wordt het oud-adres en de favoriete professor van alumni nog verwerkt. Met deze gegevens wordt door DARO niks gedaan en dit zijn dus overbodige gegevens.

[183] Bijlage A
[184] Overweging 35 AVG
[185] Artikel 9 lid 1 AVG
[186] Artikel 9 lid 2 AVG

3.4 Verzamelen en actualiseren van de persoonsgegevens

3.4.1. Verzamelen van de persoonsgegevens

De persoonsgegevens die DARO verwerkt, komen op een bepaalde wijze in RE terecht. De persoonsgegevens van alumni worden als volgt verzameld:

- Gegevensdump van studentenadministratie: iedere week krijgt DARO per mail van de studentenadministratie een Excel bestand met daarin de persoonsgegevens van de kersverse afgestudeerden van de week ervoor. Iedere afgestudeerde wordt namelijk automatisch alumnus/alumna van TiU en komt dus in de database van DARO terecht. Deze gegevensdump vindt iedere maandag plaats. De persoonsgegevens van alumni komen in een map die bestaat uit zes Excel bestanden per mail binnen. De studenten-assistenten gaan hiermee aan de slag. Zij importeren de gegevens, zoals bekend bij de studentenadministratie, uit het bestand in de database. Dit is de meest gangbare manier van het verzamelen van persoonsgegevens van alumni.
- Gegevens van corporate relaties: deze persoonsgegevens verzamelt DARO via een businesskaart, website of via een email van desbetreffende relatie, waarin zij hun gegevens kenbaar maken. Deze persoonsgegevens worden handmatig in RE opgevoerd en verwerkt.
- Bankgegevens: indien een betrokkene aangeeft te willen doneren of steunen, dan heeft DARO het bankrekeningnummer nodig van betrokkene. Deze bankgegevens verkrijgt DARO per telefoon of via een machtigingskaart die betrokkene invult.

3.4.2. Actualiseren van de persoonsgegevens

Persoonsgegevens kunnen in de loop der jaren verouderen. Dit kan bijvoorbeeld het geval zijn als een persoon verhuist of een nieuwe bankrekening- en/of telefoonnummer heeft. Het is vanzelfsprekend dat (oud)studenten niet hun hele leven op hetzelfde adres blijven wonen of voor eeuwig hetzelfde telefoonnummer hebben. Om de verwerkte persoonsgegevens te actualiseren verzoekt DARO de alumni regelmatig om hun gegevens bij te werken, indien hun gegevens gewijzigd zijn. Dit doet DARO op de volgende momenten/manieren:

- Webformulier ‘update your details’: op de webpagina van DARO is een formulier te vinden waarmee alumni wijzigingen in hun persoonsgegevens kunnen doorgeven aan DARO.
- Tijdens de diploma-uitreiking: de kersverse alumni krijgen bij de diploma-uitreiking een diplomamap. Naast het diploma en andere documenten, bevat de map ook een kaart van DARO. Met deze kaart feliciteert DARO uiteraard de alumni, maar hierop staat ook een verzoek van DARO aan de alumni om hun gegevens bij te werken. Het kan namelijk voorkomen dat zij in tussentijd al verhuisd zijn of een nieuwe baan hebben.
- PostNL: TiU heeft met PostNL een overeenkomst gesloten en dit betreft het volgende. Indien een persoon verhuist, kan hij op een formulier aangeven dat zijn/haar universiteit op de hoogte moet worden gebracht over de verhuizing. Indien alumni deze mogelijkheid benutten, ontvangt DARO van PostNL daaromtrent een bericht. Deze wijziging voert DARO vervolgens door in de database.
- Project met Building Blocks: DARO is sinds kort een project gestart met het bedrijf Building Blocks. Dit bedrijf is ingeschakeld om LinkedIn profielen van alumni te scrapen. Dit betekent dat dit bedrijf werkgeversinformatie van aangeleverde alumni op LinkedIn opzoekt en verzamelt. Dit kan alleen als de gegevens van alumni openbaar zijn. Op deze manier verzamelt en actualiseert DARO de werkgeversgegevens.
- CASE Survey: Jaarlijks wordt een enquête uitgezet door een benchmark organisatie (International CASE Alumni Relations Survey). Ook DARO doet jaarlijks, sinds 2013, mee met deze survey. DARO geeft dan percentages door met betrekking tot alumni. Zo wordt bijgehouden van hoeveel alumni de mailadressen bekend zijn, van hoeveel alumni het telefoonnummer bekend is, hoeveel procent alumni gedoneerd hebben etc. De uitkomst hiervan wordt met andere universiteiten vergeleken, zodat de

universiteiten kunnen zien hoe zij het doen. Als uit dergelijke survey blijkt dat er veel mailadressen ontbreken, dan onderneemt DARO actie door de alumni brieven en mails te sturen. Deze actie komt echter onregelmatig voor en gebeurt niet op een vastgesteld moment.

Tot slot stuurt DARO regelmatig, met bijvoorbeeld een uitnodiging voor een alumni-evenement, een herinnering waarin wordt verzocht om de gegevens te actualiseren. Dit doet DARO niet structureel maar wel regelmatig.

3.4.3 Bewaartermijnen

Met het oog op het beginsel van opslagbeperking, dient de verwerkingsverantwoordelijke de opslagperiode van persoonsgegevens tot een strikt minimum te beperken. Dit kan de verwerkingsverantwoordelijke doen door bewaartermijnen voor het verwijderen van persoonsgegevens te hanteren. Binnen DARO worden er geen bewaartermijnen gehanteerd met betrekking tot de verwerkte persoonsgegevens. De persoonsgegevens in RE worden daarom in principe oneindig bewaard. DARO heeft namelijk de persoonsgegevens nodig om te kunnen controleren of een bepaalde persoon afgestudeerd is aan TiU. Indien een betrokkene verzoekt om verwijdering uit de database, dan voert DARO dit op twee verschillende manieren door. De ene keer worden alle contactgegevens van deze persoon verwijderd. De naam en studiegegevens blijven dan wel in RE staan. De andere keer wordt desbetreffende persoon niet uit RE verwijderd, maar krijgt deze persoon een 'do not contact' etiket. Dit etiket betekent dat deze persoon niet meer benaderd wilt worden door DARO.

3.5 Verplichtingen van DARO

3.5.1 Algemeen

De verwerkingsverantwoordelijke krijgt verplichtingen opgelegd ten aanzien van de gegevensverwerkingen. Over het algemeen betekent dit dat de verwerkingsverantwoordelijke verplicht is conform de AVG te handelen, om onrechtmatige gegevensverwerkingen te voorkomen. Daarnaast is de verwerkingsverantwoordelijke, met het oog op het transparantiebeginsel, verplicht om informatie omtrent de verwerkingen van persoonsgegevens van betrokkenen in beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal te presenteren. DARO is bewust van het feit dat de betrokkenen het recht toekomt hierover geïnformeerd te worden, maar dit wordt nog niet gedaan. Op de webpagina van DARO wordt deze informatie niet duidelijk gepresenteerd. Zo is onderaan het webformulier 'update your details', waarmee betrokkenen hun gegevens kunnen bijwerken, een korte tekst gewijd om aan te geven dat bij het invullen van het formulier toestemming wordt gegeven voor het verwerken van de gegevens en voor welke doeleinden deze worden gebruikt. Dit is echter niet genoeg aangezien de AVG een aantal criteria opgesomd heeft waaraan de verstrekte informatie moet voldoen.[187]

3.5.2 De registerplicht

De verwerkingsverantwoordelijke is verplicht een register bij te houden van alle verwerkingen, indien de organisatie meer dan 250 medewerkers in dienst heeft of de verwerking niet incidenteel plaatsvindt.[188] De verwerkingen binnen DARO vinden niet incidenteel, maar structureel plaats. Iedere week komt er een nieuwe datadump binnen die verwerkt wordt. Daarnaast worden de persoonsgegevens constant vernieuwd en bijgewerkt indien nodig. Het verwerken van persoonsgegevens gebeurt dus niet incidenteel, maar structureel. Daarom dient ook DARO een verwerkingsregister bij te houden. Momenteel heeft DARO een inventarisatieschema gemaakt van de gegevensverwerkingen binnen DARO.[189] Dit schema is een Excel bestand waarin staat wie de (interne) verwerkingsverantwoordelijke is, wat de doeleinden van de gegevensverwerkingen zijn, de

[187] Artikel 14 lid 1 jo 2 AVG
[188] Artikel 30 lid 1 AVG
[189] Bijlage A

categorie betrokkenen en persoonsgegevens die worden verwerkt, de gebruikers/ontvangers van de persoonsgegevens, een korte beschrijving van de beveiliging van de database en de bewaartermijn. Het overgrote deel van de punten die in het verwerkingsregister dienen worden opgenomen, zijn al beschreven in het inventarisatieschema.

Uit het interview met de FG blijkt dat de ingestelde Werkgroep bezig is met een tooling voor de verwerkingsregisters. Het is de bedoeling dat de afdelingen die een verwerkingsregister nodig hebben, met behulp van deze tool hun register inrichten. DARO kan rekening houden met de onderdelen die in ieder geval in het register dienen terug te komen. Deze zijn beschreven in paragraaf 2.5.2 van het vorige hoofdstuk.

3.5.3 De beveiliging van persoonsgegevens

Voor de beveiliging van de verwerkte persoonsgegevens kan er onderscheid worden gemaakt tussen organisatorische en technische beveiligingsmaatregelen. Daarnaast wordt er gekeken naar de datalekken bij afdeling DARO.

3.5.3.1 Organisatorische beveiligingsmaatregelen

DARO verwerkt de persoonsgegevens in RE. Niet iedere persoon heeft toegang tot de database. Alleen medewerkers van DARO, waaronder ook de studenten-assistenten en stagiaires, hebben toegang mits dit noodzakelijk is voor de uitoefening van de functie. Daarnaast hebben afdeling Career Office en International Recruiting Marketing toegang tot de database. Career Office heeft de gegevens nodig om te kunnen achterhalen waar studenten na afronding van de studie terecht kunnen komen. Hiermee kunnen zij carrière mogelijkheden voor studenten schetsen. International Recruiting Marketing heeft de gegevens van (buitenlandse) alumni nodig om met hun hulp nieuwe internationale studenten te werven. Om toegang te krijgen tot de database, dient een medewerker een login te hebben. Zonder login kan er geen toegang worden verkregen. De databasebeheerder, beheert alle rechten met betrekking tot het verstrekken van toegang en is verantwoordelijk voor de verwerkingen in de database. De beheerder kan controleren welke personen toegang hebben en wat zij wijzigen in de database. Niet alle wijzigingen kunnen worden onderschept door de beheerder, omdat het systeem daarvoor te beperkt is. Eindverantwoordelijke blijft wel de Managing Director van DARO. Tot slot is er vanuit het CvB besloten dat binnen iedere afdeling minimaal één persoon wordt aangewezen om de implementatie van de AVG te realiseren. Binnen DARO is de database beheerder de aangewezen persoon om de implementatie van de AVG binnen DARO te realiseren en na implementatie de naleving ervan te controleren.

Om de medewerkers te instrueren over het gebruik van de database en daarmee ook het gebruik van de persoonsgegevens, krijgen de nieuwe medewerkers een korte werkinstructie. De database beheerder of de studenten-assistenten die hem ondersteunen geven deze instructie. Deze werkinstructie staat niet op papier en duurt ongeveer een half uur. Tijdens deze instructie wordt uitgelegd hoe de medewerker in de database data kan opzoeken, waar de data vervolgens te vinden is en hoe de medewerker dit kan wijzigen.

3.5.3.2 Technische beveiligingsmaatregelen

Naast organisatorische beveiligingsmaatregelen, dient een verwerkingsverantwoordelijke ook technische beveiligingsmaatregelen te nemen om de verwerkte persoonsgegevens te beschermen. De database waarin DARO persoonsgegevens verwerkt is technisch beveiligd. De technische beveiliging is niet in handen van DARO zelf, maar van Library and IT Services (hierna: LIS). Zoals de medewerker van LIS aangaf draait de database op een database cluster, waarop meerdere databases van TiU draaien.[190] Via toegangscontroles zijn de databases beveiligd. Alleen functioneel beheerder, technisch applicatie beheerder en

[190] Bijlage H

back office personeel heeft digitaal toegang tot de database. Verder zijn de databases voorzien van firewalls. Deze firewalls staan niet standaard op open maar dicht. Alleen op de werkplekken waar de toegang tot de database nodig is, staat de firewall open. Daarnaast dienen gebruikers van de database een gebruikersnaam en wachtwoord te hebben om toegang te krijgen.

De data in de database is niet ge-encrypt. Dit achten de juristen van de TiU nog niet nodig. Bij wetenschappelijk onderzoek wordt de data bijvoorbeeld regelmatig wel ge-encrypt. Dit gebeurt meestal op verzoek van leverancier. Wat betreft de data in de database, wordt encryptie nog niet voorgeschreven door afdeling Legal.

Wat betreft de privacy by design en privacy by default principes, kan hierover het volgende gezegd worden. Het is niet duidelijk geworden of er binnen DARO gewerkt wordt met deze principes. Geen van de medewerkers weet of er, jaren geleden, bij het opzetten en implementeren van de database met de privacy van betrokkene rekening is gehouden. Ook wat betreft Mailplus is niet duidelijk geworden of er rekening wordt gehouden met deze principes. Zowel de medewerkers van DARO als de medewerkers van LIS konden hierop geen antwoord geven, simpelweg omdat de database al een aantal jaren wordt gebruikt. De privacy by default principe ziet meer toe op social mediaplatformen en is daarom in dit praktijk onderzoek buiten beschouwing gelaten.

3.5.3.3 Versleutelde gegevensverwerking

Sinds afgelopen jaar is binnen DARO afgesproken dat bestanden, afkomstig uit de database en bestaande uit persoonsgegevens, niet meer als bijlage per mail verzonden worden. De bestanden worden voortaan via een beveiligde verbinding van TiU verzonden. De website waarop de bestanden worden geüpload, wordt beheerd door afdeling LIS. Deze beveiligde verbinding heet SecureFilesender.[191] Deze verbinding zorgt er voor dat documenten niet meteen zichtbaar zijn bij het versturen van een mail. De bestanden worden door de afzender op deze website als bijlage toegevoegd en worden vervolgens omgezet in een downloadbare link. Vervolgens verstuurt de afzender deze link per mail naar de ontvanger. De ontvanger kan de bestanden dan downloaden door op de link te klikken. De ontvanger wordt dan doorverwezen naar de SecureFilesender webpagina. Hier kan de ontvanger dan op de download knop klikken en de bestanden inzien. Indien ontvanger de data download krijgt de verzender hiervan een mailbericht. De afzender kan zelf ook bepalen voor welke termijn de link te downloaden en te bekijken is. Na verloop van de termijn kan de ontvanger de link niet meer downloaden en openen. Daarnaast kan de afzender ervoor kiezen om er een wachtwoord aan te koppelen. Dit wachtwoord dient de afzender dan via een andere communicatiekanaal door te sturen aan ontvanger. Pas als de ontvanger over dit wachtwoord beschikt, kan hij het bestand downloaden en openen. Het (optionele) wachtwoord dient als extra beveiligingscontrole. Dit optionele wachtwoord wordt met name gebruikt in de gevallen dat de ontvanger zich buiten DARO bevindt, bijvoorbeeld bij het versturen van data naar een verwerker.

DARO heeft hiertoe besloten omdat de mailboxen van medewerkers vol met persoonsgegevens, afkomstig uit de database, zaten. Mocht een van de mailboxen van de medewerkers gehackt worden, dan beschikt de hacker over veel persoonsgegevens, wat absoluut niet de bedoeling is. Dit is een vorm van versleutelde gegevensverwerkingen, aangezien het doorsturen in versleutelde vorm ook als verwerking wordt aangemerkt. Zonder de link te openen en te downloaden kunnen de persoonsgegevens niet worden ingezien door ontvanger.

[191] Bijlage G

3.5.3.4 Datalekken

Indien persoonsgegevens ergens terechtkomen waar ze niet horen te zijn, is er sprake van een datalek. Hiervan moet aan de AP melding worden gemaakt. TiU heeft naar aanleiding van de inwerkingtreding van de meldplicht datalekken onder de Wbp, een protocol meldplicht datalekken opgesteld voor de medewerkers.[192] TiU vindt het namelijk van belang dat iedere medewerker weet wat het protocol is, bij een eventuele datalek. Dit begint bij het feit dat iedere medewerker moet weten dat hij zo spoedig mogelijk intern een melding maakt van een mogelijk datalek, zodat door afdelingen LIS en Legal Affairs beoordeeld kan worden wat de ernst is van het incident. Het uitgangspunt is om ook bij twijfel een interne melding te doen, want er kan beter te veel dan te weinig gemeld worden. Het protocol bevat een drietrapsraket. Medewerkers moeten zich namelijk eerst afvragen of er sprake is van verwerking van persoonsgegevens, of er sprake is van een (mogelijk) datalek en indien aan beide trappen is voldaan dan moet er een interne melding worden gedaan. De medewerker dient dan een interne melding te doen door een mail te sturen naar een emailadres dat speciaal is aangemaakt voor de meldingen van datalekken binnen TiU. In de mail dient de medewerker een zo uitgebreid mogelijke beschrijving van het incident aan te geven. De mails die binnenkomen op dit mailadres komen terecht bij onder andere de FG en Legal Affairs, maar ook bij enkele andere personen en afdelingen. Deze medewerkers nemen naar aanleiding van de melding contact op met de melder om te beoordelen of er daadwerkelijk sprake is van een datalek. Daarnaast heeft de Werkgroep ook een procedure op papier gezet met betrekking tot datalekken. Dit is echter een intern document waarin staat wie binnen de werkgroep, welke werkzaamheden verricht bij een mogelijke datalek.

DARO is bekend met de meldplicht datalekken en het Protocol.[193] Binnen DARO heeft zich namelijk al eens een datalek voorgedaan. De werklaptop van een medewerker werd in een parkeergarage uit de auto gestolen. Deze laptop is een gegevensdrager, met daarop (mogelijk) persoonsgegevens. De medewerker in kwestie heeft direct de FG van TiU hiervan op de hoogte gesteld. De FG heeft de medewerker vervolgens onmiddellijk opgedragen het wachtwoord te wijzigen. Dit heeft de medewerker toen ook gedaan. Vervolgens heeft de medewerker samen met de FG het lek beoordeeld. Uit eigen beweging heeft de medewerker vervolgens alle betrokkenen, waarvan persoonsgegevens op de laptop stonden, over de diefstal geïnformeerd. Vanaf de melding van de medewerker, heeft de FG het overgenomen en een melding gedaan bij de AP. Tot op heden heeft de FG nooit een tegenbericht gehad van de AP.

3.5.4 Privacy Impact Assassment

Binnen DARO is niet duidelijk of er een gegevensbeschermingseffectbeoordeling is uitgevoerd om het effect van de beoogde verwerkingsactiviteiten op de bescherming van de persoonsgegevens in kaart te brengen. Wellicht heeft dit twee jaar geleden plaatsgevonden, aangezien er toen ook een inventarisatie van de gegevensverwerking heeft plaatsgevonden.[194] Daarnaast wordt door LIS regelmatig een audit uitgevoerd met betrekking tot de systemen waarmee TiU werkt, zoals uitgebreid beschreven wordt in paragraaf 3.5.5. Ook heeft de FG tijdens het interview aangegeven dat er een ‘’pre-PIA’’ wordt ingebouwd in het verwerkingsregister. De verwerkingsverantwoordelijke kan aan de hand hiervan bepalen of een PIA noodzakelijk is voor de gegevensverwerkingen en het systeem. Dit wordt dan aan de hand van een vragenlijst gedaan. De verwerkingsverantwoordelijke dient deze vragenlijst te beantwoorden en hieruit zal dan blijken of een PIA noodzakelijk is. Indien dit het geval is kan de verwerkingsverantwoordelijke een PIA uitvoeren. De verwerkingsverantwoordelijke en een informatiespecialist voeren deze PIA uit en kunnen gestuurd en gesteund worden door de FG.

[192] Bijlage C
[193] Bijlage C
[194] Bijlage A

3.5.5 Verwerkersovereenkomst

De TiU maakt gebruik van een modelovereenkomst van SURF (ICT-samenwerkingsorganisatie onderwijs en onderzoek). De basis van deze verwerkersovereenkomst heeft de TiU overgenomen en zich eigen gemaakt.[195] De TiU heeft er enkele bepalingen uit gehaald, toegevoegd en verzwaard. Uiteraard dienen de afdelingen van TiU, bij het uitwisselen van data aan derde partijen, gebruik te maken van deze verwerkersovereenkomst. Dit is ook wat DARO doet. DARO heeft met verschillende partijen een verwerkersovereenkomst gesloten. Hiervoor gebruikt DARO de verwerkersovereenkomst van TiU. Deze verwerkersovereenkomst is niet actueel aangezien deze gebaseerd is op de Wbp. Spoedig zal de AVG van toepassing zijn en zal de verwerkersovereenkomst aan de bepalingen uit de AVG moeten voldoen.

Naar aanleiding van de inwerkingtreding van de AVG en de naderende toepassing hiervan, is SURF bezig geweest met het opstellen van een nieuwe verwerkersovereenkomst. In de AVG staan namelijk enkele standaardbepalingen opgesomd die expliciet terug dienen te komen in de verwerkersovereenkomst. Deze verwerkersovereenkomst is gereed en hiermee is De Werkgroep aan de slag gegaan, om het zich eigen te maken. De werkgroep houdt de hoofdlijnen van deze verwerkersovereenkomst aan, maar er worden nog enkele bepalingen gewijzigd, toegevoegd, verwijderd en/of aangevuld.

Onder paragraaf 2.5.6 van het vorige hoofdstuk staan de bepalingen die standaard in een verwerkersovereenkomst moeten worden opgenomen.[196] Bij de verwerkersovereenkomst hoort een bijlage waarin wordt ingevuld wat de doeleinden zijn van de gegevensverwerking, de categorie persoonsgegevens die worden verwerkt en de categorie betrokkene waarop de verwerkingen betrekking hebben. Ook dient de verwerker de passende maatregelen, ter bescherming van de persoonsgegevens, die getroffen zijn aan te tonen. Verwerker mag volgens de overeenkomst geen sub-verwerkers, zonder toestemming van verwerkingsverantwoordelijke, inschakelen. Daarnaast heeft TiU zich de mogelijkheid verschaft audits uit te voeren bij de verwerker. Tot slot is het vernietigen of terugsturen van persoonsgegevens naar verwerkingsverantwoordelijke ook opgenomen in de verwerkersovereenkomst.

Indien DARO aan afdeling Legal Affairs doorgeeft dat zij een verwerkersovereenkomst heeft gesloten, dan weet afdeling LIS hier ook van. Medewerkers van afdeling LIS controleren vervolgens de beveiliging van de software waarvan de derde partij gebruik maakt. De beveiliging van de derde partij moet voldoen aan bepaalde beveiligingsstandaarden. De beveiligingsstandaard hangt af van de gevoeligheid van de te verwerken persoonsgegevens. De derde partij moet zelf een beveiligingsrapport, van minder dan een jaar oud, overleggen waarin de beveiligingsmaatregelen worden beschreven. Dit rapport wordt vervolgens door de medewerkers van LIS gecontroleerd.

Soms kan het voorkomen dat een derde partij geen beveiligingsrapport toont. In dit geval gaan de medewerkers van LIS in overleg met deze partij. Eventueel test het CERT team van de TiU (Computer Emergency Response Team) zelf de beveiliging. Het CERT team beschikt namelijk over personen die een penetratietest kunnen uitvoeren. Dergelijke test houdt in dat de beveiliging van software wordt onderzocht op kwetsbaarheden, door als het ware (proberen) in te breken in de beveiliging. De kwetsbaarheden worden tijdens een penetratietest daadwerkelijk gebruikt om in de beveiliging van de software in te breken. Mocht het blijken dat het niet veilig is, gaat LIS in discussie met de derde partij. In de gevallen dat LIS tot de conclusie komt dat het echt niet veilig is, adviseren zij het MT om niet in zee te gaan met betreffende partij. LIS is dus strikt met betrekking tot de beveiligingsstandaarden waaraan de beveiliging van derde partijen moet voldoen.

[195] Bijlage D
[196] Artikel 28 AVG

Deze technische audit vindt in de praktijk allereerst plaats ten tijde van het sluiten van een verwerkersovereenkomst. In de verwerkersovereenkomst is ook opgenomen dat TiU zich het recht voorbehoud om, bij het ontstaan van kwetsbaarheden, de software te controleren op deze kwetsbaarheid. Dit gebeurt niet op structurele basis, maar wel zodra er ergens in de wereld een lek plaatsvindt en het risico zich voor doet dat deze kwetsbaarheid ook bij de verwerker intreedt.

3.5.6 Privacy beleid
Aan de hand van een privacy beleid kan een verwerkingsverantwoordelijke aantonen dat voldaan wordt aan de AVG. Dit volgt uit de verantwoordingsplicht die berust op verwerkingsverantwoordelijke.[197]

DARO zelf heeft geen 'eigen' privacy beleid. Vanuit TiU zijn er reglementen en stukken beleid met betrekking tot verwerking van persoonsgegevens opgesteld en van toepassing. Daarnaast heeft DARO, in samenwerking met de juristen van TiU een korte instructie opgesteld. Hierin worden de medewerkers geïnstrueerd om de persoonsgegevens van alumni niet zomaar met derden of andere organisatieonderdelen te delen.

TiU heeft drie verschillende reglementen met betrekking tot bescherming van persoonsgegevens. Alle drie de reglementen lijken veel op elkaar maar richten zich op drie verschillende personen. Er is een reglement dat toeziet op de bescherming van persoonsgegevens van studenten, een met betrekking tot de medewerkers en de andere met betrekking tot de relaties van TiU.[198] Het reglement dat betrekking heeft op relaties van TiU, is van toepassing op alumni, zoals beschreven staat in de bijlage van het reglement.

Dit reglement bevat, conform de Wbp, regels voor een zorgvuldige omgang met het verzamelen en verwerken van persoonsgegevens van relaties van TiU. Het is een korte samenvatting van de Wbp, met toelichting. Zo bestaat het reglement uit kopjes als: algemeen toetsingskader, beveiliging, verstrekking, kennisgeving en rechten van betrokkene etc. Aangezien dit reglement een uitwerking is van de Wbp, is het niet meer recent.

Zoals de FG van TiU tijdens het interview aangaf bestaat er al wel beleid met betrekking tot bescherming van persoonsgegeven, maar niet eenduidig en duidelijk.[199] De stukken beleid zitten namelijk nog versnipperd. Momenteel is de ingestelde Werkgroep bezig met het opstellen van een algemeen en strategisch privacy beleid. Het algemeen privacy beleid wordt een overkoepelend document met verwijzingen naar bestaande documenten. Naast deze beleidsstukken, kan DARO ter inspiratie gebruik maken van het modelbeleid van SURF.[200]

3.6 Rechten van betrokkene
De betrokkene heeft enkele (nieuwe) rechten waarop hij zich kan beroepen ten aanzien van de verwerking van zijn persoonsgegevens. De betrokkene komt deze rechten toe en de verwerkingsverantwoordelijke dient te zorgen voor de invulling aan deze rechten. De betrokkene kan een beroep op zijn rechten kenbaar maken bij de organisatie die zijn gegevens verwerkt.

De betrokkene heeft het recht om in een beknopte, transparante, begrijpelijke en toegankelijke vorm informatie te verkrijgen over de verwerking van zijn persoonsgegevens

[197] Artikel 5 lid 2 AVG
[198] Bijlage B
[199] Bijlage E
[200] 'Privacy-modelbeleid', *www.surf.nl* 26 juni 2017

en over de mogelijkheid om zijn rechten uit te oefenen.[201] Dit wordt tot op heden in geen enkele vorm gedaan door DARO.

Uit de interviews met de medewerkers blijkt dat DARO wel bereid is volledig mee te werken indien een betrokkene een beroep doet op zijn rechten. Tot op heden zijn de verzoeken van betrokkene op één hand te tellen. De verzoeken betroffen meestal het verzoek om geen contact meer op te nemen met betrokkene. Op de webpagina van DARO is niet duidelijk waar een betrokkene zijn beroep op zijn rechten kenbaar kan maken. Het is niet alleen onduidelijk, op de webpagina van DARO is hiervoor geen mogelijkheid geboden. Wel kan de betrokkene naar aanleiding van een mailbericht zich afmelden voor mailings van DARO. Onderaan de mails die betrokkene ontvangen is hiervoor een 'unsubscribe' knop ingebouwd. Hiermee kan de betrokkene aangeven dat hij geen contact met DARO wenst.

Via de website van TiU is dit wel mogelijk. Op de website kan de betrokkene zijn rechten uitoefenen door een formulier in te vullen en op te sturen. Deze formulieren zijn echter moeilijk te vinden, omdat ze pas gevonden worden als er bepaalde termen in de zoekopdracht worden genoemd. TiU heeft hiervoor drie verschillende formulieren opgesteld.

- Via het eerste formulier kan de betrokkene verzet aantekenen tegen de verwerking van zijn persoonsgegevens. De betrokkene dient zich te identificeren, door middel van een paspoort, rijbewijs of TiU kaart. Vervolgens moet de betrokkene zijn relatie met TiU aangeven, zoals student, medewerker of andere relatie. Tot slot dient de betrokkene beknopt de bijzondere omstandigheden uit te leggen op grond waarvan hij verzet aantekent.
- Formulier twee betreft een verzoek tot inzage in de persoonsgegevens die van de betrokkene worden verwerkt door TiU.
- Formulier drie betreft een verzoek om verbetering, aanvulling, verwijdering of afscherming van persoonsgegevens van betrokkene.

Alle drie de formulieren hebben dezelfde opmaak. De betrokkene dient het formulier in vullen en op te sturen naar het CvB van de TiU. Zij nemen het verzoek in behandeling en uiterlijk binnen vier weken wordt er gereageerd op het verzoek van betrokkene. De formulieren zijn via de website van TiU te raadplegen.

[201] Artikel 12 jo 14 AVG

Hoofdstuk 4 Conclusies en aanbevelingen

4.1 Conclusies en aanbevelingen

Dit hoofdstuk staat in het teken van de conclusies en de daarop berustende aanbevelingen. Hier zal antwoord worden gegeven op de centrale vraag die ten grondslag ligt aan dit onderzoek. De centrale vraag luidt: ''Welke aanbevelingen kunnen DARO worden gedaan, na de beoordeling van de werkwijze betreffende het verwerken van persoonsgegevens van oud-studenten aan de hand van de bepalingen uit de AVG, zodat DARO aan de eisen van de AVG kan voldoen door, indien nodig, de werkwijze aan te passen?'' De conclusies zullen hieronder gepresenteerd worden met bijbehorende aanbevelingen. Allereerst wordt een algemene conclusie getrokken met betrekking tot de gegevensverwerkingen binnen DARO. Vervolgens worden de specifieke conclusies die gericht zijn op bepaalde aspecten van de AVG gepresenteerd.

4.1.1 Algemene conclusie

De medewerkers binnen DARO zijn zich in hoge mate bewust van de privacy van de betrokkenen. Ze worden regelmatig geïnstrueerd door afdeling Legal over aanpassingen in het recht omtrent de verwerking van persoonsgegevens. Dit heeft zijn vruchten afgeworpen aangezien de medewerkers met hoge mate van bewustzijn omgaan met persoonsgegevens. TiU stelt zich ten doel om een hoge mate van awareness te creëren bij haar medewerkers. Van DARO kan gezegd worden dat dit doel bereikt is. De medewerkers delen niet zomaar persoonsgegevens van betrokkene met derden en andere organisatieonderdelen van TiU. Awareness wat betreft het gebruik van de persoonsgegevens waarover DARO beschikt is dus zeker aanwezig.

4.2 De rechtmatigheid van de gegevensverwerkingen

Het verwerken van persoonsgegevens is enkel toegestaan indien dit rechtmatig is. Rechtmatigheid wordt gebaseerd op een grondslag en een specifiek en uitdrukkelijk omschreven doel. In het geval van DARO kan er geconcludeerd worden dat hiervan sprake is. DARO baseert de gegevensverwerkingen op:

- gerechtvaardigd belang van verwerkingsverantwoordelijke;
- toestemming van betrokkene;
- vitaal belang.

Alle drie de grondslagen zijn wettelijk toegestane grondslagen.[202] Het feit dat de verwerking van het land van alumni gebaseerd wordt op vitaal belang is onduidelijk en feitelijk niet correct, aangezien deze grondslag uitdrukkelijk toeziet op het leven van betrokkene. De verwerking van deze persoonsgegevens dient zoals de rest, behalve de verwerkingen van bankgegevens, gebaseerd te worden op gerechtvaardigd belang van verwerkingsverantwoordelijk. Verder is onderaan het formulier 'update your details' merkwaardig genoeg een toestemmingsvakje opgenomen. Dit zorgt voor verwarring aangezien de gegevensverwerkingen van DARO in eerste instantie niet gebaseerd zijn op toestemming van betrokkene, maar gerechtvaardigd belang van verwerkingsverantwoordelijke. Deze toestemmingsverklaring impliceert dat de eerste verwerking ook op toestemming van betrokkene is gebaseerd, terwijl dit niet het geval is. Dit toestemmingsvakje dient weg gelaten te worden onder het formulier en kan indien gewenst vervangen worden door een informatieve tekst over de grondslag en doelen van de gegevensverwerkingen binnen DARO.

DARO heeft de doeleinden waarvoor de gegevens worden verwerkt, beschreven in het inventarisatieschema. Deze doeleinden zijn zoals het hoort volgens de AVG, specifiek en uitdrukkelijk omschreven. Indien de betrokkene het doel van de gegevensverwerkingen onder ogen krijgt, weet hij direct welk doel de gegevensverwerkingen dienen.

[202] Artikel 6 lid 1 AVG

In principe verwerkt DARO alleen algemene persoonsgegevens. Het komt toch voor dat er (on)bewust ook bijzondere persoonsgegevens worden verwerkt. Van de telefoongesprekken tijdens de jaarlijkse belcampagnes wordt namelijk verslag gemaakt en als een betrokkene aangeeft dat hij aan bepaalde ziekte lijdt, dan komt dit in de database terecht. Hierdoor verwerkt DARO ook bijzondere persoonsgegevens, terwijl hiervoor een algeheel verbod geldt, tenzij. DARO voldoet niet aan de voorwaarden voor het verwerken van bijzondere persoonsgegevens, daarom is het aan te bevelen om hier per direct mee te stoppen en deze gegevens te wissen.[203] Dit levert namelijk overtreding van de AVG op wat kan leiden tot een sanctie. Deze medische gegevens zijn ook niet noodzakelijk voor het bereiken van de doeleinden van DARO. Om dit in de toekomst te voorkomen wordt aanbevolen om een protocol op te stellen voor de belstudenten waarin wordt aangegeven welke gegevens wel en welke gegevens niet opgeschreven en verwerkt mogen worden. Daarnaast wordt het oud-adres en de favoriete professor van alumni verwerkt. Ook deze verwerkingen dienen te stoppen, met het oog op het minimaliseren van de gegevensverwerkingen en het doelbindingsbeginsel, aangezien deze gegevens niet noodzakelijk zijn voor het bereiken van het doel.

Naast de verwerkingen in de database, verwerkt DARO ook persoonsgegevens in Mailplus. Hierin worden mailinglijsten opgesteld, waarmee mails worden uitgezet naar bepaalde groepen. Mailplus slaat deze lijsten automatisch op. Indien een betrokkene naar aanleiding van een eerdere mail een wijziging doorvoert, dan wordt dit in de database aangepast en niet in Mailplus. Dit betekent dat de gegevens in de database dan niet meer corresponderen met de gegevens in Mailplus, wat kan leiden tot het gebruiken van achterhaalde en onjuiste gegevens. Om dit te voorkomen dient DARO de mailinglijsten die niet meer gebruikt worden, nadat er een mail is verzonden, uit Mailplus te verwijderen. In RE staan namelijk ook de contactmomenten met de alumni opgeslagen. Indien er in Mailplus een campagne is geprogrammeerd met diverse op elkaar volgende mails, is het niet aan te bevelen om de mailinglijsten te verwijderen aangezien er nog mails zullen volgen.

4.3 Verplichtingen van DARO ten aanzien van de gegevensverwerkingen

4.3.1 Algemene verplichtingen van DARO

Volgens de verplichtingen uit de AVG moet DARO zorgen voor het actualiseren en juist houden van de verwerkte persoonsgegevens. DARO onderneemt hiervoor regelmatig actie door mails uit te zetten met ‘update your details’ en tijdens diploma-uitreikingen hierop te hameren. Het is aanbevolen om dit voort te zetten en indien mogelijk op een vastgelegd tijdstip een mail hieromtrent uit te zetten. Indien betrokkenen hierop reageren met of wel een bijwerking van de persoonsgegevens of een antwoord dat er niets gewijzigd is, kunnen deze betrokkenen uit de mailinglijst worden gehaald zodat ze de volgende keer niet in de mailinglijst meegenomen worden.

De verwerkingsverantwoordelijke is verplicht om de betrokkene te voorzien van informatie omtrent de gegevensverwerkingen. Deze informatie wordt door DARO (nog) niet gepresenteerd aan betrokkene. Weliswaar staat er in één zin samengevat waarvoor de gegevens verwerkt worden, maar dit is niet voldoende volgens de AVG. Logische aanbeveling dat hierop volgt is het feit dat dit nog wel moet gebeuren gezien het transparantiebeginsel en de verplichting van verwerkingsverantwoordelijke om de betrokkene hierover te informeren. DARO kan dit doen door een privacy verklaring op de website te plaatsen, waarmee betrokkene over de gegevensverwerkingen wordt geïnformeerd.

[203] Artikel 9 lid 2 AVG

4.3.2 Beveiliging van de persoonsgegevens
DARO dient passende en effectieve beveiligingsmaatregelen te treffen ter bescherming van de verwerkte persoonsgegevens. DARO heeft organisatorische beveiligingsmaatregelen getroffen om de persoonsgegevens te beschermen. Zo kunnen alleen medewerkers die bevoegd zijn en waarvan noodzakelijk is dat zij toegang hebben, bij de database. Daarnaast heeft DARO een functioneel beheerder van de database in dienst, die onder andere mutaties in de database controleert. Intern verantwoordelijke is de Managing Director van DARO. Indien er nieuwe medewerkers bij DARO aan de slag gaan, krijgen zij een korte werkinstructie waarin zij geïnstrueerd worden over het gebruik van de database en de verwerkte persoonsgegevens. Deze instructie is vrij kort en staat nog niet op papier. Het is aan te raden deze werkinstructie op papier te zetten en te verplichten voor nieuwe medewerkers om onjuiste gebruik van de database en persoonsgegevens tegen te gaan. Daarnaast is het aan te bevelen om regelmatig de medewerkers bij te scholen omtrent het gebruik van de database, aangezien niet iedere medewerker evenveel gebruik maakt van de database. Hierbij kan ook meteen aandacht worden besteed aan de privacy van betrokkene, door te benadrukken dat het steeds belangrijker wordt. Hierdoor wordt ook meteen een stuk awareness bij de medewerkers gecreëerd. De technische beveiligingsmaatregelen zijn getroffen door en in handen van afdeling LIS. Zij hebben de database voorzien van de nodige beveiligingsmaatregelen, met onder andere firewalls en antivirussen. Zij voeren regelmatig audits uit om de beveiliging te testen.

Het is niet duidelijk geworden of DARO volgens de ‘privacy by design’ en ‘privacy by default’ principes werkt. De database waarvan DARO gebruik maakt, is al enige tijd in gebruik en daarom is niet te achterhalen of bij het opzetten van dit systeem rekening is gehouden met bovengenoemde principes. Ook wat betreft Mailplus is niet duidelijk geworden of deze principes in acht worden genomen. Of dit enigszins nog te achterhalen valt, is te betwijfelen. Dit gezien het feit dat de medewerker die als eerste en actief deelnam aan het opzetten van de database, niet meer voor TiU werkt. Wat betreft Mailplus zou DARO hieromtrent een vervolgonderzoek in kunnen stellen, om te achterhalen of de software deze principes wel hanteert. Om dergelijke situaties in de toekomst te voorkomen is de aanbeveling die hierop volgt om in de toekomst bij het opzetten van een nieuw systeem, waarin persoonsgegevens worden verwerkt, deze principes mee te nemen en op papier uit te werken. Hiermee kan DARO dan aantonen dat al bij het begin van het opzetten van het informatiesysteem rekening wordt gehouden met de privacy van betrokkene.

Wat DARO onder andere goed doet, is het gebruik maken van versleutelde gegevensverwerking bij het versturen van persoonsgegevens. Het gebruik maken van versleutelde gegevensverwerking wordt sterk aanbevolen in de AVG. DARO maakt gebruik van SecureFilesender. Deze website zet de persoonsgegevens om in een downloadbare link. Hieraan kan, als extra beveiliging, een wachtwoord worden gekoppeld. Dit wachtwoord ontvangt de ontvanger via een andere weg dan per mail, bijvoorbeeld per sms. Met behulp van het wachtwoord en de link kan de ontvanger toegang tot de persoonsgegevens krijgen. Deze werkwijze dient DARO voort te zetten en het is aan te raden om de extra beveiliging, door er een wachtwoord aan te koppelen, te allen tijde toe te passen bij het verzenden van persoonsgegevens naar derden.

De verwerkingsverantwoordelijke dient bewaartermijnen te hanteren voor het verwijderen van persoonsgegevens indien ze niet meer relevant zijn. DARO hanteert (nog) geen bewaartermijnen om praktische redenen. DARO houdt in opdracht van TiU van alle alumni, persoonsgegevens bij. Dit betekent dat de persoonsgegevens van de alumni, min of meer hun gehele leven relevant zijn voor DARO. Mocht een betrokkene komen te overlijden, dan kan DARO ervoor kiezen om alle contactgegevens en andere persoonsgegevens te verwijderen. Alleen de naam en afgeronde studie kan DARO dan bewaren met het oog op het bijhouden van het totaal aantal alumni van TiU, overige (contact)gegevens dienen wel verwijdert te worden.

4.3.3. Meldplicht datalekken
Gezien het feit dat het melden van datalekken al enige tijd onder de Wbp verplicht was en de AVG dit heeft overgenomen, is gekeken naar de datalekken binnen DARO. Tot op heden is pas één keer een datalek voorgekomen. Dit datalek is goed opgepakt en volgens het opgestelde protocol van TiU afgehandeld. Daarnaast weten alle medewerkers wat een datalek is en dat ze een (mogelijke) datalek moeten melden. Het is daarom aan te bevelen om deze werkwijze voort te zetten en het protocol na te leven.

4.3.4 De registerplicht
Omdat DARO structureel persoonsgegevens verwerkt, is het verplicht een register van de gegevensverwerkingen bij te houden. Het inventarisatieschema waarin de gegevensverwerkingen binnen DARO in kaart zijn gebracht, voldoet qua inhoud grotendeels al aan de verplichte inhoud van een verwerkingsregister. Op het moment van schrijven is de Werkgroep bezig met het implementeren van een tooling voor het verwerkingsregisters binnen TiU, waar DARO ook gebruik van gaat maken. DARO moet er op toezien dat dit register de verplichte bepalingen, zoals beschreven in hoofdstuk 2 paragraaf 2.5.2, bevat.[204]

4.3.5 Privacy Impact Assassment (PIA)
In het verwerkingsregister dat in de vorige alinea besproken wordt, komt een pre-PIA.
Deze pre-PIA komt in de vorm van een vragenlijst met betrekking tot de gegevensverwerkingen. Aan de hand van de geïntegreerde vragenlijst kan DARO concluderen of het uitvoeren van een PIA noodzakelijk is. DARO dient hier zeker gebruik van te maken, aangezien de medewerkers niet weten of er al eerder een PIA is uitgevoerd. De FG ondersteunt de afdeling bij het uitvoeren van een PIA, door onder andere advies uit te brengen. Deze mogelijkheid zal DARO zeker moeten benutten en de aspecten zoals beschreven in hoofdstuk 2 paragraaf 2.5.4 me te nemen in de beoordeling.[205]

4.3.6 De verwerkersovereenkomst
De Werkgroep heeft een nieuwe verwerkersovereenkomst opgesteld, die geactualiseerd is naar de AVG. De bepalingen die expliciet zijn genoemd in de AVG en terug dienen te komen in de verwerkersovereenkomst, zijn opgenomen in de verwerkersovereenkomst. DARO maakte voor de inwerkingtreding van de AVG al gebruik van een verwerkersovereenkomst die opgesteld is door TiU. Daarom zal DARO ook nu gebruik gaan maken van deze verwerkersovereenkomst. Aangezien deze verwerkersovereenkomst geactualiseerd is en voldoet aan de AVG is het logisch dat DARO hiervan gebruik gaat maken.

4.3.7 Het privacy beleid
DARO beschikt (nog) niet over een privacy beleid. Binnen TiU is de Werkgroep bezig met het verzamelen van de bestaande beleidstukken. Met behulp van deze stukken gaan zij een strategisch beleidsstuk opstellen. Aan de hand van deze stukken en het strategisch beleid dient DARO een privacy beleid op te stellen. Met een privacy beleid kan DARO namelijk naleving van de AVG aantonen. Om inzicht te krijgen over wat er in een privacy beleid hoort, kan DARO gebruik maken van het model beleid van SURF. DARO kan met behulp van dit model haar eigen privacy beleid opstellen, toegespitst op de verwerking van persoonsgegevens binnen DARO. [206]

4.4 Rechten van betrokkene
Het recht van betrokkene om informatie te ontvangen over de verwerking van zijn persoonsgegevens wordt niet beantwoord door DARO, terwijl het verschaffen van deze informatie aan betrokkene wel verplicht is. De AVG stelt criteria aan de inhoud van deze

[204] Artikel 30 lid 1 AVG
[205] Artikel 35 lid 7 AVG
[206] 'Privacy-modelbeleid', *www.surf.nl* 26 juni 2017.

informatieverstrekking en dit dient nageleefd te worden.[207] Het feit dat DARO de persoonsgegevens niet via betrokkene ontvangt maar via de studentenadministratie, betekent dat DARO de betrokkene de nodige informatie dient te verschaffen. Welke informatie en in welke vorm deze verstrekt moet worden, is uitgebreid beschreven in hoofdstuk 2, paragraaf 2.6.1 van dit onderzoek. Aangezien DARO de persoonsgegevens van betrokkene voor communicatie met deze betrokkene gebruikt, dient DARO deze informatie uiterlijk op het eerste moment van contact met betrokkene te verstrekken. Het is daarom aan te bevelen om bij de allereerste mail aan alumni, deze informatie te verstrekken. Dit kan DARO doen door een link te plaatsen in de mail, zoals de 'unsubscribe' knop. Deze link moet er dan voor zorgen dat de betrokkene met één druk op de knop bij deze informatie komt.

Daarnaast is voor betrokkene niet duidelijk waar hij zijn rechten kan uitoefenen. Aangezien de rechten van betrokkene uitgebreid en verstevigd zijn, is dit onder de AVG van essentieel belang. DARO dient zoals hierboven al vermeld een tekst op de website te plaatsen waarmee informatie wordt verschaft over de gegevensverwerkingen. Daarbij dient DARO ook meteen de mogelijkheid te bieden om een beroep op de rechten van en door betrokkene kenbaar te maken. Momenteel zijn hiervoor formulieren opgesteld door afdeling Legal Affairs, maar deze zijn moeilijk vindbaar op de website. Aan DARO de taak om deze eenvoudig toegankelijk te maken voor betrokkene.

Tot op heden zijn de verzoeken van betrokkene om verwijdert te worden uit de database op één hand te tellen. Indien dergelijke verzoeken binnen kwamen, kreeg desbetreffende betrokkene een 'do not contact' etiket. Gezien de strenge regels die de AVG stelt, zal deze werkwijze niet (meer) volstaan. Maar aangezien betrokkene met dergelijk verzoek aangeeft niets meer met TiU te maken willen hebben, rijst de vraag of de gegevens nog relevant zijn en of het nog meerwaarde heeft om toch de gegevens te behouden en daarmee een sanctie te riskeren. Desbetreffende persoon wenst nooit meer in contact te komen met TiU, dus zullen zijn persoonsgegevens ook geen bijdrage leveren aan het realiseren van de doelen van DARO. DARO wordt aanbevolen om dergelijke verzoeken in de toekomst te honoreren en door te voeren, om zo geen risico op sancties te lopen.

Aangezien de AVG zorgt voor versteviging en uitbreiding van de rechten van betrokkene zal DARO nog zorgvuldiger om moeten gaan met de persoonsgegevens van betrokkene en diens rechten. Het is wachten op de eerste uitoefeningen van de rechten van en door betrokkenen, aangezien het hoofdstuk met de rechten van betrokkene het deel te zijn dat inconsistent en/of slordig opgeschreven lijkt te zijn.[208]

[207] Artikel 14 lid 1 jo. 2 AVG
[208] Zwenne & Mommers, *Tijdschrift voor Compliance* 2016, p. 11.

Bronnenlijst

Literatuur

Engelfriet, Meij & Kager 2017
A.Engelfriet, L. Meij en P. Kager, *Algemene Verordening Gegevensbescherming: Artikelsgewijs commentaar.* Amsterdam, Nederland: IUS Mentis 2017.

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

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

Tijdschriften en blogs

De Jong, 2016
J.P. de Jong, '*Algemene verordening gegevensbescherming',* Ars Aequi 2016

De Vries & Goudsmit 2016
H. de Vries & M. Goudsmit, *'Voorsorteren op de Algemene Verordening Gegevensbescherming',* Nederlands Juristenblad 2016, afl. 22

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

Wet en regelgeving

Algemene wet bestuursrecht
Algemene Verordening Gegevensbescherming
De Grondwet
Europees Handvest voor de Rechten van de Mens
Europees Verdrag betreffende de Werking van de Europese Unie
Uitvoeringswet Algemene Verordening Gegevensbescherming
Wet bescherming persoonsgegevens

Parlementaire stukken

Kamerstukken II 2011/12, 32 761, nr. 32

Elektronische bronnen

www.autoriteitpersoonsgegevens.nl

www.nu.nl

www.privacycompany.eu

www.surf.nl

www.taaladvies.net

www.tilburguniversity.edu.nl